ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

Secure Sharing of Patient Data and Appointment Coordination

Pranjal Borkar[1], Om Yamgawali[2], Sanskruti Anasane[3], Abhishek Dalvi[4], Prajwal Kale[5], Prof. Shraddha Utane[6]

[1,2,3,4,5]*Student, H.V.P.M's College of Engineering & Technology Amravati, India*

[6]*Assistant Professor, H.V.P.M's College of Engineering & Technology Amravati, India*

Abstract: *Encrypted Patient Data Sharing and Appointment Coordination," focuses on enhancing healthcare systems by integrating secure data management with efficient scheduling. A unique patient identification system ensures seamless updates to medical records, reducing duplication and improving continuity of care. Advanced encryption techniques, including AES and RSA, safeguard sensitive data during storage and transmission, while blockchain technology ensures transparency, immutability, and secure sharing. The system enables real-time appointment scheduling, automated reminders, and priority-based coordination, simplifying patient access to healthcare services. Additionally, aggregated and de-identified patient data is shared with government agencies, allowing for real-time disease monitoring and geospatial mapping. This supports targeted public health interventions and resource allocation in areas with high disease prevalence.*

Keywords: Encrypted Patient Data Sharing, Appointment Coordination, Healthcare Systems, Secure Data Management, Patient Identification System, Medical Records, Advanced Encryption Techniques, Real-Time Appointment Scheduling, Real-Time Disease, Public Health Interventions, etc.

I. INTRODUCTION

1. Overview:

Better health is important to human happiness and the welfare of society. It plays a vital role in the economic progress of the nation. Ill health, casualty, emergencies occur every day and the diseases are expected to be diagnosed and treated. A health record is a collection of clinical data related to the patient's mental and physical health, gathered from different sources. Health record consists of a patient's medical history, examination, diagnosis, treatment, results of lab investigation, scanning reports, alerts like allergic to etc. These health records can be managed both manually and digitally.

The traditional method which is followed in most of the hospitals for maintaining records is the manual method which includes papers and books. This method has serious limitations such as a need for large storage areas and retrieval of records is difficult. In the present era computerization of clinical records has become popular as the storage and retrieval of the records is easy. However, the chances of manipulation without identification has become a serious concern.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

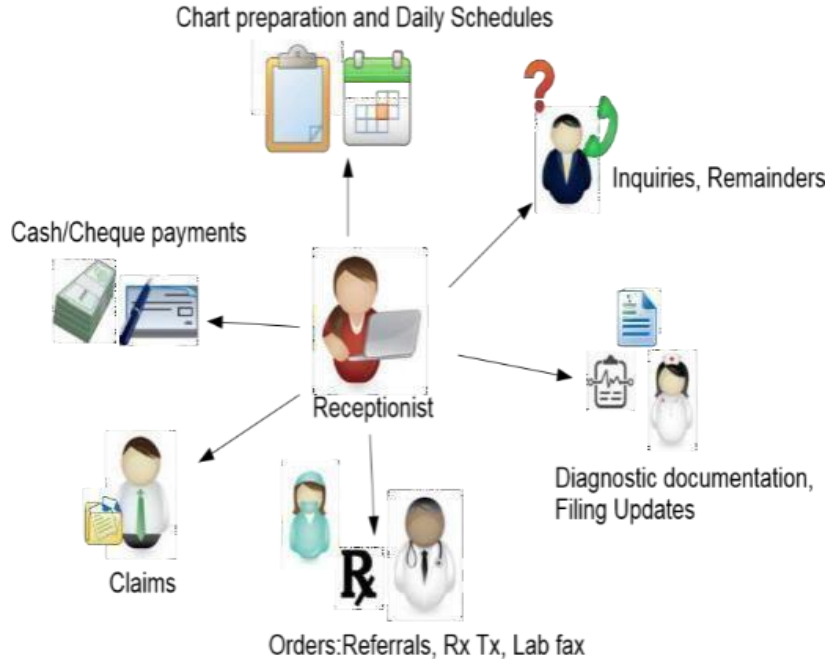

Figure 1: Existing Centralize

Another major perturb is the maintenance of patient records confidentially as the patient can hold the doctor and the hospital responsible for breaking the confidentiality of his medical records. Also, paper-based records are often incomplete, giving rise to unwanted repeat testing and medication. There is wastage of time since this system needs more manual power for transferring records by mail or faxes as these are dispersed and are not centralized. Even accessing of medical records by doctors is limited. Health records can be easily and quickly shared between medical institutions by integrating digital technologies in the healthcare system.

