VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY
Department of Computer Engineering

Project Report on

Patient Record System Using Blockchain

Submitted in partial fulfillment of the requirements of the degree

BACHELOR OF ENGINEERING IN **COMPUTER ENGINEERING**

By

Jeet Dalal D12A/10

Swaraj Khadge D12A/29

Harsh Tuli D12A/65

Mayuresh Sawant D12A/55

Project Mentor
Mrs. Lifna C.S

University of Mumbai
(AY 2023-24)

VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY
Department of Computer Engineering

CERTIFICATE

This is to certify that the Mini Project entitled **"Patient Record System using Blockchain"** is a bonafide work of **Jeet Dalal (D12A/10), Swaraj Khadge (D12A/29), Harsh Tuli (D12A/65), Mayuresh Sawant (D12A/55)** submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **"Bachelor of Engineering"** in **"Computer Engineering" .**

(Prof. Lifna C.S)
Mentor

(Prof. Dr. Nupur Giri)
Head of Department

(Prof. Dr. J.M. Nair)
Principal

Mini Project Approval

This Mini Project entitled "**Patient Record System Using Blockchain"** by **Jeet Dalal (D12A/10), Swaraj Khadge (D12A/29), Harsh Tuli (D12A/65), Mayuresh Sawant (D12A/55)** is approved for the degree of **Bachelor of Engineering** in **Computer Engineering.**

Examiners

1..
(Internal Examiner Name & Sign)

2..
(External Examiner name & Sign)

Date:

Place:

Declaration

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

---------------------------------------	---------------------------------------
(Jeet Dalal D12A/10)	(Swaraj Khadge D12A 29)
---------------------------------------	---------------------------------------
(Harsh Tuli D12A/65)	(Mayuresh Sawant D12A/55)

Date:

ACKNOWLEDGEMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to Assistant Professor **Mrs. Lifna C.S** (Project Guide) for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions.

We are deeply indebted to Head of the Computer Department **Dr.(Mrs.) Nupur Giri** and our Principal **Dr. (Mrs.) J.M. Nair ,** for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement several times.

Index

List of Abbreviations :

Abbreviation	Full Form
RAM	Random Access Memory
CPU	Central Processing Unit
UX	User Experience
NoSQL	Not Only SQL
JSON	JavaScript Object Notation

List of Figures :

List of Tables :

Abstract

Data-sharing in healthcare is critical for a complete patient care experience. A patient goes to multiple hospitals/ clinicians in their healthcare journey but their medical data is not being recorded in a confidential and integral way by any authority. Doctors at some different clinics might need to refer to a patient's medical history to make good decisions for treatment. We aim to build a blockchain solution using hyperledger fabric that can offer a way to share the patient's medical data with various healthcare-related organizations while maintaining data integrity, confidentiality and patient privacy. Hyperledger blockchain technology addresses the challenges of data security, privacy, and interoperability in the healthcare sector. Hyperledger Fabric, with its permissioned blockchain network and robust privacy controls, offers a promising solution for securely managing and sharing sensitive health information while ensuring compliance with regulatory requirements. The proposed EHR system leverages Hyperledger Fabric's features such as fine-grained access control, immutable ledger, and smart contracts to enable patient-centric data management, transparent auditability, and seamless interoperability between healthcare providers. By employing Hyperledger blockchain technology, this study aims to enhance trust, transparency, and efficiency in healthcare data management, ultimately improving patient outcomes and healthcare delivery.

KEYWORDS : Blockchain, Electronic Health Record, Hyperledger Fabric

Chapter 1 : Introduction

1.1 Introduction

The project focuses on harnessing the power of blockchain technology to revolutionize Electronic Health Records (EHR) management. In today's rapidly evolving healthcare landscape, Electronic Health Records play a pivotal role in facilitating efficient patient care, clinical decision-making, and healthcare operations. However, traditional EHR systems often encounter significant challenges that hinder their effectiveness and potential. Issues such as data fragmentation across disparate systems, security vulnerabilities leading to data breaches, and lack of interoperability between healthcare providers and systems have emerged as pressing concerns. These challenges not only impede the seamless exchange of critical patient information but also compromise the integrity, privacy, and security of sensitive health data. Furthermore, the siloed nature of existing EHR systems inhibits comprehensive patient care coordination and prevents healthcare providers from accessing a holistic view of a patient's medical history and treatment journey.

1.2 Motivation

The imperative need to revolutionize Electronic Health Records (EHR) management serves as the driving force behind our project. Current EHR systems often struggle with fragmentation, security vulnerabilities, and interoperability issues, leading to compromised patient care and inefficient healthcare operations. Our motivation stems from the vision of a seamless and secure EHR ecosystem that prioritizes data integrity, privacy, and interoperability. By leveraging blockchain technology, we aim to create a robust and transparent platform that empowers healthcare providers to access, share, and manage patient information seamlessly while ensuring privacy and compliance with regulatory standards. Our goal is to enhance patient outcomes, streamline care coordination, and foster trust and transparency in the healthcare ecosystem by revolutionizing EHR management.

Problem Definition :

In today's healthcare landscape, a significant challenge lies in the need for improved security, transparency, and simplicity in Electronic Health Records (EHR) management. Current EHR systems often lack efficient response times and user-friendly interfaces, leading to frustration among healthcare professionals and compromising the effectiveness of patient care. Furthermore, ensuring the accuracy of medication availability and ordering processes presents additional hurdles in EHR systems, with security and transparency being paramount concerns.

To address these challenges, this project aims to develop an innovative EHR system leveraging blockchain technology. By integrating blockchain into EHR management, we seek to enhance security, transparency, and simplicity in accessing and managing patient health records. Blockchain's decentralized and immutable nature offers a promising solution to safeguard patient data, ensure transparency in healthcare transactions, and streamline medication ordering processes.

The primary objective of this project is to create a user-centric EHR system that provides a seamless and secure interaction experience for healthcare professionals and patients alike. By prioritizing data security, transparency, and user-friendliness, our goal is to revolutionize EHR management and improve patient outcomes in the healthcare ecosystem.

Existing Systems :

Existing Electronic Health Records (EHR) systems, while valuable in modern healthcare, are not without their limitations. One significant lacuna is interoperability issues, where data exchange between different systems and providers remains challenging, leading to fragmented patient information and potential errors in care coordination. Additionally, user interface design can be complex and cumbersome, impacting user experience and efficiency. Another concern is data security, with instances of breaches and unauthorized access posing risks to patient privacy and confidentiality. Furthermore, the high implementation costs and ongoing maintenance expenses associated with these systems can present barriers to adoption, particularly for smaller healthcare practices with limited resources. Despite these lacunas, existing EHR systems continue to evolve and improve, driven by the ongoing need for more efficient and effective healthcare delivery.

Lacuna of the existing systems :

While the objectives for enhancing Electronic Health Records (EHR) systems are clear and commendable, several lacunas in existing systems must be addressed to achieve these goals effectively.

One significant lacuna lies in the realm of data security. Existing EHR systems often lack robust cryptographic techniques to safeguard patient health data adequately. This vulnerability leaves patient information susceptible to breaches and compromises patient privacy and confidentiality. Another critical lacuna is interoperability. Current EHR systems struggle to facilitate seamless sharing of data across different healthcare providers and systems. This fragmentation of data hampers care coordination and decision-making, leading to disjointed patient care experiences.

Furthermore, patient empowerment is hindered by the centralized nature of existing EHR systems. Patients have limited control over their health data and consent management processes. Decentralized identity solutions offer a potential remedy, but their implementation remains limited in current EHR systems. Moreover, the lack of immutable record-keeping poses a challenge to ensuring data integrity and traceability in EHR transactions. Without tamper-proof records, it becomes difficult to verify the accuracy and authenticity of patient health data, undermining trust in the system.

Finally, compliance and auditability remain elusive in many existing EHR systems. Transparent audit trails of EHR transactions are essential for regulatory compliance and accountability. However, current systems often fall short in providing adequate auditability, leaving room for non-compliance and regulatory risks.

