A

Major Project Report

on

SECURE MEDICAL RECORD MANAGEMENT USING BLOCKCHAIN TECHNOLOGY

Submitted in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology

By

P. Varun Reddy

(20EG105715)

CV. Sai Phanish Reddy

(20EG105710)

Y. Dhilip Reddy

(20EG105518)

Under The Guidance Of

S. Bhagya Rekha

Assistant Professor

Department of CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANURAG UNIVERSITY VENKATAPUR (V), GHATKESAR (M),

MEDCHAL (D), T.S 500088

(2023-2024)

DECLARATION

We hereby declare that the Report entitled **"SECURE MEDICAL RECORD MANAGEMENT USING BLOCKCHAIN TECHNOLOGY"** submitted for the award of Bachelor of technology Degree is my original work and the report has not formed the basis for the award of any degree, diploma, associate ship or fellowship of similar other titles. It has not been submitted to any other University or Institution for the award of any degree or diploma.

Place: Anurag University, Hyderabad

P. Varun Reddy
(20EG105715)

CV. Sai Phanish Reddy
(20EG105710)

Y. Dhilip Reddy
(20EG105518)

ANURAG UNIVERSITY | SCHOOL OF ENGINEERING

CERTIFICATE

This is to certify that the project report entitled **"SECURE MEDICAL RECORD-MANAGEMENTUSING BLOCKCHAIN TECHNOLOGY"** being submitted by **Mr. P. Varun Reddy** bearing the Hall Ticket number **20EG105715**, **Mr. CV. Sai Phanish Reddy** bearing the Hall Ticket number **20EG105710**, **Mr. Y. Dhilip Reddy** bearing the Hall Ticket number **20EG105518** in partial fulfilment of the requirements for the award of the degree of the Bachelor of Technology in Computer Science and Engineering to the Anurag University is a record of bonafide work carried out by them under my guidance and supervision for the academic year 2023 to 2024.

The results presented in this report have been verified and found to be satisfactory. The results embodied in this report have not been submitted to any other University or Institute for the award of any other degree or diploma.

Signature of Supervisor
S. Bhagya Rekha
Assistant Professor
Department of CSE

Signature of Dean CSE
Dr. G. Vishnu Murthy
Dean, CSE

External Examiner

ACKNOWLEDGEMENT

We would like to express our sincere thanks and deep sense of gratitude to project supervisor **S. Bhagya Rekha, Assistant Professor, Department of Computer Science and Engineering,** Anurag University for her constant encouragement and inspiring guidance without which this project could not have been completed. Her critical reviews and constructive comments improved our grasp of the subject and steered us towards the fruitful completion of the work. Her patience, guidance and encouragement made this project possible.

We would like acknowledge our sincere gratitude for the support extended by **Dr. G. VISHNU MURTHY, Dean, Department of Computer Science and Engineering,** Anurag University. We also express my deep sense of gratitude to **Dr. V. V. S. S. S. BALARAM**, **Academic Co-ordinator, Dr. Pallam Ravi**, **Project Co-ordinator** and Project review committee members, whose research expertise and commitment to the highest standards continuously motivated me during the crucial stage our project work.

We would like express our special thanks to **Dr. V. VIJAYA KUMAR, Dean School of Engineering,** Anurag University, for his encouragement and timely support in our B. Tech program.

P. Varun Reddy
(20EG105715)

CV. Sai Phanish Reddy
(20EG105710)

Y. Dhilip Reddy
(20EG105518)

ABSTRACT

In today's digital age, safeguarding personal information, particularly sensitive data like medical records, is paramount. Recognizing the inherent risks associated with sharing such information online, there's a pressing need for robust solutions that prioritize privacy and security. Enter our innovative project, which aims to develop a highly secure application for storing medical records on a blockchain a technology renowned for its immutable and decentralized nature. Through the utilization of smart contracts within the Ethereum blockchain network, we're poised to revolutionize how medical data is managed and protected. At the core of our application lies a meticulous process for registering hospitals, which serve as authorized entities entrusted with inputting and accessing medical details. By restricting access solely to registered hospitals, we ensure stringent control over who can interact with the sensitive data, bolstering security measures significantly. With a commitment to leveraging cutting-edge blockchain technology, our project not only addresses the immediate concerns surrounding data privacy but also sets a new standard for securely managing medical records in the digital realm. Through continuous innovation and adherence to best practices, we're poised to make a lasting impact on the landscape of healthcare data management.

INDEX

LIST OF FIGURES

NOMENCLATURE

CSS	Cascading Style Sheets
DAPP	De-centralized Application
EHR	Electronic Health Record
EVM	Ethereum Virtual Machine
ETH	Ether
HTML	Hypertext Markup Language
NFT	Non-Fungible Tokens

CHAPTER 1
INTRODUCTION

1.1 OVERVIEW

In contemporary times, the significance of information security cannot be overstated across various domains. With data misuse capable of inciting chaos and profound disruptions, safeguarding information is imperative. Data holds immense value to individuals and society alike, making its protection a top priority. Threat actors, such as hackers and intruders, constantly probe databases and servers of social media platforms and other applications, seeking to exploit vulnerabilities for personal gain. Thus, robust security measures are indispensable to thwart unauthorized access and prevent data exploitation.

Information security encompasses more than just barring unauthorized users; it extends to ensuring data integrity, accessibility, and confidentiality. Health data, in particular, holds immense significance in an individual's life, often containing personal details, diagnosis, and treatment information. The confidentiality and integrity of such data are paramount, as individuals are hesitant to disclose sensitive health information to others. However, traditional methods of storing and accessing medical data in hospitals are prone to security breaches, posing significant risks to data integrity and confidentiality.

Despite advancements in technology, including cloud services offering expansive storage and management capabilities, concerns regarding security persist. While cloud technology provides scalability and convenience, relying on third-party services introduces inherent risks. Cloud vendors levy charges based on storage usage and service utilization, making it imperative to weigh the cost against the security implications.

Addressing these challenges necessitates innovative approaches to information security, particularly in the healthcare sector. Implementing robust encryption protocols, access controls, and auditing mechanisms can bolster data protection measures.

1.2 Research Motivation

The motivation behind researching and developing a robust and secure application for storing medical records on a blockchain stems from the increasing threat posed by the accessibility of personal information on the internet, particularly concerning sensitive data like medical records. With the proliferation of digital platforms and the interconnectedness of networks, the risk of unauthorized access, data breaches, and exploitation of personal information has escalated significantly.

Traditional methods of storing and managing medical records have proven susceptible to various vulnerabilities, including unauthorized access, data tampering, and centralized points of failure. To address these challenges and mitigate the risks associated with storing medical data online, there is a pressing need for innovative solutions that leverage emerging technologies to enhance security, transparency, and privacy.

Blockchain technology, with its decentralized and immutable ledger system, offers a compelling framework for securely storing and managing medical records. By utilizing smart contracts within the Ethereum blockchain network, we can establish a trusted and transparent system for registering hospitals as authorized users, thereby ensuring that only accredited institutions can input and access medical data.

The primary aim of our project is to develop a sophisticated application that leverages blockchain technology and smart contracts to enhance the security, privacy, and integrity of medical records stored online. Through our research and development efforts, we aim to contribute to the advancement of secure healthcare data management practices, ultimately safeguarding the privacy and confidentiality of individuals' medical records in an increasingly digital world. By exploring the potential of blockchain technology in this context, we aspire to establish a new standard for the secure storage and management of medical data, benefiting both individuals and healthcare providers alike.

1.3 Problem Statement

The medical record maintenance application leveraging blockchain technology aims to enhance data security and transparency by restricting certain users from modifying data

and adding blocks to the existing blockchain network. This core objective ensures that only authorized users have access to the system, preserving the authenticity of the data. Another key objective of the application is to uphold transparency in the medical data entered into the network.

By utilizing blockchain technology, the application ensures that all transactions are recorded in a transparent and immutable manner, providing a clear audit trail of data entries and modifications. An analysis of the existing system reveals several disadvantages, prompting the development of the proposed system. Blockchain technology enables the maintenance of transaction ledgers across the network, promoting transparency by allowing all users to access transaction history. Additionally, this property of the application eliminates data redundancy by ensuring that each patient's medical data is stored securely on the blockchain without duplication. Overall, the proposed system leverages blockchain technology to overcome the limitations of the existing system, providing enhanced security, transparency, and efficiency in medical record maintenance while offering a user-friendly experience for authorized users.

1.4 Applications

Secure medical record management using blockchain technology holds immense potential across various applications within the healthcare industry.

1. **Patient Data Security and Privacy**: Blockchain technology ensures that patient medical records are securely stored and tamper-proof. By encrypting data and utilizing decentralized networks, patient information remains confidential and accessible only to authorized individuals.

2. **Interoperability and Data Exchange**: Blockchain facilitates seamless interoperability between different healthcare providers and systems. It enables secure and transparent sharing of medical records across various healthcare entities, ensuring continuity of care and reducing administrative burdens..

3. **Medical Research and Clinical Trials**: Blockchain can streamline the process of medical research and clinical trials by securely storing and sharing patient data. Researchers can access anonymized data while maintaining patient privacy, accelerating the pace of medical discoveries and drug development.

4. **Healthcare Supply Chain Management**: Blockchain technology can enhance the transparency and efficiency of healthcare supply chains. By tracking the provenance of medical supplies and pharmaceuticals, it helps prevent counterfeiting, ensure quality control, and improve patient safety.

5. **Health Insurance Claims Processing**: Blockchain can optimize health insurance claims processing by securely recording and verifying transactions. Smart contracts can automate claims processing, reducing fraud, minimizing administrative costs, and expediting reimbursement for healthcare providers.

6. **Telemedicine and Remote Patient Monitoring**: Blockchain facilitates secure communication and data sharing in telemedicine and remote patient monitoring applications. Patients can securely share their medical data with healthcare providers, enabling remote consultations and real-time monitoring of health metrics.

7. **Medical Credentialing and Licensing**: Blockchain can streamline the process of medical credentialing and licensing by securely verifying and storing practitioners' qualifications and licenses. This ensures compliance with regulatory requirements and enhances the integrity of healthcare provider networks.

8. **Personalized Medicine and Precision Healthcare**: Blockchain enables the secure storage and sharing of genomic data and other personalized health information. This allows healthcare providers to deliver tailored treatments and interventions based on individual patient profiles, improving patient outcomes and reducing healthcare costs.