In this respect there are intense queries about the storage of patient's data, providing authorization to access the data, security & immutability of the data. These problems can be solved by developing a decentralized digital health infrastructure that is by integrating Blockchain technology into the healthcare system. Blockchain technology has the capability to rebuild the modern economy by maintaining and updating record.

Within the next decade, health care services and applications are expected to generate trillions of dollars in revenue due to their integration as part of the Internet of Things (IoT) paradigm. Most remarkably, smart healthcare has shown significant reduction to mortality rates and cost of healthcare, while improving quality, for instance, by reducing emergency room (ER) visits and hospital stays . Being voluminous, health care records are best stored in the cloud to enable easy access and sharing of information among the different stakeholders. In addition, the security and privacy measures offered by the cloud increase the resiliency of data. However, the use of cloud storage does not allow interoperability between the different care providers. In addition, the

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

integrity and authenticity of the data cannot be guaranteed. One possible technology to enhance integrity, authenticity, and consistency of stored and exchanged medical records is Blockchains. Blockchains can guarantee security of sensitive data by tracking access to confidential medical records and ensuring authorized access. Blockchains can serve as a distributed database that hardens medical reports against tampering. As a distributed trusted mechanism, Blockchains addresses security issues associated with a deployed distributed database of patient records which could be managed by different advisories such as caregivers, hospitals, pharmacies, insurance companies, regulators and the patients themselves. Blockchains as a technology relies on public key cryptography and hashing mechanisms as a mean to keep track of historical transactions pertained to distributed patients' records while preserving confidentiality, integrity and availability. This will ensure that records are not lost or being wrongly modified, falsified or accessed by unauthorized users.

In Blockchains, patients' records can only be appended to the database, but not removed. New information can be securely linked to a previous record using cryptographic hashing. Records are added to the blockchain based on a consensus among the majority of miners in the blockchain. Miners are a set of special nodes working together to validate new transactions added to a blockchain. To be able to add a record to a blockchain, miners have to compete to solve a difficult mathematical problem known as Proof of Work (POW) which takes 10 minutes on average.

2. Limitations:

A study was conduct in Finland to find the experiences of nursing staff with the EHR, it was concluded that EHR systems faced the problems related to thembeing unreliable and having a poor state of user-friendliness. The EHR system also faces some other problems which are:

- **Interoperability:** It is the way for different information systems to exchange information between them. The information should be exchangeable and must be usable for further purposes. An important aspect of EHR systems is its Health Information Exchange (HIE) or in general data sharing aspect. With a number of EHR systems being deployed in various hospitals they have a varying level of terminologies, technical and functional capabilities which makes it to have no universally defined standard. Moreover, at technical level the medical records being exchanged should be interpretable, and that interpreted piece of information could be further use.

- **Information Asymmetry:** Today the greatest problem in healthcare sector defined by the critics is information asymmetry which refers to one party having better access to information than the other party. In case of EHR systems, or in general healthcare sector is suffering from this problem as doctors or hospitals have access to the patientsrecords, thus making it central. If a patient wants to access his medical records he would have to follow a long and tedious process to access them. The information is centralized to only a single healthcare organization and its control is only provided to the hospitals or organizations.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

- **Data Breaches:** Data breaches in healthcare sector also calls for the need of a better platform. A study was done for analyzing the data breaches in EHR systems and it depicted that 173 million data entries have been compromised in these systems since October 2009. Another study conducted by Argaw et al., explains that hospitals have become a target of cyberattacks and an increasing trend has been witnessed by the researchers while conducting this study that a lot of research work has been done in this domain.