Relevance of the project :

The significance of integrating blockchain technology into Electronic Health Records (EHR) management within modern healthcare contexts cannot be overstated. This integration addresses pressing concerns regarding data security, interoperability, and patient-centered care, all of which are increasingly prioritized in today's healthcare landscape. Blockchain presents a multifaceted solution to the enduring challenges faced by conventional EHR systems. Through its decentralized structure and advanced cryptographic techniques, blockchain ensures robust data security, effectively mitigating risks associated with unauthorized access and breaches. Moreover, its inherent interoperability capabilities streamline the exchange of EHR data across various healthcare providers and systems, fostering improved coordination of care and decision-making processes.

Crucially, blockchain empowers patients by affording them greater control over their health data and consent management through decentralized identity solutions. By maintaining an immutable ledger of EHR transactions, blockchain bolsters data integrity and traceability, minimizing the potential for errors and fraudulent activities within patient health records. Additionally, blockchain enables transparent audit trails of EHR transactions, thereby promoting compliance with regulatory standards and enhancing overall accountability across the healthcare ecosystem.

Chapter 2 : Literature Survey

A. Brief Overview of Literature Survey

The literature review explores a wide array of scholarly articles examining the integration of blockchain technology into Electronic Health Records (EHR) management. Throughout the studies, blockchain emerges as a central focus, offering potential solutions to critical challenges in healthcare data management and security.

Research articles [1] and [2] delve into the practical implementation of blockchain-based EHR systems, underscoring the importance of data security, integrity, and patient confidentiality. They demonstrate how blockchain technology ensures secure storage of records, fine-grained access controls, and enhanced data integrity, all in line with patient-centered care principles and regulatory compliance.

A particular study [3] delves into the operational hurdles faced by current EHR systems and proposes strategies to fully integrate blockchain technology. It highlights the transformative potential of blockchain in EHR management, presenting opportunities for improved security, interoperability, and patient involvement.

Other papers [4] and [5] scrutinize the performance aspects of blockchain-driven EHR implementations, showcasing promising outcomes such as heightened availability rates and decreased vulnerability to cyber threats. They underscore how blockchain has the capacity to revolutionize healthcare data management, ultimately leading to enhanced patient care and healthcare delivery.

Lastly, a scholarly article [6] examines the use of HyperLedger Fabric, a blockchain framework, in healthcare applications. It focuses on Fabric's confidentiality mechanisms, which empower patients to exert greater control over their EHRs and manage access permissions effectively.

Overall, the literature underscores a growing interest in leveraging blockchain technology to tackle the multifaceted challenges of EHR management. It underscores the need for secure, interoperable, and patient-centric solutions in contemporary healthcare contexts.

Title	Source	Date of Publication	Problem Addressed	Inference and findings
Analyzing the performance of a blockchain-based personal health record implementation	Journal of Biomedical Informatics Volume 92, April 2019, 103140	March 4, 2019	Patients struggle to access, manage, and share their data, lacking transparency in consent mechanisms.	The outcome demonstrated commendable performance, with an average response time of less than 500 ms. Additionally, the prototype's blockchain implementation exhibited an impressive 98% availability rate.
Using Blockchain for Electronic Health Records Ayesha Shahnaz, Usman Qamar, Ayesha Khalid.	IEEE Access Volume 7	October 9, 2019	Problems regarding patient data security, integrity and management	Implementation of blockchain for EHR for secure record storage and granular access.
Blockchain-based electronic healthcare record system for healthcare 4.0 applications	Journal of Information Security and Applications	November 21, 2019	Interoperability, Security of Data,Ownership of Data.	EHR sharing system using Blockchain eliminates security and ownership problems of data.
Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Shuyun Shuyun Shi,Debiao He,Li Li,Neeraj Kumar,Muhammad Khurram Khan,Kim-Kwang Raymond Choo	Journal of Computer and security Volume 7 (Science direct)	July 15, 2020	Mainly privacy problems for all of raw/encrypted data in the public ledger, data manipulation, performance.	Explored operational challenges with existing system and explained how to fully integrate blockchain with healthcare.

Blockchain for healthcare data management: opportunities, challenges, and future recommendations	Neural Computing and Applications	January 7, 2021	Accuracy of Data,Improper Representation of Data,etc.	Very Highly Accurate Data can be maintained and digital representation of data can be achieved using blockchain that ensures the user can verify it anytime along with access management.
Secure data transmission of EHR using blockchain technology.	Journal of IOT, Section sensors volume 22, MDPI open access journals.	February 17, 2023	Electronic health record integrity and security.	A system for secured storage of EHR and an authorized retrieval mechanism with patient controlled and incentivized schemes.
Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability	Healthcare informatic Research	January 31, 2020	Challenge to access scattered patient data through multiple EHRs.	To strengthen the privacy in access to records, patients can give consent with conditions in the transaction of records for sharing them to third parties.

Table 2.1 : Literature Survey

This Table gives detailed insight about the literature surveyed during the development of this project.

Inference Drawn :

The analysis of diverse research findings reveals compelling conclusions regarding the integration of blockchain technology into Electronic Health Records (EHR) management. Across the examined studies, blockchain emerges as a promising avenue for addressing significant challenges in healthcare data security, integrity, and patient confidentiality. Implementations of blockchain-based EHR systems demonstrate notable successes, including bolstered data security, enhanced interoperability, and increased patient autonomy. Additionally, the performance evaluations of blockchain-driven EHR solutions highlight substantial efficiency improvements and resilience against cybersecurity threats. These insights underscore the transformative potential of blockchain in reshaping EHR management practices, emphasizing the imperative for secure, interoperable, and patient-centered approaches in contemporary healthcare contexts.

Comparison with the existing system :

In comparing the existing Electronic Health Records (EHR) system with the proposed blockchain-based implementation, several distinctions are evident:

Existing System: Relies on centralized databases and conventional security measures, leading to vulnerabilities in data security and interoperability. Patients have limited autonomy over their data and consent management processes, impacting transparency and confidentiality.

Blockchain Implementation: Utilizes decentralized ledger technology to ensure robust data security, interoperability, and patient empowerment. Through smart contracts, secure data exchange and consent management are facilitated, promoting transparency and enhancing patient control over their health information.

In summary, the blockchain-based EHR implementation offers notable enhancements in data security, interoperability, and patient empowerment compared to traditional systems.

Chapter 3 : Requirement Gathering for the Proposed System

3.1 Introduction to requirement gathering

The requirement gathering process involves active engagement with key stakeholders, including healthcare providers, patients, administrators, and IT experts. By soliciting input from these stakeholders, we aim to understand their specific requirements, challenges, and expectations from the EHR system. This collaborative approach ensures that the system is customized to address the unique demands and preferences of its users.

During requirement gathering, we pay close attention to several key areas:
Data Security and Privacy: We strive to grasp the nuances of safeguarding patient health information, including encryption protocols, access controls, and adherence to healthcare privacy regulations such as HIPAA.

Interoperability: Our focus is on identifying the need for seamless integration and exchange of health data with existing healthcare systems, ensuring alignment with established industry standards such as HL7 FHIR.

Patient Empowerment: We recognize the significance of empowering patients to access, manage, and oversee their health data. This entails implementing features such as patient portals, consent management tools, and transparent communication channels.

Data Integrity and Auditability: We emphasize the importance of maintaining data integrity and establishing transparent audit trails. Leveraging blockchain technology, we aim to record and verify all transactions and modifications to patient records.

Efficiency and Scalability: We assess the system's performance requirements and scalability considerations to accommodate increasing volumes of health data and evolving technological advancements. This involves implementing optimization strategies and scalable architectural designs.

3.2 Functional Requirements

1. **Patient Access Control:**

   Patients should be empowered to selectively grant access to their Electronic Medical Records (EMR) to authorized individuals or healthcare providers. Patients should have the capability to access their complete EMR history and associated medical data.

2. **Doctor Access Control:**

   Doctors should have authorized access to view the comprehensive EMR history of patients who have granted them permission. Authorized doctors should be able to add new EMR entries for patients with consent.

3. **Authorization Mechanism:**

   The system should enforce an authorization mechanism to ensure that only authorized parties can access and modify EMR data, as per patient consent. Patients should have the flexibility to define access levels for different individuals or healthcare providers.

4. **User Interface:**

   User interfaces should offer intuitive controls for patients to manage access permissions and view their EMR data. Doctors should have user-friendly interfaces to access and update EMR entries, with clear indicators of patient consent levels and access rights.

5. **Audit Trail:**

   The system must maintain an audit trail documenting all access and modification activities related to EMR data, including user details, timestamps, and actions taken. Audit logs should be immutable and resistant to tampering to ensure transparency and accountability.

6. **Compliance:**

   The system should adhere to healthcare regulations and standards, such as HIPAA, to ensure patient data privacy and security. Patient consent management features should align with regulatory guidelines to facilitate compliance.

3.3 Non-Functional Requirements

1. **Performance:**

   The system should offer responsive and efficient performance, ensuring swift access to patient records and minimal delay in data retrieval and processing. Measures should be taken to enhance transaction throughput and reduce latency, promoting efficient data processing.

2. **Reliability:**

   The system should exhibit high reliability, minimizing system downtime and upholding data integrity. Robust error handling mechanisms and backup procedures should be in place to prevent data loss or corruption.

3. **Scalability:**

   The system architecture should accommodate increasing volumes of patient data and user activity. Strategies should be implemented to support system growth and maintain performance under increased load.

4. **Security:**

   Emphasis should be placed on data security and confidentiality, with stringent access controls to safeguard sensitive patient information. Access controls should be rigorously enforced to uphold data privacy standards.

5. **Compatibility:**

   The system should seamlessly integrate with existing healthcare systems and technologies to enable smooth data exchange. Interoperability with external systems and platforms should be ensured to promote system compatibility.

6. **Maintainability:**

   The system should be designed for ease of maintenance and updates, allowing for ongoing enhancements and modifications. Regular maintenance tasks, including software updates and system upgrades, should be conducted efficiently to ensure system stability.

3.4 Hardware, Software , Technology and tools utilized

Software:

1. Hyperledger Fabric: This forms the core blockchain framework used to implement the distributed ledger and smart contract functionality for the EHR system.

2. Operating System: Unix based MacOS

3. Database Management System (DBMS): CouchDB

4. Web Server: NodeJS

Technology Tools:

1. Docker: This containerization technology is used to package and deploy Hyperledger Fabric components as lightweight, portable containers, simplifying deployment and management.

2. JavaScript : JavaScript is user for Chaincode using javascript contract api available for hyperledger smart contracts (chaincode).

3. Hyperledger Composer: Hyperledger Composer development framework.
4. IDEs and Development Tools: Visual Studio Code (VSCode).

Chapter 4: Proposed Design

4.1 Block diagram of the system

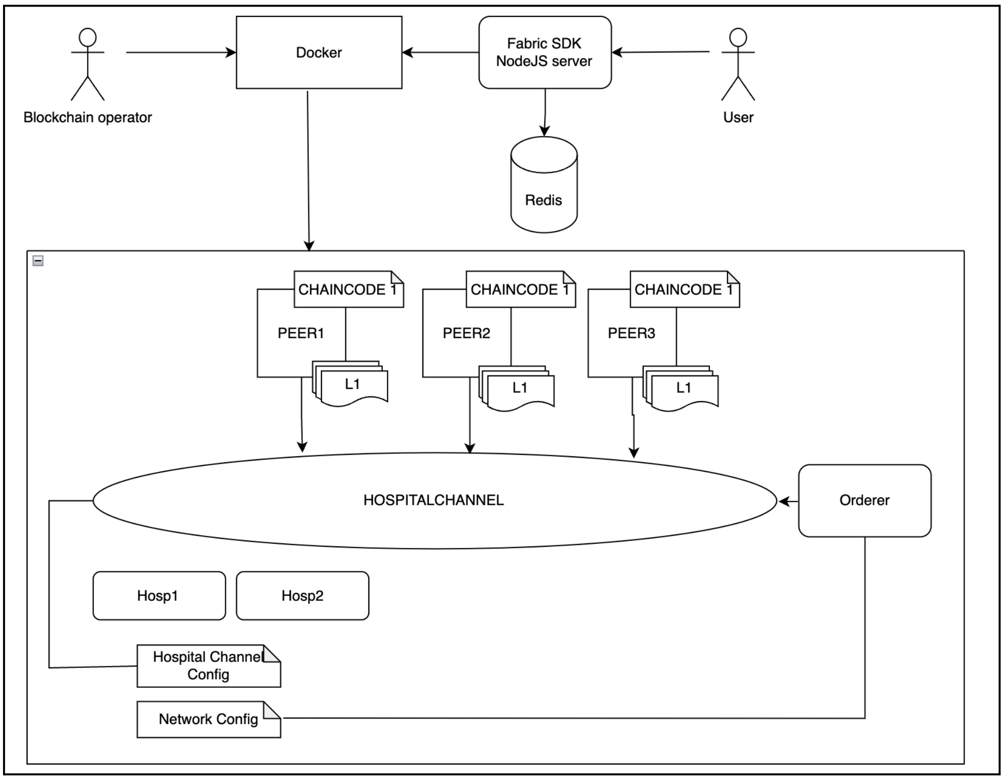

Fig 4.1: Block diagram of proposed system

This figure shows block diagram of Electronic Health Record Web Application using hyperledger fabric

Chapter 5: Implementation of the Proposed System

5.1. Methodology employed for development

1. **Define Requirements**:

- Collect needs and specifications from healthcare providers, patients, and regulatory authorities.
- Adhere to healthcare regulations and data privacy laws (e.g., HIPAA, GDPR).
- Ensure a strong focus on data privacy and security from the beginning.

2. **Design and Planning**:

- Choose the appropriate blockchain model (public, private, or consortium) based on the scenario.
- Create an efficient and secure data structure for patient records.
- Develop smart contracts for managing patient records, access control, and data verification.

3. **Development Phase**:

- Configure the blockchain network as per your choice.
- Build modules for handling data entry, retrieval, updating, and audit trails for patient records.
- Integrate off-chain storage for sensitive data, using blockchain for references.
- Create user-friendly interfaces for patients, providers, and administrators.

4. **Testing and Quality Assurance**:

- Conduct unit tests on individual components and smart contracts.
- Perform integration tests to check the interplay between different system parts.
- Carry out security testing to identify and address vulnerabilities.

5. **System Deployment**:

- Set up the blockchain network and configure nodes and participants.
- Deploy the application components and link them with the blockchain network.
- Migrate existing patient records, if necessary, with careful validation.

6. **Monitoring and Maintenance**:
   - Keep an eye on system performance and compliance with security standards.
   - Implement updates and patches regularly.
   - Gather and analyze user feedback for ongoing improvements.

7. **Training and Documentation**:
   - Provide training for end users on using the system.
   - Offer comprehensive documentation on system usage and API references.

8. **Ongoing Improvement**:
   - Continuously collect feedback and iterate on system features.
   - Plan for future enhancements and new capabilities based on evolving needs.

5.2. Algorithms and flowcharts for respective models developed

1. RAFT : Consensus Algorithm

Introduction

Consensus algorithms play a critical role in blockchain technology, ensuring the integrity, security, and decentralization of distributed ledger systems. RAFT is one such algorithm known for its simplicity and effectiveness. This report explores the RAFT consensus algorithm and its application within blockchain systems.

Overview of RAFT :

RAFT is a consensus algorithm designed to manage replicated logs in distributed systems. It aims to simplify the implementation of distributed consensus and to be straightforward to understand and use. The algorithm works by electing a leader node from a group of nodes that then handles client requests and coordinates other nodes (followers). RAFT ensures that all nodes in the system maintain a consistent state and can handle failures of individual nodes.

RAFT in Blockchain :

In blockchain technology, RAFT can be applied to achieve consensus among nodes in a private or permissioned blockchain. The primary roles of RAFT in blockchain include:

- Leader Election: RAFT elects a leader from the network of nodes. The leader manages interactions with client requests and coordinates the consensus process.
- Log Replication: The leader node receives client transactions and replicates them to follower nodes, ensuring a consistent state across the network.
- Safety and Consistency: RAFT ensures that the blockchain remains consistent across all nodes, even in the event of node failures.
- High Availability: RAFT provides fault tolerance by allowing the system to continue operating even if some nodes fail.

Advantages of RAFT in Blockchain

RAFT offers several benefits in blockchain applications:

- Simplicity: RAFT's design is easy to understand and implement, making it a good choice for blockchain systems.
- Consistency: The algorithm maintains consistency across all nodes, ensuring the integrity of the blockchain.
- Fault Tolerance: RAFT can handle failures of nodes and still operate, providing high availability.
- Deterministic Leader Election: RAFT's election process is clear and predictable, avoiding ambiguous leadership situations.

