SHSP: A Scalable Framework for Healthcare System using Polygon Blockchain

A DISSERTATION

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

MASTER OF TECHNOLOGY
IN
INFORMATION SYSTEMS

Submitted by

DIVYA KUNTAL

2K21/ISY/08

Under the supervision of

Prof. DINESH K VISHWAKARMA

Department of Information Technology
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

MAY, 2023

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, DIVYA KUNATL, Roll No - 2K21/ISY/08 students of M.Tech (Department of Information Technology), hereby declare that the project Dissertation titled "SHSP: A Scalable Frame- work for Healthcare System using Polygon Blockchain" which is submitted by me to the Department of Information Technology, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi   Divya Kuntal

Date: 30.05.2023

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "SHSP: A Scalable Framework for Healthcare System using Polygon Blockchain" which is submitted by Divya Kuntal, Roll No 2K21/ISY/08, Department of Information Technology, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi — Prof. DINESH K VISHWAKARMA

Date: 30.05.2023 — **SUPERVISOR**

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I wish to express my sincerest gratitude to Prof. DINESH K VISHWAKARMA for his continuous guidance and mentorship that he provided me during the project. He showed me the path to achieve my targets by explaining all the tasks to be done and explained to me the importance of this project as well as its industrial relevance. He was always ready to help me and clear my doubts regarding any hurdles in this project. Without his constant support and motivation, this project would not have been successful.

Place: Delhi Divya Kuntal

Date: 30.05.2023

Abstract

In the world of healthcare where we produce data every single time, data security, interoperability, and scalability are the challenges. Traditional healthcare systems more often struggle with these issues, resulting in data breaches, and patients having limited control over their own health data. To tackle these challenges, we propose an innovative framework(SHSP) A Scalable Framework for Healthcare System using Polygon Blockchain. that utilizes the Matic network a scalable layer 2 solution. Polygon offers fast and cost-effective transactions, making this suites for healthcare applications. In this paper, we propose a scalable framework that leverages the power of the Polygon blockchain to create a robust healthcare system. Our framework incorporates various components, including patient data management, interoperability and access control to build a secure and efficient healthcare ecosystem. Patient data management ensures that health records are securely stored on the blockchain while access control ensures that only authorized entities can access and update patient data. Smart contracts are utilized to enforce access control policies and automate healthcare processes, eliminating reliance on intermediaries and improving system efficiency. By leveraging the unique features of the Polygon blockchain, our framework offers a scalable and more secure solution for healthcare systems, enabling efficient data management, improved interoperability, and security.

Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

1.1 Background

Healthcare providers, administrators, and researchers increasingly rely on Electronic Health Records (EHRs), which are computerized compilations of healthcare operations and assessments. [1]. Structured and unstructured data are both present in electronic health records [2]. Diagnoses, medications, and test values are all examples of the types of structured data found in EHRs. However, examples of unstructured data include clinical documentation such as notes, and discharge summaries created by healthcare professionals. When doctors enter their notes on a patient's condition into an electronic health record (EHR), they do it in free text. Electronic health record (EHR) adoption has skyrocketed in recent years. It has risen drastically in the US, going from 10% to almost 96% in just ten years. The sum is up by well over 85 percent [3]. The same pattern holds true for Australia's GP offices, major hospitals, and medical service providers [4,5]. The widespread use of EHRs has resulted in a data volume large enough to be classified as "Big Data," which includes the processing and use of the vast amounts of information stored in EHRs. There is a need to invent technological devices that can organize, evaluate, and recognize patterns within this information because the ability of the human intellect to analyze, understand, and interpret information is limited. The next phase in creating an EHR ecosystem is to conduct an analysis of data on EHRs big data, which includes the implementation of information mining and processing of natural language techniques. To deal with the explosion of free-form text in the medical field, researchers have turned increasingly to cutting-edge Machine Learning (ML) methods [6,7]. Many medical and healthcare contexts [8] include the diagnosis of heart disease and other cardiovascular issues [9]. Blockchain is an exciting new technology with the potential to revolutionize healthcare data administration by enabling greater data efficiency and ensuring trust [10-15]. Decentralized storage, transparency, data integrity, verification, data access flexibility, connectivity, and security are remarkable and built-in properties that allow BT to employ extensively in the healthcare industry [16-17]. Electronic health records (EHRs) could play a vital role in modern healthcare system , with an increase in data According to a study, it has been predicted that by 2020, the volume of unstructured medical data was double in just 73 days. Unstructured data, which includes things like clinical reports, free-text documents, and medical notes, refers to information that doesn't have a set format or organization. This type of data accounts for approximately 80% of the total healthcare data, making it challenging to effectively analyze and extract valuable insights [18]. However, managing EHRs can be complex, especially in large healthcare organizations with multiple stakeholders. Blockchain technology (BT) offers a promising solution, providing a secure and decentralized approach for transferring medical data [19]. In this paper, we propose a framework called SHSP (Scalable Healthcare System using Polygon Blockchain) for a blockchain-based EHR management system. SHSP aims to enhance the scalability, efficiency, security, and interoperability of EHRs in large healthcare organizations. By leveraging the distributed nature of blockchain and consensus algorithms, SHSP efficiently handles a large volume of EHRs while ensuring security through cryptographic techniques. We use a popular blockchain framework which is Matic network to create a secure network that enables seamless sharing of patient data among different providers and systems. We also discuss technical issues related to blockchain-based EHR administration. SHSP offers as an example of how BT may change EHR administration and draws attention to the possibility for more developments in this field.

1.2 Problem Statement

The healthcare industry is facing numerous challenges that hinder the smooth exchange of information, compromise patient care, and impede efficient healthcare management. These challenges include problems with managing data in a fragmented way, difficulties in achieving interoperability among various stakeholders, and concerns about the security and privacy of patient information Traditional healthcare institutions are finding it difficult to deal with these problems, which has led to inefficiencies, data breaches, and subpar patient outcomes. industry's current solutions frequently aren't scalable, affordable, or capable of handling the expanding volume of healthcare data. As healthcare organizations strive to adapt to technological advancements and embrace digital transformation, there is an urgent need for an innovative solution that can overcome the limitations of traditional systems and provide a scalable framework to improve healthcare operations, data management, and patient care. Blockchain technology emerges as a promising solution with the potential to revolutionize the healthcare industry. Blockchain can successfully address the issues facing healthcare systems by providing decentralized, transparent, and secure data management capabilities. There aren't many comprehensive frameworks that are particularly suited to the business. The potential of certain blockchain platforms, like the Polygon blockchain, for healthcare applications, must be thoroughly investigated and assessed because there are several alternative blockchain platforms, including Ethereum and Hyperledger, each having its own advantages and disadvantages. As a result, the major objective of this thesis is to design and create a scalable framework that responds to the problems of fragmented data management, restricted interoperability, and data security issues.

1.3 Thesis Motivation

Healthcare systems must be secure, efficient, and scalable since patient data is growing more and more quickly. Blockchain technology has shown promise in terms of transparency, immutability, and decentralized data management, and it has become a potential solution to the issues that traditional healthcare systems face. However, scale issues with current blockchain technology typically prevent their widespread implementation in the healthcare sector. The necessity to provide a scalable architecture for healthcare systems that make use of the Polygon blockchain is what spurred the creation of this thesis. Polygon is a Layer 2 scaling solution developed on the Ethereum network. Polygon is a great option for creating scalable healthcare applications because of its fast throughput, cheap transaction costs, and compatibility. The main goal of this thesis is to create a strong framework that can successfully fulfill the scalability needs of healthcare systems by using the distinctive features and capabilities of Polygon. In addition, the framework needs to expressly address the requirements of healthcare organizations, practitioners, and patients in order to guarantee data protection, integrity, and accessibility. This framework will help change the healthcare environment by improving interoperability, medical data management efficiency, and overall healthcare service delivery. The ultimate goal of this research is to advance the healthcare systems by providing a comprehensive solution that combines the benefits of blockchain technology, specifically the Polygon blockchain, with the scalability requirements of the healthcare industry. By creating a robust and efficient framework, this research strives to revolutionize healthcare data management, improve patient care, and foster innovation within the healthcare ecosystem. In summary, this thesis addresses the pressing need for scalable healthcare systems by proposing a framework that leverages the unique capabilities of the Polygon blockchain. This project intends to provide a strong solution that unleashes the full potential of decentralized and secure healthcare systems by fusing blockchain technology with healthcare requirements. By encouraging openness, efficiency, and better healthcare outcomes, the suggested paradigm will ultimately be advantageous to healthcare practitioners, providers, and most crucially, patients for handling their data.

1.4 Overview of Blockchain Technology

Blockchain, a distributed and decentralized digital ledger technology, has the potential to completely change a variety of sectors throughout the world. Blockchain was initially developed as the underpinning technology for virtual currencies like Bitcoin, but it now has a wide range of uses that provide new prospects for efficiency, security, and transparency across many industries. BT is used to create a distributed digital ledger that cannot be altered. BT will provide a secure, transparent, and decentralized platform for storing and exchanging important data and value without the need for intermediaries. This innovative technology ensures the integrity and confidentiality of data through cryptographic techniques and consensus algorithms. It offers a reliable and trustworthy means of data exchange, promoting trust and accountability in various industries. Additionally, the decentralized nature of blockchain eliminates the reliance on intermediaries, reducing costs, enhancing efficiency, and promoting transparency in transactions and data exchanges [20]. Every node in the system maintains a copy of the ledger and uses consensus techniques to confirm transactions. The system runs on a distributed network of nodes. A permanent and immutable record of all transactions is created by recording transactions in blocks and adding those blocks to a chain of prior blocks. BT has potential uses in many other industries, including finance, supply chain management, and healthcare, while being predominantly identified with cryptocurrencies like Bitcoin. The distributed and decentralized nature of BT, together with the usage of cryptographic methods, all contribute to its security [22]. These are a few significant methods that BT provides security:

- Decentralization: Because blockchain is intended to be decentralized, no single party has complete control over the network. that's why it is challenging for a single entity to alter the records or influence the network.
- Consensus Processes: For validating transactions and protect the integrity of the ledger, blockchain depends on consensus mechanisms. It is difficult for anyone node to make unauthorized changes due to these procedures, this will guarantee that all nodes in the network concur on the ledger's current state.

• Cryptography: Blockchain secures transactions and restricts illegal access to the data by implementing a variety of cryptographic techniques, such as hashing and digital signature.
• Immutability: when any transaction is done on the blockchain and then added to the blockchain it becomes immutable. This means that the data cannot be altered or erased, ensuring its integrity and authenticity. The blockchain acts as a permanent record that cannot be changed, providing a robust and secure system for data storage and exchange. This unique feature of blockchain guarantees the immutability and tamper-proof integrity of data.

Although it has enormous promise, blockchain technology still has problems. Among the problems that need more study and development are scalability, energy use, regulatory frameworks, and interoperability. Nevertheless, continuous developments and alliances in the blockchain industry are resolving these issues and spurring innovation. Blockchain technology has been a disruptive factor in several sectors, providing efficiency, security, and transparency. Because of its decentralized structure, transparency, and cryptographic security, transactions may be trusted and middlemen are not required. Blockchain technology has the ability to transform conventional processes and improve the way we do business, interact, and share information. Applications range from supply chain management to healthcare and banking. We may anticipate fresh developments as blockchain research and development proceed in order to fully realize its promise and usher in a new era of decentralized and trustless systems. Blockchain, the technology that powers cryptocurrencies like Bitcoin, has drawn a lot of interest due to its potential to alter established institutions and businesses. Explore the core ideas and elements that give blockchain its strength and innovation as a decentralised ledger system in order to fully grasp its potential and consequences. Blockchain, at its heart, is a distributed ledger that keeps an ever-expanding collection of information called blocks. A chain-like structure is created by each block, which consists of a series of transactions or data that are cryptographically connected to the one before it. This cryptographic linking, achieved through hash functions, ensures the immutability and integrity of the data stored in the blockchain. Decentralization lies at the heart of blockchain technology. Blockchain is an alternative to centralised systems, where data and transactions are controlled by a single entity. Blockchain relies on a network of participants, known as nodes, to jointly maintain and validate the ledger. In addition to doing away with the need for middlemen, this decentralized design improves security and resilience by removing single points of failure and decreasing the possibility of fraud or manipulation. Consensus processes inside a blockchain network are crucial for maintaining transaction consistency and agreement. Different consensus techniques, including proof-of-work (PoW), proof-of-stake (PoS), and delegated proof-of-stake (DPoS), make sure that network users agree on the legitimacy and chronological sequence of transactions. To participate in the consensus process for any of these algorithms, individuals must donate computer resources, stake their tokens, or allocate their voting power. Depending on the chosen consensus method, adding new blocks to the blockchain either entails mining or validation. In PoW-based blockchains, miners compete to find solutions to challenging mathematical problems. The winner receives a newly created Bitcoin and the right to add the next block.

1.4.1 Types of Blockchain

Different network types that use blockchain technology are included; each has unique properties and degrees of accessibility. Let's examine the three most common types: consortium blockchain , private blockchain, and public blockchain.

Public Blockchain (Permissionless): A public blockchain, commonly referred to as a permissionless blockchain, is a network that is accessible to everyone. Due to the decentralized nature of its operation, any user is free to sign up, verify transactions, and add new blocks. Bitcoin is among the most well-known instances of a public blockchain.

Consortium Blockchain (Public Permissioned): Public permissioned blockchains, also known as consortium blockchains, operate on a hybrid format that combines features from both public and private blockchains. A small number of nodes or participants are allowed to join and participate to the consensus mechanism in a consortium blockchain. Blockchain consortiums are frequently created within a given sector or when several firms work together on a particular use case. They provide some decentralisation while retaining some central control in the early stages. In contrast to public blockchains, consortium blockchains often include known and pre-selected participants, allowing for speedier consensus and better scalability.

Private Blockchain: The most regulated kind of blockchain network is a private one. When access to the blockchain is restricted to a particular business or a small group, they are frequently used inside those confines. Private blockchains demand specific permission to join the network, in contrast to public blockchains, which are accessible to everyone. Private blockchains provide more privacy and control. Which nodes may process transactions, carry out smart contracts, or function as miners depends on the network's governance. With a permissioned system, access to and participation in the blockchain may be more tightly regulated. As a result, compared to public blockchains, private blockchains can offer improved scalability and quicker transaction processing.

1.5 Blockchain Architecture

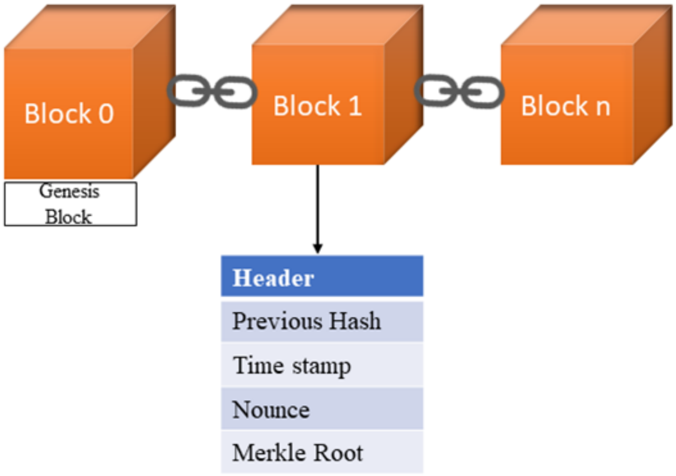


Figure 1.1: Blockchain Architecture With Genesis Block

Elements, nodes, and consensus methods are the three basic building blocks of the blockchain architecture. Each element is essential to maintaining the blockchain's stability and integrity.

Blocks: A blockchain is made up of blocks, each of which contains a list of transactions or other information. Cryptographic hashes are used to bind these blocks together in time. Each block's hash is calculated using its own data as well as the hash of the one before it. The term ”blockchain” refers to the continuous chain of blocks created by this connecting technique. The architecture makes the blockchain tamper-evident and unchangeable by guaranteeing that any change to one block renders all future blocks invalid.

Nodes: The members of the blockchain network called nodes are in charge of upholding and verifying the reliability of the blockchain. Due to the fact that every node has a copy of the full blockchain, it is decentralized and robust. There are two sorts of nodes: complete nodes and lightweight nodes. Lightweight nodes rely on full nodes for transaction verification, whereas full nodes hold the whole blockchain and take part in validation. Nodes are decentralized, which increases security and prevents illegal tampering by guaranteeing that no single party has total authority over the blockchain.

Consensus Mechanisms: Consensus techniques are essential for guaranteeing that the legitimacy and chronological sequence of transactions are agreed upon by each node in the network. These procedures support decentralized decision-making and safeguard the blockchain's reliability. There are several consensus algorithms, each with a different strategy. Proof-of-work (PoW) is the most well-known consensus process, in which nodes compete to solve challenging mathematical problems. The first node to solve the puzzle receives a payment and is designated as the block validator. Proof-of-stake (PoS), which selects validators based on their stake or ownership of a specific amount of cryptocurrency tokens, is another well-known consensus mechanism. Consensus mechanisms make sure that only legitimate transactions are recorded on the blockchain and stop bad behavior like double-spending or fraudulent transactions.

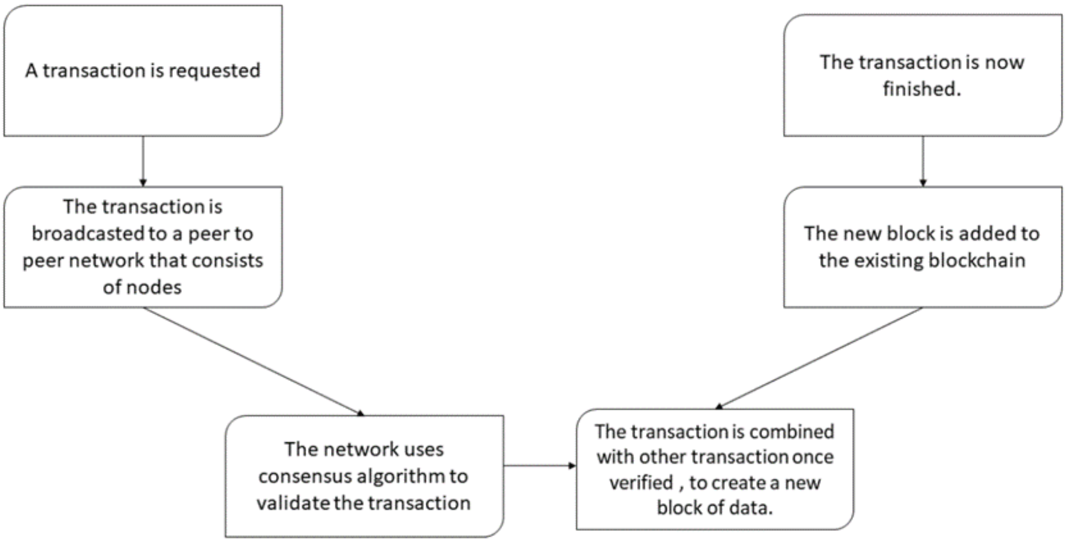

A transaction is requested
The transaction is broadcasted to a peer to peer network that consists of nodes
The network uses consensus algorithm to validate the transaction
The transaction is combined with other transaction once verified , to create a new block of data.
The new block is added to the existing blockchain
The transaction is now finished.

Figure 1.2: How Blockchain Technology Works

In conclusion, blockchain technology's underlying decentralized and secure ledger system is known as blockchain architecture. It is made up of blocks, nodes, and consensus processes that work together to provide a reliable, efficient, and transparent system for storing and confirming transactions. Blockchain architecture has the potential to transform businesses throughout the world by opening up new opportunities for secure and effective digital transactions thanks to its inherent advantages of transparency, security, and trust.

1.6 Healthcare System Limitations

Traditional healthcare systems face several limitations that can impact their effectiveness in delivering optimal care. Some of these limitations include:

1 Lack of Real-time Data: Traditional systems often rely on paper-based records or outdated electronic health record (EHR) systems that may not provide immediate access to patient information. This delay in accessing crucial data can lead to delayed decision-making and potentially compromise patient care, particularly in urgent situations.

2 Centralized Data Storage: Patient data in traditional systems is typically stored in centralized databases managed by healthcare organizations. This centralized approach creates a single point of failure and increases the risk of security breaches and data loss. Additionally, patients have limited control over their own data, reducing their ability to manage and share it as needed.

3 Limited Patient Engagement: Traditional systems often offer limited avenues for patients to actively participate in their healthcare. Access to personal health records may be restricted, making it challenging for patients to take an active role in their own care management. This limitation can hinder shared decision-making, patient education, and self-care practices.

4 High Costs: Implementing and maintaining traditional healthcare systems can be expensive. The infrastructure required, including hardware, software licenses, and ongoing maintenance, can incur significant costs. Furthermore, integrating different systems and ensuring interoperability can further contribute to high implementation expenses.

5 Interoperability Challenges: Seamless data exchange and integration between different healthcare systems is a complex challenge in traditional setups. The lack of standardized data formats and protocols makes it difficult to share patient information across different providers and systems.

This fragmentation hampers care coordination and continuity, affecting the overall quality of healthcare.

6 Limited Scalability: Traditional systems may struggle to scale effectively as healthcare demands and data volumes increase. Expanding existing infrastructure to accommodate growing needs can be a complex and costly endeavor, posing challenges in providing efficient and accessible healthcare services.

7 Regulatory and Privacy Concerns: Compliance with regulations and privacy requirements, such as HIPAA, adds complexity to traditional healthcare systems. Ensuring adherence to these regulations while enabling data sharing and protecting patient privacy can be a delicate balance.

Overcoming these limitations requires innovative approaches and technologies, such as blockchain, to address the inherent challenges of traditional healthcare systems. By leveraging these advancements, healthcare organizations can enhance the quality of care, improve data accessibility and security, and empower patients to actively participate in their own healthcare journey.

1.7 Healthcare System Challenges

1 Fragmented Data Management: Patient information is often scattered across different systems or databases, making it difficult to access and integrate. This fragmentation can lead to incomplete or inaccurate medical records, causing delays or errors in diagnosis and treatment.

2 Limited Interoperability: Healthcare systems struggle to seamlessly exchange patient data between different providers and organizations. This lack of interoperability hampers care coordination and results in gaps in patient care, as crucial information may not be readily available when needed.

3 Security and Privacy Concerns: Safeguarding patient information is critical, but traditional systems face challenges in ensuring data security and privacy. Breaches and unauthorized access to patient records can have severe consequences, including identity theft and compromised patient confidentiality.

4 Inefficiencies in Administrative Processes: Administrative tasks in healthcare, such as appointment scheduling and billing, often rely on manual and paper-based workflows.

5 Lack of Scalability: As the healthcare industry grows and generates an increasing volume of data, traditional systems may struggle to scale effectively. The existing System not have the capacity to handle the growing demands.

Addressing these challenges is crucial for improving the healthcare system and enhancing patient care. By leveraging innovative technologies like the Polygon blockchain, it becomes possible to develop a scalable framework that tackles these challenges head-on. This framework can offer secure data management, promote interoperability among healthcare stakeholders, streamline administrative processes, and ultimately contribute to better healthcare outcomes.

1.8 Application of Blockchain In healthcare

By tackling important issues like data security, interoperability, and patient privacy, blockchain technology has the potential to transform the healthcare sector. Healthcare firms may increase data sharing, streamline processes, and improve patient outcomes by utilising the special capabilities of blockchain. Let's look at some blockchain uses in the healthcare sector.

- EHRs

A secure, decentralized, platform for storing and exchanging electronic health records (EHRs) will be managed with the help of BT[22-23], which significantly improves patient privacy, data security, and healthcare provider access to medical records. Patients can retain ownership of their health data and see who has access to it by using BT to store EHRs in a secure ledger that is immune to hacking and gives proof of changes that are ever made on the system and have every record of it. With minimized chances of data theft and data breaches, patient privacy will surely increase. and also in comparison to traditional centralized databases, blockchain's distributed and decentralized design will provide a greater enhancement of security and reliability, reducing the likelihood of data loss or corruption. Finally, BT will make it easy for healthcare service providers to share medical records which would improve the efficiency and quality of whole healthcare System [24]. The potential advantages of blockchain in EHR administration are enormous and need additional investigation. Despite the difficulties and restrictions that currently stand in the way of the broad deployment of blockchain in healthcare, such as legal issues and technological constraints[25].

- Supply Chain Management

BT can give a safe and transparent way to track pharmaceutical products through the supply chain ensuring their authenticity and safety. Pharmaceutical firms would make an irreversible record of a product's route from the maker to the end consumer by employing BT solutions. This will have details such as the product's origin, production and expiration dates, and transportation and storage conditions. Due to the tamper-evident and tamper-resistant features of the blockchain, any attempts to alter or hack the data stored on the blockchain can be quickly and effectively addressed which will add an additional degree of security and confidence to this supply chain system. In addition, the use case of blockchain can also facilitate the identification and resolution of any supply chain issues or potential counterfeit products, ultimately improving patient safety and reducing healthcare costs. The MediLedger Project and the PharmaLedger Project are two examples of the numerous initiatives and pilot projects that have been started to integrate blockchain into the pharmaceutical supply chain. These initiatives want to explore the capabilities and benefits of blockchain in ensuring the authenticity and safety of pharmaceutical products and could have the way for wider adoption of blockchain in healthcare management.

- Clinical Trials

Clinical trial data and outcomes may be shared on a safe, decentralized platform using BT, increasing efficiency and transparency. The use case of blockchain can enable the secure and transparent sharing of data and results from clinical trials among different stakeholders, including researchers, regulators, and patients. By producing a clinical trial data record that is both immutable and tamper-evident, blockchain can help to prevent fraud and make sure to have the integrity of clinical trial results. And also Blockchain can also speed up data interchange and simplify the clinical trial process, which will ultimately result in more rapid and accurate drug development. even though we have the potential benefits of blockchain in clinical trials, there are still so many challenges to overcome, including regulatory, scalability data standardization, and the need for interoperability with existing systems[26].

- Public Health Management

BT offers a safe and decentralized platform for recording and exchanging health data, which has the potential to improve public health management. Blockchain's tamper-evident and decentralized nature can ensure the privacy and ethics of sensitive health data while enabling secure sharing between different stakeholders[27]. By giving decision-makers more precise and timely data, can increase the efficacy of public health initiatives and policies. Additionally, blockchain can facilitate more efficient and secure management of vaccine supply chains, reducing the risk of counterfeit or substandard vaccines.

- Claims and Billing Management

BT has the ability to improve the efficiency and accuracy of claims and billing management in healthcare by automating processes and reducing the need for intermediaries. By the help of BT, claims will be processed instantly and payments can be made in real time. This can result in cost savings and better transparency for both providers and patients. Also, blockchain can improve fraud detection by allowing the creation of a secure and tamper-evident audit record of all transactions. However, the implementation of blockchain in claims and billing management faces obstacles such as data privacy and interoperability with existing systems [28]. In addition, study and development are needed to conquer these challenges and fully use the potential of blockchain in improving claims and billing management.

Table 1.1: The Potential of Blockchain Technology in the Medical Industry.

Application	**Description**
Secure and Immutable Health Records	Blockchain enables the creation of tamper-proof health record systems, ensuring data integrity, privacy, and patient control over their health information.
Interoperability and Data Exchange	Blockchain facilitates secure and efficient data exchange between healthcare systems, improving care coordination and clinical decision-making.
Clinical Trials and Research	Blockchain streamlines consent processes, securely stores trial data, and provides transparency and traceability in research studies, accelerating medical advancements.
Supply Chain Management	Blockchain enhances supply chain transparency, traceability, and accountability, preventing counterfeit drugs and ensuring safe delivery of medications to patients.
Claims Adjudication and Billing	Blockchain automates claims verification and payment processes, reducing administrative burdens and improving efficiency in billing and reimbursement.
Data Security and Privacy	Blockchain ensures data security through cryptography and decentralized storage, granting patients control over their health information and fostering trust between stakeholders.
Medical Research and Intellectual Property	Blockchain simplifies management of intellectual property rights, protecting research data, patents, and licenses, and promoting innovation in the healthcare industry.

The seven stages of the blockchain-based healthcare data management process are shown in Figure 1.3 Data management, data sharing, data storage (such as cloudbased apps), and EHR are all examples of applications built on BT that will be covered in further depth below. Data Management, data sharing, data storage (such as cloud-based apps), and EHR are all examples of applications built on BT that will be covered in further depth below.

- Data Management The fact that many businesses, particularly healthcare institutions, are data-driven and that the amount of data created now and, in the future, thanks to technologies like the IoT, is rising exponentially, there are persistent breaches of data security and privacy [47]. Therefore, many institutions' credibility and financial resources have been severely damaged. Health data users should be separated into categories based on their functions, with access controlled according to the level of authorization granted to each category. BT can be employed to guarantee such access is secure and discreet.

• Electronic Health Record Paper-based medical records are cumbersome because they need accurate tracking of a patient's health condition over time [48]. Also, they are vulnerable to inaccurate information, which can lead to inappropriate treatment of patients. The development of Information Technology (IT) allowed for the implementation of EHRs, significantly reducing the need for such initiatives. Access to EHR enables medical practices to increase treatment quality [49]. Additionally, EHR allows for improved disease management and higher levels of preventative treatment. The digital record also enables improved decision-support features and enhanced teamwork among medical professionals. Consequently, its importance is becoming more widely acknowledged in the medical field [50].

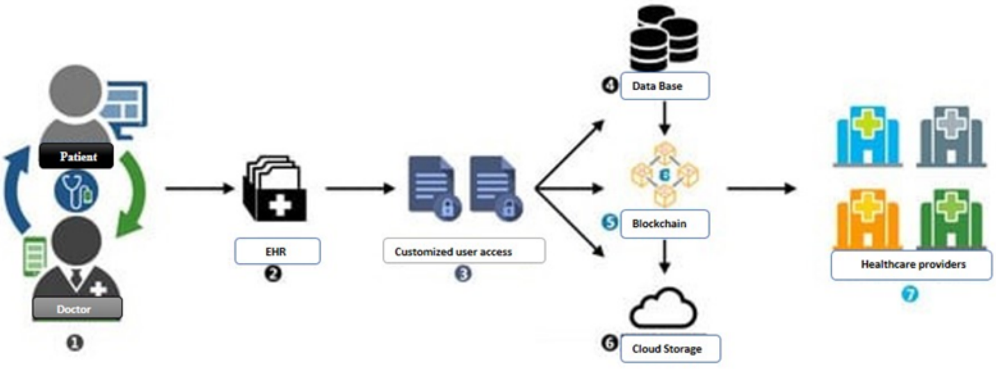


Figure 1.3: Blockchain-Based Healthcare Data Management [29].

Chapter 2

LITERATURE REVIEW

The use of BT in the healthcare industry has gained traction due to its potential for providing a durable medium for storing and sharing electronic health records (EHRs). The blockchain network ensures data immutability, making it a tamper-proof and non-repudiable solution. Two different approaches have emerged for blockchain implementation in data storage. There are two different approaches to utilizing blockchain in healthcare. The first approach involves storing the entire EHR on the blockchain network, where all the data is recorded and stored directly on the blockchain network. The second approach involves storing only the metadata or summary information of the EHR on the blockchain, while the actual EHR data is stored in third-party cloud storage.

Tan et al., (2022) [30] the researchers explore the utilization of blockchain technology (BT) in combination with smart contract implementations to establish a decentralized, verifiable, and unchangeable database. The proposed approach aims to address critical concerns in the healthcare industry, such as ensuring immutable storage, enabling real-time changes to electronic health records (EHR), and safeguarding patient privacy, particularly when utilizing outsourced services. The decentralized nature of blockchain ensures that data stored within the system cannot be easily tampered with or modified without proper authorization. This immutability feature can instill trust and confidence among healthcare providers, patients, and other stakeholders involved in the ecosystem. One significant advantage of the suggested method is the ability to enable real-time changes to EHR. Traditional databases often require complex procedures and multiple parties' involvement to update or modify patient records. The suggested approach allows for immutable storage, real-time changes to EHR, and the protection of patient privacy when using an outsourced service. The authors evaluate the proposed method against current options in terms of performance and safety. The findings show that the suggested method is feasible and meets the necessary functional and security criteria

Al Asad et al., (2021) [31 developed a permissioned blockchain using proof of authority (PoA) technology to provide confidentiality, permission sharing, and efficient distributed healthcare record administration. Furthermore, discussed the benefits of using de facto standards like Fast Health Interoperable Resources (FHIR) to facilitate the meaningful exchange of healthcare information among all parties involved and the significance of managing medical records in an interoperable manner. The study relies on simulated PoA use to learn about the performance of such a consensus process while using BT for safe information exchange.

Chelladurai et al., (2021) [32] established smart contracts on the blockchain to traditionally meet the needs of patients, doctors, and healthcare professionals. The proposed system introduces health models on the decentralized blockchain, such as immutable patient log creation using the Modified Merkle Tree data structure to store and quickly retrieve health records, medical record updates, health information exchange between providers, and viewership contracts. Many studies have been conducted to test the efficacy of the suggested system. The suggested system's performance regarding resources, transactions per second, and latency has been assessed using qualitative and quantitative indicators. The research also introduces the idea of viewing contracts, which gives individuals discretion over who has access to their medical information. Patient privacy and control over sensitive information are ensured via viewership contracts, which let people specify who can read their medical records. This feature gives patients the ability to actively manage their health information and makes sure that doctors and other healthcare providers only access the information they need with the patient's permission. The researchers performed a number of experiments utilizing both qualitative and quantitative indicators to evaluate the efficacy of the proposed system. They evaluated the system's resource utilization, transactions per second, and latency, among other performance metrics. The findings of these assessments provide insights into the efficiency and effectiveness of the proposed system in managing healthcare data on the blockchain.

Abbas et al., (2023) [33] In the study conducted by Abbas et al. (2023) [35], the authors focused on addressing the primary constraints of the current Electronic Healthcare System (EHS), namely, scalability and privacy limitations. The objective of the study was to propose alternate approaches that can enhance scalability, usability, and data protection within the healthcare system. Complete and up-to-date patient records play a vital role in the healthcare field.

Ensuring the availability of comprehensive patient records is crucial for accurate diagnosis, treatment planning, and efficient coordination among healthcare professionals. The study recognized the significance of developing effective Electronic Health Record (EHR) systems that enable the seamless exchange of patient information in real-time. The proposed model implementation in the study incorporates various technologies to overcome the limitations of existing systems. Blockchain- sharing technology forms the foundation of the proposed model, enabling secure and transparent sharing of patient data across multiple healthcare providers. Author proposed the current Electronic Healthcare System and the primary constraints of current systems are their lack of scalability and privacy; thus, the purpose of this study is to define alternate approaches for achieving scalability, usability, and data protection in the healthcare system. It is essential in the healthcare field to provide complete, up-to-date patient records. Instant availability of patient records for improving efficiency and coordination is another quality that helps academics to think about effective EHR systems. The proposed model implementation makes use of blockchain-sharing technology, hyper-ledger protocols, and Proof-of-Authority.

Rathee et al., (2020) [34] establish a foundation for the safety of healthcare multimedia data using BT by producing a hash for each piece of information, allowing users throughout the network to be alerted to any unauthorized changes to data or medication. Simulation improvements are attributable to the usage of Blockchain have been used to confirm the findings, which show an 86% success rate in the face of product drop ratio, wormhole attack, falsification attack, and probabilistic authentication.

Lee et al., (2019) [35] This paper presents SHAREChain, a healthcare data-sharing framework that focuses on enhancing the reliability and interoperability of shared data. framework is designed to ensure data integrity through the use of BT and restrict data sharing to authenticated institutions via a consortium blockchain network. The system architecture is based on the XDS actor and transaction concept, with the FHIR standard used to ensure data interoperability. The paper compares and analyzes SHAREChain with existing solutions and highlights the advantages of using a blockchain registry instead of traditional databases. Although this construction is efficient, it does not provide measures for ensuring the privacy and confidentiality of the outsourced data as encryption is not utilized during data outsourcing. Thus, future research could explore ways to enhance the security of the proposed framework through the deployment of encryption techniques to safeguard sensitive healthcare data from unauthorized access or disclosure.

Andola et al., (2019) [36] proposed a new approach for managing healthcare systems called Secure Healthcare Management System using Blockchain (SHEMB), which employs blockchain-based searchable symmetric encryption (SSE) to enable secure data access and retrieval without involving any third parties. SHEMB consists of three phases - interoperability, storage, and retrieval - for storing and accessing encrypted electronic health records (EHRs) on the blockchain network. To maintain the integrity of the blockchain network, it is essential to consider the potential for malicious nodes, such as doctors, patients, or departments, that may be compromised by attackers. User-side and server-side verifiability are crucial in preventing any malicious activities on the pinged server or user nodes. However, the present effort does not specifically address this issue. The system enables authorized parties to search for and retrieve particular information while maintaining the overall security and privacy of the data by encrypting the EHRs with searchable symmetric encryption. Involving third-party intermediaries is no longer necessary, speeding the data management process and lowering the risk of vulnerabilities. According to the study, it's critical to take into account potentially hostile nodes in the system in order to protect the integrity of the blockchain network. Threats to the security and privacy of healthcare data might come from bad actors including rogue physicians, patients, or departments. User-side and server-side verifiability are therefore essential elements. The use of blockchain-based SSE provides a promising approach to protect sensitive healthcare data while enabling efficient and secure access and retrieval.

J. Vora et al., (2019)[37] proposed a BHEEM framework for EHR management that leverages the power of BT. Specifically, BHEEM utilizes a permissioned blockchain that restricts data access to authorized users. Access control and consent management are enforced through the use of smart contracts. It enhances the scalability and flexibility of the proposed framework. but it has some limitations which is Scalability means The BHEEM framework is based on a permissioned blockchain, which may not be scalable enough to handle large volumes of data or user requests.

A. P. Singh et al., (2021) [38] The framework proposed in this study offers a shared data-sharing platform for various stakeholders in the healthcare system. Blockchain technology is utilized as a distributed ledger, allowing each participant to securely store and access health data on the network. The framework aims to improve data security, data privacy, and data sharing in the healthcare system. coming to limitation in this framework they upload the data on blockchain which make it bulky and also scalability is the issue here. With blockchain, participants have control over their own data and can decide who can access and view it. Smart contracts can be implemented to enforce data access policies, ensuring that only authorized individuals or organizations can access specific healthcare data.This enhances patient privacy and confidentiality, fostering trust among stakeholders within the healthcare ecosystem. However, it is important to note that the framework has certain limitations that need to be addressed. One limitation is the potential increase in data size and storage requirements. As data is uploaded onto the blockchain, it can contribute to the overall bulkiness of the network. This can lead to increased storage demands and potentially impact the scalability of the system. Efforts should be made to optimize data storage and improve efficiency to mitigate these challenges. Scalability is another aspect that needs consideration.

McSeth, et al., (2021) [**39**] The paper utilizes HyperLedger Fabric, a private BT, as the framework for its testing scenarios aimed at exploring various criteria and use-cases for healthcare applications. as seen the performance of this framework may be impacted such as the number of nodes in the network and the complexity of the smart contracts being used. It's worth noting that HyperLedger Fabric is a permission-based blockchain, which can limit scalability and adaptability compared to permissionless blockchains. While permissioned blockchains provide certain advantages, such as enhanced privacy and control over the network, they may also impose limitations on scalability and adaptability compared to permissionless blockchains. The requirement for specific authorization and agreement among authorised parties may add complications and perhaps limit the system's capacity to scale. Additional study and development are required to solve these drawbacks and improve the scalability and adaptability of the HyperLedger Fabric infrastructure. To increase the network's scalability and performance, strategies including sharding, off-chain processing, and improvement of consensus methods might be investigated. Additionally, advancements in hardware and infrastructure can contribute to enhancing the efficiency of the HyperLedger Fabric framework.

Amit Kumar, et al., (2022) [**40**] The paper presents a framework that aims to safeguard the privacy and security of sensitive healthcare documents when shared among multiple healthcare participants. This framework is based on blockchain technology and employs decentralized data management on peer-to-peer distributed computing platforms to ensure robust privacy and security measures. The proposed framework has been evaluated using Hyperledger Fabric. again, the same as above they are using hyper ledger and in this framework, they upload the whole records directly to the network which makes it bulky and there is also a limitation on using Hyperledger in comparison to public blockchain. a framework is presented with the objective of safeguarding the privacy and security of sensitive healthcare documents during their sharing among multiple healthcare participants. The framework is designed based on blockchain technology and leverages decentralized data management on peer-to-peer distributed computing platforms to ensure robust privacy and security measures. For development and testing, the suggested framework uses Hyperledger Fabric as the underlying blockchain platform. With the use of channels and smart contracts, Hyperledger Fabric offers a permissioned blockchain architecture with capabilities like access control and privacy. The framework intends to address the privacy problems related to exchanging healthcare documents while retaining the required security measures by utilizing these features. It is crucial to keep in mind that one drawback of the architecture is that it necessitates immediately uploading all medical information to the blockchain network. And the choice of using Hyperledger Fabric, which is a permissioned blockchain, introduces certain limitations compared to public blockchains. Permissioned blockchains require explicit permissions and consensus among authorized entities, which may restrict the openness and decentralization that public blockchains offer. While permissioned blockchains like Hyperledger Fabric provide enhanced privacy and control over the network, they may not be as adaptable and scalable in certain scenarios. To mitigate the limitations associated with data bulkiness and the use of a permissioned blockchain, future research and development efforts could explore techniques such as data partitioning, off-chain storage solutions, and optimization strategies to improve the efficiency and scalability of the framework.

Wang et al., (2019) [51] suggest a novel method for exchanging individual health records that uses BT to prove the authenticity of the shared data. The novel system employs searching attribute-based encryption and symmetric encryption to safeguard privacy, keyword search, and fine-grained access control while exchanging personal health data. Moreover, the new scheme utilizes blockchain to maintain scheme keys, removing the potential for a single failure point associated with centralized key management. Lastly, the investigation of security threats and performance benchmarks confirm the safety and practicality of the method.

Wang et al., (2018) [52] employed attribute-based encryption (ABE)and Identity-based encryption (IBE) to protect sensitive patient information, while identity-based signatures (IBS) can be used to authenticate online transactions. Authors offer a new cryptographic primitive term that combined attribute-based/identity-based encryption and signature (C-AB/IB-ES) that combines the features of ABE, IBE, and IBS into a single system. It greatly reduces the complexity of system management and eliminates the requirement for additional cryptographic systems to provide different degrees of security. Table 3 indicates the comparison table of the literature of review.

Table 2.1: Blockchain Technology Contributions in Various Papers

Paper	**Year**	**Blockchain Technology**	**Key Contributions**
Tan et al.,	2022	Smart Contracts	Immutable storage, real-time changes, privacy
Al Asad et al.,	2021	Proof of Authority	Efficient healthcare record administration
Chelladurai et al.,	2021	Decentralized Blockchain	Health models, patient log, information exchange
Abbas et al.,	2023	Blockchain-sharing technology	Alternate approaches for healthcare system
Rathee et al.,	2020	Blockchain Technology	Hash-based data security, authentication
Andola et al.,	2019	Blockchain-sharing technology	Secure data access, retrieval, and privacy
J. Vora et al.,	2019	Permissioned Blockchain	Access control, consent management
A. P. Singh et al.,	2019	Blockchain Technology	Improved data security, privacy, and sharing
McSeth et al.,	2021	HyperLedger Fabric	Impact of node number and smart contracts
Amit Kumar et al.,	2022	Blockchain Technology	Robust privacy, decentralized data management
Wang et al.,	2019	Blockchain Technology	Authenticity, privacy, and fine-grained data access
Wang et al.,	2018	Attribute-based/Identity-based Encryption and Signature	Enhanced security and simplified system management

Chapter 3

Requirements

3.1 Hardware Requirements

As per as Hardware requirement is concern we have implemented Our project on Operating System backed by Microsoft windows version 10, with storage of 1 TB HDD and 256GB SSD and RAM 16GB.

3.2 Software Requirements

3.2.1 MetaMask

It provides a user-friendly interface for managing Polygon-based digital assets, such as MATIC tokens, and interacting with decentralized applications (dApps) on the Polygon network. It acts as a bridge between a user's web browser and the Polygon network, allowing users to securely store, send, and receive MATIC tokens, as well as interact with dApps built on the Polygon blockchain directly from their browser. MetaMask generates a unique pair of public and private keys for every account created within the wallet[44].

- Public Key : The public key is typically a hexadecimal string that starts with "0x" and is used to receive funds and interact with the blockchain. It is publicly shareable and can be used by others to send Matic or other tokens to the associated Blockchain network address.
- Private Key: On the other hand, the private key must be kept secret and never disclosed to anybody. It is employed to sign deals and demonstrate control over the corresponding Blockchain address. Users may send transactions, engage with smart contracts, and administer their assets in MetaMask using the private key.

What makes MetaMask appealing is its user-friendly approach. It eliminates the need for technical expertise or complex software downloads. By simply installing the MetaMask extension, users can effortlessly create a digital wallet and manage their cryptocurrencies without any complications. Security is a significant aspect of MetaMask. It guarantees that users may safely save their personal data, such as access keys, on their own device. Since there is no need to transmit critical information with outside websites or applications, this function offers piece of mind. On behalf of the user, MetaMask manages the essential interactions. Through its user-friendly interface, MetaMask gives users a clear picture of their bitcoin holdings and transaction history. Even transaction prices may be customised, giving consumers the option to prioritise cost reduction or speedier transactions according on their preferences. MetaMask has interesting possibilities for those who are interested in cryptocurrencies. It makes it simple to participate in DeFi (decentralised financial apps) and makes it easier to interact with non-fungible tokens (NFTs). The Ethereum blockchain serves as a key for MetaMask, opening up an universe of cutting-edge experiences. MetaMask is a user-friendly tool that streamlines bitcoin management and communication with websites and applications built on the Ethereum platform. It places a high priority on user security, provides open asset monitoring, and makes it possible to participate in different NFT and decentralised financial activities.

3.2.2 IPFS

An novel and decentralized system called IPFS (Interplanetary File System) enables the safe and secure archival of hypermedia. We use IPFS as a database in our system, utilizing its sophisticated features. An novel and decentralized system called IPFS (Interplanetary File System) enables the safe and secure archival of hypermedia. We use IPFS as a database in our system, utilizing its sophisticated features. With IPFS, users can create and access content using unique content addresses that are generated based on the cryptographic hash of the content itself. It means instead of relying on traditional URLs or file paths, IPFS uses content-based addressing, making it highly resilient to censorship, tampering, and data loss [45].

- Encryption: Users of IPFS can encrypt their material to ensure that it is private and safe during storage and transmission. Users can opt to add additional encryption layers, like Filecoin for decentralized storage, or use industry-standard encryption protocols, such SSL/TLS, to encrypt material.
- Data Integrity: Data integrity is ensured by IPFS using cryptographic hashes, which makes it impervious to hacking and illegal alterations. Any modification to the content produces a new hash, which is easily verifiable and ensures the accuracy of the data being saved.

Files are not kept in a single place or on a particular server while using IPFS. but they are divided up and dispersed throughout a network of machines that are a part of the IPFS network. This distributed nature allows for simultaneous file retrieval from numerous sources, which speeds up and improves the reliability of file retrieval. The content-addressable storage mechanism of IPFS is one of its main advantages. In IPFS, files are not identifiable by their name or location but rather by their content. Every file has a specific cryptographic hash that acts as its address. This means that files can be accessed and verified based on their content, ensuring integrity and reducing the risk of tampering or data corruption. When a file is added to IPFS, it is automatically versioned, and any subsequent changes or updates to the file are stored as a separate version. This allows for efficient tracking of file history and the ability to retrieve previous versions if needed. Additionally, By deduplicating identical data bits and maximizing storage capacity throughout the network, IPFS prevents duplicate storage. Additionally, IPFS supports data persistence and censorship resistance. Files on IPFS are resistant to censorship efforts and single points of failure since they are dispersed across many nodes. The file can still be downloaded from other nodes in the network even if one goes down or is inaccessible.

3.2.3 Solidity

It is a specialized programming language created with the intention of building smart contracts for Ethereum and other blockchain systems. Solidity allows programmers create smart contracts that operate on the Ethereum Virtual Machine in this situation (EVM). Making ensuring the smart contracts are trustworthy and safe is the main goal of Solidity. Additionally, it allows inheritance, allowing you to reuse code and create more intricate applications. Solidity can handle all of your data needs. It provides a variety of kinds, including arrays, Booleans, texts, addresses, and numbers. If you want a data structure that is more specialized, you may even design your own. Solidity also provides you with choices like if statements, loops, and switch statements if you want to manage how your code runs. Comparable to having a toolbox Solidity also cares about security. It lets you control who can access certain functions and data by using visibility modifiers. This helps prevent unauthorized access and keeps things in check. If something goes wrong during execution, Solidity has exception-handling mechanisms to deal with errors and make sure things don't go haywire. To make communication easier, Solidity has function modifiers and events. Function modifiers let you tweak how functions behave and add extra checks. Events allow you to send structured logs that can be captured by external systems, making it easier to interact with things happening outside the blockchain. Developing with Solidity is made easier by the tools and frameworks available in its ecosystem.

IDEs like Remix and Truffle offer features that help you write, debug, and test your code. There are also tools for analyzing the code and making sure everything is secure and correct. But like anything else, Solidity has its challenges. So, developers have to be extra careful and thoroughly test their code before it goes live. And learning Solidity and blockchain development in general can be a bit tough at first, as it requires understanding the unique aspects of blockchain platforms.

3.2.4 Truffle

It is a development framework that makes building decentralized applications (dApps) on the Ethereum blockchain easier. It offers a range of tools to streamline the development, testing, and deployment of dApps. Developers can use Truffle to write, compile, and manage smart contracts, which are agreements that run on Ethereum and define dApp rules. Truffle's smart contract management features help developers organize and deploy contracts, ensuring smooth integration with the Ethereum network. One of Truffle's standout features is its built-in testing framework. Testing is crucial for decentralized apps and smart contracts, and Truffle provides a robust testing environment. Developers can write comprehensive tests to ensure their dApps are reliable and functional. Truffle also includes a development console, an interactive environment for developers to work with their dApps. The console lets developers execute commands, query contract data, and simulate transactions, providing insights and enhancing the development experience. Truffle seamlessly integrates with other tools like Ganache and Metamask. Ganache is a personal blockchain for Ethereum development, enabling local deployment and testing of dApps. Metamask allows easy interaction with the Ethereum network through browser extensions. In addition to development capabilities, Truffle supports the deployment and management of dApps in real-world environments. It offers features to configure deployment settings, handle contract migrations, and interact with deployed contracts. Overall, Truffle empowers developers by providing a user-friendly framework for building dApps on Ethereum. Its tools for smart contract management, testing, and integration simplify the development process and contribute to the growth of the decentralized ecosystem.

3.2.5 Testing Environment

The Mumbai Testnet is a development environment provided by Polygon (formerly Matic Network) for testing and deploying decentralized applications (dApps) and smart contracts on the Polygon network. It provides developers with a high-performance, inexpensive environment to test their code and runs independently of the Ethereum mainnet. Before releasing their apps to the Polygon main net, developers may find and fix flaws and vulnerabilities by utilizing the Mumbai Testnet. They can execute transactions, calculate gas costs, communicate with smart contracts, and assess scalability and performance. The Mumbai Testnet provides a realistic environment for developers to assess their applications' behavior and efficiency under different conditions. They can utilize Ethereum development tools and frameworks compatible with Polygon, and the testnet offers a faucet service to obtain test tokens for risk-free testing. Overall, the Mumbai Testnet on Polygon is a crucial platform for developers to ensure the reliability, scalability, and performance of their applications before launching them on the Polygon network.

3.2.6 UI

A well-liked framework called Angular makes it possible to create engaging user interfaces. Developers may easily include dynamic UI components into their apps by using Angular to construct them.. We use angular for our project UI.

Chapter 4

Proposed Framework (SHSP)

4.1 Smart Contracts

A smart contract is a low-level code script that runs on a blockchain platform. It was originally coined to refer to the automation of legal contracts in general. Smart contracts have gained popularity due to the advent of blockchain technology and have found numerous important applications in the real world, such as crowdfunding. However, smart contract development still remains somewhat of a mystery to many developers due to its special design and applications. Smart contracts have a high requirement for code security, but developers currently have no effective way to assure code security. Some tools like code auditing and formal verification techniques are highly desired. Developers mainly use testing and code reviews to help ensure code correctness. This decentralized nature ensures that no single entity has control over the contract, making it resistant to censorship or manipulation. The blockchain serves as a trusted and immutable source of truth, where the execution and outcome of the smart contract can be verified by all participants. A smart contract's code is uploaded to the blockchain when it is created, and a special address is given to it. Smart contracts also support complex logic and multi-step processes. They can include variables, conditional statements, loops, and even interact with other smart contracts or external data sources through predefined interfaces called "oracles." These features enable the creation of sophisticated applications and systems that operate autonomously, reducing the need for human involvement and potential points of failure. Another critical aspect of smart contracts is their transparency. Anyone may audit and confirm the behavior of the contract by looking at its code and execution history, which are both publicly accessible on the blockchain. Participants can independently verify the integrity of the contract and make sure it functions as intended because of this openness, which fosters confidence among them. Despite the fact that smart contracts have many advantages, there are certain things to take into account. To prevent flaws or faults that might be used against the developer, the code must be properly developed and inspected. Since immutability is a core characteristic of blockchain technology, it could be difficult to amend or reverse the contract in the event of a coding error or unanticipated incident. In many jurisdictions, the laws and regulations governing smart contracts are still developing. Despite the fact that smart contracts can enforce an agreement's terms, their legal enforceability and interpretation might differ [46].

4.2 Ethereum vs Polygon

Ethereum is a permissionless blockchain platform that has the ability to enable the creation and execution of smart contracts and decentralized applications (dApps). Ethereum has a native cryptocurrency, Ether (ETH), as a means of fueling transactions and executing smart contracts. One of the key characteristics of Ethereum is its flexibility which allows developers to build a different range of dApps which they want. With a thriving developer community and constant innovation, Ethereum exhibits high perplexity, constantly evolving and adapting to changing market needs. The development of Ethereum projects and applications is often marked by burstiness, with dynamic and diverse sentence structures, combining longer, more intricate sentences with shorter ones, reflecting the creative and ever-evolving nature of this revolutionary blockchain platform [41]. Polygon, which was known as Matic Network, is a layer 2 scaling solution for the Ethereum blockchain. It aims to address the scalability and transaction cost issues associated with Ethereum by offering a sidechain that operates in parallel to the Ethereum mainchain. Polygon provides faster and cheaper transactions compared to Ethereum, making it suitable for applications that require high throughput and low transaction fees. The Polygon network is designed to support a wide range of dApps and smart contracts, providing developers with the flexibility to build and deploy various use cases, from gaming to decentralized finance (DeFi) and more. With its unique consensus mechanism and interoperability features, Polygon has gained significant attention in the blockchain community, leading to a growing ecosystem of projects and partnerships[42]. The Polygon network is built to accommodate a broad range of decentralized applications (dApps) and smart contracts, giving developers the freedom to create and implement a variety of use cases, including gaming, decentralized finance (DeFi), and more. The blockchain world has paid substantial attention to Polygon because of its distinct consensus method and interoperability characteristics, which has sparked an expanding ecosystem of initiatives and collaborations [16]. its consensus mechanism ensures the security and integrity of transactions while promoting interoperability between different chains. The interoperability aspect of Polygon enables seamless communication and data exchange between the Ethereum mainchain and the Polygon sidechain, expanding the possibilities for cross-chain applications. As Polygon continues to gain traction and recognition within the blockchain community, its ecosystem has witnessed significant growth. Polygon's emergence as a layer 2 scaling solution for Ethereum has addressed the pressing scalability and transaction cost issues.