9. **Public Health Surveillance and Epidemiology**: Blockchain technology can facilitate real-time public health surveillance by securely aggregating and analyzing population health data. This allows healthcare authorities to monitor disease outbreaks, track epidemiological trends, and implement timely interventions to mitigate public health risks.

10. **Medical Identity Management**: Blockchain offers a secure and decentralized solution for managing medical identities, such as patient IDs and health records. Patients maintain ownership and control over their identities, reducing the risk of identity theft and fraud. Additionally, healthcare providers can efficiently verify patient identities and access relevant medical information, enhancing patient safety and streamlining care delivery.

CHAPTER 2
LITERATURE SURVEY

1. Ayesha Shahnaz; Usman Qamar; Ayesha Khalid "Using Blockchain for Electronic Health Records", India.09 October

Blockchain has been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management. In this paper, we discuss how blockchain technology can be used to transform the EHR systems and could be a solution to these issues. We present a framework that could be used for the implementation of blockchain technology in the healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining Granular access rulesfor the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chain storage of the records. This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain- based solution.

The paper discusses the potential of blockchain technology to address key challenges faced by Electronic Health Record (EHR) systems in the healthcare sector. It emphasizes the importance of security, privacy, confidentiality, and decentralization in managing sensitive health data. The proposed framework aims to leverage blockchain's decentralized and immutable nature to enhance data security, integrity, and management in EHR systems. Key aspects include implementing granular access rules for users, addressing scalability concerns through off-chain storage solutions, and providing a secure and integral platform for storing electronic health records. The framework holds the promise of improving patient outcomes, streamlining healthcare processes, and fostering trust among patients and healthcare providers

2. William J Gordon, Christian Catalini "Blockchain technology for Healthcare: Facilitating the transition to patient- driven Interoperability"

Interoperability in healthcare has traditionally been focused around data exchangebetween business entities, for example, different hospital systems. However, there has been a recent push towards patient-driven interoperability, in which health data exchangeis patient-mediated and patient-driven. Patient-centered interoperability, however, bringswith it new challenges and requirements around security and privacy, technology, incentives, and governance that must be addressed for this type of data sharing to succeedat scale. In this paper, we look at how blockchain technology might facilitate this transition through five mechanisms: (1) digital access rules, (2) data aggregation, (3) dataliquidity, (4) patient identity, and (5) data immutability. We then look at barriers to blockchain-enabled patient-driven interoperability, specifically clinical data transaction volume, privacy and security, patient engagement, and incentives. We conclude by notingthat while patient-driving interoperability is anexciting trend in healthcare, given these challenges, it remains to be seen whether blockchain can facilitate the transition from institution-centric to patient-centric data sharing.

3. Gulara Muradova, Mehran Hematyar, "Protecting and Securing Medical Records Using Blockchain Technology" S IEEE access Dec 1 2020.

This paper explains about the increasing technology usage in the healthcare industry and rapid digitalization occurring across the world in the domain of healthcare. Blockchain is one of the trending technologies which helps in providing maximum possible security to the data and prevent the data from digital thefts and cyberattacks. Theword "blockchain" is made up of two words "block" and "chain", which ultimately means a chain of blocks. Blockchain is a decentralized information and reporting system. In the blocks, any information can be entered and recorded. In the Blockchain, these blocks of information are linked together in a chain, forming a sequence of information. This technology is a distributed database that anyone can check in on those transactions.

Most healthcare information, from electronic-based medical records in health systems to patient registries and histories, in these days grew up organically for example from custom in-house systems, little or Medium Medical department and largely standards or protocols-free. Databases of healthcare data containing the histories of many patients (medical records) are of enormous value. They can be mined for correlations between patients and a huge range of behaviors, seemingly unrelated conditions, and demographic factors to identify early warning triggers that can be used to bolster preventative

care management. We need access to as much of this data as possible. The problem is accessing several claims sources in a way that's secure enough.

Any information can be recorded in any block, from a person's crimes to the display of account information for assets. In the Blockchain, the information is containedin the blocks and linked together in a chain. The difference with other systems is that the information stored on this type of system is shared among all members of the network and it is almost impossible to delete and manipulate the recorded information using encryption. Consider the following blockchain, for example, each block showing a clinicwhere patient's names and records are recorded. If a character is added to the hospital's patient name information, the hash block will change and subsequent blocks will be invalidated, which is why this technology is called the blockchain.

4. Zhijie Sun, Dezhi Han, Dun Li "A blockchain-based secure storage scheme for medical information" EURASIP Journal on Wireless Communications and Networking volume 20

This paper explains about the importance of medical data and the necessity of maintaining its privacy in the public sector. This paper discusses the application of blockchain technology to medical information management and also puts light on decentralized management and secured storage with the help of distributed consensus andauthentication mechanisms.

Medical information consists of patient's personal and diagnosis data which is considered as highly sensitive. The recent advent in technology is affecting all parts of human life and is changing the way we use and perceive things previously. Just like the changes technology has offered in various other sectors of life, it is also finding new waysfor improvement in the healthcare sector. The main benefits that advancement in technology is offering are to improve security, user experience and other aspects of the healthcare sector.

Before the advent of modern technology, the healthcare sector used paper based systems to store the medical records, i.e., using handwritten mechanisms. This paper- based medical record system was inefficient, insecure, unorganized and was not tamper-proof. It also faced the issue of data- duplication and redundancy as all the institutions that the patient visited had various copies of the patient's medical records.

This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Blockchains hold batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer network.

5. Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte ,"Health Record Management through Blockchain Technology" , IEEE Xplore , 2019.

This paper discusses the transition from a centralized approach to maintaining health records to a patient-centered, decentralized model facilitated by blockchain technology. It begins by highlighting the importance of having a healthy population for societal progress and underscores the significance of health records in monitoring individual health over time.

The paper identifies data breaches as a significant concern in the healthcare sector, citing statistics such as the estimated cost per record of data breaches for healthcare organizations and the number of patient records affected by breaches. It suggests that the traditional institution-driven approach to record maintenance has not effectively mitigated these risks, as patients lack control over their data, increasing the likelihood of misuse.

To address these challenges, the paper proposes a patient-centered approach to health record maintenance that leverages blockchain technology. Blockchain's decentralized and distributed ledger architecture is seen as a solution for enhancing data security, preventing manipulation, and empowering patients with control over access to their records.

Furthermore, the paper discusses the potential applications of blockchain beyond record maintenance, including impact on billing, record sharing, medical research, and combating identity theft and financial data crimes. It emphasizes the role of smart contracts in simplifying processes such as record creation, validation, and access control within the healthcare ecosystem.

6. Usman, M., & Qamar, U, Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. In 2019 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), ELSEVIER

The research focuses on the development and implementation of a blockchain-based Electronic Medical Records (EMRs) management system to address the challenges associated with sharing sensitive healthcare data securely. EMRs contain highly sensitive and private information related to patient diagnosis and treatment, and their frequent sharing among healthcare peers is crucial for effective patient care.

The paper discusses how traditional methods of sharing medical records face significant challenges, including the risk of data exposure or tampering during the sharing process. To overcome these challenges, the researchers propose leveraging blockchain technology to establish a secure and efficient system for managing and sharing EMRs.

The proposed blockchain-based EMR management system aims to ensure privacy, security, and easy accessibility of medical records. By utilizing blockchain's decentralized and immutable ledger, the system provides a transparent and tamper-proof platform for storing and sharing EMRs among authorized parties.

A prototype of the EMR management system is implemented using the Hyperledger permissioned blockchain platform. Hyperledger's permissioned architecture allows for controlled access to the blockchain network, ensuring that only authorized participants can view and interact with EMR data.

CHAPTER 3

SYSTEM ANALYSIS AND DESIGN

3.1 EXISTING SYSTEM

3.1.1 Revolutionizing Healthcare Data Security

Everyday large data gets accumulated in the medical field. It includes various details of the patients including their personal details, diagnosis details and treatment details. Traditionally all such data is either stored in hard disks/drives or in any third partyservers.

These traditional systems as they rely on general servers and personal computersare very prone to the security attacks and breaches. Hospitals which depend on third partyservers for the maintenance of the medical data, they barely use passwords for authentication. But they provide very less security when we consider such systems in thelong run. They give no promise that they will provide security to the great extent. So likethis in the existing system we have a lot of disadvantages.

3.1.2 Working of Revolutionizing Healthcare Data Security:

In the proposed system of secure medical data management using blockchain technology, the process begins with the creation of a decentralized network where medical data is stored securely in blocks, forming a tamper-proof ledger. Each block contains encrypted patient details, diagnosis information, and treatment records. Smart contracts govern access control, ensuring that only authorized users, such as healthcare providers and patients, can access and modify specific data based on predefined permissions.

Blockchain technology ensures data integrity and security through its decentralized nature, cryptographic hashing, and consensus mechanisms. Patient data remains

encrypted and is only accessible through secure authentication methods, such as cryptographic keys or biometric verification. Additionally, the transparent nature of blockchain enables auditing and traceability of all data transactions, enhancing accountability and trustworthiness.

3.1.3 Limitations of Revolutionizing Healthcare Data Security:

Scalability: Blockchain networks may face scalability challenges when handling large volumes of medical data, leading to slower transaction processing times and increased resource consumption.

1. **Integration Complexity:** Integrating blockchain technology with existing healthcare systems and protocols may require significant effort and resources, leading to potential interoperability issues.
2. **Regulatory Compliance:** Ensuring compliance with healthcare regulations, such as HIPAA (Health Insurance Portability and Accountability Act), can be complex due to the decentralized and immutable nature of blockchain.
3. **Data Privacy Concerns:** While blockchain offers enhanced security, concerns regarding patient privacy and data anonymization remain, especially in cases where sensitive information could be inadvertently exposed through data linkage or analysis.
4. **Access Control Challenges:** Designing and implementing robust access control mechanisms within blockchain networks requires careful consideration of user roles, permissions, and data sharing protocols to prevent unauthorized access or data breaches.

   Despite these limitations, the adoption of blockchain technology for secure medical data management represents a significant step towards mitigating the vulnerabilities inherent in traditional systems and safeguarding patient information against security threats and breaches. Ongoing research and development efforts aim to address these challenges and further optimize the effectiveness and efficiency of blockchain-based solutions in the healthcare domain.

3.2 PROPOSED SYSTEM

3.2.1 OVERVIEW

Taking all the disadvantages of the existing system into consideration, it is observed that blockchain technology can provide a lot of benefits. Blockchain technologyhas the capability to be safe from many cyberattacks and can work very efficiently even on a large scale. Here there is a web application which gives the basic interface for the users

to interact with the blockchain network. And the entire data which is generated everyday will be stored on the blockchain network in the form of blocks.

