

MINOR PROJECT-I
A Report On
“COMBINATION OF BLOCKCHAIN AND EHR”

Submitted By
RACHIT PATEL
2K22/SWE/13

MASTER OF TECHNOLOGY
IN
SOFTWARE ENGINEERING

Under the guidance of
Ms. Shweta Meena
Assistant Professor

Department of Software Engineering
Delhi Technological University, Delhi



MAY-2023

DELHI TECHNOLOGICAL UNIVERSITY
SHAHBAD DAULATPUR, DELHI-110042

Declaration

I hereby certify that the work contained in the report titled "**Combination of Blockchain and EHR**" submitted as part of the requirements for the award of the MASTER OF TECHNOLOGY degree in Software Engineering at DELHI TECHNOLOGICAL UNIVERSITY, New Delhi, is an authentic record of my own work completed during my degree under the supervision of **Ms. Shweta Meena**. I have not applied for any other degree or credential with the work that is detailed in this report.

RACHIT PATEL

RollNo:2K22/SWE/13

Date:

Place: New Delhi

Certificate

This is to confirm that RACHIT PATEL (2k22/SWE/13) has successfully completed the minor project titled "**Combination of Blockchain and EHR**" under my supervision as part of the MASTER OF TECHNOLOGY degree in Software Engineering at DELHI TECHNOLOGICAL UNIVERSITY.

Ms. Shweta Meena

Department of Software Engineering

Delhi Technical University

Date

Acknowledgement

I am grateful to Ms. Shweta Meena (Assistant Professor, Department of Software Engineering) and all of the Department of Software Engineering faculty members at DTU. They all gave us a lot of help and advice for the minar project.

I'd also want to thank the University for providing us with the laboratories, infrastructure, testing facilities, and environment that allowed us to continue working without interruption.

In addition, I want to express my gratitude for the assistance and expertise our lab assistants, seniors, and peers have provided.

RACHIT PATEL

RollNo:2K22/SWE/13

Date:

Place: New Delhi

TABLE OF CONTENTS

Title Page-----	i
Declaration -----	ii
Certificate -----	iii
Acknowledgement -----	iv
List of Figures-----	2
List of Tables-----	3
ABSTRACT -----	4
CHAPTER – 1 INTRODUCTION -----	5
1.1 Background -----	5
1.1.1 Blockchain -----	5
1.1.2 Electronic Health Records -----	6
1.1.3 Blockchain and EHR-----	7
CHAPTER – 2 LITERATURE REVIEW -----	8
2.1 Existing System -----	8
2.1.1 Benefits of EHR -----	8
2.2 Current Scenrio -----	8
2.2.1 Stats – Data Leakage of EHR-----	8
2.2.2 Threats on EHR -----	10
CHAPTER – 3 RESEARCH METHODOLOGIES -----	11
3.1 Methodology Used -----	11
3.2 Research Questions -----	11
3.3 Research Goals -----	11
CHAPTER – 4 RESULT ANALYSIS-----	12
CHAPTER – 5 CONCLUSION & FUTURE WORK -----	23
REFERENCES -----	24

LIST OF FIGURES

FIGURE	PAGE	TITLE
FIGURE 2.1	9	HEALTH MARKET SIZE
FIGURE 2.2	10	BREACHES OF DATA
FIGURE 4.1	12	BESURE PROPOSED SYSTEM
FIGURE 4.2	13	BHEEM PROPOSED SYSTEM
FIGURE 4.3	13	MECHAIN PROPOSED SYSTEM
FIGURE 4.4	14	MEDBLOC PROPOSED SYSTEM
FIGURE 4.5	15	MEDBLOCK PROPOSED SYSTEM
FIGURE 4.6	15	MEDSAFE PROPOSED SYSTEM
FIGURE 4.7	16	MEDSHARE PROPOSED SYSTEM
FIGURE 4.8	17	SWAASTHYA SAMPATHEEPROPOSED SYSTEM
FIGURE 4.9	17	BIIMED & HIS PROPOSED SYSTEM
FIGURE 4.10	18	SEFRA PROPOSED SYSTEM
FIGURE 4.11	19	MEDREC PROPOSED SYSTEM
FIGURE 4.12	19	PROVCHAIN PROPOSED SYSTEM
FIGURE 4.13	20	MEDICHAIN PROPOSED SYSTEM

LIST OF TABLES

TABLE	PAGE	NAME
TABLE 2.1	9	DATA BREACHES IN 2022
TABLE 4.1	20	RESULTS OF PROPOSED MODELS

Abstract

The healthcare system around the world are facing tough challenges in maintaining and running their workflow in an efficient and orderly manner. Due to the sudden rise in healthcare data in today's world specifically after the outbreak of the covid 19 epidemic, the enhancement of the health system to manage the large amount of data generated is the top priority. This massive amount of data if not handled and analyzed effectively can lead to a situation where data is of no use and could result in supply chain malfunctioning in healthcare system. The main issues that arise in such situations are firstly the integrity of the data, secondly the sharing of the data from one platform to another in a safe and secure environment which means data interoperability and thirdly data accessibility which means the data should be easily accessible when needed after proper authentication only. To solve these issues the concept of using Electronic health records (EHR) arises with the combination of Blockchain technology, as these two technologies could address all the above three issues faced in handling private data efficiently and also could provide many other perks and benefits.

Currently, many organizations and developing countries are using the EHR system for storing their healthcare data for their citizens but the problem arises that all this data is still stored in the centralized based storage system either it may be a centralized server or it may be a remote cloud storage. Reliability on this centralized third-party storage is not a good choice as these centralized storages are prone to security attacks that could lead to data leaks or illegal data updation or alteration. To overcome this problem concept of blockchain was acceptable with the combination of EHR in the healthcare world so that the data so stored in the network is not in control of any single centralized third party as blockchain-based networks are decentralized and distributed and on the other side it also solves the issues of data privacy, data sharing, and data accessibility. In the last few years, blockchain-based networks have overpowered the current ongoing approaches of the network because of its feature of security, peer-to-peer transaction, and decentralized distribution of peer and anonymous contents and properties.

Chapter 1

INTRODUCTION

This chapter provide a brief introduction about the latest and highly demanded technology that is blockchain technology and Electronic Health records concepts and how the combination of two would work for increasing the security of the sensitive medical records.

As we are moving towards more and more digitalization large amount of data is also generated that needs to be stored and analyzed in safe and secure surrounding. Data and information in today's world is considered as the most important assest even more valuable than a collection of gold. And if the data is of the healthcare system the significance of the data to be protected increases by many folds. A large amount of GDP in any developing country is spent only on the healthcare department which includes both developing the health system and also developing the measures to protect the data so generated from the healthcare systems. Due to the rapid growth and enhancement large amount of data is gathered and stored. The current EHR systems are not capable of handling this type of massive crucial data as they lack is security there is no transparency in the system which results in a situation where there is no trust between the parties and also because are more susceptible to the cyber attacks that could alter and manipulate the data.

To overcome this serious problem the combination of two technologies blockchain and EHR are used. EHR contains all the information about the person's medical history, medical insurance details, prescriptions, etc. Secondly, blockchain is the technology that provides the concept of decentralization and distributed network that is not controlled by any single authority as done in centralized networks. Handling EHR and its sensitive data demand a technique that should be effective in protecting its integrity and also should provide an easy-to-access environment for authenticated users, this is where the concepts of blockchain come in to play as they fulfill all the requirements efficiently.

Current research on blockchain and healthcare is scarce, but the technology is poised to transform the current healthcare system by enhancing patient information security and accessibility. This would effectively overturn the current healthcare hierarchy and create a new system where patients are in charge of managing their own care.

1.1 Background for the technologies

1.1.1 Blockchain

Blockchain is one of the biggest technology innovation of the current century that have its application in almost every sector of the industry in the society like banking,education,financial and security . Blockchain is responsible for revolutionizing many industries due to its application and features like high degree of security and tamperproofing.Industries that are highly benefited by this technology are banking sectors, heathcare sector and education sector.

The blockchain technology is expected to change and revolutionized the way of performing the transaction in the world . It will shift the world for a centralized based network to a peer to peer decentralized network that is more secure and tangible

Blockchain is a network that is shared, immutable ledger that make facilitates the process of recording transactions and tracking of data and information in a network. An asset can be tangible like real estate, automobile , digital cash, house or intangible like intellectual patents, copyrights of product,idea or branding. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

1.1.2 Electronic Health Records

As the name implies, electronic health records are computerized collections of patient information, including medical history, medication information, insurance information, and other relevant information. EHR, commonly referred to as electronic medical records, is simply the digital equivalent of the patient's paper chart. The information gathered might be in the form of .jpeg,.png, .pdf or any format that could result in the collection of data.

The primary goal of transferring patient data from a paper-based, conventional method to this digitalized EHR system is to provide the accessibility of the data instantly in a hassle free manner wherever and whenever needed. Another benefit of these systems is that they instil a sense of security in the system because no one can access a patient's private information without proper authentication. The issue the non-EHR system where facing was first, whenever the patient is transferred from one hospital system to another the transfer of data of the concerned patient was the issue as it would be a time-consuming process, and secondly was that due to this time-delay in data transfer the patient health be got affected as he or she would not get proper treatment for the time data is transferred and lastly the major problem was of data security, the traditional medical databases lack security they are quite prone to data leak or any cyber attack that could result in loss of sensitive information like patient's medical history and also could result in illegal alteration of data that might be fatal for the patient health.

The primary responsibilities of any medical system are data confidentiality, data integrity, and lastly, data availability and accessibility. All these three features are effectively accomplished by the EHR systems by utilizing properly designed software to build and manage these EHR systems inside the organization. This appropriate methodical working makes it possible to properly analyze the data, which aids in the creation of timely and improved medical programs for the patient's benefit. Hence maintaining patient medical records improves productivity and lowers error rates also the EHR aids in giving patients a thorough medical history. There should be systems in place for exchanging medical information with other departments and organisations.

EHR has various benefits, including improving patient care and automating numerous processes for the business. They also make it possible for doctors to communicate with one another remotely and in real-time, ensuring that any professional working with a patient has access to a current, accurate, and comprehensive file. Additionally, they are very configurable and may be set up to meet the needs of your medical practice.

1.1.3 Blockchain and EHR

EHR contains data that is vital and extremely sensitive as it contains complete information about the patient's medical history, medical insurance details, medicines taken, and all other necessary information and this data should be handled in safe and secure environment. That's why if there is a data breach or an unauthorized manipulation of the sensitive data included in EHR, it may result in a situation that is unavoidable and may occasionally result in loss of life and financial resources. The majority of EHR data in the current era of digitization is also housed in centralized storage systems, making them extremely insecure and providing an easy access point to private information because these systems lack the necessary security. And if the security measures established are adequate, then also the patient's private data is under the authority of some other third party that could be accessed by them directly or indirectly.

Therefore, the combination of EHR and blockchain is the best option for solving all the problems mentioned above because it offers a system where patient data is stored in a well-organized and systematic way, and on the other side, the blockchain network gives it security, privacy, accessibility, and a feeling of transparency to the users. This approach, is effectively addressing the three main security concerns of any security system that are namely data integrity, data confidentiality, and data availability.

Managing the pharmaceutical supply chain and preserving patient data are just two uses of blockchain technology that the medical sector is already making use of. This system can maintain an unaltered, decentralised, and transparent record of patient data, making it the perfect tool for the medical sector. Transparency and accountability of data are major concerns in this type of data since they are essential for sharing the data. Blockchain technology and its fundamental ideas address these issues by maintaining a DLT. Blockchain is ideally suited for managing health care data due to its emphasis on distribution, sharing, and encryption.

Chapter -2

LITERATURE REVIEW

2.1 Existing System

India, a country of more than 1.3 billion individuals, needs a healthcare infrastructure that enables the efficient and secure processing of each person's health data. India's population is diverse in terms as geographic location, socioeconomic status, language, religion, and heritage. The Indian government has demonstrated its commitment to achieving UHC by 2030 through the introduction of the National Health Protection Scheme (NHPS) under the "Ayushman Bharat Yojana."

2.1.1 Benefits of EHR:

EHR also makes sure that a lot of medical records are accessible at once, which can be utilised to create machine learning algorithms and forecast better patient recommendations. Since everyone with access rights may view a patient's whole chart using an EHR, there is less chance of making assumptions about their medical history and consulting with several specialists. Any patient can receive emergency care more effectively by reviewing EHRs from any location.

- Automate and enhance the provider workflow.
- Data can be created and managed by approved vendors.
- Kept in a digital format that can be sent across several entities.
- Share information with businesses like labs, consultancies, imaging centres, pharmacies, ERs, and clinics at work and in school.
- Raises standards of care; improves diagnostic skills and patient outcomes.
- Giving patients complete, accurate, and current information that is needed for treatment instantly.
- Securely sharing the patient's medical electronic data with respected patients and other authorized medical professionals.
- Assisting medical professionals in safer care, medical error reduction, and patient diagnosis by using the data and its analysis.
- Interoperability, as when the patient wishes to change his/her medical professional his data now could be transferred easily and in a secure manner.
- Increasing efficiency and accessibility of data by utilizing the dedicated software for building and maintaining the EHR systems results in the proper handling of data and also easy access due to its workflow.
- This also results in an increase in revenue due to the increasing sense of security in the system patient starts building trust in the organization for their data and hence the revenue increase due to the increase in patient count in the organization.

2.2 CURRENT SCENARIO FOR BLOCKCHAIN EHR USAGE TRENDS

2.2.1. STATS-DATA LEAK AND CYBER CRIME ON EHR

EHR contain a patient's name, medical history, insurance information, financial information related to the purchase of medications, present and past addresses, background information regarding their

health, and names of heirs and family members. This makes EHR a target for hackers who want to obtain wealth of information and use it to their advantage.

- With a 74% increase from 2021 to an average of 1,463 attacks per week, the healthcare sector saw the largest percentage increase in weekly cyberattacks of any industry sector worldwide according to the HIPAA journal posted on January 10 ,2023 .
- 5,150 healthcare data breaches involving 500 or more records have been reported to the HHS Office for Civil Rights between 2009 and 2022. 382,262,109 healthcare records were exposed or improperly disclosed as a result of such breaches.
- A study conducted by the regional cybersecurity think tank CyberPeace Foundation found that from January to November of the year, there were around 1.9 million assaults targeting the healthcare sector in India. According to the CPF study, the bulk of assaults targeted internet-facing systems running out-of-date Windows server designs, supporting the remote desktop protocol, with server message block and database services enabled.

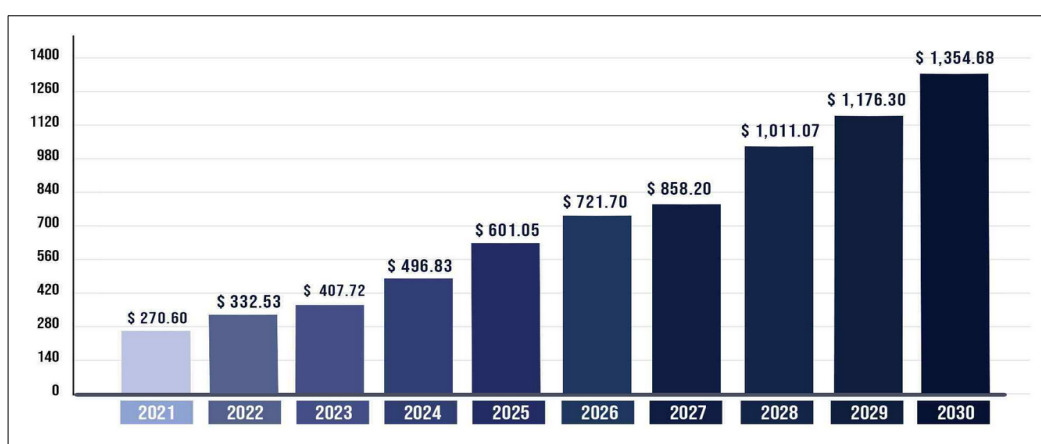


Figure 2.1 : Digital Health Market size ,2021 to 2030

- A study has shown that by 2020, the amount of medical data will double in 73 days. 80% of the data surrounding the healthcare is in an unstructured format
- 10 Largest healthcare data breaches in year 2022

Company Name	Data Breaches (in millions)
OneTouchPoint	4.11
Eye Care Leaders	3.6
Advocate Aurora Health	3
Connexin Software	2.2

Shields Health Care Group	2
Professional Finance Company	1.91
Baptist Medical Center/Resolute Health in Texas	1.71
Community Health Network	1.5
Novant Health	1.36

Table : 2.1 : Data breaches in 2022

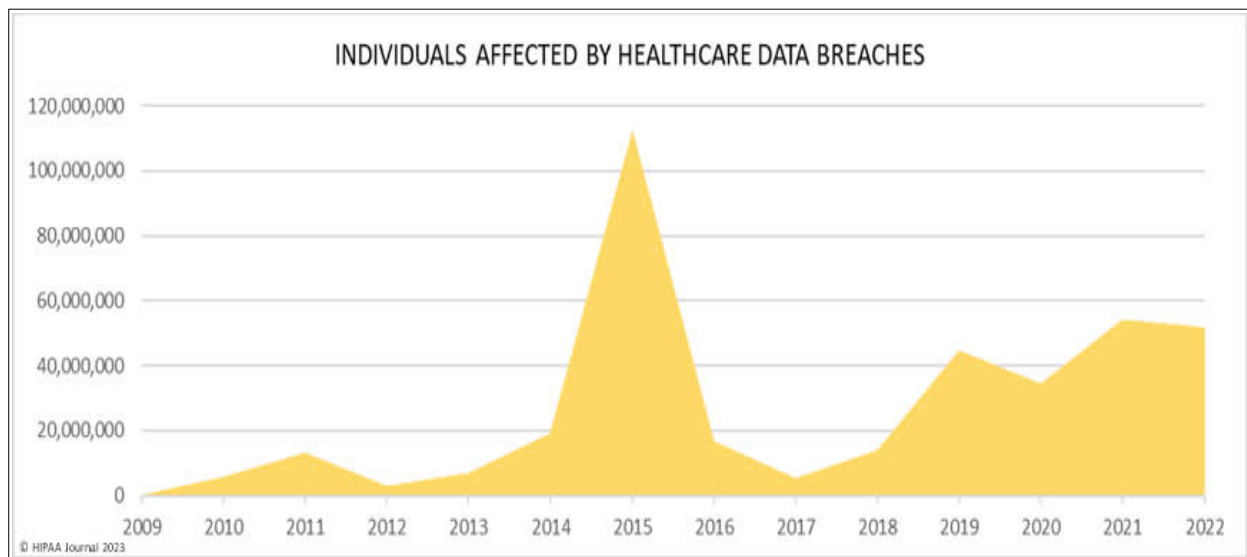


Figure 2.2 : Data breaches on Healthcare Data(2009-2022)

2.2.2 THREATS TO EHR

- Leakage of EHR data's contents. The cloud server can extract information about the contents of EHRs using the related keys and the ciphertext of the EHRs. The doctors can ask to see EHRs that were made later or have nothing to do with the consultation at hand.
- Attacks on the provenance record through forgery and removal. The doctor may alter or delete outsourced provenance records in order to profit by working together with the cloud server.
- Attacks on the provenance record are rejected. A doctor may contest the fact that he created some provenance documents.

Chapter - 3

RESEARCH METHODOLOGIES

This chapter provides the description about the methodology that was followed for conducting the required review study.

3.1 Methodology used

The systematic literature review is one of the primary areas of study for research methodology. In order to conduct this study, we adhere to SLR standards as well as the PRISMA guidelines for reporting items for systematic reviews and meta-analyses.

For doing the following review a data set of 13 papers have been selected from the recognized databases like IEEE Xplore, Science Direct, ACM etc.

3.2 Research Questions

Following are the research questions are main core for the research findings .

RQ1: What are the different proposed systems that are ready for real time implementation?

- To identify all the proposed systems and features of the system that could be implemented in real-time soon using concepts of Blockchain and EHR.

RQ2: What are the different frameworks of EHR and Blockchain?

- To identify the current ongoing researches and proposed frameworks for the EHR using blockchain concepts.

RQ3: To what extent the combination of EHR and Internet of things and cloud storage are evolved and its benefits.

- To identify the advancement of EHR using the abilities of the current ongoing technology of IOT, cloud storage and computing backed with concepts of blockchain.

3.3. RESEARCH GOALS

This research aims to analyze the existing studies, standards, tools, and techniques in realizing EHR based proposed models and frameworks with the further combination with ethereum, IOT and cloud based technologies. Also EHR management in the areas of focus, i.e. EHR data storage, data integrity, data privacy and data security.

CHAPTER – 4

RESULTS ANALYSIS

This particular chapter provides a brief analysis about the various proposed frameworks and models that are been selected in the inclusion principle that was designed for this review study.

4.1 BESURE : Cloud-Assisted eHealth System [7]

In this paper the authors have looked into genuine and real time based cloud-assisted eHealth solutions in there research. They have suggested a blockchain-based secure data provenance method for eHealth systems as well as a password-based subsequent-key-locked encryption technique to guarantee the privacy of EHRs. Based on the two techniques, developed BESURE and proved that it is both efficient and secure. The testing of the performance for the product was done using the experimental approach in which they have successfully achieved the desires results for proving there product to be effective and secure for solving the issue of data privacy and integrity in current EHR systems.