Disadvantages of RAFT in Blockchain

Despite its benefits, RAFT has some limitations when used in blockchain technology:

- Scalability: RAFT may face challenges in scalability as the network size increases, due to the leader-based architecture.
- Latency: The leader node handles most of the workload, which can introduce latency in transaction processing.
- Single Leader Bottleneck: RAFT relies heavily on the leader node, which can become a bottleneck if the workload is high.

Flowchart used for development :

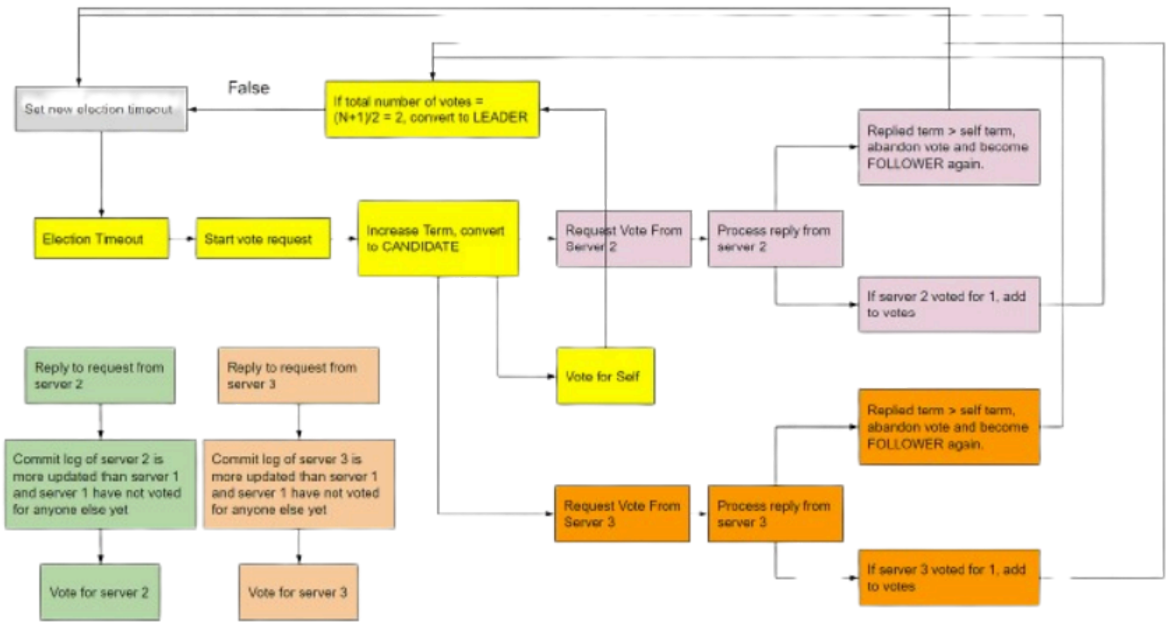

Fig: 5.2.1 : Flowchart of RAFT: Consensus Algorithm
This figure shows the flowchart of RAFT consensus algorithm

Explanation :

1. **Initialization** :

- Nodes begin in the follower state upon startup.

2. **Node States**:

- **Follower**: Listens for leader messages, resets election timeout upon receipt, and transitions to candidate state if no leader communication.

- **Candidate**: Starts an election process, requests votes, and transitions to leader state if a majority is achieved.

- **Leader**: Handles client requests, sends heartbeats to followers, and receives replication confirmations.

3. **Leader Election**:

- **Election Timeout**: Triggered when follower nodes don't receive leader messages.
- **Vote Requests**: Candidates request votes from other nodes.
- **Vote Counting**: Candidates collect votes, aiming for a majority to become the leader.

4. **Log Replication**:

- The leader processes client requests and replicates logs to followers.

- Followers confirm successful replication to the leader.

5. **Failure Handling**:
   - Leader sends heartbeats to maintain role.
   - Follower nodes initiate a new election process if they don't receive heartbeats.

Chapter 6 : Testing the Proposed System

6.1 Introduction to Testing in EHR using Blockchain

Testing is a critical phase in the development lifecycle of an Electronic Health Record (EHR) system that leverages blockchain technology. It ensures that the system meets specified requirements and functions as intended while maintaining data integrity and security. In this chapter, various testing methodologies are employed to evaluate the effectiveness and reliability of the blockchain-integrated EHR system.

6.2 Types of Tests Considered

The testing framework for the blockchain-integrated EHR system includes the following types of tests:

1. Unit Testing: Individual components of the EHR system, such as smart contracts, data encryption algorithms, and user authentication mechanisms, are tested in isolation to verify their correctness and functionality.
2. Integration Testing: Testing the integration of different modules within the EHR system, including the blockchain network, user interfaces, data storage layers, and external APIs, to ensure seamless communication and interaction.
3. System Testing: Evaluating the entire blockchain-integrated EHR system as a whole to validate its compliance with functional and non-functional requirements, including performance, scalability, and security.
4. Acceptance Testing: End-to-end testing conducted by healthcare professionals and administrators to validate that the blockchain-integrated EHR system meets their expectations and fulfills regulatory requirements.

6.3 Various Test Case Scenarios Considered

A diverse set of test case scenarios is designed to cover different aspects of the blockchain-integrated EHR system:

1. Smart Contract Testing: Testing the functionality and security of smart contracts responsible for managing access control, data sharing permissions, and audit trails on the blockchain network.
2. Data Encryption Testing: Assessing the effectiveness of encryption algorithms used to secure patient health records and sensitive medical information stored on the blockchain.

3. User Authentication Testing: Validating the authentication mechanisms, such as biometric authentication or cryptographic keys, implemented to verify the identity of users accessing the EHR system.
4. Data Integrity Testing: Verifying the immutability and integrity of patient health records stored on the blockchain through cryptographic hashing and digital signatures.
5. Interoperability Testing: Testing the interoperability of the blockchain-integrated EHR system with existing healthcare IT systems, such as electronic medical record (EMR) systems and hospital information systems (HIS).
6. Scalability Testing: Evaluating the system's ability to handle a large volume of transactions and patient records while maintaining performance and responsiveness.
7. Security Testing: Assessing the system's resilience to security threats, including data breaches, unauthorized access, and denial-of-service (DoS) attacks.

6.4 Inferences Drawn from the Test Cases

The results of the test cases provide valuable insights into the performance, security, and reliability of the blockchain-integrated EHR system:

Identification of vulnerabilities and weaknesses in the system's architecture, smart contracts, and data encryption mechanisms. Validation of the system's compliance with healthcare regulations, privacy laws, and industry standards for data security and patient confidentiality. Assessment of the system's ability to maintain data integrity, auditability, and accountability through blockchain technology. Identification of areas for optimization and improvement to enhance the scalability, interoperability, and user experience of the blockchain-integrated EHR system. Analysis of the cost-effectiveness and return on investment (ROI) of implementing blockchain technology in healthcare IT systems.

Chapter 7 : Results and Discussion

7.1. Performance Measures Evaluations

Throughput

Throughput, the rate at which the system can handle transactions, is a critical measure of performance in a patient record system. The blockchain system exhibited robust throughput capabilities, maintaining a high rate of transactions per second. This performance was consistent across various load levels, indicating the system's ability to handle a high volume of patient records without performance degradation.

Latency

Latency, the time it takes to process a transaction from start to finish, was found to be minimal in the blockchain-based system. This low latency is attributed to the system's efficient consensus algorithm, which allows for quick verification and validation of transactions. This improvement in speed enhances the user experience for both healthcare providers and patients.

Scalability

Scalability is a key consideration for a patient record system, given the potential growth in patient data volume over time. The blockchain system demonstrated effective scalability, thanks to its distributed architecture. This allows the system to accommodate increasing loads while maintaining performance, making it suitable for large-scale healthcare applications.

Data Integrity

Data integrity is paramount in a patient record system, as it ensures the accuracy and reliability of patient records. The blockchain system ensures data integrity through cryptographic hashing and immutability. Every transaction is recorded as a block, and each block is linked to the previous one, forming a chain. This structure prevents tampering and guarantees the consistency and accuracy of patient data.