The end users for this application will be doctors and the patients. All the details of the patients will be stored in the blocks and newly generated blocks are added on the blockchain network. Here the doctor will be the only user who has the access to change the data which is entered in the network. And only doctors can add the details of the patient to the blockchain network. The application also uses smart contracts to execute the backend transactions.

Smart contracts are used to verify the users on the blockchain network. They verify the ownership of the users in the network in order give them the access to the usersto make necessary changes in the data. Smart contracts use the unique ids or hash value of every individual to verify their work in the blockchain network. In this way the proposed system provides a lot of security and is more advantageous than the existing system of maintaining the medical record

3.2.2 Secure Medical Data Management Using Blockchain

System design is the most crucial and significant component of any framework because it is used to create the system from its theory. The modules, architecture, and other components that make up the framework of the entire system are included in this section. As previously stated, the goal of this proposed architecture is to provide a decentralized, blockchain-basedsystem for electronic health records that is temper-proof, safe, and confidential.

The system design section of the proposed architecture for a decentralized, blockchain-based electronic health records (EHR) system is crucial for translating theoretical concepts into practical implementation. It outlines the modules, architecture, and other components required for the functioning of the entire system. This section delineates various modules such as user authentication, data encryption, smart contracts, data storage, consensus mechanisms, and user interface. It also elaborates on the architecture of the system, including network architecture, data flow architecture, scalability architecture, and integration architecture. Additionally, it identifies key components such as the blockchain platform, cryptographic tools, access control mechanisms, and audit trail

mechanisms. Overall, the system design serves as a blueprint for developing a robust, secure, and interoperable platform for managing electronic health records in a decentralized manner.

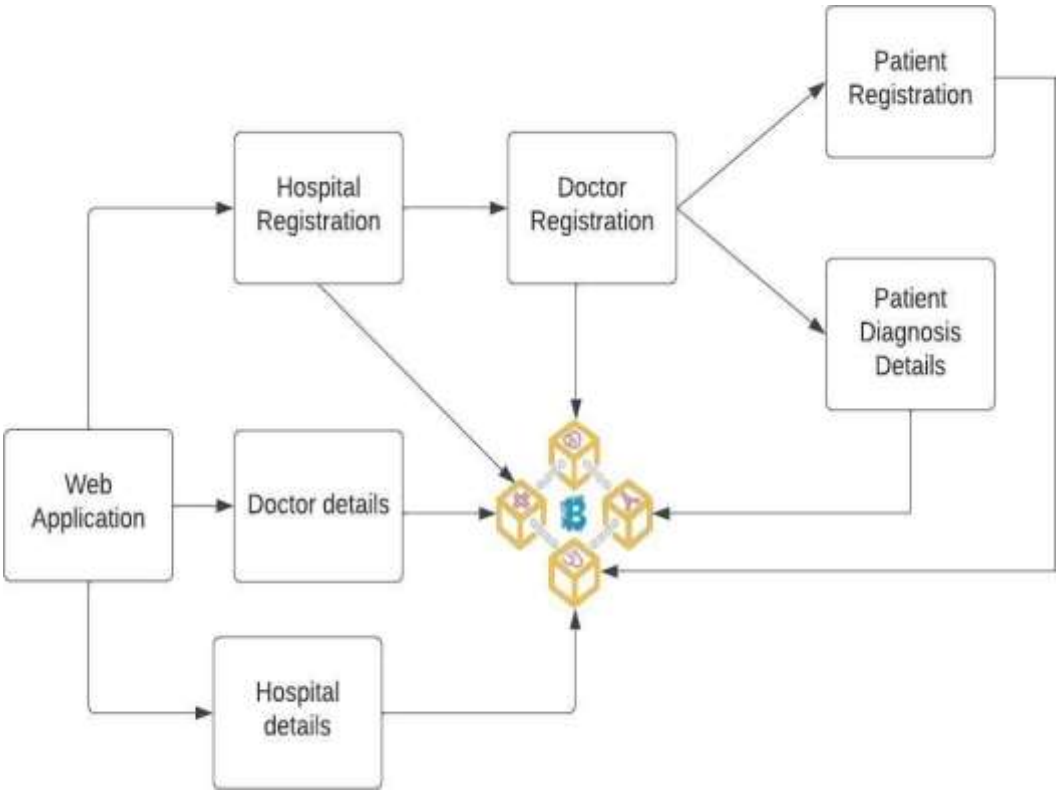

Fig 3.1 Proposed System model

The design of web application, which contains registration pages for hospitals, doctors, andpatients, is a crucial part of the system. The registration process allows each user to create aunique identity and securely store their data in a blockchain-based database. This providesa high level of security and ensures that sensitive medical data is protected from unauthorized access. To retrieve data from the system, users can search for specific blocks using a block number. Each block contains a unique set of data related to a specific user or transaction, making it easy to retrieve and verify information. This design approach ensuresthat the medical record management system is secure, transparent, and easily accessible to authorized users.

An important aspect of our project design is the use of unique IDs to access data. Each hospital, doctor, and patient registration page generates a unique ID that is associated withthe data they provide. This ensures that only authorized users can access their data and provides an additional layer of security to the system.

The unique IDs are used to authenticate users and grant them access to their specificdata. This means that hospitals can only access data related to their patients, doctors can only access data related to their appointments and treatments, and patients can only access their own medical records.

This approach helps to prevent unauthorized access to sensitive medical data, ensuring that only authorized users can view and modify it. It also simplifies the data retrieval process by allowing users to easily locate and access their data using their uniqueID.

Overall, the use of unique IDs in our project design is a crucial aspect of our secure medical record management system. It enhances security, improves data accessibility, andensures that only authorized users can access and modify sensitive medical information.

3.2.3 Applications of Secure Medical Data Management Using BlockChain

1. **Ensuring Patient Confidentiality with Blockchain**: Blockchain technology provides a secure and tamper-proof solution for storing patient medical records, safeguarding sensitive information through encryption and decentralized networks. Access is restricted to authorized individuals, ensuring patient data remains confidential and protected.
2. **Streamlining Healthcare Data Exchange**: Blockchain fosters seamless interoperability among healthcare providers and systems, facilitating secure and transparent sharing of medical records. This promotes continuity of care and reduces administrative burdens associated with disparate systems, enhancing overall efficiency.
3. **Accelerating Medical Research Through Secure Data Sharing**: Blockchain streamlines the process of medical research and clinical trials by securely storing and sharing patient data. Researchers can access anonymized data while upholding patient privacy, accelerating medical discoveries and drug development.

4. **Enhancing Transparency in Healthcare Supply Chains**: Blockchain technology enhances transparency and efficiency in healthcare supply chains by tracking the provenance of medical supplies and pharmaceuticals. This mitigates counterfeiting, ensures quality control, and improves patient safety.
5. **Optimizing Health Insurance Claims Processing**: Blockchain optimizes health insurance claims processing by securely recording and verifying transactions. Smart contracts automate claims processing, reducing fraud, administrative costs, and expediting reimbursement for healthcare providers.
6. **Empowering Telemedicine and Remote Monitoring**: Blockchain enables secure communication and data sharing in telemedicine and remote patient monitoring applications. Patients can securely share medical data with healthcare providers, enabling remote consultations and real-time monitoring of health metrics.
7. **Simplifying Medical Credentialing and Licensing**: Blockchain streamlines medical credentialing and licensing processes by securely verifying and storing practitioners' qualifications. Compliance with regulatory requirements is ensured, enhancing the integrity of healthcare provider networks.
8. **Personalized Healthcare Through Secure Data Management**: Blockchain facilitates secure storage and sharing of personalized health information, enabling tailored treatments based on individual patient profiles. This improves patient outcomes and reduces healthcare costs through precision medicine.
9. **Real-time Public Health Surveillance with Blockchain**: Blockchain technology facilitates real-time public health surveillance by securely aggregating and analyzing population health data. This enables healthcare authorities to monitor disease outbreaks, track epidemiological trends, and implement timely interventions to mitigate public health risks.
10. **Empowering Patients with Decentralized Medical Identity Management**: Blockchain offers a secure and decentralized solution for managing medical identities, reducing the risk of identity theft and fraud. Patients maintain control over their identities, while healthcare providers can efficiently verify patient information, enhancing safety and care delivery.

3.2.4 Advantages of Secure Medical Data Management Using BlockChain

1. **Enhanced Security**: Blockchain employs cryptographic techniques to ensure the security and integrity of medical records. Data stored on the blockchain is encrypted and tamper-proof, reducing the risk of unauthorized access, data breaches, and tampering.

2. **Decentralization**: Blockchain operates on a decentralized network, eliminating the need for a central authority to manage data. This reduces the risk of a single point of failure and enhances resilience against cyber attacks and system downtime.

3. **Transparency and Auditability**: Blockchain provides a transparent and auditable record of all transactions and data modifications. Each transaction is timestamped and appended to the blockchain, enabling stakeholders to trace the history of data access and modifications.

4. **Data Integrity**: The immutability of blockchain ensures the integrity of medical records. Once data is recorded on the blockchain, it cannot be altered or deleted without consensus from the network participants, maintaining the accuracy and reliability of medical information.
5. **Interoperability**: Blockchain facilitates seamless interoperability between different healthcare systems and providers. By standardizing data formats and protocols, blockchain enables secure and transparent data exchange, improving collaboration and continuity of care.

6. **Patient Empowerment**: Blockchain enables patients to have greater control over their medical data. Patients can securely access, manage, and share their health records with healthcare providers, enhancing patient autonomy and engagement in their healthcare decisions.

7. **Efficiency and Cost Reduction**: Blockchain streamlines administrative processes and reduces overhead costs associated with traditional data management systems. Smart contracts automate tasks such as claims processing and data verification, improving efficiency and reducing operational expenses.

8. **Improved Compliance**: Blockchain helps healthcare organizations comply with regulatory requirements such as HIPAA (Health Insurance Portability and Accountability

Act). The transparent and auditable nature of blockchain facilitates regulatory audits and ensures adherence to data privacy and security standards.

9. **Faster Access to Medical Records**: Blockchain enables healthcare providers to access patient medical records more quickly and efficiently. With permissioned access controls and secure authentication mechanisms, authorized users can retrieve relevant patient information in real-time, improving patient care and treatment outcomes.

10. **Facilitation of Research and Innovation**: Blockchain accelerates medical research and innovation by providing secure and transparent access to anonymized patient data. Researchers can analyze large datasets more effectively, leading to new discoveries, treatments, and advancements in healthcare.

