Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766294

DIGITIZATION OF SECURE BLOCKCHAIN BASED ELECTRONIC HEALTH RECORD SYSTEM USING SMART CONTRACT

Mrs.D.Mohanapriya,Mr.P.Mathivanan,Ilakkiyalakshmi.G,Indhu.G, Lina.R
Assistant Professor, ManakulaVinayagar Institute of Technology,Puducherry
Assistant Professor, Kalaignarkarunanidhi Institute of Technology, Coimbatore
Student, ManakulaVinayagar Institute of Technology,Puducherry
Email:mohanapriyacse@mvit.edu.in, ilakkiyaganesan65@gmail.com,
indhug2000@gmail.com, linaravi1605@gmail.com

Abstract: The health economy has been an innovative technology since time-honored. Preserving andmaintaining patient data are essential in a routine life. Patient's medical information is very important for every individual not only for patients but also for doctors who are examining them .We use the idea of Blockchain technology in healthcare to monitor these details and protect each person's personal information. Building a health information invention without the connectivity of a shady third-party infrastructure is a worry for the health economy. Due to the accessibility problems and leakage of information faced by the hospital management in other technologies.we come up with SHA-512(Secure Hashing Algorithm) which converts the patient information into the hash value using Ethereum platform.which will stop unauthorized entry.Electronic Health Records are essential to integrating with blockchain technology and smart contracts because SHA-512 offers greater protection than the other algorithms.

Indexterms: SHA-512(Secure Hashing Algorithm), Ethereum platform, EHR(Electronic Health Record)

I. INTRODUCTION

The Blockchain technology is meant to provide well architected secure, tampered proof platform that allows medical records to stored with other healthcare related information. To maintain anonymity, cryptographic methods are used. The model has features like fine-grained and adaptable access control, revocability of permission, auditability, and tamper resistance. A thorough security study would demonstrate that the model is demonstrably safe in terms of privacy and tamper resistance. According to the performance study, the model outperforms the current strategy in the literature review in terms of overall performance.

Working of Blockchain:

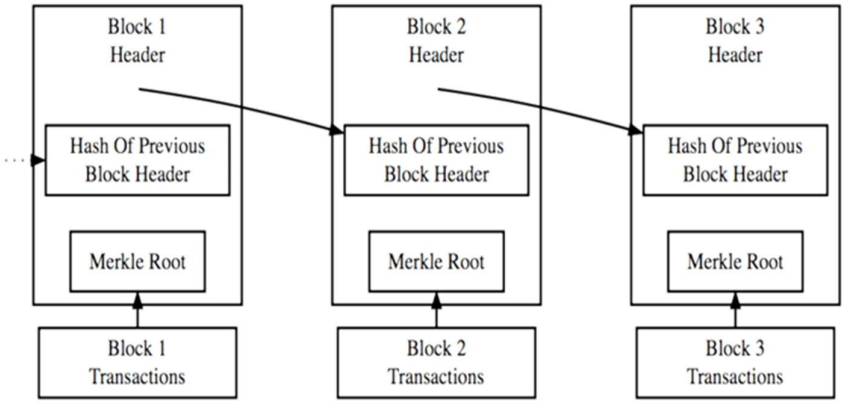

Figure 1: Working of Blockchain

1)The transaction is recorded in blocks.Known as Genesis Block, the first block. There is a hash number in every transaction.
2) The transaction will be checked to make sure whether it is valid. Every block contains the previous transaction's hash value and the present block's hash value.
3) Every transaction is verified and it is added to the block. Verification is carried out by contrasting the hash value with the hash value of the block before it. Any change in the transaction results a change in hash value indicating a third-party access