3. Objectives:

- ***To Ensure Confidentiality of Medical Records*** **–** Utilize blockchain technology to secure patient data and prevent unauthorized access.
- ***To Enhance Data Security*** **–** Provide a tamper-proof system for storing and managing medical records.
- ***To Ensure Legal and Ethical Compliance*** **–** Protect patient privacy in accordance with legal and ethical requirements.
- ***To Secure Storage and Access Control*** **–** Restrict access to personal details such as medical history, test results, and treatment plans to authorized healthcare providers.
- ***To Build Trust Between Patients and Healthcare Providers*** **–** Enhance patient confidence in the security of their medical information.
- ***To Encourage Accurate Patient Disclosure*** **–** Foster an environment where patients feel safe to share detailed medical information.
- ***To Improve Healthcare Decision Making*** **–** Enable healthcare providers to make informed decisions based on secure and reliable patient data.
- ***To Enhance Patient Health Outcomes*** **–** Support better healthcare delivery by ensuring data integrity and accessibility.

II. LITERATURE REVIEW

1. Literature Survey:

Satoshi Nakamoto et al. [1], the basic idea was to have a cryptographically secured and a decentralized currency that would be helpful for financial transactions. Eventually, this idea of blockchain was being used in various other fields of life; healthcare sector also being one of them intends to use it. A number of researchers have carried out the research on this area, these research works focus on the fact that whether the idea of using blockchain for healthcare sector is feasible or not. They also identify the advantages, threats, problems or challenges associated by the usage of this technology. Some researchers also discussed the challenges that would be faced while actually implementing this on a larger scale.

Gordon and Catalini et al. [2], conducted a study that focused on the methods by which blockchain technology would facilitate the healthcare sector. They identified, thathealthcare sector is controlled by hospitals, pharmaceutical companies and other involved third parties. They specified data sharing as the key reason why blockchains should be used in healthcare.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

This study also identified four factors or approaches due to which healthcare sector needs to transform for usage of blockchain technology. These include way for dealing of digital access rights, data availability, and faster access to clinical records and patient identity. It also discusses the on-chain and off- chain storage of data. The study also included the challenges or barriers faced by usage of blockchain technology these were huge volume of clinical records, securityand privacy, patient engagement.

Kuo et al. [3], conducted a review that discussed several applications of blockchain in biomedical and healthcare sector. The authors identified that using blockchains for this domain offers many advantages and some of these are decentralization, persistence of clinical or medical records, data pedigree, and continuous accessibility to data and lastly secure information being accessible to biomedical or healthcare stakeholders. The limitations of blockchain technology were identified to be, confidentiality, speed, scalability and threat of malicious attack, i.e., 51% attack.

Zhang et al. [5], proposed a scalable solution to the blockchain for clinical records. The basic aim of this study was to design such an architecture that complies with the Office of National Coordinator for Health Information Technology (ONC) requirements. This study identified the barriers that this technology faces mainly include concerns related to privacy, security of blockchain, and scalability problems related to huge volume of datasets being transmitted on this platform, and lastly there is no universal standard enforced for data being exchanged on blockchain. This study also include a demonstration of a decentralized application (DAPP) based on the design formulated on the ONC requirements as mentioned before. They also included the lessons learnt and how can FHIR chain be improved.

2. Findings:

The literature survey is the major tool for examining as well as identifying the various methods are in practice. For such an activity, the major source of the corpus is nothing but research articles. So, here also, we considered a good number of research articles to identify the current practices in the domain of Healthcare. Our literature survey able to provide a list of various methods practiced in those articles. Also, mentioned the effective practices for certain articles from the perspective of those corresponding authors.

Health is important to human happiness and the welfare of society. It plays a vital role in the economic progress of the nation. Ill health, casualty, emergencies occur every day and the diseases are expected to be diagnosed and treated. A health record is a collection of clinical data related to the patient's mental and physical health, gathered from different sources. Health record consists of a patient's medical history, examination, diagnosis, treatment, results of lab investigation, scanning reports, alerts like allergic to etc. These health records can be managed both manually and digitally.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

III. PROBLEM STATEMENT IDENTIFICATION

This chapter introduces the problem analysis of System for Electronic Medical Health Records Sharing based on Blockchain, which determine the degree of problem and also introduces the objectives of working system which defined the flow of working system. To analyze the problem of sharing electronic medical health records using blockchain, let's first understand the traditional system's limitations and then explore how blockchain can address these issues:

1. **Data Security and Privacy:** In traditional systems, EMHRs are stored in centralized databases, making them vulnerable to data breaches and unauthorized access. