BLOCKCHAIN IN PATIENT DATA MANAGEMENT

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

M.MANVITHA

22501A05A4

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 **“BLOCKCHAIN IN PATIENT DATA MANAGEMENT”** that is being submitted by **M.MANVITHA (22501A05A4),** 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

A personal health record (PHR) is a patient-managed digital record that consolidates medical data from various sources, including medical institutions, wearable health devices, and self-reported information. Research indicates that increased patient engagement with their health data leads to better healthcare outcomes. A PHR system should be patient-centric, ensuring that only patients can access, modify, or share their records unless they grant explicit and secure access rights to other entities. This approach enhances trust, usability, and security in managing personal medical data.

Several enterprise PHR platforms, such as Microsoft HealthVault, Google Health, and Apple Health, have aimed to provide digital health record management. However, their centralized nature raises concerns regarding data security, privacy, and the risk of unauthorized access. With increasing cybersecurity threats, centralized healthcare data repositories have become vulnerable to breaches, unauthorized modifications, and data exploitation. The absence of strong security mechanisms in centralized systems increases the likelihood of exposing sensitive patient information.

Blockchain technology offers a potential solution to these challenges by providing a decentralized, immutable, and transparent framework for secure health data management. It ensures data integrity by keeping medical records tamper-proof and auditable. Security and privacy are enhanced through encryption and cryptographic techniques, preventing unauthorized access. Blockchain also supports interoperability by allowing seamless data sharing between healthcare providers while ensuring that patients maintain control over their records.

To enhance the efficiency of blockchain-based PHR systems, additional technologies can be integrated. The InterPlanetary File System (IPFS) facilitates off-chain storage of large medical records while keeping cryptographic proofs on-chain. Reputation-Governed Trusted Oracles (RGTO) consist of reputation-based computational nodes that handle off-chain tasks like retrieving files from IPFS and performing cryptographic operations. Proxy Re-Encryption (PRE) allows patients to dynamically grant or revoke access to their medical records by securely re-encrypting the data.

A well-designed PHR system should offer granular access control, allowing patients to authorize specific individuals or institutions to access selected records. The system should also support automated emergency access, where predefined rules enable medical professionals and relatives to retrieve records in critical situations. Additionally, privacy-preserving protocols ensure that patient autonomy is maintained, even in cases of incapacitation. With these enhancements, a blockchain-based PHR system provides a secure, patient-controlled, and efficient way to manage personal health records.

2. BACKGROUND

Healthcare data management plays a crucial role in ensuring the accuracy, security, and accessibility of patient records. However, traditional healthcare systems often face challenges such as data breaches, interoperability issues, and restricted patient access to their medical information. These issues not only compromise patient privacy but also create inefficiencies in medical treatment and coordination.

2.1 Challenges in Traditional Patient Data Management

2.1.1 Security & Privacy Risks

- Patient data stored in centralized databases is vulnerable to cyberattacks and unauthorized access.
- According to IBM Security (2023), the healthcare industry has the highest data breach costs, with an average of $10.93 million per incident [1].
- Hackers often target hospitals, as medical records contain sensitive personal and financial data.

2.1.2 Lack of Interoperability

- Healthcare providers use different database systems that do not easily communicate with one another.
- World Health Organization (2022) reports that the lack of interoperability leads to delays in patient care and administrative inefficiencies [3].
- Patients often have to carry physical copies of medical reports when visiting different doctors.

2.1.3 Limited Patient Control Over Data

- Most hospital databases restrict direct patient access, requiring them to request records manually.
- HealthIT.gov (2023) states that only 40% of patients in the U.S. have full access to their medical history [4].
- Without control over their data, patients cannot easily share records with different healthcare providers.

2.1.4 Data Integrity Issues

- In traditional systems, data can be modified or deleted, leading to medical errors.
- Unauthorized alterations in records may cause incorrect diagnoses and improper treatments.

2.2 Role of Blockchain in Patient Data Management

Blockchain offers a decentralized, secure, and transparent method for managing patient records. It ensures data integrity, privacy, and interoperability while giving patients full control over their health information.

2.2.1 Security & Privacy

- Blockchain uses cryptographic encryption to protect sensitive medical data.
- Patient records are stored in a distributed ledger, reducing the risk of a single-point failure or data breach.

2.2.2 Interoperability & Seamless Data Sharing

- With blockchain, healthcare providers can access real-time, verified patient data, improving coordination between hospitals and clinics.
- A study by Kuo et al. (2017) highlights that blockchain-based healthcare systems can reduce data silos and improve data exchange efficiency [5].

2.2.3 Patient Control & Transparency

- Patients can grant or revoke access permissions to doctors, hospitals, or insurance companies using smart contracts.
- Data updates are recorded permanently, ensuring a clear history of medical changes.

2.2.4 Immutability & Trust

- Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring accurate and reliable medical records.
- This prevents fraud and medical identity theft.

3. BLOCKCHAIN BASICS

Blockchain technology provides a secure, decentralized, and transparent framework for managing patient records. The following key blockchain concepts are essential in healthcare data management.

3.1 Decentralization

- Traditional healthcare systems store patient data in centralized databases, making them vulnerable to cyberattacks and system failures.
- Blockchain distributes data across multiple nodes, eliminating single points of failure and improving security. [1]

3.2 Immutability

- Once recorded, data on the blockchain cannot be altered or deleted, ensuring a reliable and tamper-proof medical history.
- Any updates to patient records are stored as new transactions, maintaining a complete audit trail. [5]

3.3 Cryptographic Security

- Patient data is protected using cryptographic techniques like hashing and encryption, ensuring only authorized individuals can access or modify records.
- This reduces risks related to unauthorized access and data breaches. [2]

3.4 Smart Contracts

- Self-executing contracts automate processes like granting access to records, processing insurance claims, and enforcing compliance with healthcare regulations.
- These contracts improve efficiency and eliminate the need for intermediaries. [4]

3.5 Interoperability

- Blockchain enables seamless data sharing across different healthcare providers, reducing administrative inefficiencies.
- Standardized blockchain-based frameworks improve coordination and prevent medical errors.[3]

3.6 Patient Ownership and Access Control

- Patients have complete control over their medical data and can grant or revoke access permissions as needed.
- This enhances transparency, security, and patient autonomy in healthcare data management. [4]

4. USE CASE OVERVIEW

The use case for a Blockchain-Based Patient Data Management System aims to enhance the security, transparency, and accessibility of medical records using blockchain technology. The system ensures secure patient record storage, controlled data access, and interoperability among healthcare providers.

4.1. Objectives

The primary objective of this blockchain-based system is to eliminate paper-based records and create a fully digital, decentralized platform for secure and tamper-proof patient data storage. Traditional healthcare databases are vulnerable to data breaches, mismanagement, and inefficiencies in record sharing. Blockchain technology ensures patient data is immutable, securely stored, and easily accessible by authorized parties.

A major challenge in healthcare is data security and unauthorized access. Blockchain's immutability and cryptographic encryption ensure that patient data cannot be altered or accessed without consent, thereby reducing cyber threats.

Another critical goal is to enhance interoperability between healthcare providers. Currently, patient records are scattered across different hospitals and clinics, making it difficult for doctors to retrieve complete medical histories. Blockchain enables seamless and instant access to patient records, improving diagnosis accuracy and treatment efficiency.

The system also aims to improve emergency care. In critical situations, doctors can quickly access verified patient history, allergies, and ongoing treatments through blockchain, eliminating delays caused by paperwork and fragmented databases.

Additionally, the system allows patients to control their data. With self-sovereign identity, patients can grant or revoke access to their medical records, ensuring data privacy and compliance with regulations like GDPR and HIPAA.

By reducing administrative burdens, blockchain-based healthcare systems lower operational costs for hospitals and insurance companies while improving the efficiency of patient data management.

4.2. Scope of the System

The Blockchain-Based Patient Data Management System focuses on securely storing, managing, and sharing patient data. The system includes:

- **Hospitals & Clinics:** Issue and update digital patient records in a tamper-proof blockchain ledger.
- **Patients:** Access their medical records, grant/revoke permissions, and share records securely.
- **Doctors & Healthcare Providers:** Retrieve verified patient data instantly for accurate diagnosis and treatment.

- **Insurance Companies:** Verify patient treatment history for fast and fraud-proof claims processing.
- **Regulatory Authorities:** Ensure compliance with health data security standards through transparent auditing.
- **Blockchain Network:** A decentralized ledger ensuring data integrity, access control, and smart contract execution.

4.3 Overall System Architecture

4.3.1 Regulatory Agency

A trusted governing body could be the government or the Department of Health in the country. This entity deploys the main smart contract and is part of the MPA that approves the sharing of absent patient medical documents. The regulatory agency is also responsible for verifying the identities of any person or entity that registers into the network, whether that is the patient, guardian, doctor, hospital, oracle, or healthcare payer. The regulatory agency is ultimately managed by its employees through the decentralized application (DApp).[6]

4.3.2 Person

A general type of entity that by default is registered either as a patient or a guardian, depending on whether the entity is managed by the patient personally or by a trusted guardian or guardians. A patient can issue claims to become a guardian of other patients. Becoming a guardian enables the patient to be part of the MPA to approve the sharing of medical documents in cases where the patient is absent. Furthermore, patients can issue claims to register as doctors, permitting them to request patient medical documents. All claims issued by the patient must be verified by the MPA. Guardian claim requests are verified by receiving patient and regulatory agency approvals, whereas doctor claim requests are verified by receiving hospital and regulatory agency approvals.