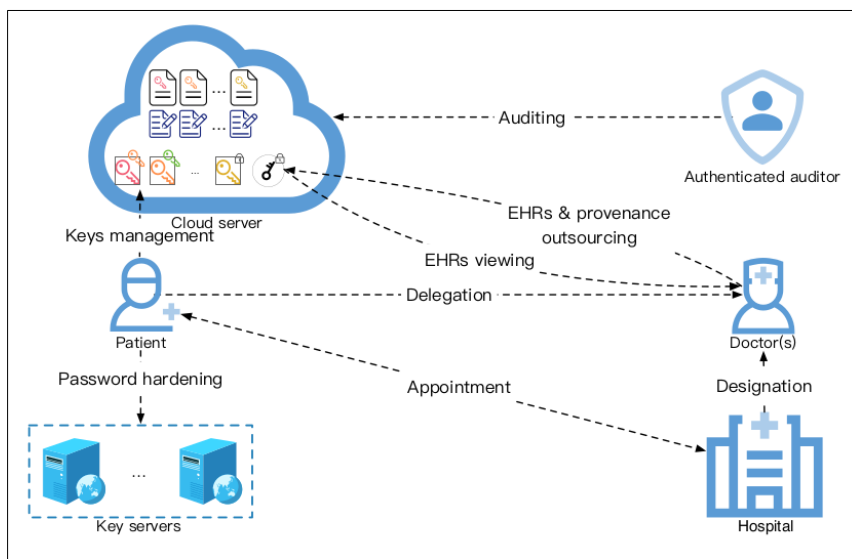


Fig 4.1 : Shows the proposed model for BESURE model

4.2 BHEEM : Framework for Securing Electronic Health Records [8]

In there research paper the authors ,have suggested a Blockchain-based framework for effective EHR storage and upkeep. Additionally, there proposed system for maintenance offers patients, providers, and third parties efficient, secure access to medical data while protecting patient privacy. The purpose of there research is to examine how the architecture they offer satisfies the interests of patients, providers, and third parties while maintaining privacy and security issues in the healthcare 4.0. However, the suggested framework still offers significant privacy protection and data integrity by using smart contracts to partition information, despite the fact that it would be extremely unlikely to completely conceal all information while keeping an accessible and interoperable system.

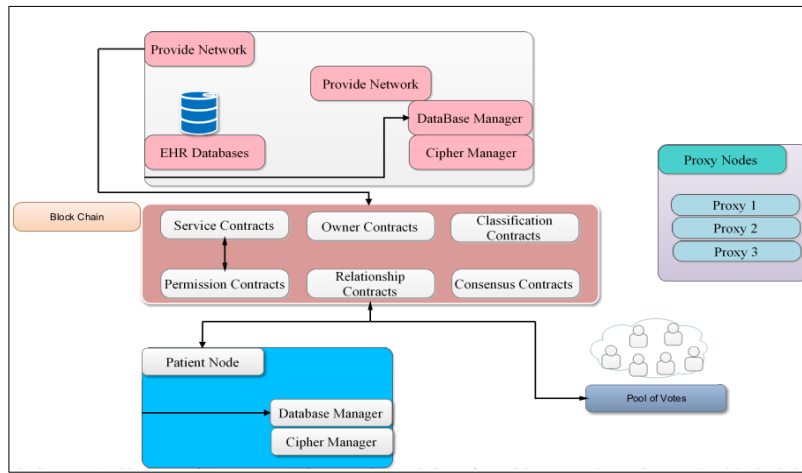


Fig 4.2 : Shows the proposed model for BHEEM EHR maintenance model

4.3 MECHAIN : A Multilayer Blockchain Structure [9]

The authors in the paper have provided a system as a solution to the problems associated with integrating blockchain technology into hierarchical EHR systems, they present MEChain (proposed framework) in their paper. MEChain is a multi-layer blockchain topological structure for secure EHR system. The fundamental idea behind their strategy is to divide nodes into two types: first complete and second semi-nodes according to different health organisation scales. To manage and relay the requests from the semi-nodes, they have constructed a multi-layer system and deployed a semi-leader for handling and transmitting requests. They also offer a novel hierarchical consensus algorithm that is tailored for the hierarchical structure and guarantees security on both tiers and above all it also reduces the expenses and wait times involved in request confirmation. The system also provides a real-time verification technique, a periodic verification mechanism, and a data storage mechanism to reduce storage costs while ensuring data security in order to guarantee data integrity. **ADVANTAGE-** The findings demonstrate that our system has good throughput, minimal communication overhead, short confirmation latency, and low storage cost.

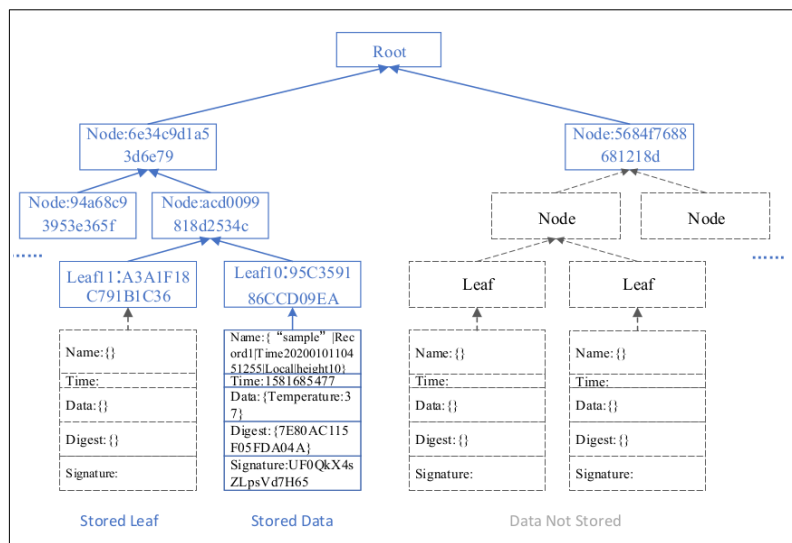


Fig 4.3 : Shows the proposed multi layer model for EHR system : MECHAIN model

4.4 MEDBLOC : EHR system for sharing and accessing medical data [10]

The author in this paper have introduces MedBloc, a blockchain-based shared EHR system as a solution that attempts to connect New Zealand's dispersed and diversified health IT landscape and can address many of the problems with the country's current healthcare system. They have successfully and effectively showed that MedBloc is a completely, user-driven, shared EHR system that makes it simple for both patients and medical professionals to access and exchange health records through a client-focused service. Patients can provide and withdraw consent at any time by using smart contracts and cryptographic techniques. Where on the other side healthcare practitioners can obtain consent and provide records that are encrypted and securely stored on the blockchain after proper authentication. With the help of its strong encryption system, the proposed system MedBloc also safeguards the privacy of its patients. The immutable access control limits imposed by MedBloc prevent any unauthorised acts from being carried out.