Table 4.1: Ethereum vs Polygon

Features	**Ethereum**	**Polygon**
Scalability	Limited Scalability	Multichain solutions offer better scalability
Native token	ETH	MATIC
Transaction Speed	27-30	65,000
Consensus Mechanism	Proof of Work	Proof of Stake Plasma-based sidechain
Security	Large hash power securing Pow-based consensus	Relies on Ethereum mainchain's security, PoS-based consensus mechanism, and network validators
Finality time (sec)	300	2.3
Architecture	Stateful Multichain	-
Transaction Fees and Gas Prices	High	Low

• Scalability: Ethereum faces main limitations in terms of scalability, while Polygon addresses this challenge by providing the multichain solutions which will offer improved scalability. The use of sidechains enables higher throughput and performance.

• Transaction Speed: While Polygon claims a transaction speed of 65,000 transactions per second, Ethereum handles about 27–30 transactions per second. Applications created on the Polygon network are more effective as a result of the enhanced throughput.

• Security: The robust PoW-based consensus process and Ethereum's high hash power serve as primary security measures. On the other hand, Polygon makes use of the Ethereum mainchain's security as well as its PoS-based consensus system and network validators.

• Finality Time: The finality time for Ethereum is around 300 seconds, but the finality time for Polygon is closer to 2.3 seconds. Transaction confirmation is facilitated by the reduced finality time on Polygon.

• Architecture: Ethereum is a stateful blockchain with support for multiple

chains. Although Polygon also uses a multichain design, it also supports sidechains, particularly Plasma-based sidechains, which offer more flexibility and scalability.
• Transaction Fees and Gas Prices: The comparatively high transaction costs and gas costs of Ethereum are well-known. For users and developers, Polygon is more affordable because to its much lower fees and gas costs.

4.3 SHSP Architecture Explained

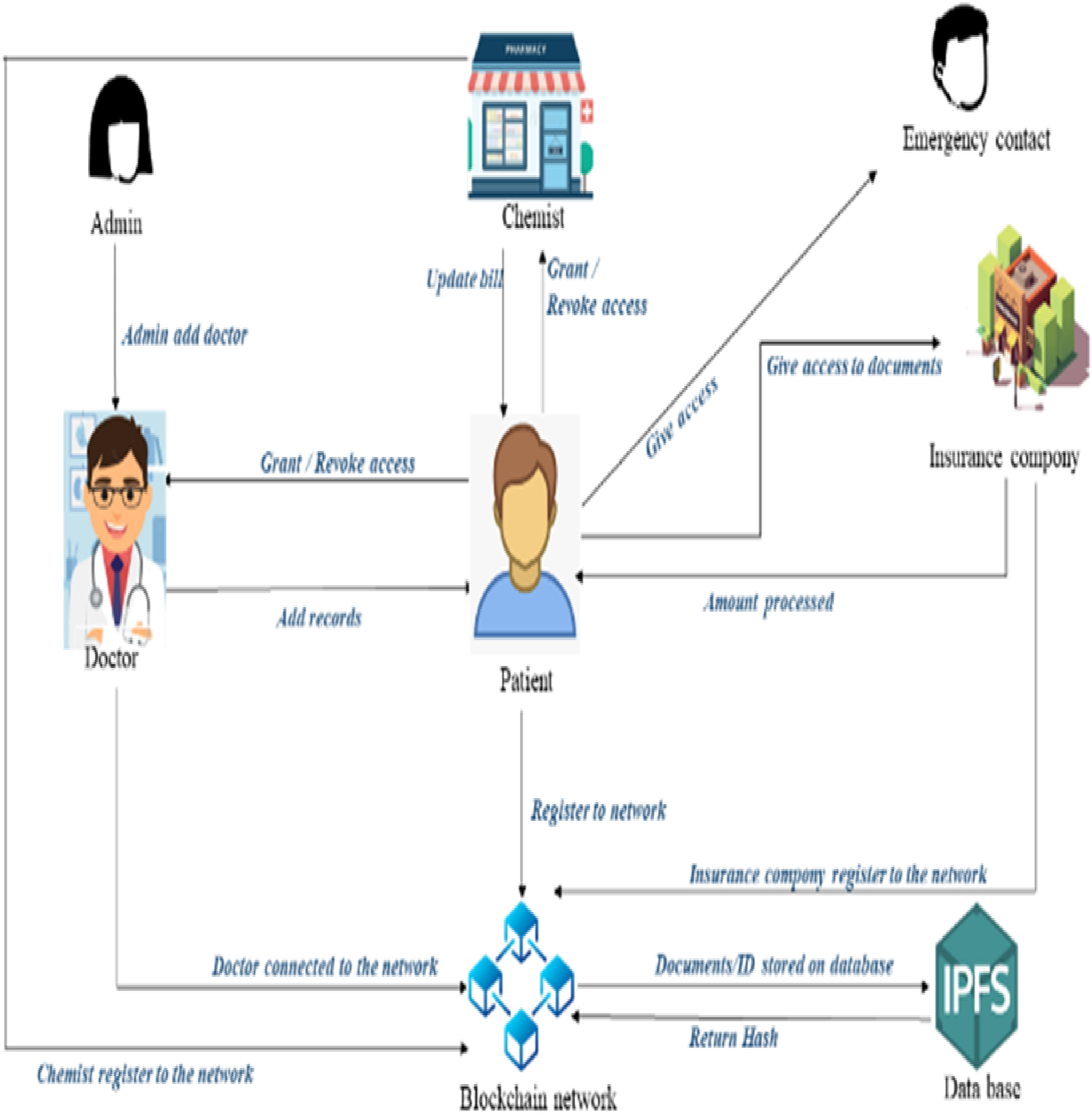


Figure 4.1: SHSP Architecture

We develop a Smart contract for this System a smart contract is a self-executing contract that uses BT to automate, verify, and enforce the terms and conditions of an agreement without relying on intermediaries[43]. It is a computer program written in programming languages that allow for conditional logic, and it is stored on a blockchain, which is a decentralized and distributed ledger that ensures transparency, security, and immutability. One of the important features of smart contracts is their trustworthiness, as they are enforced by the consensus rules of the underlying blockchain, making them transparent, immutable, and resistant to tampering. In Smart contract, we have Following entity

- Admin: The admin has the authority to add doctors to the system, ensuring the integrity of the system by adding only authentic doctors. The admin uses their public key to validate and authorize the addition of doctors to the blockchain network.

- Doctor: The doctor provides healthcare services to patients and creates medical records that are uploaded to the blockchain network using their public key. The doctor's access to the system is authenticated and verified by the admin, ensuring the authenticity of the medical records.

- Patient: The patient registers themselves with their public key and authentic ID. They can take appointments for check-ups and after the check-up, they can grant permission to the doctor to upload their medical records. The patient's access to the system is secure and can be controlled by the patient themselves, ensuring privacy and data security.

- Insurance Companies: A patient may provide insurance firms access to their medical information in order to submit an insurance claim. To process an insurance claim, the insurance companies might check the information in the medical records. This guarantees openness and confidence in the handling of insurance claims.

- Chemist: By granting the pharmacist access to check their medical information, the patient offers a prescription. The pharmacist can validate the prescription and provide the medication if necessary. Additionally, the pharmacist will upload the invoice to the patient's dashboard, guaranteeing a quick and safe transaction.

- Emergency Contact: The patient can add a reliable individual who has access to all of their medical records to the smart contract system's emergency contact function. This guarantees that the emergency contact will be able to view the patient's medical records in the event of an emergency if the patient is unable to provide access.

By incorporating these roles and functionalities into the smart contract system, the research paper presents a professional and comprehensive framework for a blockchain-based healthcare system, ensuring integrity, authenticity, privacy, and trust in the network.

4.4 Steps Involves In The Development Of SHSP

• User Wallet Creation: Users are required to have a wallet to interact with the smart contract system. MetaMask, a popular wallet, is used, providing users with a public key (wallet address) and a private key for secure access.

• Smart Contract Development: The smart contract is developed in Solidity, a widely-used programming language for creating smart contracts on blockchain platforms. The contract is carefully coded, incorporating the desired functionalities and security measures, including encryption and consensus algorithms.

• Contract Compilation: The smart contract is compiled to obtain the corresponding bytecode that can be executed on the blockchain. The compilation process ensures that the contract code is converted into a format that can be understood and executed by the blockchain network.

• Contract Deployment: The compiled smart contract is deployed on the Polygon test network, specifically the Mumbai-Test-Net, for testing purposes. The deployment process involves sending a transaction that includes the compiled contract bytecode, which is then stored on the blockchain as a deployed contract.

• Authorization Mechanism: To ensure authenticity, an authorization mechanism is implemented in the smart contract. An administrator is granted the authority to add doctors to the network using their public key. This mechanism ensures that only authorized individuals, i.e., the admin, can perform this action.

• Encryption: To maintain the confidentiality and integrity of data, encryption techniques can be used. For example, sensitive data such as doctors' credentials or patient information can be encrypted before being stored on the blockchain, using industry-standard encryption algorithms.

- Consensus Algorithm: Polygon employs a variant of the Proof of Stake (PoS) consensus mechanism known as Plasma-based PoS (Plasma PoS) to secure its blockchain network. In the Plasma PoS algorithm, a group of validators stakes tokens as collateral to create new blocks and validate transactions. Validators take turns proposing blocks and validating transactions, with their selection probability proportional to their staked token amount. The Plasma PoS consensus algorithm is designed to ensure scalability, security, and decentralization of the Polygon network.

- Transaction Validation: Transactions involving doctor additions to the network are validated before being recorded on the blockchain. This validation process includes verifying the digital signature of the admin's private key, checking the authorization status, and confirming that the transaction adheres to the defined rules of the smart contract.

- UI: We also develop a user interface with the help of angular so the every bits and pieces will connect and show in one place.

- Testing Environment: The Mumbai Test-net is a test network by Polygon, a layer-2 scaling solution for Ethereum. It allows developers to test smart contracts and dApps on the Polygon network using test tokens (MATIC) without incurring real costs. It helps identify and fix issues before deploying on the main net, ensuring a secure and reliable experience for users

4.5 Fuctions Used In Smart Contract

addDoctor: This essential function empowers the system administrator to add a doctor to the network by providing the doctor's address. By executing this function, the administrator ensures that authorized doctors can actively participate in the network and access relevant functionalities. This enables seamless collaboration and effective coordination among healthcare providers within the blockchain-based healthcare ecosystem.

addMedRecord: The significance of this function lies in its ability to create and store a patient's comprehensive medical records within the decentralized application (DApp). It involves the inclusion of various crucial details, such as an IPFS hash that securely holds the uploaded file containing the patient's lab results or other significant medical records. This ensures that patients' healthcare information is accurately documented and easily accessible, promoting efficient and informed healthcare decision-making.

addPatInfo: Designed with patient-centricity in mind, the addPatInfo function allows patients to actively contribute their own information to the network. By securely storing an IPFS hash containing the patient's relevant details, this function promotes patient empowerment and engagement. Patients play an active role in managing their healthcare information and ensuring its accuracy, thereby fostering a sense of ownership and trust within the blockchain-based healthcare system.

givePermission: This function empowers patients with the authority to grant access to specific doctors, thereby allowing them to view the patient's medical records. Patients retain complete control over their data, ensuring privacy and consent in the sharing of their sensitive healthcare information. By granting access only to trusted doctors, patients foster a sense of trust and transparency, enhancing the doctor-patient relationship and promoting personalized and effective healthcare delivery.

removeAdmin: As an integral part of the smart contract, the removeAdmin function enables the system administrator's removal from the network. This function ensures the ability to manage and maintain a trusted and secure network environment. By providing the admin's address, this function allows for necessary updates to the administrative roles, contributing to the efficient and accountable governance of the blockchain-based healthcare system.

removeDoctor: With the removeDoctor function, the system administrator can securely remove a doctor from the network by providing the doctor's address. This function helps in keeping the network up-to-date and maintaining a roster of authorized doctors. By promptly removing doctors who are no longer part of the system, this function ensures the accuracy and integrity of the network's doctor database, facilitating seamless collaboration and effective healthcare delivery.

removePermission: Patients can exercise their control and privacy preferences by utilizing the removePermission function, which allows them to revoke access from doctors who were previously granted permission to view their medical records. By offering patients the ability to manage and regulate access to their healthcare information, this function fosters a sense of autonomy, privacy, and data security. doctorList: The doctorList function serves as a valuable utility that provides a comprehensive list of doctors currently participating in the network. By accessing this function, users can obtain an up-to-date roster of authorized doctors within the blockchain-based healthcare system. This promotes transparency, trust, and accountability, ensuring that patients can easily verify the legitimacy of healthcare providers and make well-informed decisions about their healthcare.

isAdmin: The isAdmin function serves as a verification tool that allows users to confirm whether the network is operated from the admin address. By returning a true or false value, this function assists in validating the administrative privileges and maintaining the integrity and security of the system. It ensures that only authorized administrators can perform crucial administrative functions within the blockchain-based healthcare ecosystem.

isDoctor: This function allows anyone interacting with the smart contract to verify if the address corresponds to a registered doctor within the network. When calling this function, the smart contract checks the provided address against the list of registered doctors. If the address is found in the list of doctors, the function returns a boolean value true, indicating that this is the authenticated address. On the other hand, if the address is not found in the list, the function returns a boolean value of false, indicating that the address does not correspond to a registered doctor within the network. isDoctor function is a useful tool for validation and authorization purposes, enabling the smart contract to differentiate between doctors and other participants within the network based on their registered addresses.

addEmergencyContact: This function allows the patient to add a reliable individual as their emergency contact within the smart contract system. By this function, the patient can give access to the one trusted person so that in needy time they have everything This ensures that in case of an emergency where the patient is unable to provide access to their medical records, the emergency contact can securely view the patient's medical information and give access to a doctor. Adding an emergency contact through this function enhances the safety and efficiency of emergency medical care, providing healthcare providers with essential insights into the patient's medical history and aiding in informed decision-making.

isPatient: This function verifies whether the network is operated from a patient's address, returning a true or false value. It assists in confirming the patient's identity and ensuring secure interactions within the system.

viewMedRec: This function allows patients to view their own medical records, providing them with access to their healthcare information and fostering an informed and engaged patient role.

viewMedRecordOfPatient: Authorized doctors can use this function to view the medical records of their patients. It enables doctors to access relevant patient information when providing medical care, promoting efficient and comprehensive healthcare delivery.