In addition to the Ethereum private-public key pair each person possesses, patients must have an IPFS key pair, with the private key split and shared 50% (3 shares) with the regulatory agency and the remaining 50% (3 shares) kept secret with the patient. Moreover, the patient will produce a unique key pair for each medical document uploaded to IPFS. The person handling this entity manages the PHR DApp either directly on a personal device or through a trusted third-party (TTP) service.[6]

4.3.3 Hospital

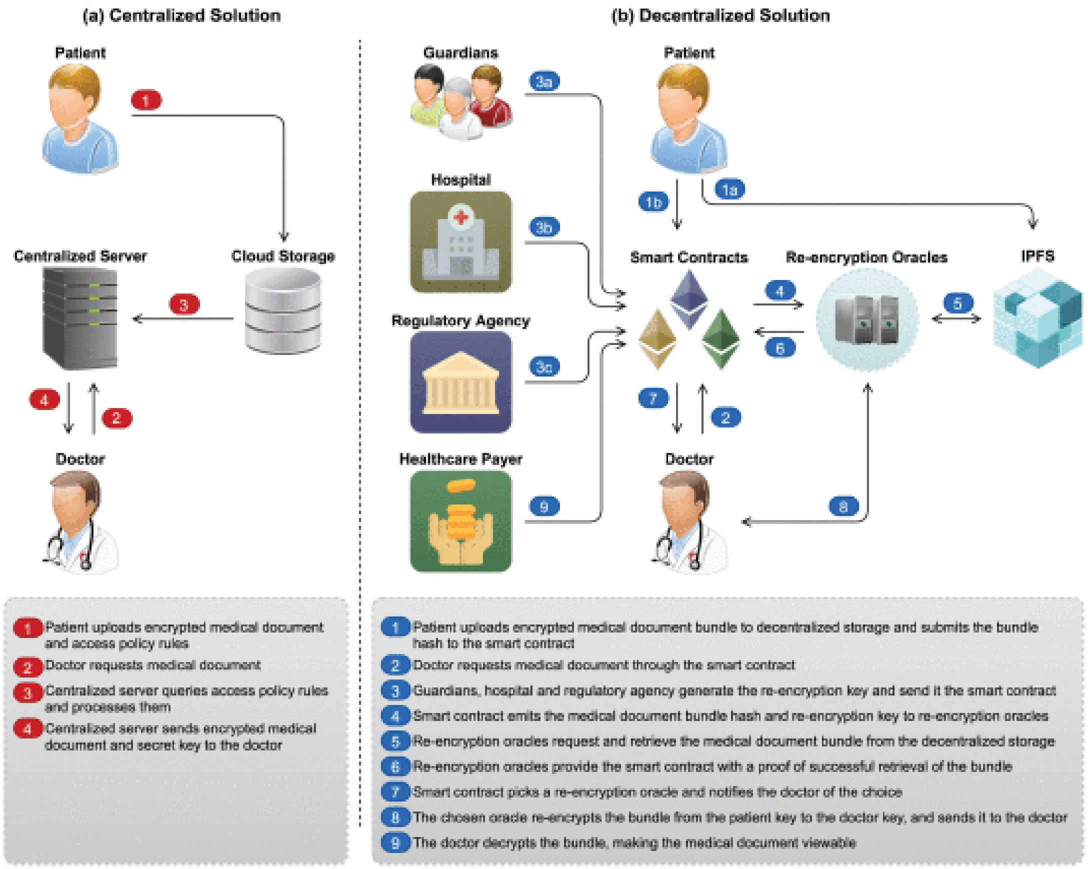
In addition to being the source of medical documents for patients, the primary responsibility of the hospital in this MPA scheme is to validate a person’s claim of being a doctor and to confirm the doctor’s claim that a patient has an emergency admission to the hospital.[6]

4.3.4 Insurance Company

Responsible for paying the decentralized storage and Oracle nodes. [6]

4.3.5 Re-encryption RGTO

An RGTO node that fetches IPFS files, performs the PRE process and acts as an Ethereum Alarm Clock (EAC) for timeout functionality in Solidity The nodes race to perform PRE to transform the medical document encryption from the patient to the doctor, after which, the winning node communicates with the doctor directly to transfer the re-encrypted medical document to the latter's local device. [6]