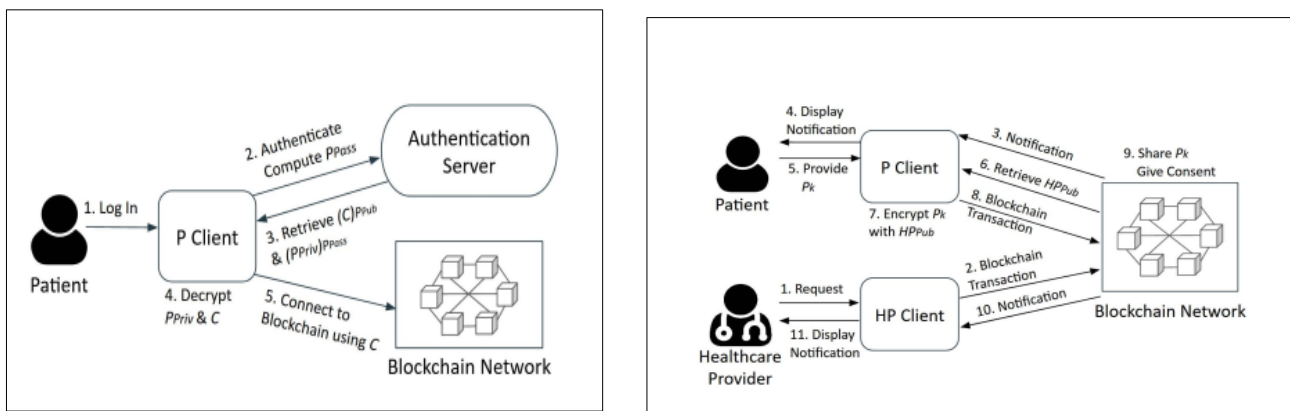


Fig 4.4 : Shows the proposed patient's authentication model and proposed sharing network

4.5 MEDBLOCK : An AI-enabled and Blockchain-driven Medical Healthcare System [11]

In there paper, the authors put forth MedBlock, a cutting-edge EHR maintenance architecture powered by blockchain and Artificial Intelligence . It enhances the effectiveness of conventional EHR systems and appears to have promise for use as a reliable EHR upkeep and maintainance solution in the midst of the COVID-19 pandemic. They have highlighted the security, privacy, trust, reliability, and data storage cost challenges with the cloud- and blockchain-based EHR system and provide insightful information about them. They have also demonstrated how incorporating AI methods can help build a reliable EHR maintenance system. They also go through the benefits of integrating IPFS with blockchain technology. Data storage is reliable and economical as a result for the proposed system in the papaer . They emphasise how the 6G network's enhanced EHR maintenance system efficiency and real-time information transfer capabilities would be particularly beneficial in a scenario like the COVID-19 pandemic. The effectiveness of the EHR maintenance architecture is then highlighted and made a topic worth discussing as it can lead to major concerns and issues if not treated effectively.

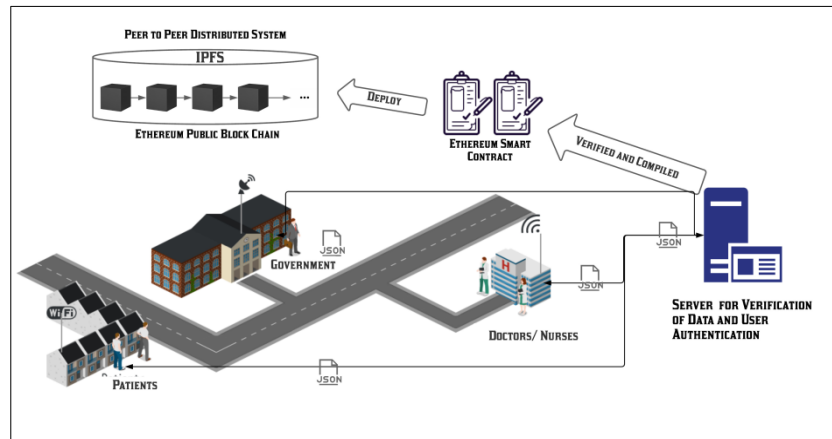


Fig 4.5 : Shows the proposed model for AI enabled MEDBLOCK model

4.6 MEDSAFE : Blockchain based EHR System [12]

In this research paper, the authors have looked at how blockchain technology could benefit the healthcare industry and could be applied and combined to electronic health records. Despite progress in the healthcare sector and technical improvements in EHR systems, they encounter the number of obstacles that blockchain, a unique technology, was able to get beyond and could also provide a needed solution based on its core principles. The authors have also demonstrated how to make granular document access controls changes in order to get secured document storage as a result. Customers will therefore find the system easy to use and understand. Additionally, because IPFS uses off-chain storage, the architecture is further safeguarded to make sure that the system handles the problem of data storage and data integrity in a secure and effective manner. Furthermore, by restricting access to medical records to individuals who are reliable and connected, role-based medical record access enhances the system and solves all the problems related to data storage, data integrity and reliability.

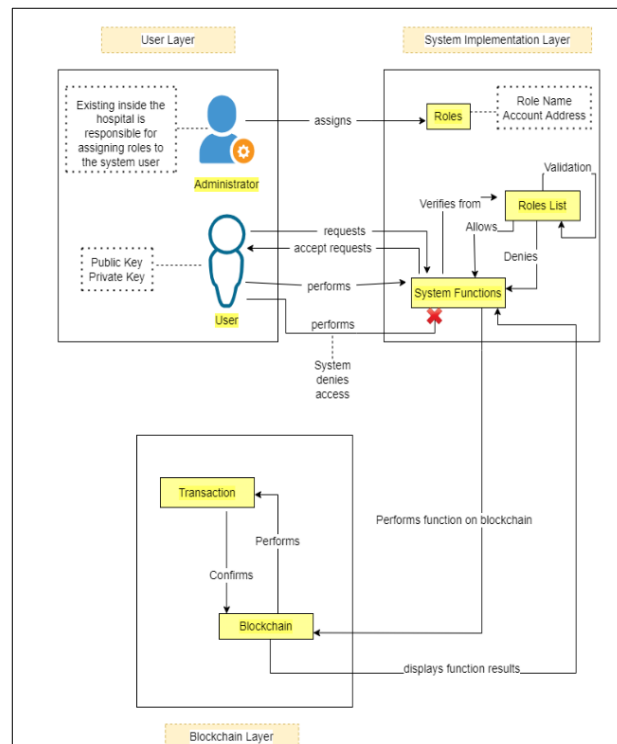


Fig 4.6 : Shows the proposed model for MEDSAFE model

4.7 MEDSHARE : A Privacy-Preserving Medical Data Sharing System [13]

In this paper, the authors have propose system called MedShare, a novel blockchain-based EHR sharing system with granular access control. In order to safeguard EHR privacy and search secrecy, they have develop and implemented a new design to generate encrypted indexes that are uploaded to smart contracts. MedShare make use of advantage of a constant-size ABE approach to protect data privacy and offer fine-grained access control on the blockchain. The proposed system also demonstrate how to create search tokens, create encrypted EHR indexes, and do effective multi-keyword boolean searches on a blockchain platform with effective and accurate search results. The authors offer a complete security analysis to demonstrate that there suggested system can safeguard the secrecy of both indexes and search tokens in order to demonstrate the security guarantee. Finally, in order to assess the viability and effectiveness of MedShare, a system prototype is created and deployed on Ethereum. Hence in this proposed system combination of EHR , ethereum and blockchian concepts are used.