11. **Immutable Data**: Blockchain's immutable ledger ensures that once data is recorded, it cannot be altered or tampered with, providing a reliable record of medical information.

Overall, the adoption of blockchain technology in secure medical record management offers numerous advantages, including enhanced security, transparency, efficiency, and patient empowerment, ultimately leading to improved healthcare outcomes and experiences.

CHAPTER 4

UML DIAGRAMS

UML stands for Unified Modelling Language. UML is a standardized general purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modelling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems. The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS: The Primary goals in the design of the UML are as follows:

- Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modelling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns, and components.
- Integrate best practices.

UML diagrams are designed to let developers and customers view a software system from a different perspective and in varying degrees of abstraction. UML diagrams commonly created in visual modelling tools include.

In its simplest form, a use case can be described as a specific way of using the system from a user's (actor's) perspective. A more detailed description might characterize a use case as:

1. A pattern of behaviour the system exhibits
2. A sequence of related transactions performed by an actor and the system
3. Delivering something of value to the actor

Use cases provide a means to:

1. Capture system requirements
2. Communicate with the end users and domain experts
3. Test the system

Use cases are best discovered by examining the actors and defining what the actor will be able to do with the system. Since all the needs of a system typically cannot be covered in one use case, it is usual to have a collection of use cases. Together this use case collection specifies all the ways of using the system.

A UML system is represented using five different views that describe the system from distinctly different perspective. Each view is defined by a set of diagrams, which is as follows:

User Model View: This view represents the system from the user's perspective. The analysis representation describes a usage scenario from the end-user's perspective.

Structural model view: In this model the data and functionality are arrived from inside the system. This model view models the static structures.

Behavioural Model View: It represents the dynamic of behavioural as parts of the system, depicting the interactions of collection between various structural elements described in the user model and structural model view.

Implementation Model View: In this the structural and behavioural as parts of the system are represented as they are to be built.

Environmental Model View: In this, the structural and behavioural aspects of the environment in which the system is to be implemented are represented.

4.1 CLASS DIAGRAM

A class diagram is a picture for describing generic descriptions of possible systems. Class diagrams and collaboration diagrams are alternate representations of object models. Class diagrams contain classes and object diagrams contain objects, but it is possible to mix classes and objects when dealing with various kinds of metadata, so the separation is not rigid.

Class diagrams are more prevalent than object diagrams. Normally you will build class diagrams plus occasional object diagrams illustrating complicated data structures or message passing structures. Class diagrams contain icons representing classes, interfaces, and their relationships. You can create one or more class diagrams to depict the classes at the top level of the current model; such class diagrams are themselves contained by the top level of the current model. We can also create one or more class diagrams to depict classes contained by each package in your model; such class diagrams are themselves contained by the package enclosing the classes they depict; the icons representing logical packages and classes in class diagrams.

We can change properties or relationships by editing the specification or modifying the icon on the diagram. The associated diagrams or specifications are automatically updated. During analysis class diagram show common roles and responsibilities of the entities that provide the System’s behaviour.

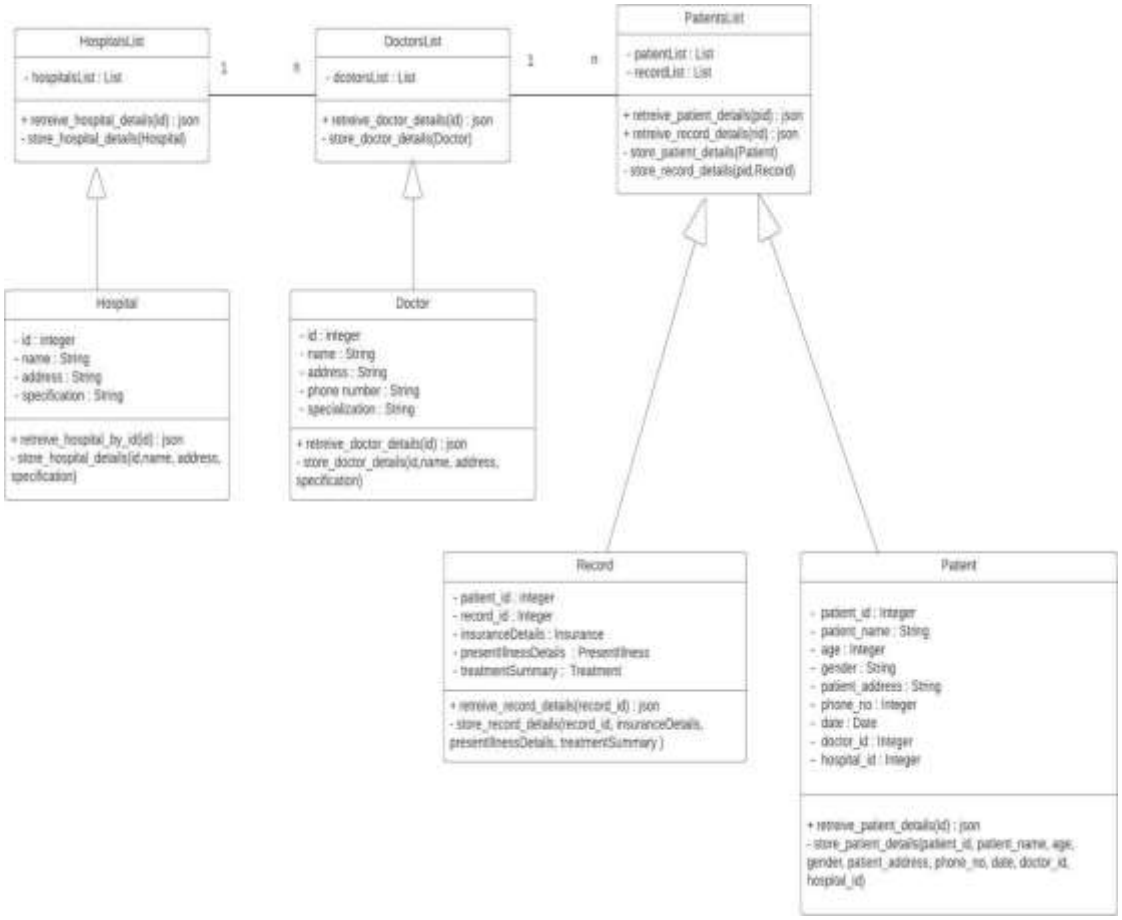

Fig 4.1.1 Class Diagram

4.2 USE CASE DIAGRAM

A use case diagram in the Unified Modelling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. Representing the goals of system-user interactions. Defining and organizing functional requirements in a system. Specifying the context and requirements of a system. Modelling the basic flow of events in a use case.

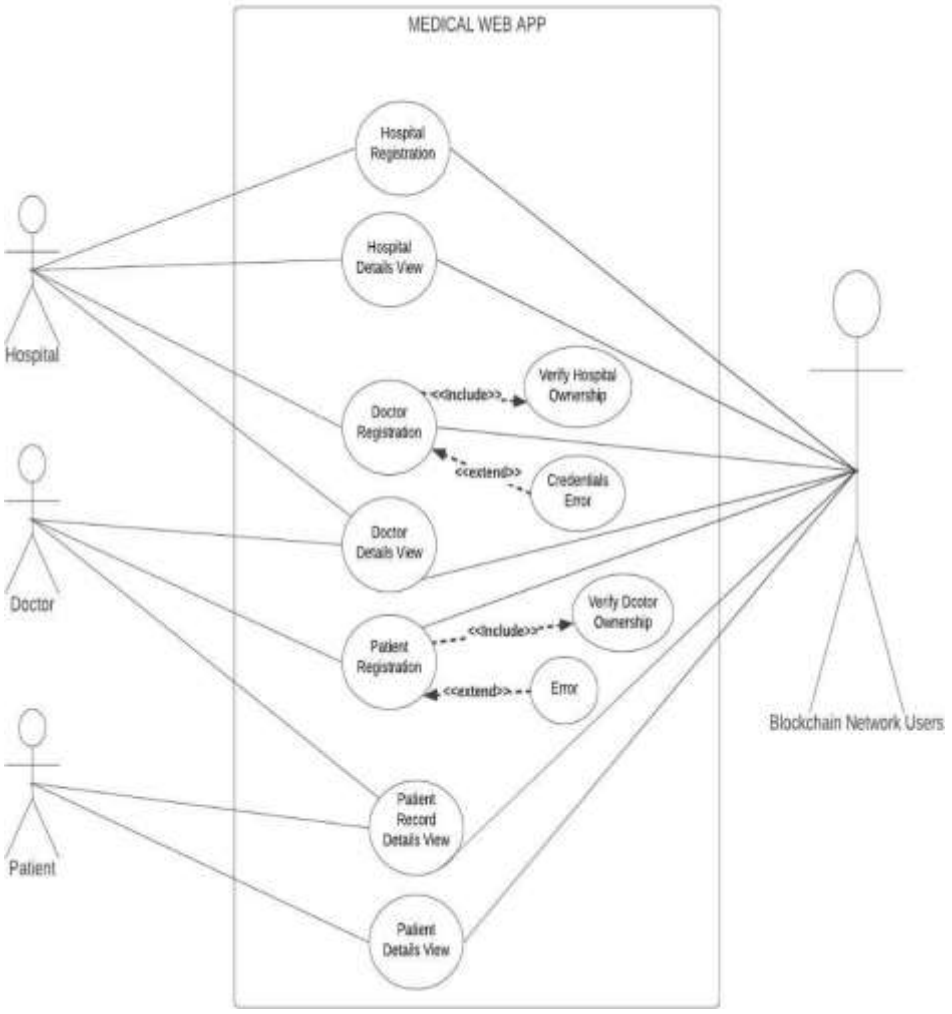

Fig 4.2.1 Use Case Diagram

4.3 SEQUENCE DIAGRAM

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages". Sequence diagrams are closely related to collaboration diagrams and both are alternate representations of an interaction. There are two main differences between sequence and collaboration diagrams: sequence diagrams show time-based object interaction while collaboration diagrams show how objects associate with each other. A sequence diagram has two dimensions: typically, vertical placement represents time and

horizontal placement represents different objects. The following tools located on the sequence diagram toolbox enable to model sequence diagrams:

• Object

• Message Icons

• Focus of Control

• Message to Self

• Note

• Note Anchor

• Life lines

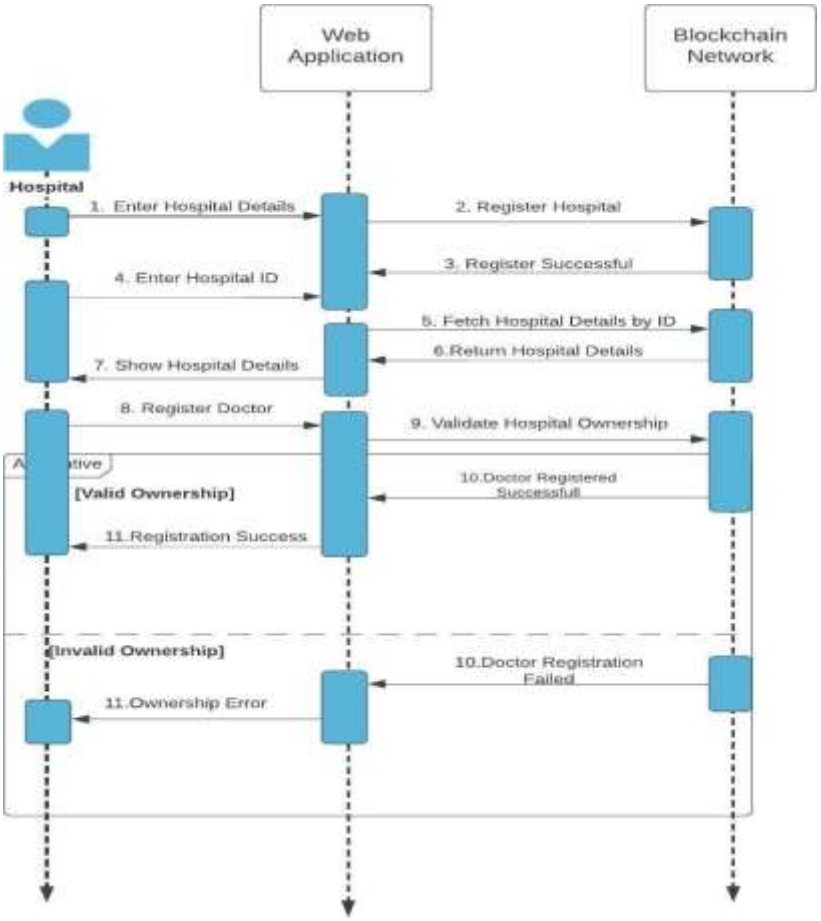

Fig 4.3.1 Hospital Sequence Diagram

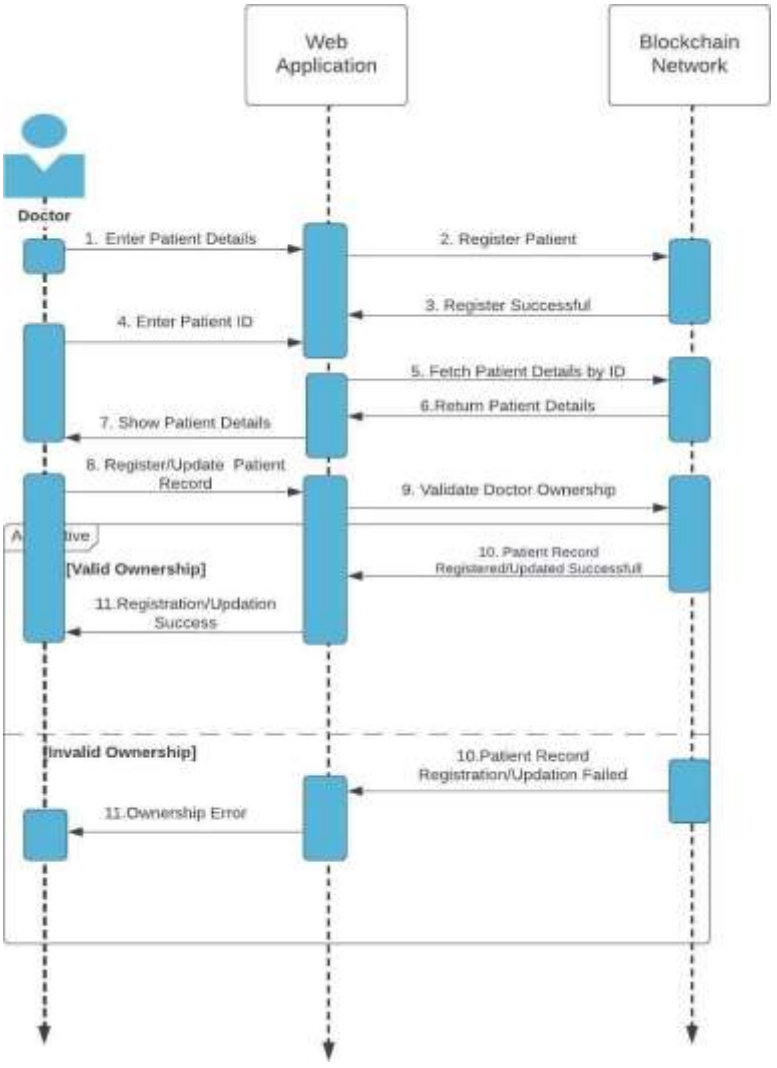

Fig 4.3.2 Doctor Sequence Diagram

4.4 ACTIVITY DIAGRAM

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions. An activity diagram shows the flow of control from activity to activity. An activity is an ongoing execution within a state machine. It is essentially a flowchart modelling the dynamic aspects of the system.

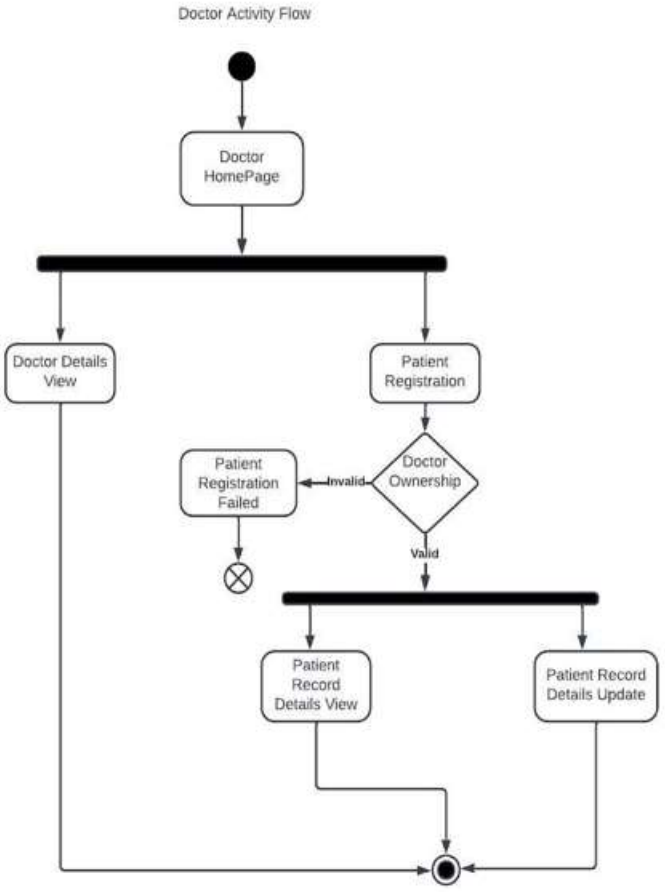

Fig 4.4.1 Doctor Activity Flow

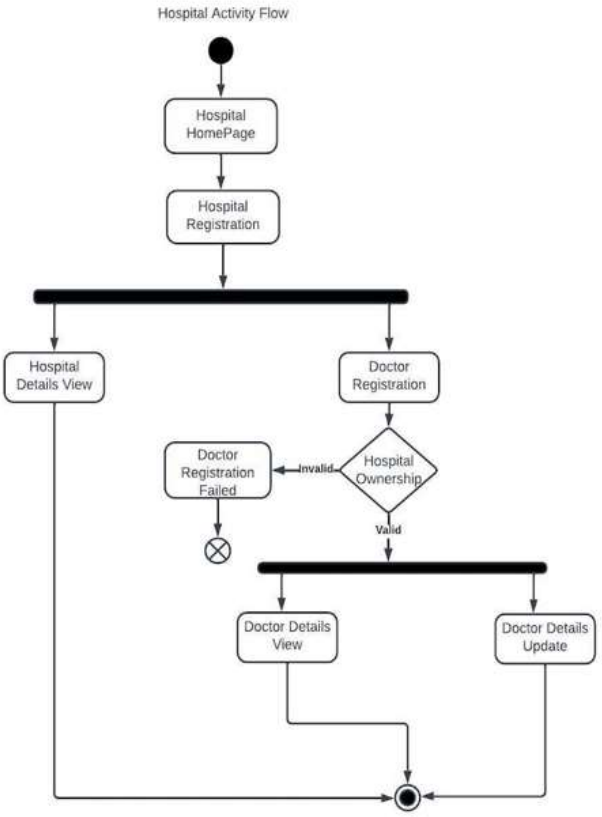

Fig 4.4.2 Hospital Activity Flow

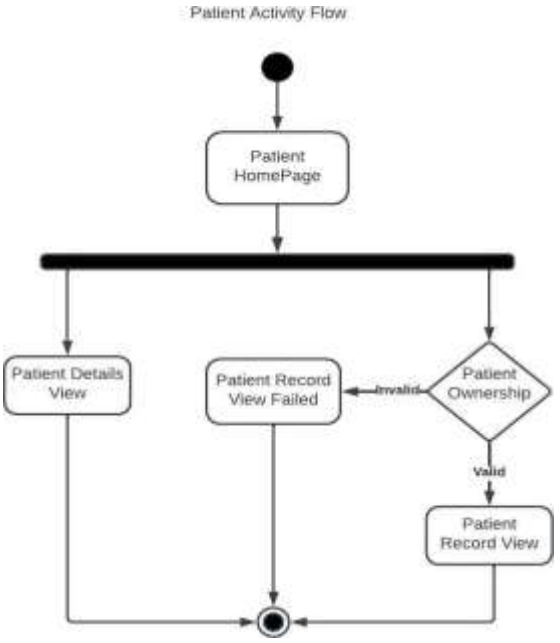

Fig 4.4.3 Patient Activity Flow

CHAPTER 5

IMPLEMENTATION

5.1 Modules

Medical record maintenance system using blockchain will have majorly three modules to work with. All these three modules are supposed to perform different tasks and would have a significance. The module of the application are:

1. Hospital module
2. Doctor Module
3. Patient Module

Module Description

Hospital Module:

The Hospital module is one of the basic modules that the medical record maintenance application has. This module maintains the basic details of the hospitalswhich are registered in the application. The hospital module takes the necessary details of the hospital while it is registering in the application. The details include thehospital name, contact no., address etc. Hospital is the only user who will be accessing this module, no other user other than hospitals can enter any details using this module but just can view the details of the hospitals which are already registered.

Doctor Module:

The doctor module is also an important module in the medical record maintenance system. This module allows the hospitals to register the doctors. The doctor module will ask the hospitals to enter the details of the doctor. The basic detailsof the doctor like his name, age, experience, specialization, qualifications and contactdetails etc. Hospitals only have the access to verify the details of the doctor and haveaccess to change any details of the doctor at any point of time. Doctors and other userscan view the details of the doctor but have no access to change the details of the doctor. Even while entering the details of the doctor, the ownership of the hospital isverified whether to know that the hospital has the authority to make modifications tothe details of the doctor.

Patient Module:

patient module is the final module in the medical record maintenance application in which more no of users will be interacting. Large no. of patients everydaywill be registered in this module. Doctor only has the access to add a patient and to makeany changes to the details of the patient. The details of the patients like their personal details, diagnosis details and the treatment details. All these details will be stored in the blockchain network in the form of the blocks. The patients can just view the details of their own, they don't even have the access to view the details of the other patients. Any doctor with the ID of the patient can view the details and make modifications to the detailsof the patients.

5.2 Introduction to the technologies used:

Solidity programming

Solidity programming is one the most widely used programming languages used to write smart contracts. Smart contracts are simply programs which are written and stored on a blockchain network and are executed when few preconditions are met. Thesesmart contracts are executed automatically when the conditions are met.

All the smart contracts are written in solidity programming language which is very similarto java. Solidity programming is an object oriented and high-level programming languageto write contracts. It is the programming language which is targeted to get executed on the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features. To write the solidity programs i.e. to develop smart contracts we use Remix IDE which is a free and open source solidity programs development tool.

Meta Mask

Mets mask is a google chrome extension which is used to create a few accounts. It also acts as a software cryptocurrency wallet to work with the Ethereum network. It allows the users to access their crypto wallets using the chrome extension or mobile app, which can be used to interact with the decentralized applications.

Meta mask will allow the users to maintain and manage the keys, broadcast transactions, send and receive Ethereum based cryptocurrencies and tokens. It also allows the

users to securely connect with the decentralized application in simple terms blockchain based application.

Ethereum blockchain network

Ethereum is one the most widely used blockchain networks. It is a decentralized network which has the concept of smart contracts. Ethereum allows anyone to deploy permanent and immutable decentralized applications onto it. Ethereum also allows the users to create and exchange the special tokens called as NFT's which are used to verify the ownership of any privileged and valid asset in the network.

Ethereum network uses a special cryptocurrency called Ether (ETH) which is given as an reward to the miners, who are responsible in making transactions successful by mining the blocks or simply transactions. It is the only cryptocurrency available on that network. Ethereum network also maintains a separate virtual machine called as Ethereum virtual machine (EVM) to execute the solidity programs to implement smart contracts. In this way Ethereum network works as a base network to work with the decentralized applications.

5.3 Process

Setting up the development environment: We had set up the development environment by installing and configuring the necessary software tools and infrastructure, such as Ganache, RemixIDE, Metamask, and a web development framework like Bootstrap. This allows us to create and test our web application locally.

Designing and deploying the smart contracts: We had designed and deployed the smart contracts for hospitals, doctors, and patients using Remix IDE. This involves writing the Solidity code for each contract, compiling it, and deploying it on the Ganache blockchain. When we deploythe smart contracts, they generate a contract address which is used to interact with the contracts from our web application.

Building the web application: We had used HTML, CSS, and javascript and web development framework such as bootstrap to create our web application. This includes creating the registrationpages for hospitals, doctors, and patients, and integrating them with the smart contracts on the Ganache blockchain. When users register on our web application, their data is stored in a new block on the Ganache blockchain.

Testing and debugging: we tested and debugged our web application to ensure that it functions correctly and securely. This includes testing different use cases and scenarios, identifying and fixing any bugs or errors, and conducting security testing to ensure that the system is secure.

Running the web application: Once our web application is built and tested, we run it on our localmachine web address. The web application is connected to our local Ganache blockchain, which allows us to interact with the smart contracts and retrieve data from the blocks.

Gas fees: Each transaction on the Ganache blockchain requires a certain amount of gas fee to be paid by the sender account. The gas fee is used to compensate the miners for processing the transaction

CHAPTER 6

SYSTEM REQUIREMENT AND SPECIFICATION

SPECIFICATIONS

Medical record maintenance application is intended to maintain the data of the patients that is generated every day in the medical field. Every-day there are many peoplewho get hospitalized and have to get treated. They approach various hospitals and doctorswill make the diagnosis and provide treatment to them. All these details will be basically stored on a hard disk or any third-party server traditionally. But all these methods are notvery efficient and have many drawbacks. Also, they are very prone to cyber-attacks. Taking all these into consideration the main purpose of this application is to provide security for the medical data of various patients.

Medical record maintenance application provides security to the patient's medicaldata and their personal details. This application uses blockchain technology which is ledger based, decentralized technology. Blockchain provides security to the data which isen-tered onto the blockchain network. Application also uses the smart contracts in the backend which are used to verify the ownership of the doctors and the patients. This method is used to verify the user whether the user is a valid user or not. Like this the application verifies all the users in the network and also keeps the data more secure. This is the main purpose of the application.

6.1HARDWARE REQUIREMENTS:

Processor: A multi-core processor with a clock speed of at least 2.5 GHz or higher wouldbe ideal for handling the computational load of blockchain transactions and data management.

Memory: A minimum of 8GB RAM is recommended to ensure smooth operation and efficient handling of large volumes of data.

Storage: A fast and reliable solid-state drive (SSD) with a capacity of at least 256 GB is recommended for storing the blockchain data and medical records.

Network Interface Card (NIC): A reliable network interface card with high bandwidth and low latency is essential to handle the traffic between the nodes in the blockchain network.

Graphics Card (GPU): A high-performance GPU is not necessary for this project, but it can be helpful for running simulations and mining cryptocurrency, if required.

Server Infrastructure: High-performance servers may be required to host the blockchain network nodes and store the encrypted medical data.These servers should have sufficient processing power, memory, and storage capacity to handle the computational requirements of blockchain transactions and data storage. Redundancy and fault-tolerance measures should be implemented to ensure continuous availability and data integrity.

Networking Equipment: Networking equipment, including routers, switches, and firewalls, are essential for facilitating communication between blockchain nodes and ensuring secure data transmission. High-speed internet connectivity with sufficient bandwidth is crucial for optimal performance and responsiveness of the application.

Other components: The project may require additional hardware components such as servers, routers, and switches depending on the complexity and scale of the network architecture.

Overall, the hardware requirements for this project would depend on the specific implementation and the number of users accessing the system. It's essential to ensure that the hardware is capable of handling the load and is scalable for future growth.

6.2 SOFTWARE REQUIREMENTS:

Backend:

Solidity programming (Smart Contracts)

Solidity programming is a high-level language used to write smart contracts,which are self-executing contracts that automatically enforce the rules and regulations of an agreement between two parties. Smart contracts are typically usedin blockchain networks, like Ethereum, to enable secure and transparent transactionswithout the need for intermediaries. Solidity is specifically designed for writing smart contracts and provides features like data structures, inheritance, and libraries for developers to build complex applications on the blockchain.

Meta Mask (Account)

Meta Mask is a cryptocurrency wallet and browser extension that enables users to securely manage their Ethereum accounts and interact with decentralized applications.

It provides a simple and intuitive user interface for sending and receiving Ether and other Ethereum-based tokens. Meta Mask also enables users to connect to decentralized applications directly from their browsers, simplifying the process of interacting with the Ethereum blockchain.

One of the key advantages of MetaMask is its ability to bridge the gap between traditional web browsing and blockchain technology. By serving as a gateway to the Ethereum blockchain, MetaMask empowers users to explore and participate in the growing ecosystem of decentralized finance (DeFi), non-fungible tokens (NFTs), decentralized exchanges (DEXs), and other innovative applications.

MetaMask also offers a range of features to enhance security and protect users' funds. It encrypts and stores private keys locally on users' devices, allowing them to retain full control over their assets. Additionally, MetaMask provides users with a seed phrase (mnemonic phrase) during setup, which serves as a backup in case of loss or device failure.

Ethereum blockchain network

The Ethereum blockchain network is a decentralized platform that enables the execution of smart contracts and the development of decentralized applications.It operates using a consensus mechanism called Proof-of-Work, which ensures thatthe network is secure and transparent. Ethereum is the second largest cryptocurrencyby market capitalization and is known for its programmability, allowing developersto build complex decentralized applications on top of its blockchain. Overall,Ethereum provides a decentralized infrastructure for building and executing trustlesstransactions and applications.

User Interface:

HTML

HTML (Hypertext Markup Language) is the standard markup language usedto create web pages. It provides a structure for web content by using tags to identifydifferent types of content, such as headings, paragraphs, and links.

CSS

CSS (Cascading Style Sheets) is a style sheet language used to define the presentation of web pages. It is used to define colors, fonts, layouts, and other visualaspects of a web page. CSS separates the presentation of a page from its content, allowing for easier maintenance and customization of web designs.

Java script

JavaScript is a programming language used to create interactive and dynamicweb pages. It can be used to add functionality to web pages, such as user input validation, animations, and dynamic content updates. JavaScript can also be used tocreate client-side and server-side web applications. It is a widely used language in web development due to its versatility and ease of use.

Bootstrap

Bootstrap is a popular front-end development framework used to create responsive and mobile-first web designs. It provides a collection of pre-designed components, such as buttons, forms, and navigation menus, that can be easily customized and incorporated into web pages. Bootstrap uses a grid system to createa flexible and responsive layout.

CHAPTER 7
FUNCTIONAL REQUIREMENTS

Functional requirements are essential specifications that define what a system should do, outlining its capabilities and behaviors.