1 Patient uploads encrypted medical document and access policy rules
2 Doctor requests medical document
3 Centralized server queries access policy rules and processes them
4 Centralized server sends encrypted medical document and secret key to the doctor

1 Patient uploads encrypted medical document bundle to decentralized storage and submits the bundle hash to the smart contract
2 Doctor requests medical document through the smart contract
3 Guardians, hospital and regulatory agency generate the re-encryption key and send it the smart contract
4 Smart contract emits the medical document bundle hash and re-encryption key to re-encryption oracles
5 Re-encryption oracles request and retrieve the medical document bundle from the decentralized storage
6 Re-encryption oracles provide the smart contract with a proof of successful retrieval of the bundle
7 Smart contract picks a re-encryption oracle and notifies the doctor of the choice
8 The chosen oracle re-encrypts the bundle from the patient key to the doctor key, and sends it to the doctor
9 The doctor decrypts the bundle, making the medical document viewable

Fig 4.3.1 An overview of (a) current centralized solutions, and (b) decentralized solutions. [6]

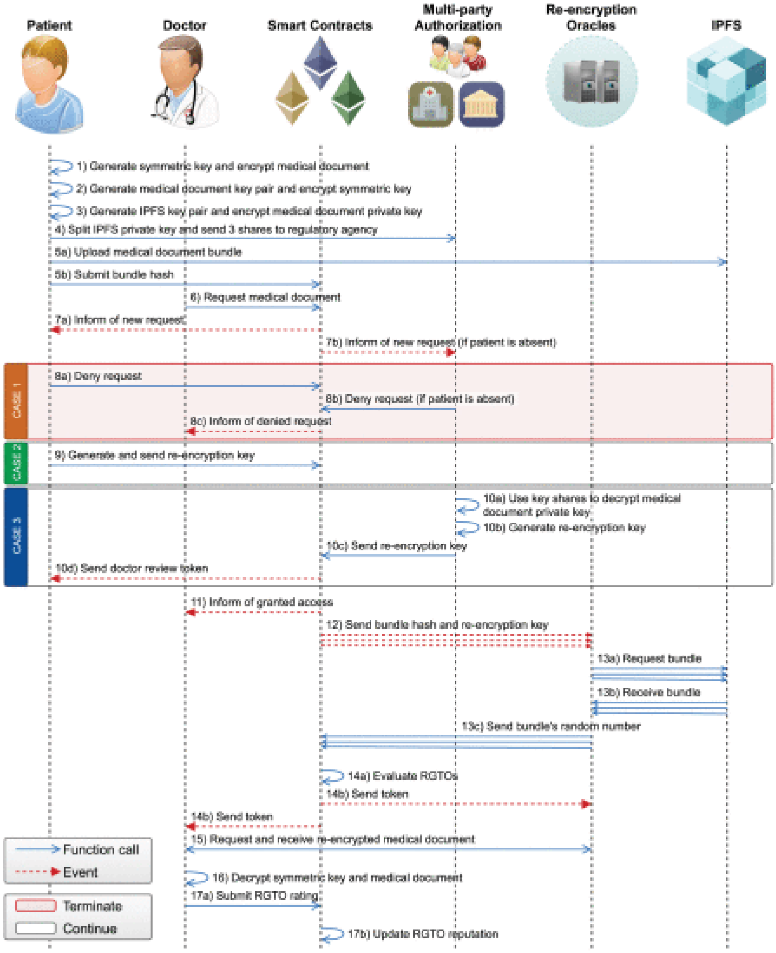

Patient
Doctor
Smart Contracts
Multi-party Authorization
Re-encryption Oracles
IPFS
1) Generate symmetric key and encrypt medical document
2) Generate medical document key pair and encrypt symmetric key
3) Generate IPFS key pair and encrypt medical document private key
4) Split IPFS private key and send 3 shares to regulatory agency
5a) Upload medical document bundle
5b) Submit bundle hash
6) Request medical document
7a) Inform of new request
7b) Inform of new request (if patient is absent)
CASE 1
8a) Deny request
8b) Deny request (if patient is absent)
8c) Inform of denied request
CASE 2
9) Generate and send re-encryption key
CASE 3
10a) Use key shares to decrypt medical document private key
10b) Generate re-encryption key
10c) Send re-encryption key
10d) Send doctor review token
11) Inform of granted access
12) Send bundle hash and re-encryption key
13a) Request bundle
13b) Receive bundle
13c) Send bundle's random number
14a) Evaluate RGTOs
14b) Send token
14b) Send token
15) Request and receive re-encrypted medical document
16) Decrypt symmetric key and medical document
17a) Submit RGTO rating
17b) Update RGTO reputation
Function call
Event
Terminate
Continue