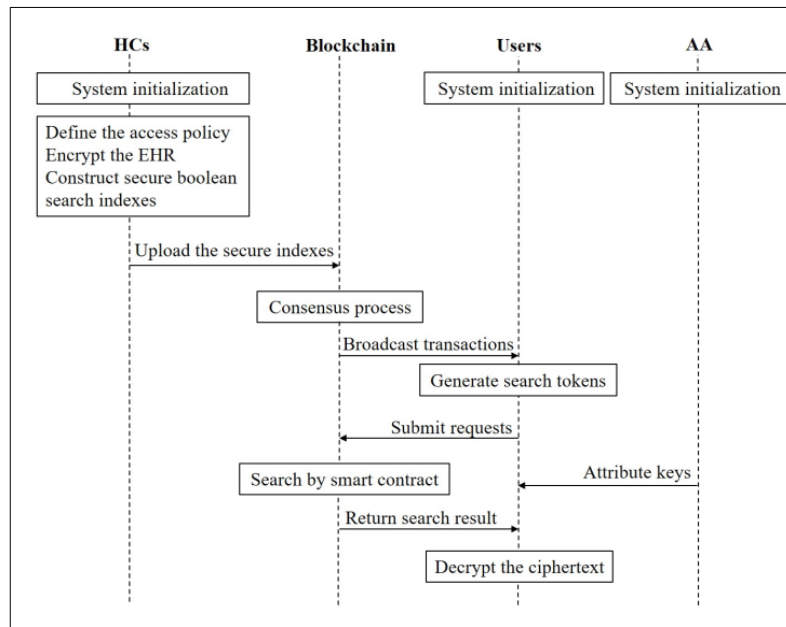


Fig 4.7 : Shows the proposed model for MEDSHARE model

4.8 Swaasthya Sampathee : Blockchain based EHR Framework [14]

In this paper, Swaasthya Sam-pathee, a blockchain-based EHR, is proposed by the authors. In Swaasthya Sampathee, the system tackles the security difficulties that are faced in conventional EHR storage and management. In this system the EHRs are saved on IPFS network and the hash of the data is maintained on an Ehereurm's Ropsten test blockchain. The patients in this case are the records' owners and have total access control over them. Additionally, data security and record immutability are enforced through the use of smart contracts for granting and revoked access authorization. In order to deliver high-quality patient services, the authors intend to implement the defined standards needs as per the Indian Public Health Standards (IPHS-2022) in future work.

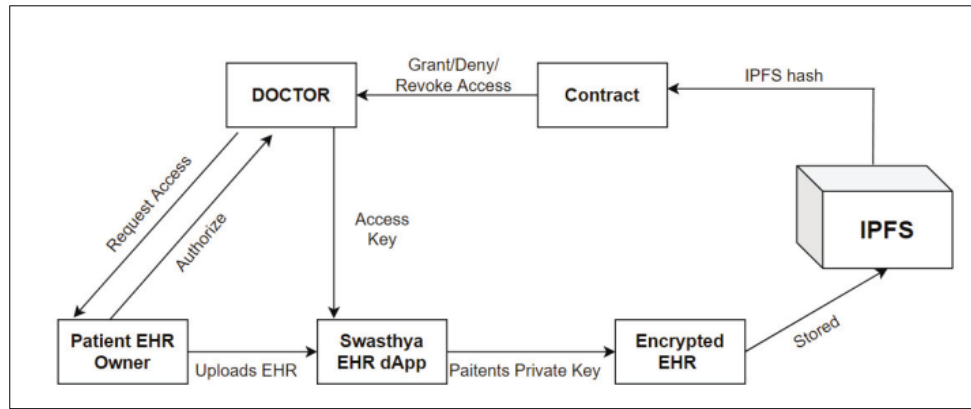


Fig 4.8 : Shows the proposed model for Swaasthya Samapath using IPFS storage model

4.9 BiiMED and HIS [2]

This paper the authors introduces BiiMED, a Blockchain platform for improving data interoperability and integrity with reference to EHR exchange and sharing of sensitive data. The suggested remedy is activated a smart contract prototype on Ethereum's Testnet using its access management system, BiiMED enables EHR sharing between healthcare providers and guarantees data integrity with a decentralised Trusted Third Party Auditor (TTPA). The Health Information System (HIS) also monitors the interactions between various medicinal drugs. The system was put to the test in terms of Turing-complete operations, scalability across large patient populations, user identity and authentication, structural interoperability at the bare minimum, and cost-effectiveness. The results of the test demonstrate how much better data integrity and interoperability BiiMED can provide. According to the authors, the goal of this proposed system was to lay the groundwork for future research aimed at creating a decentralised EHR management system that would use Blockchain technology to guarantee data sharing between healthcare facilities and ensure confidentiality, authentication, and encryption.

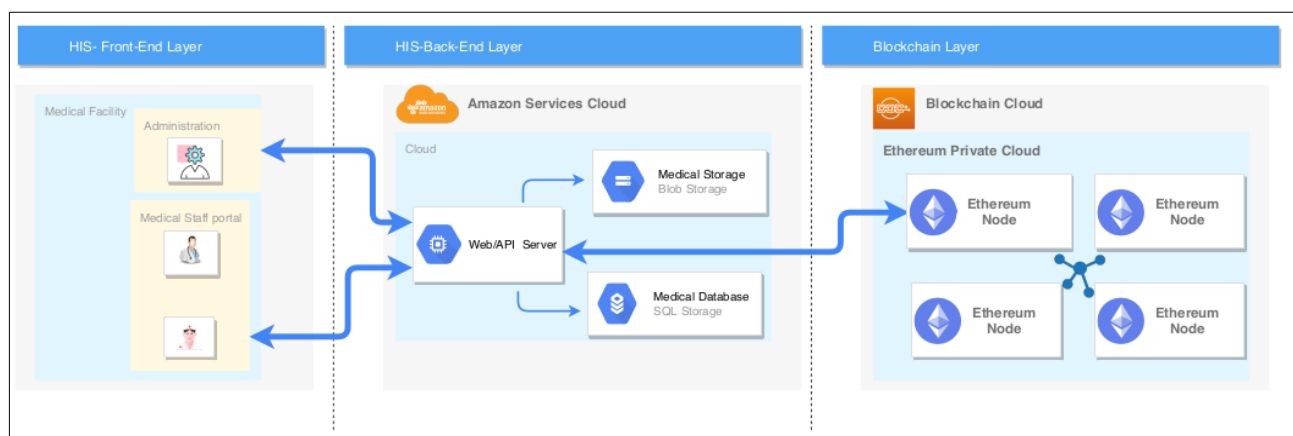


Fig 4.9 : Shows the proposed model for BiiMed and HIS models

4.10 SeFra : Security Algorithm for IoT in Healthcare [3]

The authors of this paper have proposed a system named SeFra .This research proposal focuses on the Secure framework (SeFra), which was created using a progressive temporal blockchain and is meant to increase the security of the electronic health record. Increasing user confidence on data integrity and authentication, confidentiality, and auditability in eHealth systems systems was the main goal of this investigation . The suggested method, which makes use of temporal aspects, facilitates interoperability while addressing scale issues. Context-based and temporal characteristics are used to protect electronic health records in this system. Before each record was treated to a potent hash function, the temporal property was attached to each one. A high level of security is thus ensured. Each record had the temporal property appended to it before being run through a robust hash function. High security is ensured by doing this. In order to test the Blockchain, we chose the dBFT consensus algorithm as the system's consensus mechanism.

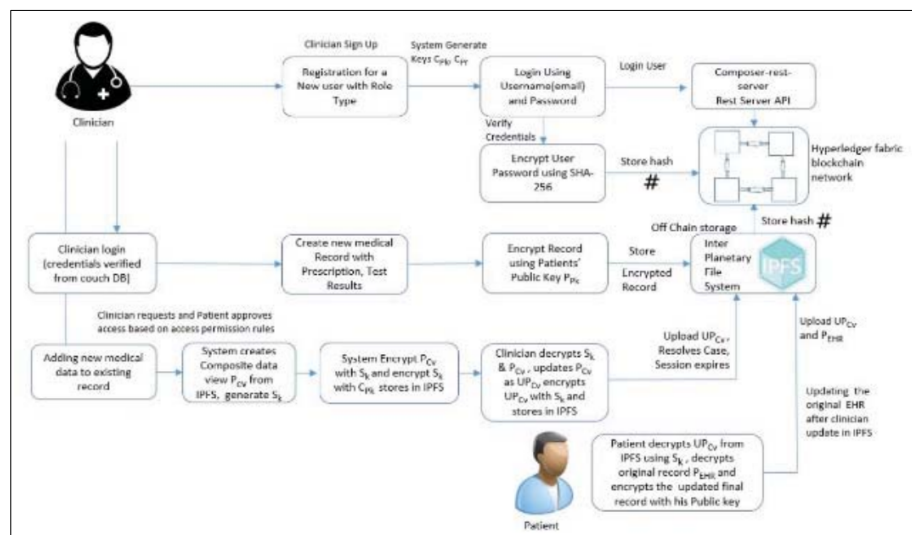


Fig 4.10 : Shows the proposed model for SeFra Framework

4.11 MedREC : EHR Management System [4]

The authors in their paper have proposed a process named, MedRec . In which they demonstrated how decentralisation concepts may be applied to massive data management in an EHR system by utilising blockchain technology and method for managing medical records that offers accessibility, interoperability, and auditability via a detailed log. MedRec, which was created with record flexibility and granularity in mind, encourages medical researchers to maintain the system by allowing patient data sharing. The MedRec system takes on tough problems such system compatibility, slow access to medical data, and growing data prominence and extent. The blockchain's Smart Contract record includes information about permissions and data access reclaim. A new patient record can be created by a medical expert with a few functions. A unique ID, such as a name or SSN, is used to identify each patient record. Each patient record has a public-key cryptographic ID associated with it.

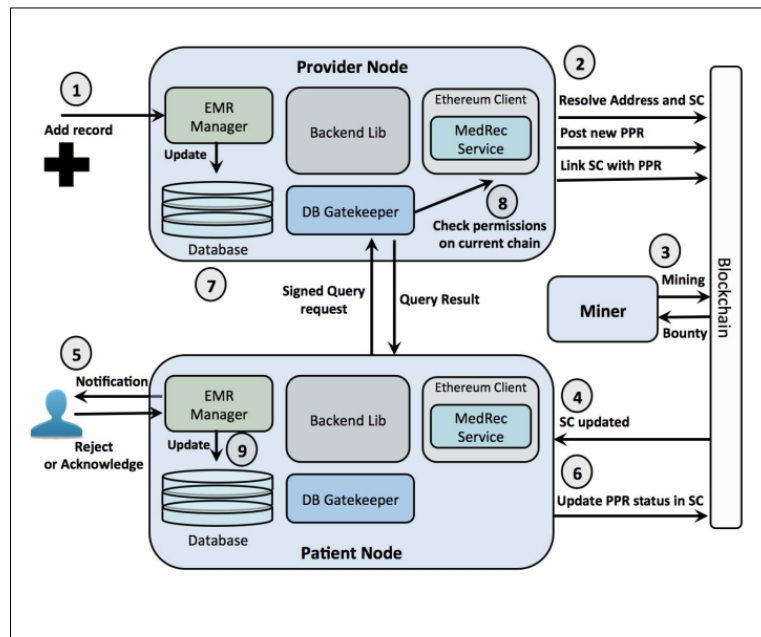


Fig 4.11 : Shows the proposed model for MedrRec model

4.12 PROVCHAIN : Data Provenance Architecture in Cloud Environment [5]

ProvChain, a data provenance architecture based solely on blockchain and cloud, was introduced by Liang et al. [7]. The data that has been kept in the blockchain is accessible to any peer. Without the aid of a third party, ProvChain automatically creates an open timestamped history of all client activities on cloud information. The data can be accessed by the provenance auditor, but they never learn who the original user was. The final one is data validation, in which records are accessible through the blockchain network and numerous nodes verify each block. Each provenance information transmission is approved by ProvChain using a blockchain receipt.

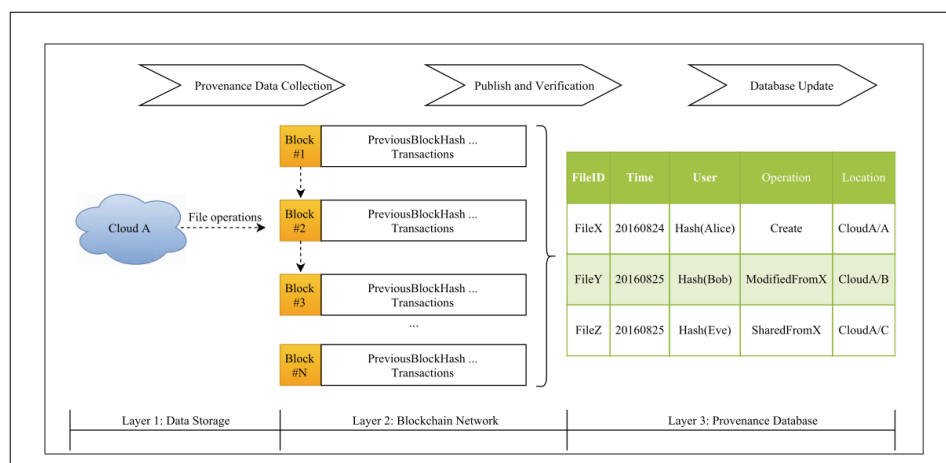


Fig 4.12 : Shows the proposed model for Provchain model

4.13 MEDICHAIN : EHR Management System [6]

The authors in their paper have proposed a system for secure transmission of data named MediChain. MediChain™ enables a secure protocol for the movement of private health data while also facilitating an effective exchange of health data among patients, carers, and healthcare professionals. The enterprise and global scales of this architecture are scalable. It offers increased protection for those assets as well as a superior ability to govern access to medical and health resources.

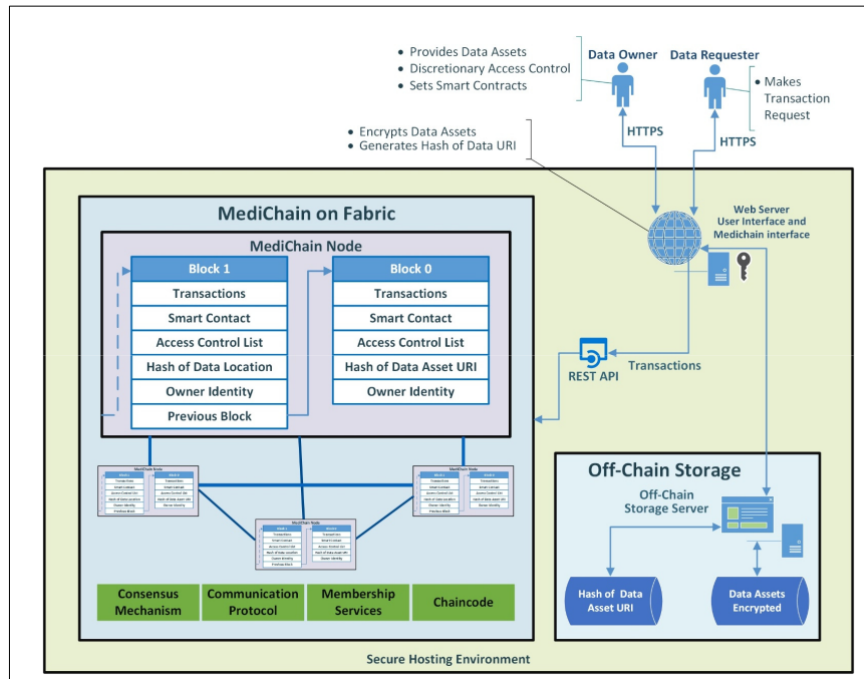


Fig 4.13 : Shows the proposed model for Medichain model

Results In tabulation form showing key features and technology used by the following proposed models :

PROPOSED FRAMEWORK/MODEL	KEY FEATURES	YEAR	TECHNOLOGY
1. BESURE[7]	<ul style="list-style-type: none"> Password based encryption mechanism(subsequent key locked) to safe gaurd the sensitive data in EHR. 	2021-Conference	Blockchain + EHR + Encription methods + Cloud Storage.
2. BHEEM[8]	<ul style="list-style-type: none"> Efficent EHR storage and management system. People have complete ownership 	2018-Conference	Blockchain + EHR + Encription methods

	of there data.		
3. MECHAIN[9]	<ul style="list-style-type: none"> • Semi Nodes and Full nodes categorization. • Multilayer structure . • semi leader for handlings request from semi nodes. 	2021-Conference	Blockchain + EHR + Hierarchical structural concepts
4. MEDBLOC[10]	<ul style="list-style-type: none"> • Patient have full access over there data. • People powered system 	2019-Conference	Blockchain + EHR + Smart contracts + Crptographic technologies.
5. MEDBLOCK[11]	<ul style="list-style-type: none"> • An AI powered , driven and maintained system for efficient maintaince of EHR 	2021-Conference	Blockchain + EHR + AI(Artifical Neural Networks)
6. MEDSAFE[12]	<ul style="list-style-type: none"> • Consenses algorithm to integrate secure document storage by doing small changes. 	2022-Conference	Blockchain + EHR
7. MEDSHARE[13]	<ul style="list-style-type: none"> • Fine access control. • ABE scheme designed for data protection. 	2021-Conference	Blockchain + EHR + Ethereum
8. SWAASTHYA SAMPATHEE[14]	<ul style="list-style-type: none"> • EHR's data is stored in IPFS data storage. • Hashes are stored in Ethereum's Ropsten test blockchain network 	2022-Conference	Blockchain + EHR + Ethereum Test Networks + IPFS
9. BIIMED[2]	<ul style="list-style-type: none"> • BiiMed- management of data sharing and validation of data between medical facilities. • HIS-For collecting ,storing and analysis of medical data. 	2020-Conference	Blockchain + EHR + Ethereum + Smart Contracts.
10. SEFRA[3]	<ul style="list-style-type: none"> • Enhanced interoperability using the temporal blockchain's 	2022-Conference	Blockchain + EHR + IOT + Temporal blockchain features.

	features		
11. MEDREC[4]		2016 Conference	- Blockchain + EHR + Smart contracts
12. PROVCHAIN[5]	<ul style="list-style-type: none"> Three layer proposed architecture for enhanced security for the data stored in cloud storage services. 	2017-Conference	Blockchain + EHR + cloud-assisted storage.
13. MEDICHAIN[6]	<ul style="list-style-type: none"> Patient Centric and off chain storage for the sensitive data. Effective EHR management system. 	2018-Conference	Blockchian + EHR + Decentralized Storage(off chain)

Table 4.1 : Result analysis

CHAPTER -5

CONCLUSION AND FUTURE WORKS

Currently, many organizations and developing countries are using the EHR system for storing their healthcare data for their citizens but the problem arises that all this data is still stored in the centralized based storage system either it may be a centralized server or it may be a remote cloud storage. Reliability on this centralized third-party storage is not a good choice as these centralized storages are prone to security attacks that could lead to data leaks or illegal data updation or alteration.

Because of this, blockchain and EHR have been coupled in order to instil a sense of security and trust in the system and encourage more people to use the software that manages medical data securely and without the risk of data leaks or data manipulation.

However, after carefully examining the selected publication's articles and papers, we came to the conclusion that Ethereum (private) and Hyperledger Fabric are the two most popular blockchain platforms for EHR management because they almost entirely satisfy the requirements.

Thus at last , It is possible to envision the development of the Blockchain as a a crucial invention and an important new element to the Internet, which previously lacked trust and security. After with the over advantage of using blockchain there are smart contracts also that make the security factor more stable.

Future studies in this area may use the study as a guide. Potential researchers will be able to create a new architecture or model with the help of the compilation of all relevant publications, their contributions, and their limits.

REFERENCES

- [1] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," pp. 1–9.
- [2] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," *2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020*, pp. 310–317, 2020, doi: 10.1109/ICIoT48696.2020.9089570.
- [3] P. Rastogi, D. Singh, and S. Singh Bedi, "Design of a Blockchain based Security Algorithm for IoT in Healthcare," *2022 2nd Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2022*, pp. 2209–2214, 2022, doi: 10.1109/ICACITE53722.2022.9823466.
- [4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.
- [5] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," *Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017*, pp. 468–477, 2017, doi: 10.1109/CCGRID.2017.8.
- [6] S. Rouhani, "MediChain TM : A Secure Decentralized Medical Data Asset Management System," *2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, no. Section II, pp. 1533–1538, 2018, doi: 10.1109/Cybermatics.
- [7] S. Li, Y. Zhang, C. Xu, N. Cheng, Z. Liu, and X. S. Shen, "BESURE: Blockchain-Based Cloud-Assisted eHealth System with Secure Data Provenance," *2021 IEEE/ACM 29th Int. Symp. Qual. Serv. IWQOS 2021*, 2021, doi: 10.1109/IWQOS52092.2021.9521289.
- [8] J. Vora *et al.*, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," *2018 IEEE Globecom Work. GC Wkshps 2018 - Proc.*, 2019, doi: 10.1109/GLOCOMW.2018.8644088.
- [9] H. Y. Wu, L. J. Li, H. Y. Paik, and S. S. Kanhere, "MEChain: A Multi-layer Blockchain Structure with Hierarchical Consensus for Secure EHR System," *Proc. - 2021 IEEE 20th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2021*, pp. 976–987, 2021, doi: 10.1109/TrustCom53373.2021.00136.
- [10] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 594–601, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00085.

- [11] C. Mistry *et al.*, “MedBlock: An AI-enabled and Blockchain-driven Medical Healthcare System for COVID-19,” *IEEE Int. Conf. Commun.*, pp. 0–5, 2021, doi: 10.1109/ICC42927.2021.9500397.
- [12] S. Sinha, S. J. Quraishi, and V. Hariharasudan, “medSafe- A Blockchain based Electronic Health Record Application,” *Proc. 2022 3rd Int. Conf. Intell. Comput. Instrum. Control Technol. Comput. Intell. Smart Syst. ICICICT 2022*, pp. 1477–1483, 2022, doi: 10.1109/ICICICT54557.2022.9917682.
- [13] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, “MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain,” *IEEE Trans. Serv. Comput.*, vol. 1374, no. c, pp. 1–14, 2021, doi: 10.1109/TSC.2021.3114719.
- [14] N. Sadashiv and S. G. Vachana, “Swaasthya Sampathee: Blockchain based EHR Framework,” *2022 Int. Conf. Ind. 4.0 Technol. I4Tech 2022*, pp. 1–6, 2022, doi: 10.1109/I4Tech55392.2022.9952557.