7.1 Output Design

Outputs from computer systems are required primarily to communicate the results of processing to users. They are also used to provides a permanent copy of the results for later consultation. The various types of outputs in general are:

- External Outputs, whose destination is outside the organization.
- Internal Outputs whose destination is within organization, and they are the
- User's main interface with the computer.
- Operational outputs whose use is purely within the computer department.
- Interface outputs, which involve the user in communicating directly.
  Output Definition: The outputs should be defined in terms of the following points.
- Type of the output
- Content of the output
- Format of the output
- Location of the output
- Frequency of the output
- Volume of the output
- Sequence of the output

The system should generate clear and concise output, such as reports, notifications, and alerts, regarding security-related events, such as unauthorized access attempts or data breaches.

Output should be presented in a format that is easy to understand and actionable for system administrators and security personnel.

7.2 Input Design

Input design is a part of overall system design. The main objective during the input design is as given below:

- To produce a cost-effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that the input is acceptable and understood by the user.

Input Stages: The main input stages can be listed as below.

- Data recording
- Data transcription
- Data conversion
- Data verification
- Data control
- Data transmission
- Data validation
- Data correction

Input Types: It is necessary to determine the various types of inputs.

The system should validate all input data to ensure its integrity and prevent injection attacks, such as SQL injection or cross-site scripting (XSS).
Input forms should include validation checks to ensure that users provide accurate and valid information, such as usernames, passwords, and access permissions.

7.3 Error Detection and Avoidance:

At this stage care is to be taken to ensure that input data remains accurate form the stage at which it is recorded up to the stage in which the data is accepted by the system. This can be achieved only by means of careful control each time the data is handled.

Even though every effort is made to avoid the occurrence of errors, still a small proportion of errors is always likely to occur, these types of errors can be discovered by using validations to check the input data.

The design of error messages is an important part of the user interface design. As user is bound to commit some errors or other while designing a system the system should be designed to be helpful by providing the user with information regarding the error, he/she has committed. This application must be able to produce output at different modules for different inputs.

7.4 Data Validation

Procedures are designed to detect errors in data at a lower level of detail. Data validations have been included in the system in almost every area where there is a possibility for the user to commit errors. The system will not accept invalid data. Whenever an invalid data is keyed in, the system immediately prompts the user, and the user has to again key in the data and the system will accept the data only if the data is correct. Validations have been included where necessary.

The system is designed to be a user friendly one. In other words, the system has been designed to communicate effectively with the user. The system has been designed with popup menus.

7.5 User Interface Design

It is essential to consult the system users and discuss their needs while designing the user interface:

User Initiated Interfaces: User initiated interfaces fall into two approximate classes:

- Command driven interfaces: In this type of interface the user inputs commands or queries which are interpreted by the computer.
- Forms oriented interface: The user calls up an image of the form to his/her screen and fills in the form. The forms-oriented interface is chosen because it is the best choice.

The user interface should be intuitive and user-friendly, allowing healthcare professionals to easily navigate and interact with security features and controls.
Security-related features, such as access controls, encryption settings, and audit logs, should be prominently displayed and easily accessible within the interface.

7.6 Performance Requirements

Performance is measured in terms of the output provided by the application. Requirement specification plays an important part in the analysis of a system. Only when the requirement specifications are properly given, it is possible to design a system, which will fit into required environment. It rests largely in the part of the users of the existing system to give the requirement specifications because they are the people who finally use the system. This is because the requirements have to be known during the initial stages so that the system can be designed according to those requirements. It is very

difficult to change the system once it has been designed and on the other hand designing a system, which does not cater to the requirements of the user, is of no use.
The requirement specification for any system can be broadly stated as given below:

- The system should be able to interface with the existing system.
- The system should be accurate.
- The system should be better than the existing system.
- The existing system is completely dependent on the user to perform all the duties.

The system should be capable of handling concurrent website traffic and interactions from potential attackers without significant degradation in performance. It should ensure timely notifications to administrators upon the detection of suspicious activity, enabling rapid response and mitigation efforts.

CHAPTER 8

SOURCE CODE

8.1 Hospital Code

```
pragma solidity >=0.4.22 <0.7.0;

contract Hospital {

mapping(uint256 => hospital) hospitallist;

struct hospital{

string hospital_name;

string hospital_address;

string hospital_spec;

}

hospital h;

address owner;

constructor() public {

owner = msg.sender;

}

// modifier to give access only to hospitalmodifier isOwner() {

require(msg.sender == owner, "Access is not allowed");

}

function store_doctor_details(uint256 hospital_id,string memory _hospital_name,string memory _hospital_address,string memory _hospital_spec)public isOwner {

h.hospital_name = _hospital_name;

h.hospital_address = _hospital_address;

h.hospital_spec = _hospital_spec;

hospitallist[hospital_id] = h;

}function retreive_hospital_details(uint256 hospital_id) public view returns (string memory,string  memory,string memory)

hospital memory h = hospitallist[hospital_id]

return (h.hospital_name,h.hospital_address,h.hospital_spec);}}
```

8.2 Doctor Code

```
pragma solidity >=0.4.22<0.7.0;

contract Doctor {

mapping(uint256 => doctor) doctorlist;

struct doctor{

string doctor_name;

string doctor_specialisation;

uint256 doctor_ph_no;

stringdoctor_address;

}

doctor d; addressowner;

constructor() public {

owner = 0xE6005Cc724c2d44F0aF23d663017a7E375DD7F35; //AddressofHospital

}

// modifier to give access only to hospital

modifier isOwner() {

require(msg.sender == owner, "Access is not allowed");

_;

}

function store_doctor_details(uint16 doctor_id,string memory _doctor_name,string memory _doctor_specialisation,uint256 _doctor_ph_no,string memory

_doctor_address)public isOwner {

d.doctor_name = _doctor_name

d.doctor_specialisation = _doctor_specialisation;

 d.doctor_ph_no = _doctor_ph_no;

d.doctor_address = _doctor_address;

doctorlist[doctor_id] = d;

}

function retreive_doctor_details(uint16 doctor_id) public view returns (string memory, string memory,uint256,string memory){

doctor memory d = doctor list[doctor_id];
```

```
return (d.doctor_name,d.doctor_specialisation,d.doctor_ph_no,d.doctor_address);
}
```

8.3 Patient Code

```
pragma solidity >=0.4.22 <0.7.0;contract Patient {
mapping(uint256 => patient) patientlist; mapping(uint256 =>attendant) attendantlist;
struct  patient{
string patient_name;
uint256 age;
string gender;
string height;
uint256 weight;
string patient_address;
uint256 phone_no;
string email_id;
uint256 date;
uint256 doctor_id;
uint256 hospital_id;
}
patient p;
struct attendant{
 uint256 patient_id;
string attendant_name;
string attendant_relation;
uint256 attendant_phn_no;
}
attendant a;
address owner;
constructor()  public {
owner = 0xE6005Cc724c2d44F0aF23d663017a7E375DD7F35; //Address of Hospital
}
```

```
// modifier to give access only to hospital

modifier isOwner() {

require(msg.sender == owner, "Access is not allowed");

_;

}

functionstore_patient_details(uint256_patient_id,string_memory_patient_name,uint256_age,string_memory_gender,string_memory_height,uint256_weight,string_memory_patient_address,uint256_phone_no,string_memory_email_id,uint256 _date)public isOwner {p.patient_name=_patient_name;

p.age=_age;

 p.gender=_gender;

p.height=_height;

p.weight=_weight;

p.patient_address=_patient_address;

p.phone_no=_phone_no;

p.email_id=_email_id;

p.date=_date;

patientlist[patient_id] = p;

}

functionstore_attendant_details(uint256_patient_id,string_memory_attendant_name,string_memory_attendant_relation,uint256_attendant_phn_no)public isOwner {

a.patient_id = patient_id;

a.attendant_name=_attendant_name;

 a.attendant_relation=_attendant_relation;

a.attendant_phn_no=_attendant_phn_no;

attendantlist[patient_id] = a;

}

function retreive_patient_details(uint256 patient_id) public view returns (string memory,uint256,string memory,string memory,uint256,string memory,uint256,string memory,uint256){ patient memory p = patientlist[patient_id];

 return(p.patient_name,p.age,p.gender,p.height,p.weight,p.patient_address,p.phone_no,p.email_id,p.date);
```

```
}

function retreive_attendant_details(uint256 patient_id) public view returns (string memory,string memory,uint256){

attendant memory a = attendantlist[patient_id];

return (a.attendant_name,a.attendant_relation,a.attendant_phn_no);

}
```