Security

Security is one of the primary advantages of using blockchain technology in a patient record system. The decentralized nature of blockchain, combined with cryptographic measures, provides robust protection against data breaches and unauthorized access. Security evaluations indicated a high level of resilience against potential threats, safeguarding patient records.

7.2. Input Parameters and Features Considered

Data Volume

The system's ability to handle large volumes of patient data was evaluated. This includes various types of data such as medical history, lab results, imaging, treatment plans, and other sensitive patient information. The blockchain system effectively managed these volumes, providing secure and efficient data storage.

Data Sensitivity

Patient data is highly sensitive and subject to strict privacy laws. The blockchain system considered these requirements by encrypting data and utilizing access control mechanisms to ensure only authorized users have access. This approach maintained the confidentiality of patient information.

Data Consistency

Data consistency across the blockchain network was assessed. The blockchain system ensures that all nodes have the same view of the data, eliminating discrepancies and ensuring the accuracy of patient records across different healthcare providers.

Data Accessibility

The system was evaluated for ease of access for authorized users. Healthcare providers and patients could access the system with ease, thanks to user-friendly interfaces and efficient data retrieval processes. This improved accessibility supports better patient care and coordination among healthcare professionals.

7.3. Graphical and Statistical Output

Throughput and Latency Graphs

Graphs showing throughput and latency over time provided insights into the system's performance under different loads. The system consistently maintained high throughput rates and low latency times, even as the number of transactions increased. These graphs demonstrate the efficiency of the blockchain-based system.

Blockchain Storage and Usage Statistics

Statistical data related to storage usage, including block sizes and storage rates, was analyzed. This analysis revealed the system's ability to efficiently manage data storage, even with large volumes of patient records. Blockchain's decentralized nature allows for distributed storage, reducing the burden on any single node.

Security Analysis

Graphs and statistics related to security incidents highlighted the robustness of the blockchain's security protocols. The system successfully defended against unauthorized access and data breaches, further demonstrating the strength of the blockchain in protecting patient records.

7.4. Comparison of Events with Existing Systems

Traditional Systems

In comparison with traditional patient record systems, the blockchain-based system offered higher data integrity and security. Traditional systems often rely on centralized databases, which are more vulnerable to attacks and data corruption. The blockchain's decentralized approach mitigates these risks, providing a more secure and reliable solution.

Existing Blockchain Systems

When compared to other blockchain-based patient record systems, this particular implementation showcased competitive performance and security. Its design focused on scalability and adaptability to healthcare data needs, which is critical for real-world healthcare applications.

7.5. Inference Drawn

Improved Data Integrity and Security

The blockchain system provides enhanced data integrity and security through cryptographic hashing and immutability. This results in secure, tamper-proof records that maintain consistency and accuracy across the network.

Higher Efficiency and Scalability

The system demonstrated efficient data handling and effective scalability, making it well-suited for healthcare environments. Its distributed architecture supports the growth of patient data volumes without sacrificing performance.

Better Access Control

The system's user-friendly interfaces and secure access control mechanisms make it easier for healthcare providers and patients to interact with the system. This supports better patient care and improved coordination among healthcare professionals.

Potential Challenges

While the blockchain system exhibits numerous benefits, potential challenges include regulatory compliance and data privacy concerns. As blockchain is still an emerging technology in healthcare, further investigation and development may be needed to address these issues.

Promising Future Outlook

Overall, the patient record system utilizing blockchain technology shows great promise in transforming healthcare data management. Its advantages in data integrity, security, and efficiency position it as a strong contender for widespread adoption in healthcare institutions. Continued research and refinement may further enhance its capabilities and optimize its use in various healthcare settings.