4)When the block is completed, (Block includes numerous operations, therefore) it is then added to chain.
There are 3 ways in blockchain will change in healthcare:
i. Electronic Health Record
The Electronic Health Record (EHR) has significant medical worth because it has documented how diseases are acquired, developed, and treated. Due to the sensitive and private nature of medical data for patients, data sharing, security, and privacy preservation are crucial issues in EHR. Electronic health records are personal and important documents for every patient. The success of electronic health records in recent years has been greatly aided by technological advancements, which have also improved security and user encounters. The security of medical documents and users' complete ownership of accurate data, however, continue to be major problems. The novel technology, specifically Blockchain, may be the best way to address the issues that have been discovered.
ii. Supply Chain
The manufacturing, distribution, and delivery of medications and other medical goods to patients are all controlled by a complex network of systems and components known as the healthcare supply chain.
Blockchain technology transactions are a crucial monitoring tool for gaining access to the entire process of moving medicines and medical supplies in the healthcare supply chain management.All transactions are documented on the database, and each server in the blockchain keeps a duplicate of each transaction, making it simple to immediately confirm the drug's origin, the seller, and the dealer. Additionally, the blockchain's distributed ledger enables healthcare professionals and authorities to verify and check the qualifications of vendors.

The medical product manufacturer, where goods are made and sent to a delivery location, is where the healthcare supply chain starts. Depending on the product, hospitals can either buy inventory or supplies directly from the manufacturer or distributor, or they can conduct the transaction through a group of purchasing organizations, which will negotiate a deal with the manufacturer on the hospital's behalf. The products are kept in storage for use by healthcare professionals and clients.

iii. Genomic Market

Genomic market is a scientific discipline which involves genomic information about a person as a part of medical care.Blockchain in Genomics are used for providing:

Genomic Data Security: From the viewpoint of data security, genomic data is delicate and important information. Blockchain offers excellent data security and accuracy. Although helpful in addressing data breaches, security measures like encryption do not offer full safety. Despite using high levels of security, many large organisations are still breached by hackers. Therefore, blockchain technology benefits businesses by offering greater security and safety against data breaches. Blockchain helps the business secure data and facilitates data exchange by using hashing methods to store data safely that cannot be altered once saved.

Genomic Data Sharing: It is now feasible to transmit private genetic information globally in a more safe manner using the blockchain network and genomic data. Blockchain's decentralization enables quick and safe data transfer between organizations. In a blockchain database, information can be kept as a record and kept private.

Immutability of genomic data: Blockchain makes genetic data immutable, enabling organizations to better safeguard information. Genomic data cannot be changed because of the decentralized nature of blockchain technology. As a result, any changes will be displayed on all servers, making the exchange of genomic data very secure.

Efficiency: The Company uses blockchain technology to increase efficiency because it removes the need for any third-party interference with the exchange of genomic data and mistakes, which makes the system quicker and more effective.

Cost savings: Because blockchain does not require the intervention of a third party, it lowers costs for organizations and builds confidence with other partners.

Need For Blockchain In Healthcare Management

- Healthcare networks must have a way to store and share medical info.
- Sharing sensitive information insecurely among numerous individuals can result in the leaking of personal data.
- Lack of client control over their personal information has negative effects, such as allowing unauthorized users to view or change confidential medical information.
- Maintaining interoperability among the different concerned names is one of the key problems with electronic health/medical records (EHR/EMR).
- Other issues with the way data is currently stored and shared through EHR/EMR platforms are data protection and privacy.

Background Study

Healthcare Breaches have long been a problem, according to the US Department of Health and Human Services Office for Civil Rights. There have been more than 3,054 hospital data breaches affecting more than 500 entries between 2009 and 2019. In those incidents, more than

230,954,151 healthcare data were lost, stolen, exposed, or improperly disclosed. In terms of people, this is greater than 69.78% of the US. In the days before contemporary technology, the healthcare industry kept medical notes on paper using a handwritten method. Data redundancy and duplication were also problems because there were multiple versions of the patient's medical information at each of the organizations the patient attended. We reviewed a number of related works and concentrated on a list of impending difficulties, particularly those linked to contemporary blockchain-enabled processes. In this article, we establish and extend a network environment with various protocols for particular operational controls of E-healthcare, such as the sharing of ledger information among active stockholders, which lowers the cost to 26.13%.

II. LITERATURE SURVEY

Many efforts have been made over the years to increase the protection and anonymity of electronic health records. Some of the literary reviews I studied are listed below:

Blockchain-Based access Control Model To Preserve Privacy For Personal Health Record Systems

The real personal health record data will be encrypted using the PHR owner's public key (master key) and kept on a cloud storage as part of the suggested model's general design to ensure secrecy. A surrogate reencryption procedure will be used to distribute the PHR. As a result, a proxy known as the gateway server will be used to store the reencryption keys and other information needed for the verification procedure. To enable search and tamper-resistance capabilities, the PHR's metadata will be kept on a private blockchain. The PHR proprietor and healthcare professionals like physicians, nurses, and others have access to the PHR. In their concept, there were five primary entities:

i. The PHR owner (PO)is a person or entity that has complete authority over his or her PHR data, is the owner of the PHR data, and is able to view or store their PHR data. A PO can grant or revoke certain permissions for others to view his or her PHR info. As a result, the PHR proprietor must present the information and reencryption keys for his or her PHR. PHR proprietor must establish a strategy for controlling access to his or her PHR data. In addition, PO can revoke access to recently added PHR data and permit some people to add additional data on PO's behalf.

ii. The user (U)is an organization that seeks access to PHR data with the associated PO's consent. The Users can come from a variety of groups, including caretakers, health insurance companies, and healthcare professionals (such as physicians and nurses). Users can receive PHR data from the gateway server and explore and obtain information through the blockchain. A user with delegated power can add new PHR data to the system or generate it.

iii. The gateway server (GS)is a computer in charge of examining each action taken inside the system to ensure its legitimacy. Encrypting the PHR data, archiving the metadata, and gaining access to the chain's record are all activities that are covered by GS. The management of the private blockchain is also the responsibility of the gateway server. There will be an SSL/TLS Secure route used for all communications between GS and other organizations. As it follows the work's specified process but is genuinely interested in the data, GS is regarded as a semi-trusted server in this work.

iv. The encrypted PHR data is kept in cloud storage (CS), which is accountable for doing so. Also, it is regarded as a semi-trusted server.

v. The private blockchain (BC), a kind of blockchain, is in charge of keeping the system's access record and metadata in storage. It is accessible to a specified set of users.

Blockchain For Secure EHRs Sharing Of Mobile Cloud Based E-Health Systems

For the construction of their e-health system in this paper, they used an Ethereum blockchain platform. On the Amazon cloud, they set up a private Ethereum blockchain network with two virtual machines running Ubuntu 16.04 LTS as the admin and two virtual machines running AWS EC2 as the miners, respectively. They used AWS Lambda functions to deploy their smart contract, which was created using the Solidity programming language. With the web3.js API, each function communicates with the cloud blockchain. Users can interact with smart contracts using their Android phone, which has an Ethereum node installed thanks to the Geth client, a command-line interface written in the Go programming language. A mobile user can create an Ethereum account to connect to our blockchain network and access data by utilizing the Geth client. The mobile application to interact with the Ethereum blockchain network was created using the web3.js library, a compact Java library for working with smart contracts and blockchain. To create a decentralized storage system, they then configured IPFS on Amazon cloud. The mobile healthcare platform BioKin, which consists of a network of wearable sensors and a mobile Android application to gather and process patient data for cloud storage, was used to build the medical records system. When using their mobile app, users upload data to IPFS on the cloud using a Java library. They used the Java-written, Android-deployed RSA asymmetric encryption technique to encrypt medical data files in the mobile gateway.

Eacms: Emergency Access Control Management System For Personal Health Record Based On Blockchain

The back-end consists of a single server that has been configured with routes, by which clients can identify and call. Every path has a related technique tied to it. To communicate with the blockchain network, these techniques employ the HF NodeSDK. Using NodeJS and the Hyperledger Composer-SDK, the back end is built. It has the ability to handle client requests and deliver the blockchain network's response. An permission to access the blockchain network is required in order to access the database through the system. This is accomplished by using data that was created in the web's Java Script Object Notation (JSON) during the login process. This network employs a single ordering node, a single peer node, and a single certificate authority (CA). When the network is launched, it establishes a channel with a peer node so that it can install a smart contract (a bespoke one) on the file system of the peer and run its startup function. Through Consortium Blockchain, Cloud-Assisted Her Sharing With Security And Privacy Protection.

In order to achieve privacy preservation and data security for EHR exchange between health institutions, they developed a cloud-assisted blockchain system in this paper that combines searchable encryption with proxy re-encryption technology.

We suggest a brand-new architecture for consortia blockchain-based cloud-assisted EHR storage and sharing that protects user privacy and ensures data security. EHR ciphertext for patients is stored in the cloud, while ciphertext for data exchange and searching is recorded on a consortium blockchain.

We create the network model, data construction, and consensus mechanism as the foundational elements of the consortium blockchain. According to the requirements of our system in the network, we define various entities and specify their authority. Including encryption, we

construct the block structure and transaction structure. Primitives for securely storing data. Additionally, we propose proof of authorization as the consortium blockchain's consensus mechanism.

We describe a consortium blockchain-based, cloud-assisted EHR sharing system that is secure and protects user privacy. The keywords and related data can only be obtained by authorized data requesters who have a searching trapdoor. Additionally, the blockchain accounts handle authorization and other access functions, guaranteeing the protection of identity privacy. When they reach an agreement with the patient, the cloud also re-encrypts the EHR ciphertext and delivers the reencrypted ciphertext to the designated data requester.

Blockchain based Implementation of Electronic Medical Health Record

To provide security and police investigation for patient medical health records served as the inspiration for this project. Security for patient medical records is necessary, but doctors and other healthcare professionals will still have access to the information.The major goal is to prevent the exploitation of patient medical records by producing concealment (confidentiality). One of the most important foundational principles of medicine is the secrecy or confidentiality of patient information. Building trust between the patient and the doctor is essential as sensitive information about a patient is to be kept private.In this paper, we presented scenarios where blockchain innovation could be useful in several social insurance contexts. Also, they demonstrated a design for the system tailored to the needs of radiation oncology data sharing and produced a version that ensures the safety, confidentiality, accessibility, and fine-grained control over extremely sensitive patient data.

Using Blockchain for Electronic Health records Using Secure Record Storage

Modern technology is having an impact on every aspect of human lives and altering how we live. For the improvement of the field of health maintenance, the change in technology must be new and contemporary. The enhancement of user experience, integrity, and security are further advantages of technology innovation. The Electronic Health Record and the Electronic Medical Records provided these.Yet, there are several challenges, such as preserving accuracy, ensuring data consistency, protecting ownership, etc. The introduction of Blockchain Technology has provided clarity on these challenges. With the help of this technology, medical records and other information connected to healthcare might be stored on a safe, impermeable platform. Prior to the development of contemporary technology, the healthcare industry employed a paper-based system, or a handwritten mechanism, to maintain medical records. This paper-based approach was disorganized and inefficient. Due to the fact that the patient's medical records were duplicated and redundant throughout all of the institutions the patient attended, this problem also arose. These systems were suggested to offer safety for patients by lowering mistakes and providing access to the information. They were utilized to store clinical notes and test data in its several components. The Electronic Health Record was created with the intention of eradicating the issues associated with paper-based records and offering a superior system that would revolutionize the healthcare industry. Although using EHR systems in hospitals and other healthcare settings was intended to improve the quality of care, these systems encountered issues with interoperability, scalability, data breaches, and information asymmetry.

III. METHODOLOGY:

We have created a prototype for the EHRCHAIN system. The following characteristics of this prototype implementation:

1. Aadhaar numbers are used in India for registration in the EHR CHAIN system, but any national-level biometric identity ID can be used in other countries to prevent the theft of personal healthcare data from the database.
2. A special pseudonym number that the patient will generate after providing some confidential data. To protect patient privacy, this pseudonym will be used to store medical information.
3. Throughout the hashing process, all identifiers and quasi-identifiers from the patient's health record are deleted, ensuring privacy even if unauthorized individuals gain access to the database.
4. Certain fundamental healthcare activities have been simulated in this EHRCHAIN system prototype.
5. This suggested solution offers enormous potential for medical study on a specific condition since identifiers/quasi-identifiers are not maintained in the EHR CHAIN health records database.
6. The patient is always able to modify their access control policy.
7. Both the patient's pseudonym and their personal data are kept in a separate encrypted EHRCHAIN Patient Profile database. Hence, this technology ensures the confidentiality and privacy of healthcare data.
8. Any third party will be able to access the data after revealing his identity for prescription or any other purpose. This proposed EHRCHAIN system will result in substantial effects.

SMART CONTRACT:

A smart contract is a protocol that specifies, automatically and electronically, the rules that a transaction must abide by. The use of smart contracts in commerce can help to improve purchase security, dependability, and simplicity. They can be traded for other assets or used in cryptocurrency. Contracts automatically go into effect when a specific transaction value satisfies a predetermined rule. This fact may help to automatically spot inconsistencies (like violations). The legal environment for electronic transactions may be more flexible due to smart contracts.

Existing Algorithm:

Ethereum	**Ethereum can be used by any individual to develop any secured digital technology and it is a decentralized worldwide platform powered by Blockchain technology**
Consensus	**This mechanism sanctions the blockchain network to certain reliability and strengthens the trust between nodes and ensures security in the environment.**
Practical Byzantine Fault Tolerance	**PBFT (Practical Byzantine Fault Tolerance issues a cryptographic algorithm such as signature verification, and hash to secure that everything stays unchangeable, unforgeable, and irrefutable.**
KawPOW	**KawPoW algorithm is a mining technique which directs to overcome problem of centralisation of mining by utilising the counter graphic processing unit (GPU) memory.**
Secure Hashing Algorithm - 256	**SHA-256(Secure Hashing Algorithm) used for securing the cryptographic values and it produces irrevocable and distinctive hashes. SHA-256 takes the length of the variable as input and output as 256-bit long hash.**
Proof-Of-Work	**PoW (Proof-Of-Work) It is used to create or add a new block and to confirm the transaction in the blockchain. Verifying the target hash is not that much difficult in POW.**
Proof-Of-Stake	**PoS (Proof-Of-Stake) With PoS, consensus is achieved by validators (which are chosen randomly depending on how many locks provided in the blockchain) It requires less energy and power.**
Proof-Of-Activity	**PoA (Proof-Of-Activity) combines proof of work (POW) and proof of Stake (PoS) procedures. PoA mechanism makes sures that the blocks of transactions added to the network are authentic and logical.**

Figure 2: Algorithm and its description

IV. MODULE DESCRIPTION:

Depending on the needs of the community, different countries make different decisions, however the majority of well-known EHR solutions support patient-centeredness because it grants patients complete access rights. The patient is the focus of this EHRCHAIN system. To create an effective system for the security and privacy of healthcare information systems, we have merged encryption and hashing approaches. It has been demonstrated that a pseudonym is employed to protect the patient's privacy. The patient will create this alias. The patient-controlled access control policy will determine what information about them can be accessed and by whom. As long as the records are depersonalized, hashing permits both primary and secondary usage while protecting privacy. The EHRCHAIN system's architecture comprises of two distinct databases, the EHRCHAIN Health Records database and the EHRCHAIN Patient Profile database, a hashing module, access control modules for patients and doctors/healthcare authorities, as well as management of data access policies and sharing. The functions of each have been detailed in the section that follows.

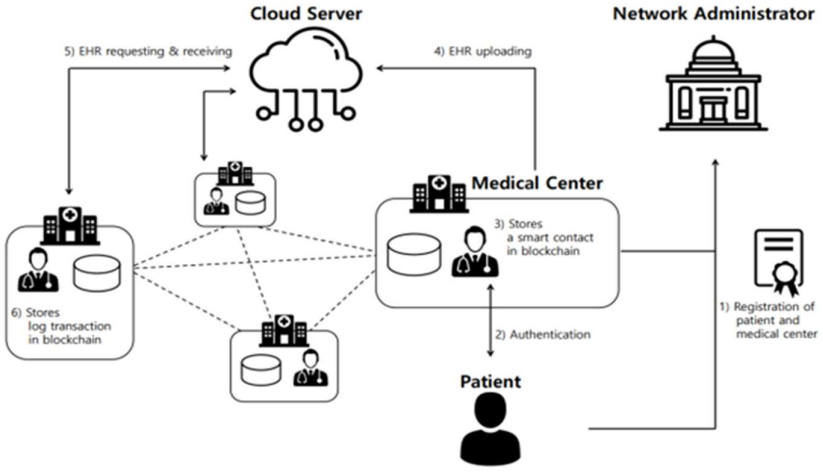

Figure 3: Proposed Architecture

EHRCHAIN databases

Patients' privacy may be endangered if a hacker is successful in accessing a database, hence high privacy must be maintained. EHRCHAIN maintains two distinct databases, one for pseudonym zed health records and the other for identifying information in encrypted form:

i. The patient's health records are stored in the EHRCHAIN Health Records database after hashing.

ii. The encrypted patient profile and encrypted patient pseudonym are stored in the EHRCHAIN patient profile database.

Hashing Module

Before storing patient/healthcare facility health records in the EHRCHAIN Health Records database, the hashing module strips all identifiers and quasi-identifiers from the patient's health record so that, in the event of database intrusion, the owner of a specific health record cannot be identified. Using the pseudonym generation technique, each patient can generate a special pseudonym (a digital long random number). Without any information being exchanged between the patient and EHRCHAIN, a pseudonym can be created locally in the patient's own surroundings. Pseudonyms cannot be inferred from patient data and do not require memory. The pseudonym is kept encrypted. Each time a new record is added, patients decrypt it.

SHA 512 Hashing

The Ron Rivest-developed one-way hash function and it is used by the SHA 512 algorithm. The SHA 0, SHA 1, SHA 256, and SHA 384 algorithms were developed into this algorithm. Publication of research on his paper, Christian Angga explains how the cryptographic algorithm SHA 512 processes input in the form of messages of any size to produce 512-bit-long message digests.Its predecessor is SHA1, and MD5 is a renewal of MD4, showing that the hash method has been linked to and developed, showing that the algorithm has been determined to have a collision vulnerability.

The new standard hash functions are currently SHA 224, SHA 256, SHA 384, and SHA 512, according to the National Institute of Standards and Technology (NIST). In general, the SHA 512 hash function executes the same hash operation as the SHA 2 operation. The SHA 512 hash function produces message digests with 512-bit sizes and 1024-bit block length.The SHA

512 cryptographic algorithm functions accepts input in the form of a message of any length or size and generating a message digest with a fixed length of 512 bits.

The processes performed in testing and analyzing this research will also be covered in this section, along with the methodical approach employed to address the research topic. To assess the system utilized to discover the present circumstances, requirements, benefits, and drawbacks of these programmers, literary studies are part of each stage. This stage involves reading a variety of books, previous research journals, papers, or articles that are appropriate or relevant. It also entails gathering materials from the internet, including proceedings, websites, journals, and source code that can be used in this research.

To assess the needs and vulnerabilities of the employed system, a needs analysis and system vulnerability analysis are conducted.

The analysis, which is concentrated on the web-based application login system encryption function, attempts to determine the benefits and drawbacks of the existing encryption technique when it is replaced by the most recent algorithm approach.

After the login procedure is complete, it shows needs analysis and design for improvement will be used to define and provide an overview of the encryption process.

The most recent hash function algorithm calling the method, code modification for patching, and implementation test results were used to mitigate.

In this work, experiments were carried out to contrast the use of the MD5 and SHA 512 encryption techniques. Penetration testing and user acceptance testing were used for testing. In order to increase data security in web-based systems, penetration testing is carried out using Brute Force techniques, whereas user acceptance testing is carried out by answering a questionnaire.

Patient’s Profile and Hash Encryption

By employing their public key, the patient's pseudonym is encrypted using public key cryptography technique. Name, date of birth, age, cellphone number, AADHAR number, email, and other fields have all been detected as including personally identifiable information. When a patient visits a new healthcare facility for the first time, this identifying information is required.

All of these personally identifiable details are encrypted using the shared key approach (symmetric key cryptography) seen in figure 4.3. The safe EHRCHAIN Patient Profile database stores encrypted profiles and encrypted pseudonyms. Pseudonym is decoded for the purpose of adding a new record using the patient's private key, which is only known to the patient.

Access Control Module

There have been discussions about various access control models. The most used model, with several variants, is RBAC. The access control module should manage the various access requirements of each healthcare system entity without affecting patient privacy.

The EHRCHAIN system will need registration from each component of the healthcare system, including patients, physicians, and health centers/authorities.

Each entity will be verified using its AADHAR Number. Hence, the applicant for access has their identity confirmed. The patient has access to all of his pseudonymized medical records. The patient must first use their private key to decode their pseudonym. Only the patient is aware of this secret key. Therefore, confidentiality is preserved.

Physicians and other healthcare professionals have less access privileges. Just those health records or portions of those data that the patients have given them permission to access are accessible. The patient must first use her or his private key to decode the pseudonym. Only the patient is aware of this secret key. The doctor or healthcare authority will next reveal their pseudonym by repeating the decryption process. The access control module will allow access to those health records with both the patient's pseudonym and the doctor's or healthcare authority's pseudonym. Hence, it will be confirmed who accessed the medical records.

V IMPLEMENTATION:

The patient can view their record in the EHR system and safely use it for the rest of their lives. The patient is given the secret key, which can be used to access the results later. Anyone who does not possess the secret key is ineligible to participate in the data retrieval procedure. As a result, the patients' health records are safer with the blockchain and can be used with their own private key as well as for future reference. The current major barrier to using the Ethereum network is the difficulty in acquiring ETH units. The units can be bought with fiat money or cryptocurrencies like Bitcoin, or they can be acquired through mining. We have created a web application user interface for the health record system, and once ETH units are accessible, posting and executing smart contracts go very smoothly. Using some distinctive identification characteristics, we can add account authentication features for greater protection. To save patient records and certificates, we will use the Ethereum network. To do that, a smart contract that serves as a blockchain gateway must be written.

Figure 3: Signup Page

The patient enters the information and joins up on the signup screen shown in the above image, which includes fundamental information.

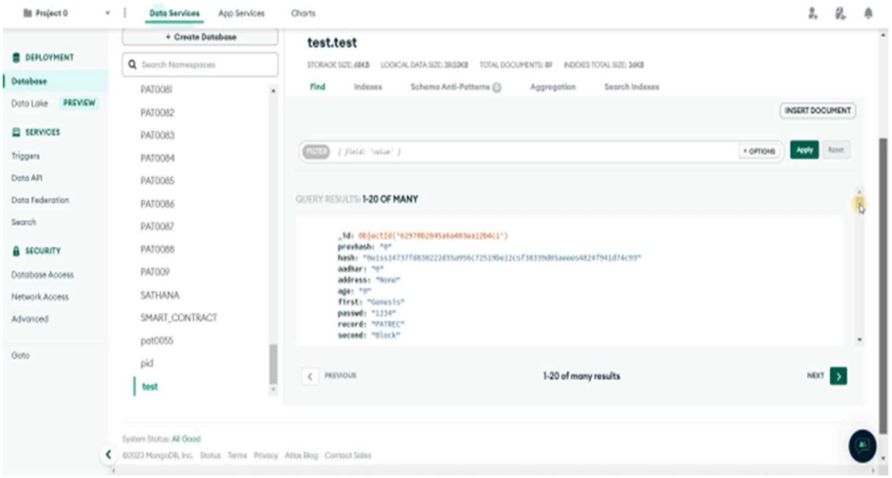

Figure 4: The data is stored in the Mongo DB.

The Mongo DB contains information about the patient and the practitioner. Each patient has a unique hash number that is produced using the SHA-512 (Secure Hashing Algorithm) in 64 bits.

HEAD BLOCKCHAIN RECORDS

BLOCK 62970b2845a6a403ea12b4c1

INDEX	VALUE
FIRST NAME	Genesis
LNAME	Block
TIMESTAMP OF CREATION	
PREVIOUS HASH	0
Hash	0e1ss14737fd838222d3Sa956c72519be12csf38339d0Saeees4824f941d74c93

BLOCK PAT001

INDEX	VALUE
FIRST NAME	
LNAME	
TIMESTAMP OF CREATION	2022-06-01 12:59:24
PREVIOUS HASH	0e1ss14737fd838222d3Sa956c72519be12csf38339d0Saeees4824f941d74c93
Hash	2902603da2e8d3a31c8256c2f9cb1794a44f73ca3d1d50ddbe5b262903591b40