Fig 4.3.2 Sequence diagram of accessing health records of active or absent patients. [6]

4.3.6 Regulatory Agency Smart Contract (RASC)

The regulatory agency deploys a universal regulatory agency smart contract (RASC) that manages all entities and provides patients, guardians, and doctors with the ability to send transactions. Moreover, RASC performs reputation evaluation and maintenance of Oracle nodes. [6]

4.3.7 Interactions and Message Sequence

1. The patient generates a symmetric key and encrypts the medical document using the key.

2. The patient generates a medical document private-public key pair and encrypts the symmetric key using the medical document public key. [6]

3. The patient generates an IPFS private-public key pair (only for the first medical document, which will be used for all future medical documents) and encrypts the medical document's private key using the IPFS public key. [6]

4. The patient uses a threshold signature to split the IPFS private key into 6 shares (3 kept on local devices and 3 securely shared with the regulatory agency). [6]

5. The patient uploads a bundle consisting of the encrypted medical document, the encrypted symmetric key, the encrypted medical document key, and a pseudo-random number to IPFS. Then, the SHA-256 hash of the bundle is submitted to RASC.

6. The doctor requests the medical document and optionally specifies whether the request is for an incapacitated patient or an emergency case. [6]
7. The RASC informs the patient of a new request. If the request was for an absent patient, the appropriate MPA will be informed as well. The MPA for an incapacitated patient requires the patient to be registered as such, validation of doctor credentials, and the approval of $\min(\lceil 0.7g\rceil,5)$ guardians, where g is the total number of verified guardians. The MPA for an emergency case requires the confirmation of emergency admission from the hospital in concern and the validation of doctor credentials. [6]
8. **Case 1:** The patient denies the request or the MPA requirements are not met within 1 hour, after which the RASC informs the doctor of denied access. The sequence terminates.
9. **Case 2:** The patient grants access, then generates a re-encryption key and sends it to RASC. The sequence continues from step 11.
10. **Case 3:** The MPA requirements are met within 1 hour. The RASC sends a reputation token to the patient to allow the rating of the doctor. The regulatory agency nodes independently use their 3 shares and decrypt the medical document private key, which is then used by one of the nodes to generate a re-encryption key and send it to RASC. The sequence continues from step 11.
11. The RASC informs the doctor of granted access. [6]
12. The RASC sends the medical document bundle hash and re-encryption key to a set of RGTOs.
13. The RGTOs request and receive the medical document bundle from IPFS, then get the random number from the IPFS bundle and send it privately to RASC.
14. The RASC evaluates the RGTOs, then updates their ratings and chooses the most reputable ones. Then, RASC sends a token to the winning RGTO and the doctor.
15. The doctor requests the re-encrypted medical document from the RGTO, which computes and sends it to the doctor. [6]
16. The doctor decrypts the symmetric key using the public key and then decrypts the medical document using the symmetric key.

Using a symmetric key instead of the patient’s IPFS public key allows large medical files to be encrypted and uploaded only once. The medical document private key, not the symmetric key, is split and shared with trusted entities, ensuring secure access while protecting the patient’s Ethereum private key. [6]

5. IMPLEMENTATION

5.1. Define the Medical Document Sharing Workflow

- **Identify stakeholders**: Regulatory Agency Owner (RAO), Regulatory Agency Member (RAM), Hospital, Person (Patient/Doctor), RGTO (Re-Encryption Gateway Operator).
- **Determine stored data**: Patient ID (hashed for privacy), Medical Document Hashes (IPFS), Guardian Claims, Verification Status, Timestamps, RGTO Reputation Scores.
- **Define key operations**: Patient Registration, Guardian Verification, Medical Document Submission, Document Request, RGTO Selection, Re-Encryption, and Access Granting.

5.2. Choose the Blockchain Type

- **Private Blockchain (Hyperledger, Quorum)**: Suitable for controlled access within a regulatory framework [5].
- **Hybrid Blockchain (Ethereum, Polkadot)**: Combines public verification with private identity management [6].
- **Public Blockchain (Ethereum, Polygon)**: Fully transparent but may incur higher transaction costs [7].

5.3. Design Smart Contracts for Medical Document Sharing

Smart contracts automate and secure the medical document sharing process, ensuring transparency, privacy, and efficiency. Below is a detailed breakdown of how smart contracts manage different stages:

5.3.1 Patient Registration – Secure Identity Verification Without Revealing Personal Data

- A patient initiates registration by providing identity credentials (e.g., government-issued ID, biometric data) [4].
- The smart contract validates the patient's identity through cryptographic techniques (e.g., Zero-Knowledge Proofs) [5].
- Once verified, the patient is assigned a unique blockchain address linked to their medical records [6].
- The registration status is hashed and recorded on the blockchain, ensuring immutability and preventing duplicate registrations [7].

5.3.2 Guardian Verification – Ensures Trusted Guardianship Claims

- A verified patient can claim a guardian by submitting the guardian's address using the addGuardian function [4].
- The guardian must verify the claim using the verifyGuardianship function [5].
- The smart contract records the guardianship claim and ensures only verified guardians can access medical documents on behalf of the patient [6].

5.3.3 Medical Document Submission – Secure Storage and Access Control

- Verified patients submit medical documents to IPFS and store the hash on the blockchain [3].
- Patients specify the number of RAMs or guardians required for access approval [4].
- The smart contract ensures the requested number of verifiers falls within a predefined range set by the RAO [5].

5.3.4 Document Request and Access Granting – Controlled and Time-Bound Access

- Verified doctors request medical documents by submitting the patient's address and the document's IPFS hash [6].
- The smart contract checks if the request requires approval from the patient, RAMs, or guardians [7].
- Access is granted for a specific period, allowing partial or full access to health records even if the patient is unavailable [8].

5.3.5 RGTO Selection and Re-Encryption – Secure Document Sharing

- RGTOs fetch medical documents from IPFS, generate pseudo-random numbers, and submit them to the smart contract [5].
- The smart contract evaluates RGTO responses based on correctness, latency, and reputation scores [6].
- The winning RGTO re-encrypts the document and sends it to the requesting doctor [7].

5.4. Develop & Deploy Smart Contracts

Example Solidity Code for Medical Document Sharing:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract MedicalDocumentSharing {
    struct Patient {
        address id;
        mapping(address => bool) guardians;
        mapping(string => bool) documents;
    }

    struct RGTO {
```

```
    uint ORReputation;
    uint ODReputation;
}

address public RAO;
mapping(address => Patient) public patients;
mapping(address => RGTO) public rgtos;

event DocumentSubmitted(address patient, string documentHash);
event GuardianAdded(address patient, address guardian);
event DocumentRequested(address doctor, address patient, string documentHash);

constructor() {
    RAO = msg.sender;
}

function registerPatient(address _patient) public {
    require(msg.sender == RAO, "Only RAO can register patients");
    patients[_patient].id = _patient;
}

function addGuardian(address _patient, address _guardian) public {
    require(msg.sender == _patient, "Only patient can add guardians");
    patients[_patient].guardians[_guardian] = true;
    emit GuardianAdded(_patient, _guardian);
}

function submitDocument(address _patient, string memory _documentHash) public {
    require(msg.sender == _patient, "Only patient can submit documents");
    patients[_patient].documents[_documentHash] = true;
    emit DocumentSubmitted(_patient, _documentHash);
    }