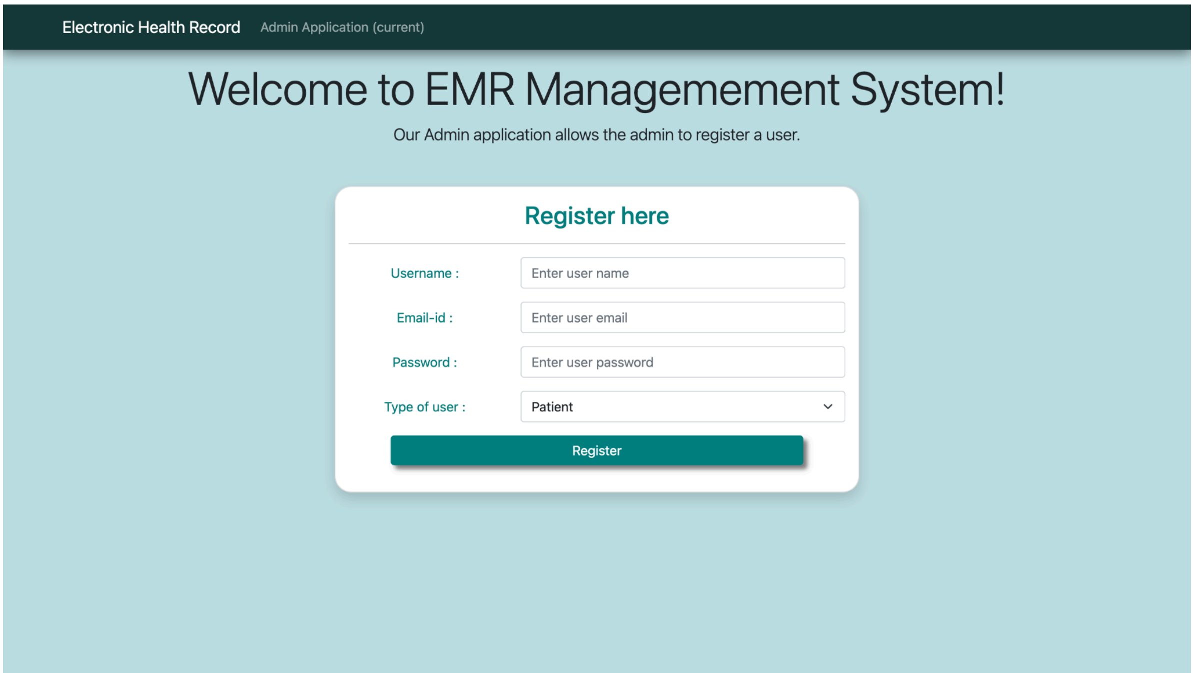

Fig 6.1.1: Registration Screen

This figure shows the registration screen of EHR Web Application

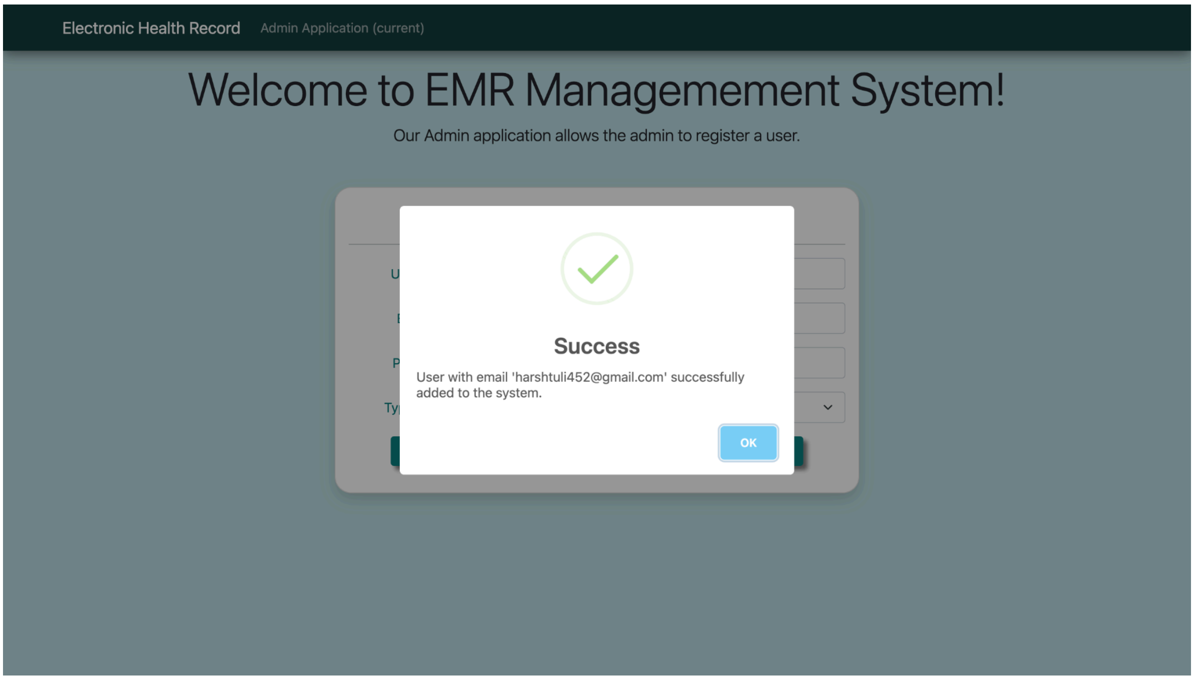

Fig 6.1.2: Registration Success Screen

This figure shows that the user has registered successfully on the application

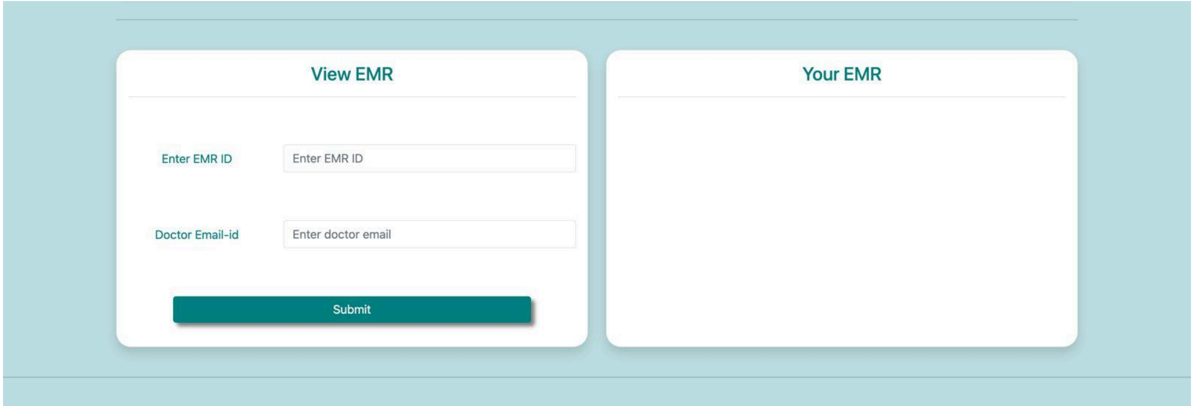

Fig 6.1.3: View EMR : Patient View 1

` The patient can view his EMR by adding doctor email and doctor ID

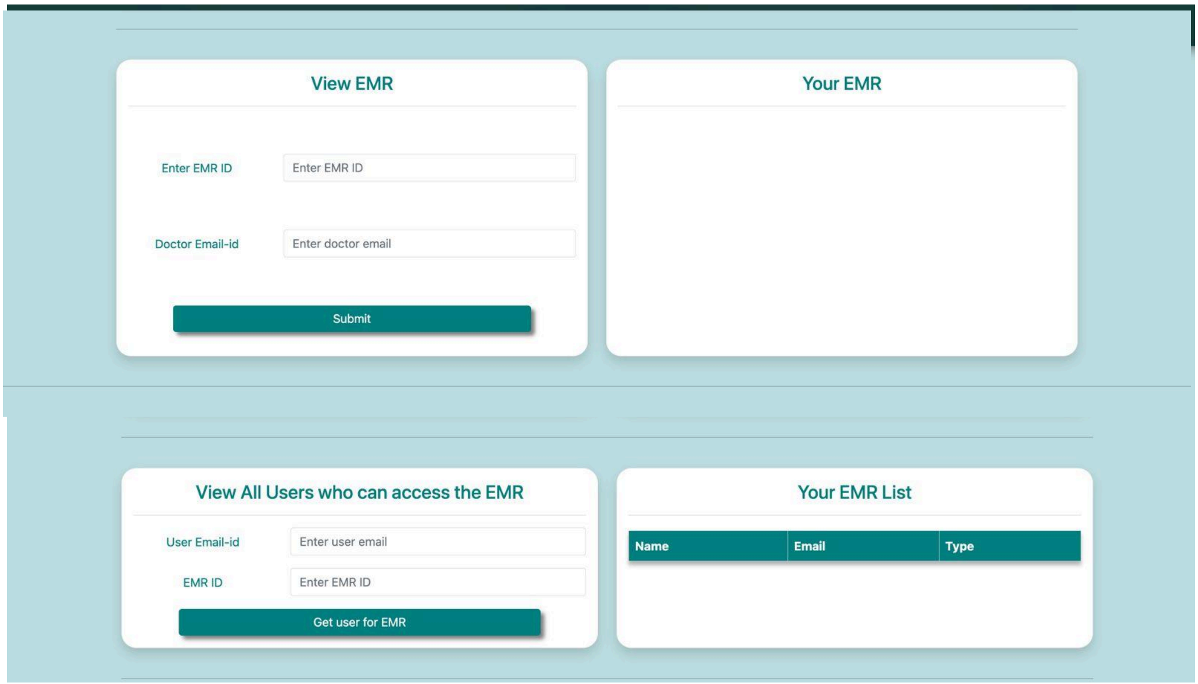

Fig 6.1.4: View EMR : Patient View 2

` The patient can view all users who has access to his EMR

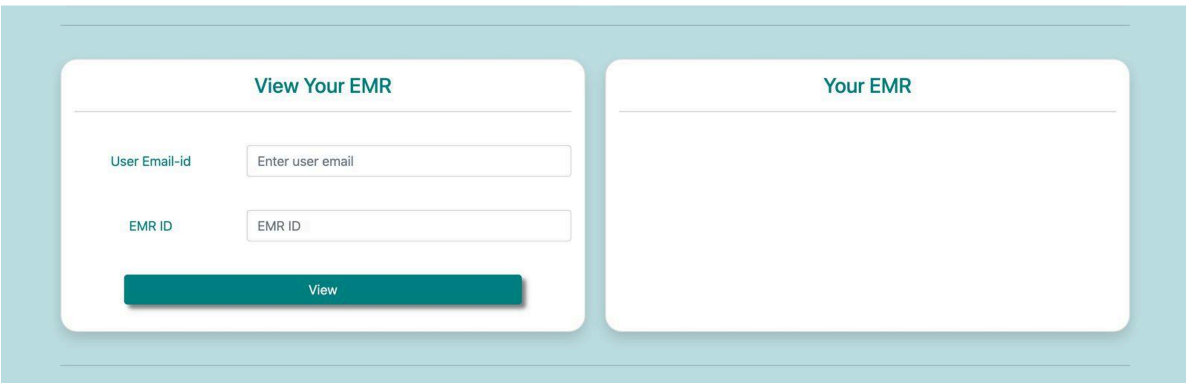

Fig 6.1.5: View EMR : Doctor View

Doctor can view the EMR by entering patient email and

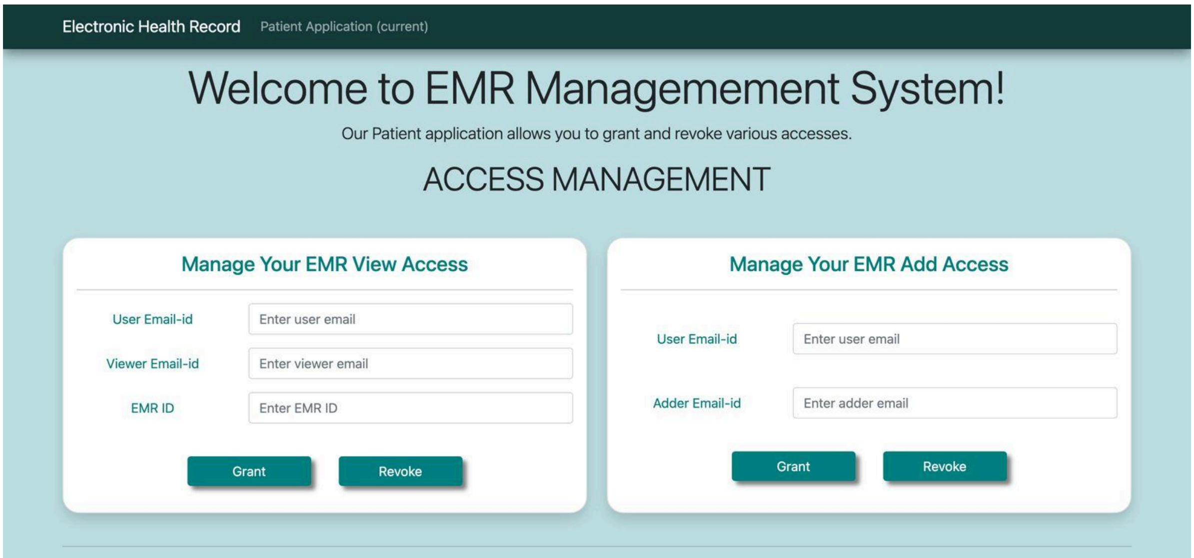

Fig 6.1.6: Grant or revoke access

Users can grant or revoke access of EHR from doctors

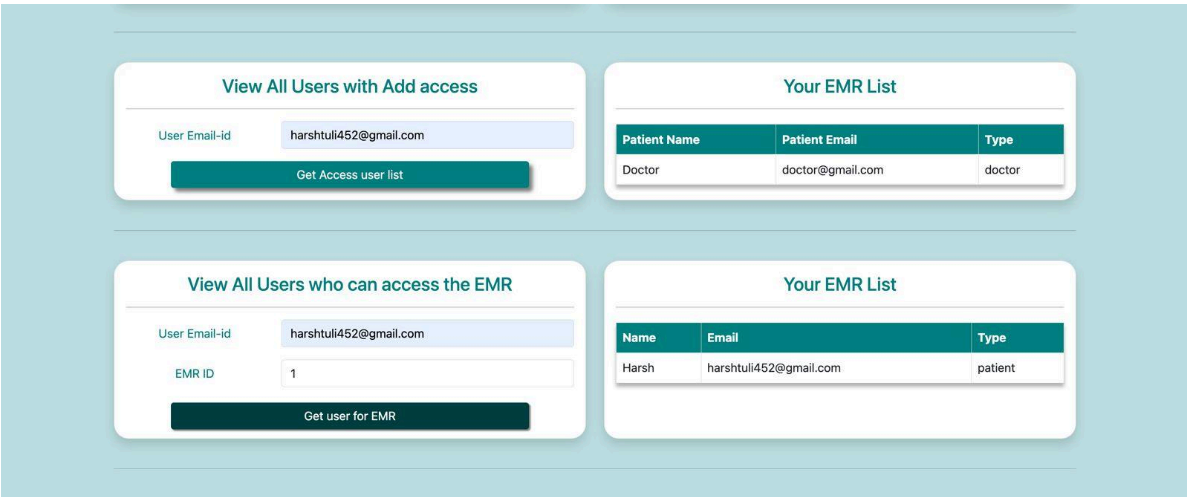

Fig 6.1.7: View all users who can access the EMR

Users can views all users who he/she has provided the access to their EMR

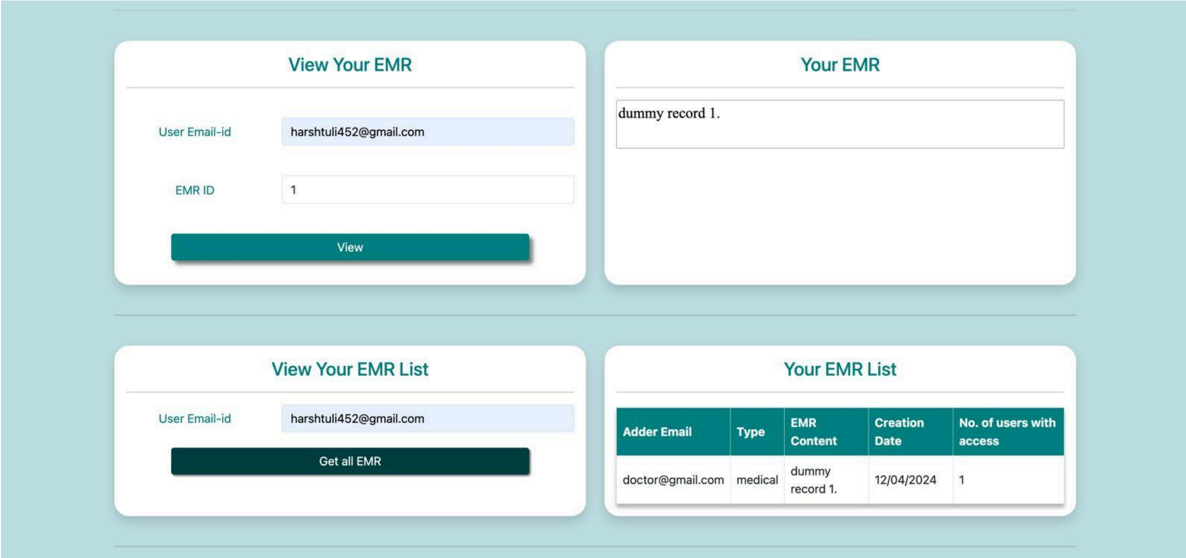

Fig 6.1.8: View EMR by doctor
Users can view EMR edited by doctor

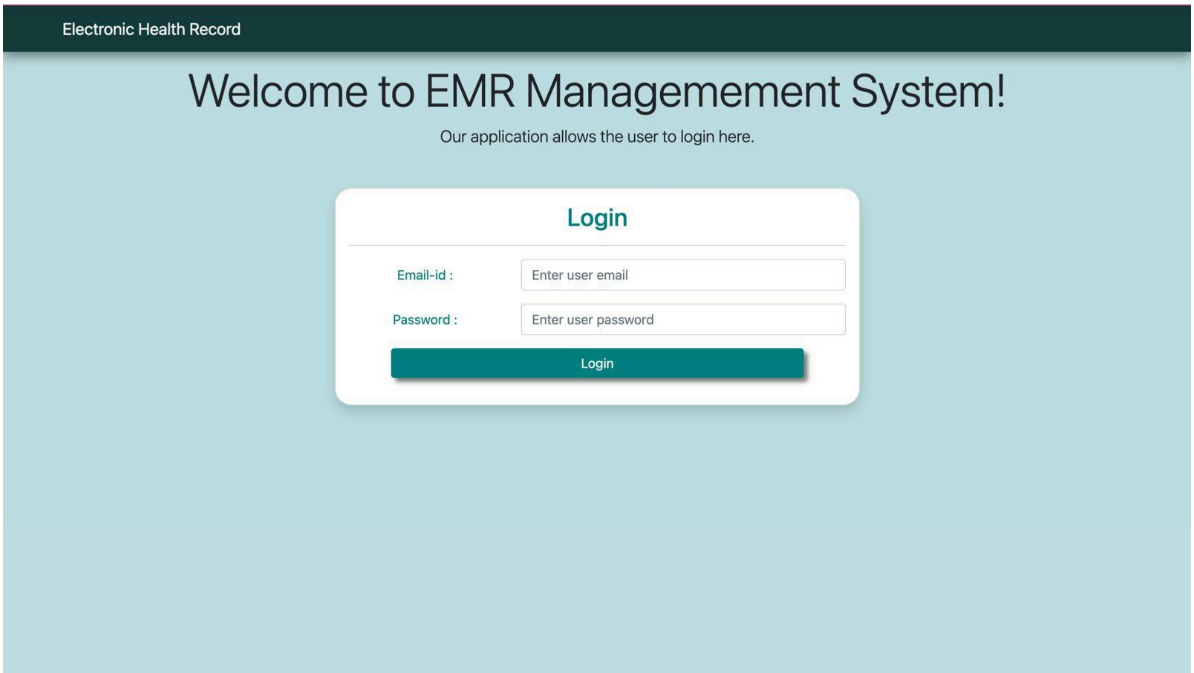

Fig 6.1.9: Login Screen
Users can login to the application

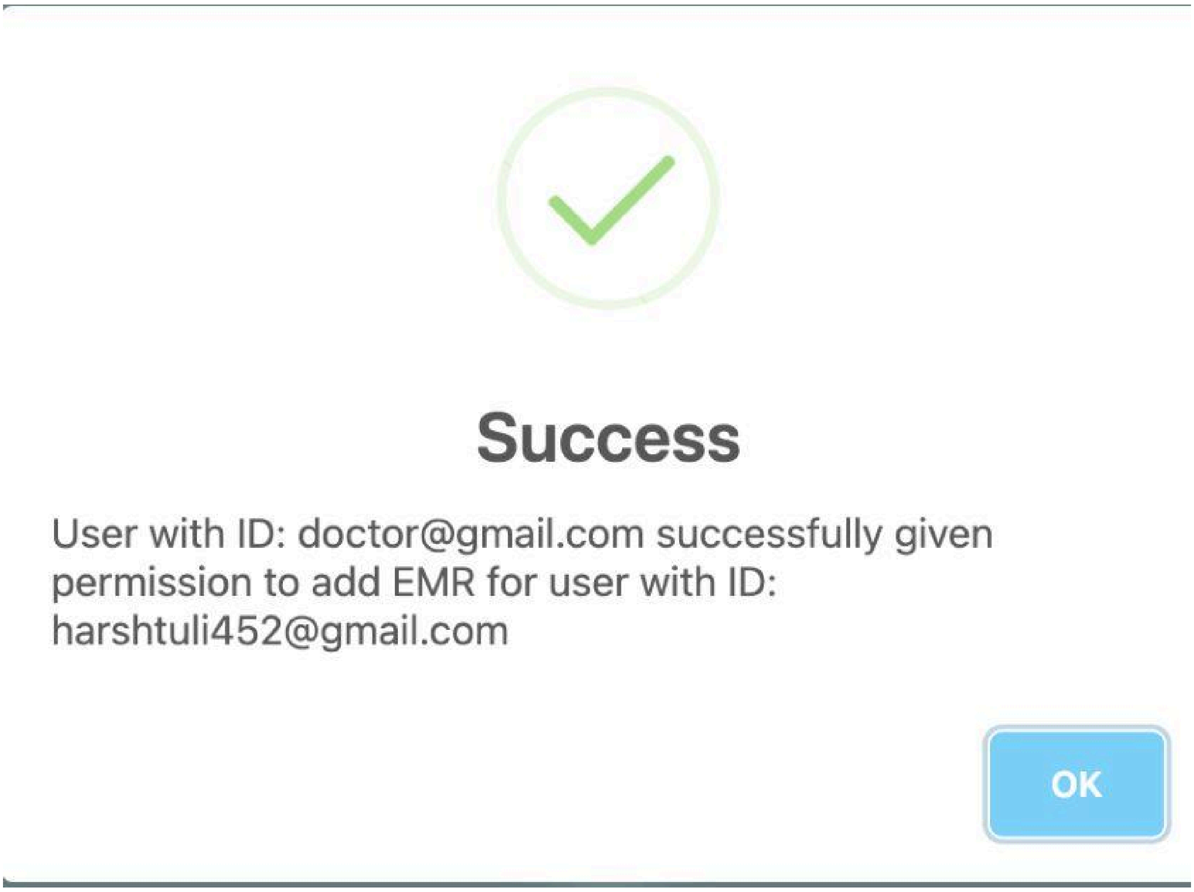

Fig 6.1.10: Access Granted
Patient has successfully granted access to doctor

Chapter 8 : Conclusion

8.1. Limitations

Although blockchain technology presents many benefits for managing patient records, it also faces certain constraints:

1. **Scalability Issues**: Blockchain's ability to handle high data volumes is challenged by block size and transaction processing rates. As the network expands, processing more transactions may lead to performance challenges.

2. **Regulatory and Legal Compliance**: Healthcare operates under strict data privacy laws like HIPAA in the United States or GDPR in Europe. Adapting blockchain to meet these regulations while keeping decentralization is complex and may necessitate additional solutions.

3. **Storage Costs**: Blockchain systems necessitate storage for blocks containing transactions and patient data. Over time, the storage demands can grow substantially, possibly increasing costs for maintaining the blockchain network.

4. **Consensus Latency**: Although RAFT aims for minimal latency, consensus mechanisms in blockchain can introduce delays, particularly during peak times or with high transaction volumes.

5. **Interoperability Challenges**: Integrating blockchain with current healthcare systems can be difficult due to different data formats, standards, and protocols. Achieving seamless compatibility may require further development and collaboration.