These functions collectively establish a robust and reliable framework for managing patient data, facilitating secure interactions between patients, doctors, and administrators within the blockchain-based healthcare system.

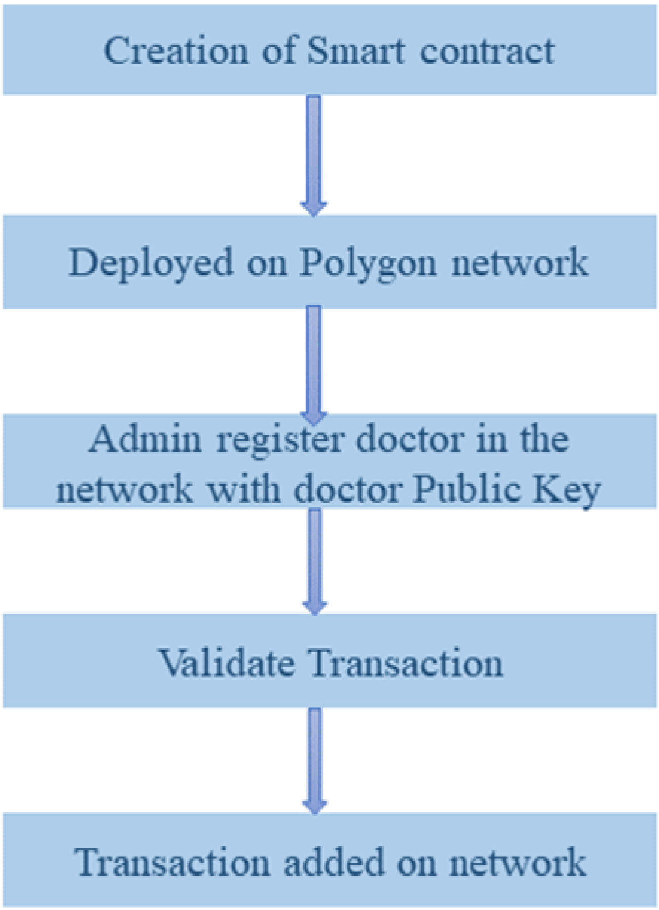

Creation of Smart contract
Deployed on Polygon network
Admin register doctor in the network with doctor Public Key
Validate Transaction
Transaction added on network

Figure 4.2: Flow For Adding Doctors To The Network.

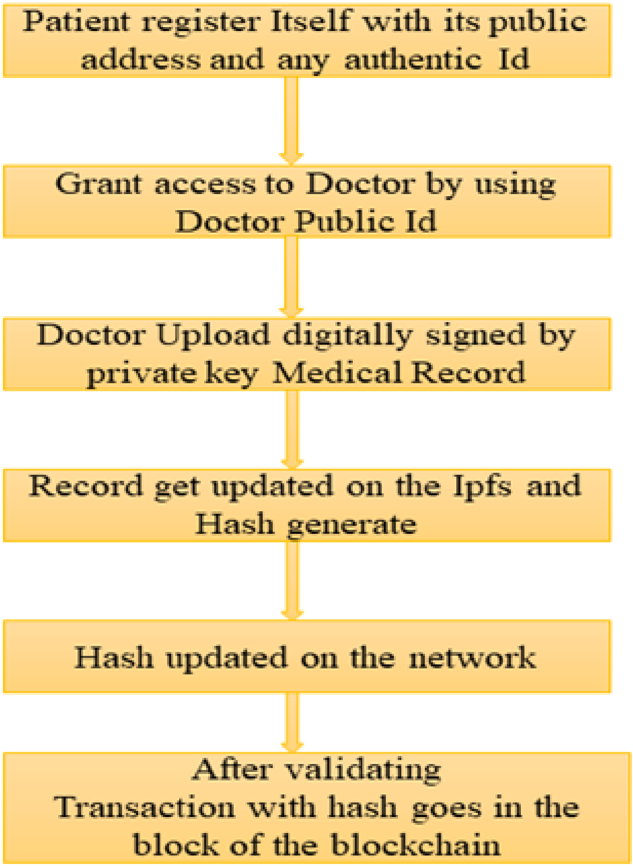

Patient register Itself with its public address and any authentic Id
Grant access to Doctor by using Doctor Public Id
Doctor Upload digitally signed by private key Medical Record
Record get updated on the Ipfs and Hash generate
Hash updated on the network
After validating Transaction with hash goes in the block of the blockchain

Figure 4.3: Flow For Adding Medical Record.

4.6 Use Cases

Here are some potential use cases for a scalable framework for healthcare systems using the Polygon blockchain:

1 Patient Medical Records Management: The framework can facilitate the secure and efficient management of patient medical records. It can enable patients to have control over their own records, granting permission to healthcare providers for access and ensuring privacy and data security.

2 Interoperability and Data Exchange: The framework can promote interoperability among different healthcare stakeholders, allowing seamless and secure exchange of patient information. This can enhance care coordination, improve clinical decision-making, and reduce redundant tests or procedures.

3 Clinical Trials and Research: The framework can be utilized to streamline the management and sharing of clinical trial data. It can ensure transparency, data integrity, and traceability, fostering trust among researchers, sponsors, and regulatory authorities. This can lead to accelerated drug discovery, improved research collaboration, and enhanced patient safety.

4 Supply Chain Management: The framework can be applied to optimize the supply chain in healthcare. It can help track and verify the authenticity of pharmaceutical products, medical devices, and supplies, reducing the risk of counterfeit or substandard products entering the market. This can enhance patient safety and streamline inventory management.

5 Telemedicine and Remote Healthcare: The framework can support the secure and efficient delivery of telemedicine services. It can enable remote patient monitoring, facilitate virtual consultations, and ensure the integrity and privacy of telehealth interactions. This can improve access to healthcare services, particularly for underserved or remote populations.

6 Health Insurance and Claims Processing: The framework can enhance the efficiency and transparency of health insurance processes. It can facilitate the verification and validation of insurance claims, reducing fraud and administrative overhead. This can lead to faster claim settlements and improved financial sustainability of healthcare systems.

These are just a few examples of how a scalable framework using the Polygon blockchain can be applied in the healthcare industry. The specific use cases may vary depending on the needs and priorities of healthcare organizations and the broader healthcare ecosystem.

4.7 Limitation

While developing a scalable framework for healthcare systems using the Polygon blockchain presents numerous benefits and potential advancements, it is important to acknowledge some limitations that may arise during the course of the thesis:

1 Adoption Challenges: Implementing a new technology like the Polygon blockchain in the healthcare industry may face resistance and adoption challenges. Healthcare organizations, stakeholders, and regulatory bodies may require time and effort to embrace and integrate the framework into their existing systems and workflows.

2 Technical Complexity: Building a scalable framework using blockchain technology involves complex technical aspects. Developing smart contracts, integrating with the Polygon blockchain, ensuring data privacy and security, and addressing interoperability issues can pose technical challenges that require expertise and careful consideration.

3 Regulatory and Legal Considerations: The healthcare industry is subject to strict regulations and privacy laws, such as HIPAA (Health Insurance Portability and Accountability Act). Ensuring compliance with these regulations and addressing legal considerations when using blockchain technology may require additional effort and expertise.

4 Scalability and Performance: While the Polygon blockchain offers scalability advantages, it is essential to assess and optimize the framework's performance to handle the increasing volume of healthcare data and transactional load. Balancing scalability with transaction speed and resource requirements can be a challenge that needs careful consideration.

5 User Acceptance and User Experience: Introducing a new framework to healthcare professionals, patients, and other stakeholders requires consideration of user acceptance and user experience. Ensuring that the framework is intuitive, user-friendly, and aligns with the workflows of healthcare professionals is crucial for its successful adoption and utilization.

6 Cost and Resources: Implementing and maintaining a blockchain-based framework may involve significant costs and resource allocation. It is important to assess the financial implications, infrastructure requirements, and ongoing operational costs associated with the framework's deployment and maintenance.

7 Network Consensus and Governance: Designing an effective consensus mechanism and governance model for the blockchain network is essential. Ensuring the consensus mechanism is secure, scalable, and decentralized, and establishing governance protocols to manage updates, upgrades, and decision-making within the network can be challenging.

It is important to recognize and address these limitations to ensure the successful implementation and adoption of the scalable framework in the healthcare industry. By considering these limitations, researchers can proactively identify potential challenges and work towards mitigating them effectively.

4.8 Future Scope

1 Expanding into Diverse Healthcare Domains: The framework has the potential to extend its capabilities beyond medical records management. It can be adapted for diverse healthcare domains such as clinical trials management, pharmaceutical supply chain tracking, or health insurance claims

processing. This expansion would revolutionize operations across various areas of healthcare, enhancing efficiency and transparency.

2 Integration with Emerging Technologies: As technology advances, integrating the framework with emerging technologies like artificial intelligence (AI), Internet of Things (IoT), and big data analytics can unlock new possibilities. By leveraging AI algorithms, real-time monitoring of patient health data can be achieved, enabling proactive healthcare interventions. Additionally, combining blockchain with IoT devices can securely capture and transmit vital health information, empowering personalized care.

3 Collaboration and Interoperability with External Systems: Enabling seamless collaboration and interoperability with external systems and stakeholders is crucial. Integrating the framework with existing electronic health record (EHR) systems, health information exchanges (HIEs), and healthcare networks would facilitate secure data sharing and improve care coordination among healthcare providers. This interconnectedness would streamline processes and enhance the continuity of patient care.

4 Strengthening Data Privacy and Consent Management: Future enhancements can prioritize reinforcing data privacy measures and implementing robust consent management mechanisms. Empowering patients with greater control over their health data and enabling granular consent for data sharing and research purposes would enhance privacy protection and build trust between patients and healthcare providers.

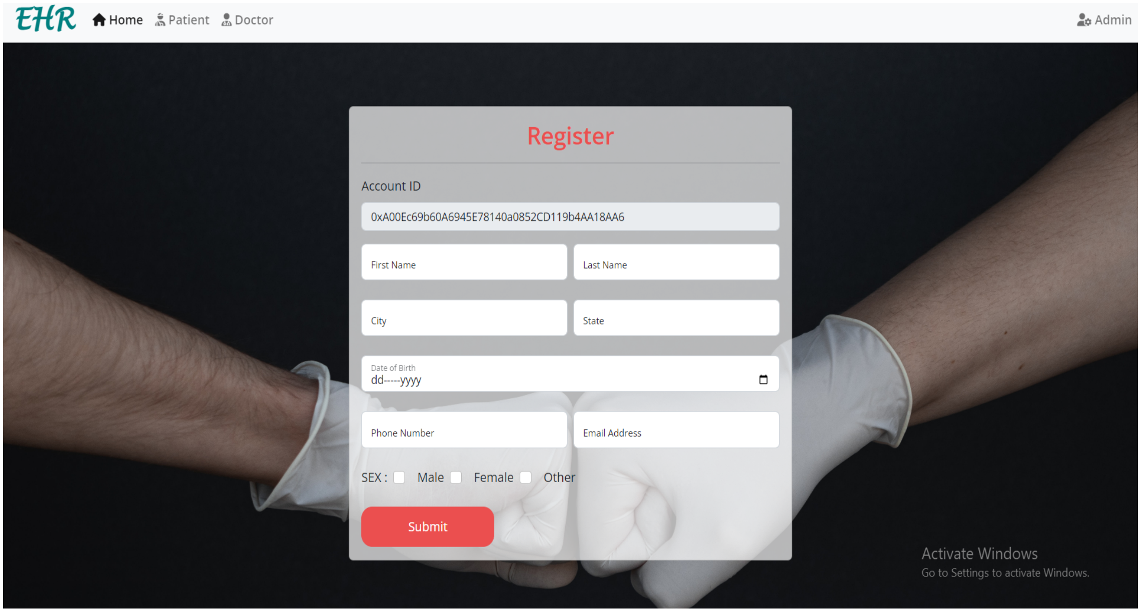
5 Adoption of Standards and Interoperability Frameworks: Aligning the framework with established healthcare standards and interoperability frameworks, such as Fast Healthcare Interoperability Resources (FHIR), would ensure seamless integration with existing healthcare systems. This alignment would facilitate standardized data exchange and interoperability between different healthcare stakeholders, optimizing information flow and improving patient outcomes.

6 Scalability and Performance Optimization: Addressing the growing volume of healthcare data requires continuous scalability and performance optimization. Exploring techniques like sharding, off-chain storage, and network enhancements can boost the framework's capacity to handle increasing transaction throughput and storage demands. This ensures a seamless user experience and efficient data processing.

7 Regulatory Compliance and Governance: To comply with regulatory requirements and instill trust, the framework can incorporate specific healthcare industry regulations, such as the General Data Protection Regulation (GDPR). Additionally, implementing governance mechanisms tailored to the healthcare sector would ensure proper oversight, data security, and adherence to industry best practices.

By pursuing these future scope areas, the scalable framework can evolve to meet the evolving needs of the healthcare industry. It would foster innovation, improve operational efficiency, and ultimately enhance patient care and outcomes.