Figure 5:Creation of genesis block

INDEX	VALUE
FIRST NAME	Ilakkiya
LNAME	Lakshmi
TIMESTAMP OF CREATION	2023-03-10 11:49:41
PREVIOUS HASH	c722beada3339fe184e196be859641a46b74dc9220cf577e769e19ff806b1210
Hash	21dc10d4bb38d2ef238a24d1290d51e58942d34dd28504817ec55a75f013d221

BLOCK PAT0088

INDEX	VALUE
FIRST NAME	Madhan
LNAME	M
TIMESTAMP OF CREATION	2023-03-13 10:44:02
PREVIOUS HASH	21dc10d4bb38d2ef238a24d1290d51e58942d34dd28504817ec55a75f013d221
Hash	925ec9dddf4804a6512ee67482925193a2f97d1ea6f18d6a576e1468a2e6f6a2

Figure 6: Creation of blocks.

All types of patient and medical information are stored as blocks, as shown in the above illustration of the origin block.

Figure 7: Patient logs in using a special patient ID and passcode

According to the image above, the patient is signing in using a special identification number (or "key") that is known only to them. Only after the patient provides permission can the practitioner access or examine the patient'smedical data

Figure 8: Patient's dashboard.

The above figure represents, once the patient signs in the dashboard of the particular patient appears and they can access log, view records and book appointment with doctors.

V CONCLUSION:

The patient can view their report and use it securely for the rest of their lives in the electronic health record system. The patient receives a confidential key that can be used to access the results later. Anyone who does not possess the secret key is not permitted to participate in the data retrieval procedure. Therefore, with the aid of Blockchain and their own private key, patients' health records are more securely stored, and they can also use that information for future reference. The current major barrier to using the Ethereum network is the difficulty in acquiring ETH units. The ETH units can be acquired through mining, exchange for fiat money, such as Bitcoin, or buy. We have created a web application user interface for the health record system, which makes the posting and execution of smart contracts incredibly seamless once the ETH units are accessible. By utilizing some distinctive identification characteristics, we can add account authentication features to increase security.

REFERENCES

1. TheinThanThwinand SangsureeVasupongayya.“ Blockchain-Based Access Control Model To Preserve Privacy For Personal Health Record Systems” 2019
2. Dinh C. Nguyen; Pubudu N. Pathirana; Ming Ding; Aruna Seneviratne. “Blockchain For Secure EHRs Sharing Of Mobile Cloud Based E-Health Systems”2019
3. Ahmed Raza Rajput;Qianmu Li; Milad TalebyAhvanooey; Isma Masood.“Eacms: Emergency Access Control Management System For Personal Health Record Based On Blockchain” 2019
4. Yong Wang; Aiqing Zhang; PeiyunZhange; HuaqunWang.“Cloud-Assisted Her Sharing With Security And Privacy Preservation Via Consortium Blockchain” 2019
5. M. SathyanarayananM.E; N. Ramyadevi; S. Deebika;R.Soumiya “Block Chain Based Implementation Of Electronic Medical Health Record” 2020

6. Ayesha Shahnaz; Usman Qamar; Ayesha Khalid. “Using Blockchain for Electronic Health Records” 2019

7. XiaominDu:BeibeiChen:Ming Ma: Yanjiao Zhang” Research on the Application of Blockchain in Smart Healthcare: Constructing a Hierarchical Framework”2021.

8. HanaaFatoum; Sam Hanna; JohnDHalamka;Douglas C Sicker; Peter Spangenberg; Shahrukh K Hashmi “Blockchain Integration With Digital Technology and the Future of Health Care Ecosystems”2021

9. I Varalakshmi, M. Thenmozhi and R. Sasi, "Detection of Distributed Denial of Service Attack in an Internet of Things Environment -A Review," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN),Puducherry,India,2021,pp.1-6,doi:10.1109/ICSCAN53069.2021.9526378.

10. D.MohanaPriya “Survey : Secure Image Processing Techniques using Blockchain application “ was published on International Journal of Management Technology and Engineering, volume IX, Issue XI, November 2019| ISSN NO : 2249-7455| page-No 701- 707.

11. Dr.N. Palanivel, "Recommendation System Based Smart Shopping Cart", International Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Vol.7, Issue 5, page no.908-914, May-2020.