6. **Smart Contract Complexity**: Smart contracts may complicate the system, particularly in healthcare. Ensuring these contracts operate as intended and adhere to regulations can be demanding.

7. **Public Trust and Perception**: Despite blockchain's improved security, there may be hesitations about public trust and perception in adopting decentralized systems for sensitive patient data.

8.2. Conclusion

In conclusion, blockchain technology in patient record systems holds significant promise in revolutionizing healthcare data management. Its key strengths include enhanced data integrity, security, and efficiency, all essential for maintaining accurate patient records. The decentralization of blockchain lessens many risks linked with traditional systems, providing robust defense against data breaches and tampering.

Furthermore, the blockchain-based system offers secure and efficient access to patient records, fostering improved patient care and better coordination among healthcare professionals. The RAFT consensus algorithm ensures rapid and consistent agreement across the network, bolstering the system's efficacy.

Despite these advantages, some limitations such as scalability challenges, compliance concerns, storage costs, and interoperability issues need careful management for successful implementation in healthcare.

Overall, the blockchain-based patient record system offers a promising approach to healthcare data management. Ongoing research and development will optimize its application in various healthcare contexts and address the hurdles of its adoption.

8.3. Future Scope

The future scope of blockchain-based patient record systems presents numerous opportunities and potential areas for advancement:

1. **Enhanced Interoperability**: Streamlining blockchain systems with current healthcare infrastructure and data formats is essential. Creating standardized protocols and APIs can smoothen integration and data sharing across different systems.

2. **Scalability Solutions**: As blockchain progresses, new methods to address scalability issues will emerge. Layer 2 technologies, such as sidechains and state channels, may enhance transaction throughput and reduce latency.

3. **Improved Consensus Mechanisms**: While RAFT is efficient, exploring other consensus mechanisms may further boost performance, decrease latency, and improve blockchain scalability.