4.9 Output



Account ID

0xA00Ec69b60A6945E78140a0852CD119b4AA18AA6

Figure 4.4: Front End Of SHSP

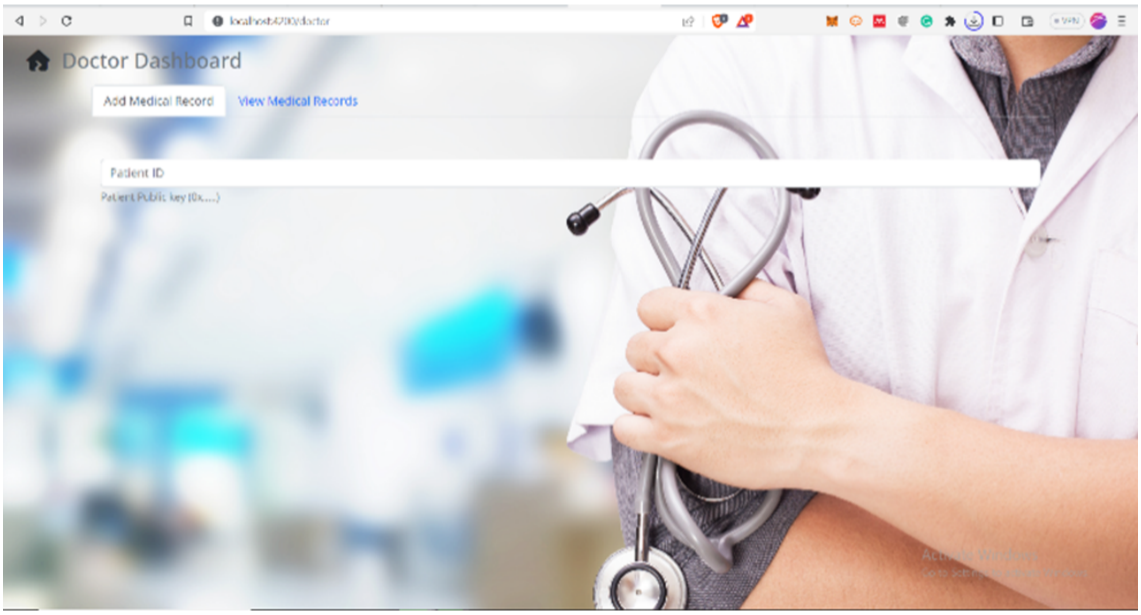
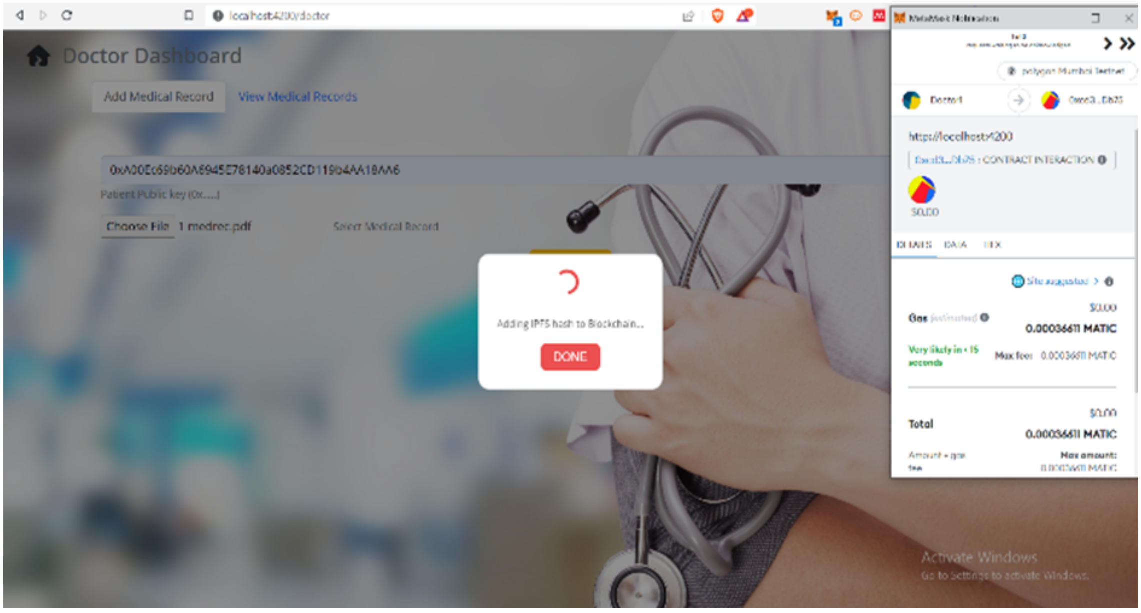


Figure 4.5: Doctor Dashboard



0xA00Ec69b60A6945E78140a0852CD119b4AA18AA6

1 medrec.pdf

Adding IPFS hash to Blockchain...

https://localhost:4200

CONTRACT INTERACTION

$0.00

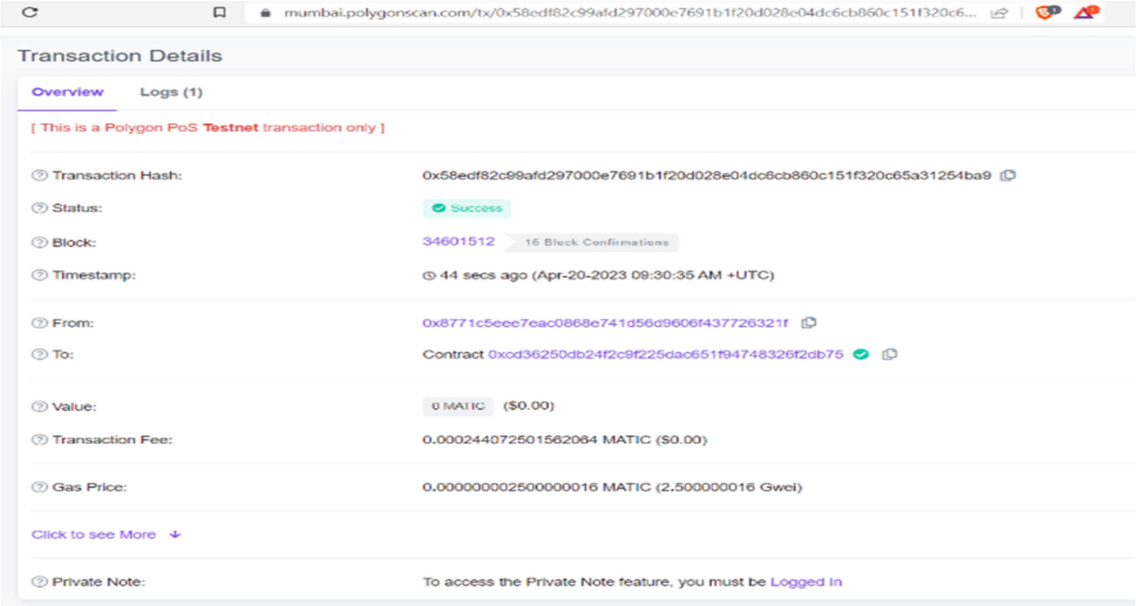
Gas (estimated) $0.00 0.00036611 MATIC

Very likely in < 15 seconds — Max fee: 0.00036611 MATIC

Total $0.00 0.00036611 MATIC

Amount + gas fee — Max amount: 0.00036611 MATIC

Figure 4.6: Doctor Updating Medical Record



mumbai.polygonscan.com/tx/0x58edf82c99afd297000e7691b1f20d028e04dc6cb860c151f320c6...

Transaction Details

[This is a Polygon PoS **Testnet** transaction only]

Transaction Hash:	0x58edf82c99afd297000e7691b1f20d028e04dc6cb860c151f320c65a31254ba9
Status:	Success
Block:	34601512 16 Block Confirmations
Timestamp:	44 secs ago (Apr-20-2023 09:30:35 AM +UTC)
From:	0x8771c5eee7eac0868e741d56d9606f437726321f
To:	Contract 0xcd36250db24f2c9f225dac651f94748326f2db75
Value:	0 MATIC ($0.00)
Transaction Fee:	0.000244072501562064 MATIC ($0.00)
Gas Price:	0.000000002500000016 MATIC (2.500000016 Gwei)

Click to see More

Private Note:	To access the Private Note feature, you must be Logged In

Figure 4.7: Record Uploded And Transaction Completes

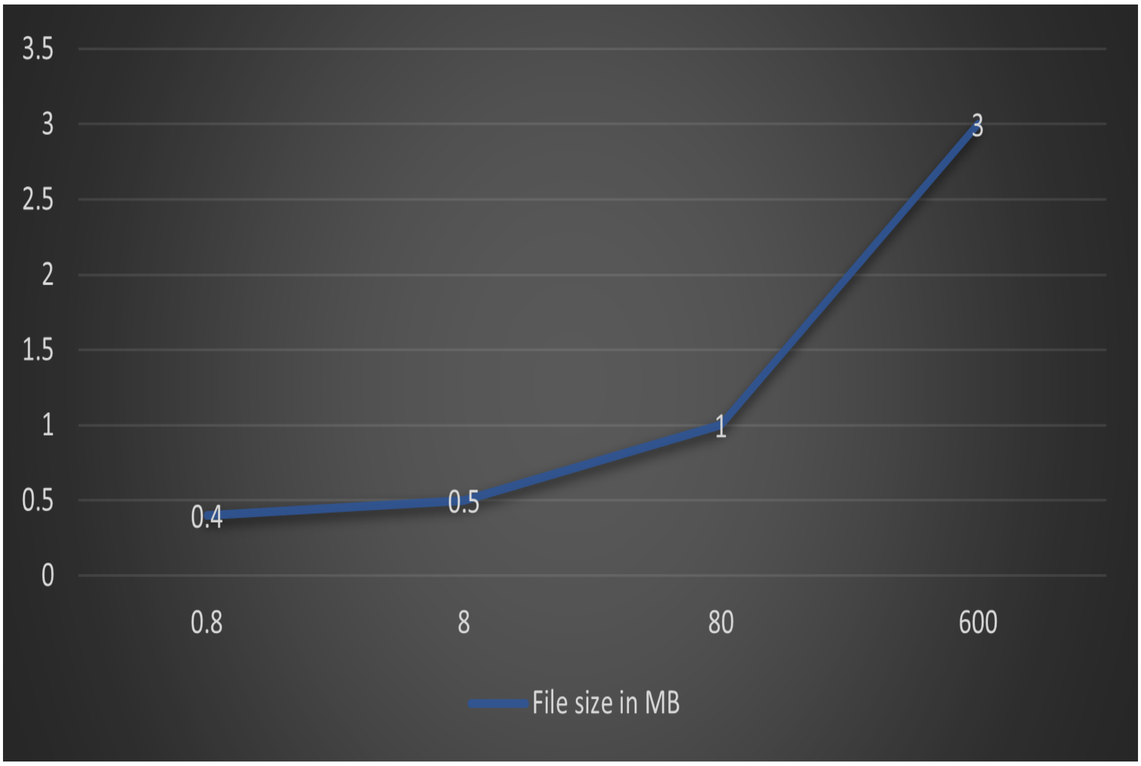


Figure 4.8: Transaction Time Taken W.R.T Record Size

Chapter 5

CONCLUSION

For improved data security, privacy, sharing, and scalability in the healthcare sector, the suggested framework leveraging the Polygon blockchain presents a viable response to the current issues. The framework tackles the scalability issue occasionally associated with BT by, among other things, exploiting the high throughput and low transaction costs of the Polygon blockchain. It utilizes a permissionless structure, which makes it more decentralized, transparent, and open to all organizations and authorities. Our system also includes two-sided verifiability, which makes it a workable option for healthcare data management. Additionally, employing IPFS adds an additional layer of protection and encryption without burdening our network. Data security and integrity are guaranteed by using blockchain as a distributed ledger, and the validation of transactions through consensus processes increases the solution's dependability. By enabling seamless data exchange across disparate stakeholders and assuring scalability to meet the expanding volume of healthcare data, the proposed framework seeks to increase the efficiency and efficacy of the healthcare system. A comprehensive solution to the problems with data security, privacy, sharing, and scalability is provided by the proposed architecture utilizing the Polygon blockchain in the healthcare industry. The Polygon blockchain's high throughput and low transaction fees are used by the framework to successfully address the scalability problems that are frequently present in standard blockchain technologies. Running on a permissionless system, it promotes decentralization and transparency by eliminating the need to rely on certain authorities or organizations. The addition of two-side verifiability enhances the framework's reliability and dependability. This feature lowers the possibility of fraud and ensures the integrity of the network by requiring authentication of both the pinged server and user nodes. The addition of IPFS (Interplanetary File System) enhances security and encryption while keeping the network's effectiveness. IPFS makes hypermedia archiving safe, secure, and resistant to data loss, manipulation, and censorship by utilizing content-based addressing. The suggested system employs blockchain as a distributed ledger, ensuring data security and integrity. The solution's reliability and trustworthiness are further increased by the consensus processes used to validate transactions. The framework promotes collaboration and interoperability throughout the healthcare system by making it simple for different stakeholders to share data. Additionally, its scalability guarantees effective management and processing of the expanding number of healthcare data. Overall, the proposed system, which makes use of the Polygon blockchain, two-sided verifiability, and IPFS, offers a complete response to the problems in healthcare data management. It enables enhanced data privacy, security, sharing, and scalability, which eventually results in more effectiveness and efficiency in the healthcare industry.

REFERENCES

[1] P. P. Ray, Di. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," *IEEE Syst J*, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] A. K. Yadav, Shweta, and D. Kumar, "Blockchain technology and vaccine supply chain: Exploration and analysis of the adoption barriers in the Indian context," *Int J Prod Econ*, vol. 255, p. 108716, Jan. 2023, doi: 10.1016/J.IJPE.2022.108716.

[3] C. De Pietro and I. Francetic, "E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks," *Health Policy (New York)*, vol. 122, no. 2, pp. 69–74, Feb. 2018, doi: 10.1016/J.HEALTHPOL.2017.11.005.

[4] H. Singh *et al.*, "Primary care practitioners' views on test result management in EHR-enabled health systems: a national survey," *Journal of the American Medical Informatics Association*, vol. 20, no. 4, pp. 727–735, Jul. 2013, doi: 10.1136/AMIAJNL-2012-001267.

[5] A. F. Klaib and M. S. Nuser, "Evaluating EHR and health care in Jordan according to the international health metrics network (HMN) framework and standards: A case study of hakeem," *IEEE Access*, vol. 7, pp. 51457–51465, 2019, doi: 10.1109/ACCESS.2019.2911684.

[6] M. Alarjani, M. Alhaider, and H. F. Ahmad, "A Review of Challenges of Block Chain with COVID-19: A Review Paper," *European Journal of Health Sciences*, vol. 8, no. 2, pp. 32–49, Mar. 2023, doi: 10.47672/EJHS.1384.

[7] X. Li *et al.*, "A Quantitative and Qualitative Review of Blockchain Research from 2015 to 2021," *Sustainability*, vol. 15, no. 6, p. 5067, Mar. 2023, doi: 10.3390/su15065067.