    function requestDocument(address _doctor, address _patient, string memory _documentHash) public {
        require(patients[_patient].documents[_documentHash], "Document does not exist");
        emit DocumentRequested(_doctor, _patient, _documentHash);
    }
}
```

5.5. Integrate IPFS for Document Storage

- **IPFS Integration**: Store medical documents on IPFS for decentralized and resilient storage [3].
- **Document Hashing**: Use IPFS hashes to reference documents on the blockchain [4].

5.6. Frontend & Web3 Integration

- **Frontend**: Built using React.js/Next.js for a user-friendly interface [5].
- **Web3 Integration**: Use Web3.js or Ethers.js for interacting with smart contracts [6].
- **Wallet-Based Authentication**: MetaMask or private keys for patient and doctor authentication [7].

5.7. Test the Smart Contracts

- **Local Testing**: Deploy on Ganache (Ethereum test environment) [5].
- **Unit Testing**: Validate smart contract logic using Truffle or Hardhat [6].
- **Security Audits**: Check vulnerabilities using Slither or MythX [7].

5.8. Deploy on a Blockchain Network

- **Testnet Deployment**: Deploy on Ethereum Testnet (Goerli, Sepolia) before the main launch [5].
- **Mainnet Deployment**: Deploy finalized contracts on Ethereum or Polygon for transparency [6].
- **Decentralized Storage**: Store non-sensitive data on IPFS for resilience [7].

5.9. Monitor & Maintain the System

- **Real-Time Monitoring**: Use Chainlink oracles for external data verification [5].
- **Event Logging**: Maintain a log of all document requests and access grants for auditing [6].

- **Security Updates**: Periodically upgrade smart contracts to address vulnerabilities [7].

5.10. Ensure Compliance & Scalability

- **Regulatory Compliance**: Align with healthcare regulations (e.g., HIPAA, GDPR) [1, 2].
- **Optimized Gas Fees**: Use Layer 2 solutions like Polygon or Optimism for cost efficiency [5].
- **Scalability Measures**: Implement sharding or sidechains for high-volume scenarios [6].

By integrating blockchain smart contracts, medical document sharing becomes tamper-proof, transparent, and privacy-preserving, ensuring secure and efficient healthcare data management [3, 4, 5, 6, 7].

6. BENEFITS

Blockchain technology offers numerous advantages in managing patient data by enhancing security, accessibility, and interoperability within the healthcare sector. Below are the key benefits of implementing blockchain in patient data management:[7]

6.1 Enhanced Security & Data Integrity

Blockchain ensures tamper-proof and immutable storage of patient records. Once data is recorded on the blockchain, it cannot be altered or deleted, reducing risks of fraud, unauthorized modifications, and cyberattacks. The use of cryptographic encryption and decentralized storage prevents unauthorized access, safeguarding sensitive medical information from breaches. [7]

6.2 Patient-Centric Data Ownership & Control

Unlike traditional healthcare systems where hospitals and clinics own patient data, blockchain enables self-sovereign identity, allowing patients to own, control, and share their medical records securely. Patients can grant or revoke access to their data using private keys, ensuring privacy and compliance with regulations like GDPR and HIPAA. [7]

6.3 Seamless Interoperability & Data Sharing

Currently, patient records are stored in isolated databases across hospitals, clinics, and laboratories, making it difficult for doctors to retrieve complete medical histories. Blockchain enables real-time access to verified patient data across different healthcare providers, reducing redundancies and improving diagnosis accuracy and treatment efficiency. [8]

6.4 Faster & More Efficient Emergency Care

In critical situations, delays in accessing patient history can be life-threatening. Blockchain allows authorized doctors and emergency responders to quickly access vital medical data, including allergies, past treatments, and ongoing prescriptions, ensuring faster decision-making and better patient outcomes. [8]

6.5 Fraud Prevention & Trust in Medical Records

Medical fraud, such as insurance scams, identity theft, and fake prescriptions, is a significant issue. Blockchain's transparent and immutable nature ensures that medical records, prescriptions, and insurance claims are authentic and verifiable, reducing fraud and building trust between patients, healthcare providers, and insurers. [9]

6.6 Streamlined Insurance Processing & Billing

Blockchain enables smart contracts to automate insurance claims processing, ensuring faster approvals and fraud-proof transactions. Since insurers can directly access verified treatment histories, claim verifications become more efficient, reducing paperwork and operational costs. [9]

6.7 Cost Reduction & Administrative Efficiency

Traditional paper-based and centralized digital healthcare systems require manual processing, leading to administrative inefficiencies and high costs. Blockchain automates record management, consent tracking, and data verification, significantly reducing operational expenses for hospitals, clinics, and insurance companies. [7]

6.8 Compliance with Regulatory Standards

Blockchain enhances compliance with healthcare regulations by maintaining secure and auditable records. Regulatory authorities can monitor data access logs to ensure that hospitals and clinics adhere to privacy standards such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). [8]

6.9 Research & Medical Innovation

Blockchain facilitates secure and anonymous patient data sharing for clinical research, drug development, and AI-based healthcare innovations. Researchers can access large datasets without compromising patient privacy, accelerating medical breakthroughs while maintaining ethical standards. [9]

6.10 Reduced Risk of Data Loss

Traditional healthcare systems rely on centralized servers, which are vulnerable to hacks, system failures, and accidental deletions. Blockchain's decentralized architecture ensures that patient records are always available, even in cases of server crashes or cyberattacks. [9]

7. CHALLENGES

7.1 Scalability Issues

Blockchain networks, especially public blockchains, face scalability limitations due to their decentralized nature. As the number of transactions and stored records increases, network congestion and slow processing times can occur. This can lead to delays in accessing medical records, which is critical in healthcare settings. [7]