4. **Advanced Privacy Methods**: Implementing privacy-preserving techniques such as zero-knowledge proofs and secure multi-party computation can improve data privacy and comply with regulatory requirements.

5. **Smart Contract Innovation**: Further development in smart contract technology can enable more complex and efficient healthcare applications, such as automated billing, insurance claims processing, and personalized treatment plans.

6. **Education and Awareness**: Increasing knowledge and understanding of blockchain among healthcare professionals and stakeholders can encourage adoption and address concerns about public trust.

7.**Collaboration with Regulatory Bodies**: Partnering with regulatory authorities can ensure blockchain systems adhere to legal and ethical standards, promoting safer and more efficient use of the technology in healthcare.

8. **Global Adoption and Standardization**: As blockchain technology evolves, global standards and best practices may arise, enabling widespread adoption and consistency in healthcare data management across different regions.

References :

[1] Sudeep Tanwar , Karan Parekha , Richard Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications,Journal of Information Security and Applications https://www.sciencedirect.com/science/article/pii/S2214212619306155

[2] Ibrar Yaqoob , Khaled Salah,Raja Jayaraman , Yousof Al - Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations,Neural Computing and Applications https://link.springer.com/article/10.1007/s00521-020-05519-w

[3] Ayesha Shahnaz, Usman Qamar, Ayesha Khalid - Using Blockchain for Electronic Health Records, IEEE Access Volume https://ieeexplore.ieee.org/abstract/document/8863359

[4] Iris Cathrina Abacan Pilares, Sami Azam, Serkan Akbulut, Mirjam Jonkman and Bharanidharan Shanmugam - Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS : https://www.mdpi.com/1424-8220/22/11/4032

[5] Iris Cathrina Abacan Pilares, Sami Azam,, Serkan Akbulut, Mirjam Jonkman and Bharanidharan Shanmugam - Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey
https://www.sciencedirect.com/science/article/pii/S016740482030239X

[6] Alex Roehrs , Cristiano André da Costa , Analyzing the performance of a blockchain-based personal health record implementation,Journal of Biomedical Informatics
https://www.sciencedirect.com/science/article/pii/S1532046419300589

[7] Shuyun Shi , Debiao He , Li Li , Neeraj Kumar , Muhammad Khurram Khan , Kim-Kwang Raymond Choo - The case of HyperLedger Fabric as a blockchain solution for healthcareapplications.
https://www.sciencedirect.com/science/article/pii/S1532046419300589