[8] R. Natarajan, G. H. Lokesh, F. Flammini, A. Premkumar, V. K. Venkatesan, and S. K. Gupta, "A Novel Framework on Security and Energy Enhancement Based on Internet of

Medical Things for Healthcare 5.0," *Infrastructures (Basel)*, vol. 8, no. 2, Feb. 2023, doi: 10.3390/infrastructures8020022.

[9] C. Wachira *et al.*, "Analysis of user interactions with a digital health wallet for enabling care continuity in the context of an ongoing pandemic," *Journal of the American Medical Informatics Association*, vol. 30, no. 4, pp. 674–682, Mar. 2023, doi: 10.1093/JAMIA/OCAD004.

[10] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services," *Future Generation Computer Systems*, vol. 100, pp. 569–578, Nov. 2019, doi: 10.1016/j.future.2019.05.059.

[11] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[12] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[13] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. Raymond Choo, "DEPARTMENT: Cloud and the Law Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" [Online]. Available: www.computer.org/cloud

[14] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, Jun. 2019, doi: 10.1016/j.future.2018.12.044.

[15] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4. Institute of Electrical and Electronics Engineers Inc., pp. 2292–2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

[16] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *International Journal of*

Medical Informatics, vol. 134. Elsevier Ireland Ltd, Feb. 01, 2020. doi: 10.1016/j.ijmedinf.2019.104040.

[17] J. Xie *et al.*, “A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2794–2830, Jul. 2019, doi: 10.1109/COMST.2019.2899617.

[18] J. Vora et al., “Ensuring privacy and security in E-health records,” in CITS 2018 - 2018 International Conference on Computer, Information and Telecommunication Systems, Institute of Electrical and Electronics Engineers Inc., Aug. 2018. doi: 10.1109/CITS.2018.8440164.

[19] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, Institute of Electrical and Electronics Engineers Inc., Sep. 2016, pp. 25–30. doi: 10.1109/OBD.2016.11.

[20] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[22] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, “Home-based exercise system for patients using IoT enabled smart speaker,” in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services, Healthcom 2017, Institute of Electrical and Electronics Engineers Inc., Dec. 2017, pp. 1–6. doi: 10.1109/HealthCom.2017.8210826.

[23] N. Sultan, “Making use of cloud computing for healthcare provision: Opportunities and challenges,” Int J Inf Manage, vol. 34, no. 2, pp. 177–184, 2014, doi: 10.1016/j.ijinfomgt.2013.12.011.

[24] L. A. Linn and M. B. Koo, “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.”

[25] 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) : 14-16 Sept. 2016.

[26] W. J. Gordon and C. Catalini, “Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability,” Computational and Structural Biotechnology Journal, vol. 16. Elsevier B.V., pp. 224–230, Jan. 01, 2018. doi: 10.1016/j.csbj.2018.06.003.

[27] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, “Blockchain Technology Use Cases in Healthcare.”

[28] Y. Xie et al., “Applications of blockchain in the medical field: A narrative review”, doi: 10.2196/preprints.28613.

[29] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain technology in healthcare: A comprehensive review and directions for future research,” *Applied Sciences (Switzerland)*, vol. 9, no. 9, May 2019, doi: 10.3390/app9091736.

[30] T. L. Tan, I. Salam, and M. Singh, “Blockchain-based healthcare management system with two-side verifiability,” *PLoS One*, vol. 17, no. 4, p. e0266916, Apr. 2022, doi: 10.1371/JOURNAL.PONE.0266916.

[31] A. Al Hussain, M. A. Emon, T. A. Tanna, R. I. Emon, and M. M. H. Onik, “A Systematic Literature Review of Blockchain Technology Adoption in Bangladesh,” *Annals of Emerging Technologies in Computing*, vol. 6, no. 1. International Association for Educators and Researchers (IAER), pp. 1–30, 2022. doi: 10.33166/AETiC.2022.01.001.

[32] U. Chelladurai and S. Pandian, “A novel blockchain based electronic health record automation system for healthcare,” *J Ambient Intell Humaniz Comput*, vol. 13, no. 1, pp. 693–703, Jan. 2022, doi: 10.1007/s12652-021-03163-3.

[33] A. Abbas and Md. A. Hamid, “Adapting hybrid approaches for electronic medical record management and sharing using blockchain sharding,” *Periodicals of Engineering and Natural Sciences*, vol. 11, no. 1, pp. 5–14, Jan. 2023, doi: 10.21533/PEN.V11I1.3405.

[34] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology,” *Multimed Tools Appl*, vol. 79, no. 15–16, pp. 9711–9733, Apr. 2020, doi: 10.1007/s11042-019-07835-3.

[35] I. Yoo, J. Bi, X. Hu, National Science Foundation (U.S.), and Institute of Electrical and Electronics Engineers, *Proceedings, 2019 IEEE International Conference on Bioinformatics and Biomedicine : November 18-21, 2019, San Diego, CA, USA.*

[36] *2019 IEEE Conference on Information and Communication Technology*. IEEE.

[37] J. Vora *et al.*, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," in *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Feb. 2019. doi: 10.1109/GLOCOMW.2018.8644088.

[38] A. P. Singh *et al.*, "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," *IEEE Trans Industr Inform*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.

[39] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, no. 1, Mar. 2021, doi: 10.1016/j.bcra.2021.100012.

[40] A. Kumar Jakhar, M. Singh, R. Sharma, and A. Sharma, "A Blockchain-based Privacy-preserving and Access-control Framework for Electronic Health Records Management," 2022, doi: 10.21203/rs.3.rs-2048551/v1.

[41] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform."

[42] "16 polygon-whitepaper-en".

[43] W. Zou *et al.*, "Smart contract development: Challenges and opportunities Smart contract development: Challenges and opportunities Pavneet Singh KOCHHAR Citation Citation Author Author Smart Contract Development: Challenges and Opportunities," 2021. [Online]. Available: https://ink.library.smu.edu.sg/sis_research

[44] K. Bhosale, K. Akbarabbas, J. Deepak, and A. Sankhe, "Blockchain based Secure Data Storage," *International Research Journal of Engineering and Technology*, vol. 5058, 2008, [Online]. Available: www.irjet.net

[45] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain," in *Proceedings - 2018 IEEE/WIC/ACM International Conference on Web*

Intelligence, WI 2018, Institute of Electrical and Electronics Engineers Inc., Jan. 2019, pp. 704–708. doi: 10.1109/WI.2018.000-8.

[46] J. Xie *et al.*, “A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2794–2830, Jul. 2019, doi: 10.1109/COMST.2019.2899617.

[47] H. T. Vo, A. Kundu, and M. Mohania, “Research directions in blockchain data management and analytics,” in *Advances in Database Technology - EDBT*, OpenProceedings.org, 2018, pp. 445–448. doi: 10.5441/002/edbt.2018.43

[48] S. J. Wang *et al.*, “A cost-benefit analysis of electronic medical records in primary care,” *American Journal of Medicine*, vol. 114, no. 5, pp. 397–403, Apr. 2003, doi: 10.1016/S0002-9343(03)00057-3.

[49] R. H. Miller and I. Sim, “Physicians’ use of electronic medical records: Barriers and solutions,” *Health Aff*, vol. 23, no. 2, pp. 116–126, 2004, doi: 10.1377/hlthaff.23.2.116.

[50] A. L. Terry *et al.*, “Implementing electronic health records Key factors in primary care Implantation du dossier de santé électronique Principaux facteurs pour les soins de première ligne,” 2008.

[51] Y. Liu *et al.*, “A Blockchain-Based Personal Health Record System for Emergency Situation,” *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/4941214.

[52] H. Wang and Y. Song, “Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain,” *J Med Syst*, vol. 42, no. 8, Aug. 2018, doi: 10.1007/s10916-018-0994-6.

PAPER NAME

thesis_content_divya.pdf

WORD COUNT	CHARACTER COUNT
13863 Words	82485 Characters
PAGE COUNT	FILE SIZE
48 Pages	3.3MB
SUBMISSION DATE	REPORT DATE
May 29, 2023 12:56 AM GMT+5:30	May 29, 2023 12:56 AM GMT+5:30

● 3% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 2% Internet database
- Crossref database
- 2% Submitted Works database
- 1% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Small Matches (Less then 10 words)

Divya kuntal <divyakunttall@gmail.com>

Acceptance Notification - IEEE 3rd CONIT 2023

2 messages

Microsoft CMT <email@msr-cmt.org>   Fri, May 12, 2023 at 7:59 PM
Reply-To: Deepak Gupta <deepak_gupta@gibds.org>
To: Divya Kuntal <divyakunttall@gmail.com>

Dear Divya Kuntal

Paper ID / Submission ID : 1113

Title : Blockchain-Enabled Healthcare Records Management: A Survey of Implementation Strategies

Greeting from3rd CONIT 2023

We are pleased to inform you that your paper has been accepted for the Oral Presentation and publication as a full paper for the- “IEEE 2023 3rd International Conference for Intelligent Technologies (CONIT), Hubballi, Karnataka, India with following reviewers’ comment.

All accepted and presented papers will be submitted to IEEE Xplore for the further publication.

Note:
All of Accepted and Presented Papers of CONIT series has been Published by IEEE Xplore and indexed by Scopus and other Reputed Indexing partners of IEEE. - http://inconf.in/index.php/publications/

You should finish the registration before deadline, or you will be deemed to withdraw your paper:

Complete the Registration Process (The last date of payment Registration is
17 MAY 2023)

Payment Links

For Indian Authors: https://rzp.io/l/S8VPeRjlo

For Foreign Authors: https://in.explara.com/e/ieee-conit-2023

(Select Stripe Payment while paying, enter your paper id , title in buyer detail)

Further steps like IEEE PDF xpress and E copyright will be given later once registration is over after the deadline.

Note :

1. Any changes with the Author name, Affiliation and content of paper will not be allowed after acceptance. if not added kindly update in cmt using edit submission option.
2.This is Hybrid Conference, both online and physical presentation mode is available,

The reviews are below.

======= Review 1 =======

*** Relevance and timeliness: Rate the importance and timeliness of the topic addressed in the paper

Gmail

Divya kuntal <divyakunttall@gmail.com>

[COPY] Regarding paper decision

4 messages

ICCS . <iccs@lpu.co.in> Mon, May 1, 2023 at 3:18 PM
To: divyakunttall@gmail.com, dinesh@dtu.ac.in

Dear Sir/Mam,

Greetings from ICCS KILBY 100 conference!

We have reached the final decision regarding your manuscript with ID 1132 to our conference KILBY100 ICCS 2023.

Our decision is to: Accept Submission and it will be submitted to the publication phase.

Submit the camera ready paper on the same mail id. as per the details in Template, Copyright Form and Author Guidelines are available here: https://aip.scitation.org/apc/authors/preppapers

Once you have registered at https://conferences.lpu.in/iccs/RegistrationForm.aspx, please proceed to make the payment as soon as possible and share the proof regarding the same to ensure a successful submission at iccs@lpu.co.in

If you have any queries or require assistance at any stage of this process, feel free to contact us. We will be more than happy to help.

Warm Regards,

Team ICCS

KILBY100

7th International Conference on Computing Sciences 2023

Divya kuntal <divyakunttall@gmail.com> Mon, May 1, 2023 at 4:09 PM
To: ananyaphdit08@gmail.com

[Quoted text hidden]

Divya kuntal <divyakunttall@gmail.com> Tue, May 2, 2023 at 12:28 PM
To: "ICCS ." <iccs@lpu.co.in>

hello sir/ma'am
i want to know that after registration where my paper will published
[Quoted text hidden]

Divya kuntal <divyakunttall@gmail.com> Wed, May 3, 2023 at 7:22 PM
To: "ICCS ." <iccs@lpu.co.in>

[Quoted text hidden]

☎ +918767682587 ✉ conitconf@gmail.com

HOME ABOUT ▾ AUTHOR INFO ▾ SPEAKERS REGISTRATIONS FEES SUBMIT PAPER-DATE EXTENDED

CO

3rd CONIT 2023

IEEE Confernece

Publications

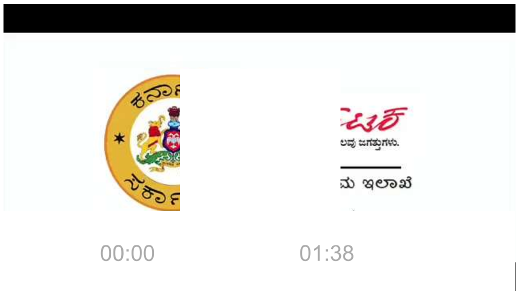
All accepted and presented papers of our previous conference has been published by IEEE Xplore .

Proceedings of 1st CONIT published by IEEE and Indexed in SCOPUS and WOS – https://ieeexplore.ieee.org/xpl/conhome/9497779/proceeding

Proceedings of 2nd CONIT published by IEEE and Indexed in SCOPUS and WOS – https://ieeexplore.ieee.org/xpl/conhome/9497779/proceeding

CONIT 2023

Karnataka



« 📢 Last 3 days to take Admission with Scholarship. Apply Now (https://adm »

ACADEMICS (HTTPS://WWW.LPU.IN/ACADEMICS/) ADMISSIONS (HTTPS://WWW.LPU.IN/ADMISSION/ADMISSIONS.PHP) PLACEMENTS (//WWW.LPU.IN/PLACEMENTS.PHP)

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

ICCS

KILBY 100

7TH INTERNATIONAL JOINT CONFERENCE ON COMPUTING SCIENCES (ICCS-2023)

in association with

Southern Federal University, Russia (https://sfedu.ru/index_eng.php)

Mizan Tepi University, Ethiopia (http://www.mtu.edu.et/)

5TH MAY 2023

CONFERENCE MODE: HYBRID

ONLINE REGISTRATION (REGISTRATIONFORM.ASPX)

SCHEDULE (PDF/KILBY100-TECHNICAL-SESSION-SHEET.XLSX)

KILBY 100 (index.php) ≡

Indexed by Scopus

All accepted papers will be published in Scopus indexed proceedings/Journals.