CHAPTER 9

RESULTS AND ANALYSIS

9 ScreenShots

Fig 9.1 Home Page of Secure Medical Record Management Application

Fig 9.2 Admin Linux Home Page

Fig 9.3 Hospital Registration

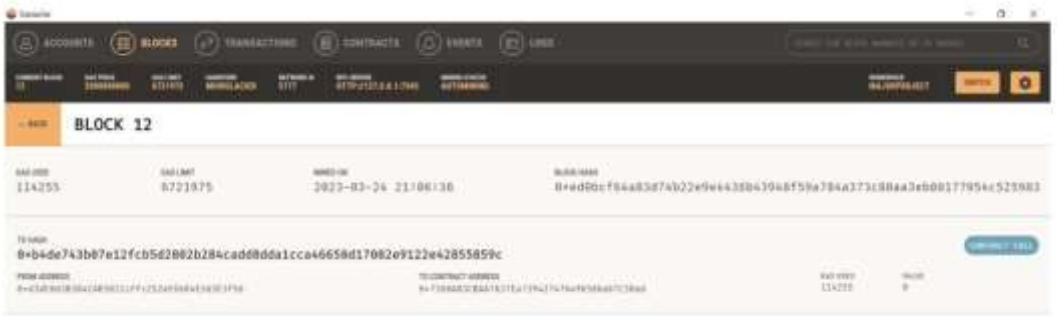

Fig 9.4 Block Added for Hospital Registered

Fig 9.5 Hospital Verification Page

Fig 9.6 Doctor Registration Page

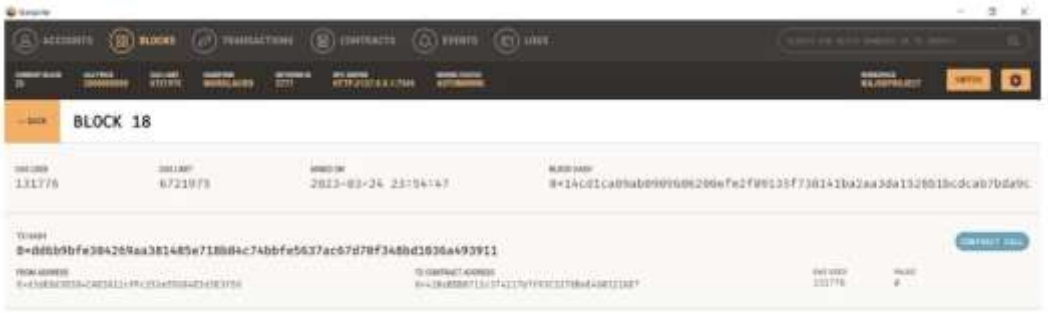

Fig 9.7 Block added for Doctor Registration

Fig 9.8 Doctor details verification page

Fig 9.9 Hospital Home Page

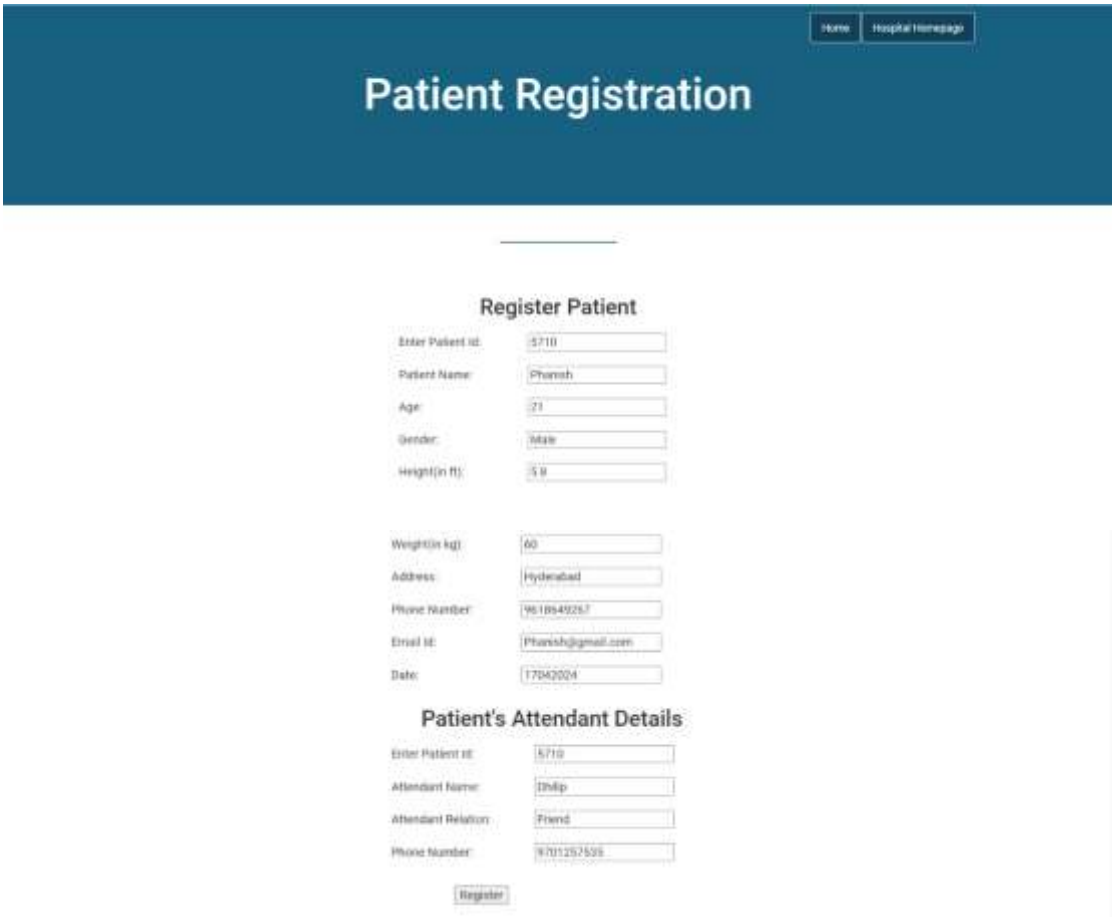

Fig 9.10 Patient Registration Page

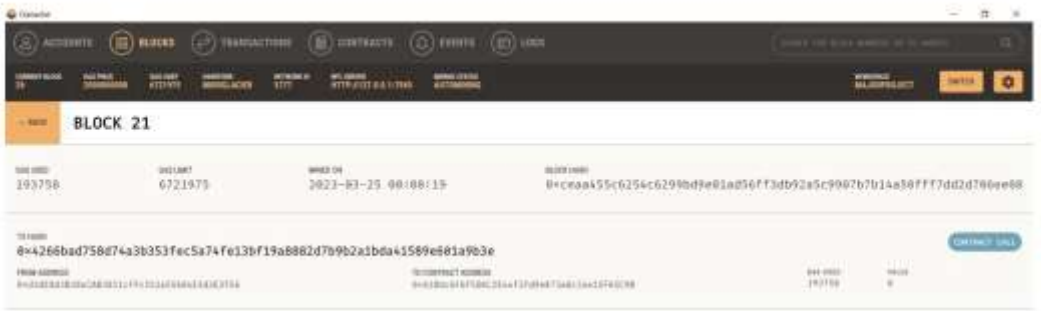

Fig 9.11 Block added upon patientregistration

Fig 9.12 Patient personal details page

CHAPTER 10
CONCLUSION AND FUTURE ENHANCEMENT

10.1 CONCLUSION

Medical record maintenance applications utilizing blockchain technology are poised to revolutionize healthcare data management, offering a multitude of benefits beyond security.

One notable advantage lies in the potential for interoperability and seamless data exchange. Blockchain's decentralized architecture enables disparate healthcare systems and providers to securely share medical records, fostering collaboration and continuity of care. By standardizing data formats and protocols, these applications break down silos and facilitate the exchange of information, ultimately enhancing patient outcomes and reducing redundant tests and procedures.

Moreover, blockchain-powered applications have the potential to streamline administrative processes and reduce healthcare costs. Smart contracts automate tasks such as insurance claims processing and billing, minimizing errors, fraud, and administrative overhead. This efficiency translates to cost savings for healthcare providers and insurers, allowing resources to be allocated more effectively to patient care.

Furthermore, these applications can empower patients by giving them greater control over their medical data. Through secure access controls and user-centric interfaces, patients can manage their health records, grant permissions to healthcare providers, and participate more actively in their healthcare decisions. This transparency and autonomy foster trust between patients and healthcare providers, ultimately leading to improved patient satisfaction and engagement.

Additionally, the use of blockchain technology in medical record maintenance opens up new opportunities for research and innovation. By securely sharing anonymized patient data, researchers can access larger datasets for analysis, leading to new insights and discoveries in healthcare. Furthermore, the ability to tokenize medical data through non-fungible tokens (NFTs) allows patients to monetize their health information ethically, contributing to the advancement of medical research while preserving privacy and consent.

Overall, medical record maintenance applications leveraging blockchain technology offer a holistic approach to healthcare data management, addressing security concerns while unlocking new possibilities for interoperability, efficiency, patient empowerment, and innovation. As these applications continue to evolve and mature, they have the potential to revolutionize the healthcare industry, driving improvements in patient care, outcomes, and experiences.

10.2 FUTURE SCOPE

As the landscape of healthcare data continues to evolve, the imperative for robust storage solutions becomes increasingly pronounced. The relentless influx of medical records, generated at an unprecedented pace, underscores the urgency of implementing scalable and resilient infrastructure to manage this deluge of information effectively. Traditional servers, constrained by finite storage capacities, struggle to keep pace with the exponential growth of medical data, necessitating innovative approaches to data management.

Enterprises in the healthcare sector are turning to private blockchain networks as a means of safeguarding the integrity and confidentiality of medical records. By leveraging the immutable and decentralized nature of blockchain technology, these networks offer unparalleled security and transparency in data storage and transmission. However, as these networks expand to accommodate larger datasets and higher transaction volumes, the limitations of conventional server infrastructure become increasingly apparent.

The scalability and storage challenges inherent in managing vast quantities of medical records underscore the need for a paradigm shift in data storage practices. Cloud technology emerges as a transformative solution, offering virtually limitless storage capacity and on-demand scalability to meet the dynamic needs of healthcare organizations. Cloud-based storage solutions empower healthcare providers to efficiently manage and store large volumes of medical data while minimizing the burden on internal IT infrastructure.

Moreover, cloud providers offer a comprehensive suite of services and tools designed to enhance data management, security, and accessibility. Advanced features such as

data encryption, automated backup, and disaster recovery mechanisms ensure the integrity and availability of medical records, even in the face of unforeseen events or cyber threats. Additionally, cloud-based analytics tools enable healthcare organizations to derive actionable insights from their data, driving improvements in patient care, clinical outcomes, and operational efficiency.

Transitioning to cloud-based storage represents a strategic investment in the future of healthcare data management. By leveraging the scalability, reliability, and flexibility of cloud infrastructure, healthcare organizations can unlock new opportunities for innovation, collaboration, and growth. Furthermore, cloud technology enables seamless integration with emerging technologies such as artificial intelligence and machine learning, empowering healthcare providers to deliver personalized and data-driven care to patients.

In conclusion, the adoption of cloud technology is essential for healthcare organizations seeking to navigate the complexities of managing and leveraging vast volumes of medical data. By embracing cloud-based storage solutions, healthcare providers can overcome the limitations of traditional server infrastructure and position themselves for success in an increasingly data-driven and interconnected healthcare landscape.

CHAPTER 11
REFERENCES

[1] Ayesha Shahnaz , Usman Qamar, and Ayesha Khalid "Using Blockchain for Electronic Health Records " , IEEE Access ,Oct, 2019.

[2] Mohammad Mouussa Madine, (Member, IEEE), Ammar Ayman Battah ,Ibbar Yaqoob, (Senior Member, IEEE), Khaled Salah, (Senior Member, IEEE),Raja Jayaraman . Yousuf AL-Hammadi , Sasa Pesic, and Samer Ellahham "Blockchain for Giving Patients Control Over Their Medical Records" , IEEE Access ,Oct, 2020.

[3] Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, Zhongdai Wu, “A blockchain-based secure storage scheme for medical information”, Cornell University.

[4] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund, "Blockchain Technology in Healthcare: A Systematic Review", MDPI, 2019.

[5] Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte ,"Health Record Management through Blockchain Technology" , IEEE Xplore , 2019.

[6] Gulara Muradova, Mehran Hematyar,"Protecting and securing medical records using blockchain technology", "Actual multidisciplinary scientific-practical problems of information security" V Republic Conference, November 29, 2019.

[7] Usman, M., & Qamar, U, Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. In 2019 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), ELSEVIER

[8] William J. Gordon, Christian Catalini "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", Computational and Structural Biotechnology Journal, June, 2018