7.2 High Implementation Costs

Integrating blockchain into existing healthcare infrastructures requires significant investment in terms of technology, training, and infrastructure updates. Hospitals and clinics need to develop new systems, ensure compliance with legal standards, and train medical professionals on blockchain usage. These high initial costs may discourage widespread adoption, especially in resource-limited healthcare systems. [8]

7.3 Data Privacy & Compliance Concerns

While blockchain enhances security, ensuring compliance with regulations like GDPR, HIPAA, and other regional data protection laws remains a challenge. Blockchain's immutable nature conflicts with regulations that require the ability to modify or delete patient data upon request. Implementing off-chain storage or zero-knowledge proofs can help balance immutability with privacy rights. [8]

7.4 Interoperability with Existing Systems

Healthcare providers use different Electronic Health Record (EHR) systems, making it difficult to seamlessly integrate blockchain with existing databases. Achieving universal data standards for blockchain-based patient records is essential to ensure smooth data exchange across hospitals, clinics, and insurance companies. [8]

7.5 Latency & Energy Consumption

Some blockchain consensus mechanisms, such as Proof-of-Work (PoW), require high computational power, leading to slow transaction processing and high energy consumption. In healthcare, real-time access to patient records is crucial, and delays could impact patient outcomes. Transitioning to energy-efficient consensus models like Proof-of-Stake (PoS) or private blockchains can mitigate these concerns. [9]

7.6 Patient & Provider Adoption Barriers

Blockchain technology is still relatively new in healthcare, and many patients, doctors, and administrators lack the technical knowledge to use it effectively. Resistance to change, lack of awareness, and concerns over complexity can slow down adoption. User-friendly interfaces, education programs, and gradual integration strategies are necessary to encourage acceptance. [9]

7.7 Legal & Ethical Challenges

The legal status of blockchain-based medical records remains uncertain in many regions. Questions regarding data ownership, liability in case of incorrect records, and cross-border data access need clear regulations. Additionally, ethical concerns arise regarding who should have access to patient data, how emergency access is granted, and how data security is enforced while maintaining patient autonomy. [9]

8. CONCLUSION

This paper proposed a decentralized blockchain-based solution for secure and transparent multi-party consent management in patient data sharing. By integrating multi-party authorization, threshold cryptography, and decentralized IPFS storage, our approach ensures secure access to encrypted medical documents while maintaining traceability and emergency access mechanisms. Reputation-governed trusted oracles mitigate blockchain-related limitations, enhancing system efficiency. We presented detailed algorithms, implementation details, and security analysis, demonstrating how our solution ensures authenticity, confidentiality, integrity, availability, and non-repudiation. Our implementation's correctness verification and cost analysis confirm its feasibility, with publicly available code and reproducible results

9. SDG's ADDRESSED

SDG 3: Good health and well-being

Ensures healthy lives and promotes well-being for all by improving healthcare access, reducing disease burdens, and strengthening medical infrastructure. Blockchain in healthcare enhances data security, interoperability, and patient-centered care, contributing to better health outcomes.

SDG 9: Industry, Innovation, and Infrastructure

Focuses on building resilient infrastructure, fostering innovation, and promoting sustainable industrial growth. Blockchain-driven healthcare solutions revolutionize medical data management, enabling efficient, secure, and scalable digital health ecosystems.

SDG 10: Reduced Inequalities

Aims to reduce disparities within and among countries by ensuring equal opportunities and access to resources. Blockchain empowers underserved populations with secure and decentralized health records, improving access to quality healthcare services regardless of socio-economic status.

10. REFERENCES

1. IBM Security. (2023). Cost of a Data Breach Report 2023.

This report provides insights into the financial impacts of data breaches across various industries, highlighting the increasing costs associated with such incidents.

https://www.ibm.com/reports/data-breach

2. Ponemon Institute. (2023). Healthcare Cybersecurity Report.

This report delves into the cybersecurity challenges faced by the healthcare sector, emphasizing the vulnerabilities and the need for robust security measures.

https://www.ponemon.org/reports/healthcare-cybersecurity-report-2023

3. World Health Organization. (2022). Interoperability in Healthcare Systems.

This publication discusses the importance of interoperability in healthcare systems and its impact on patient care and data management.

https://www.who.int/publications/i/item/interoperability-in-healthcare-systems-2022

4. HealthIT.gov. (2023). Patient Access to Health Records.

This resource highlights the significance of patient access to their health records and the policies promoting such access.

https://www.healthit.gov/topic/patient-access-health-records

5. Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220.

This paper introduces blockchain technologies, discussing their benefits, challenges, and applications in the biomedical and healthcare domains.

https://academic.oup.com/jamia/article/24/6/1211/4108087

6. The IEEE paper discusses a blockchain-based approach to secure and interoperable Health Information Exchange (HIE) networks. It enhances patient data security, control, and accessibility in healthcare systems.

https://ieeexplore.ieee.org/document/9294064/metrics#metrics

7. A Systematic Review of Blockchain Technology Benefits and Threats:

pmc.ncbi.nlm.nih.gov

8. Benefits and Concerns Associated with Blockchain-Based Health Information Exchange Systems:

bmcmedinformdecismak.biomedcentral.com

9. Blockchain in Healthcare: Benefits, Use Cases, and Challenges:

tmasolutions.com

11. APPENDIX

https://drive.google.com/drive/u/0/folders/1Xdahx4NySzySP5W309f5KPsQjWExf7Jx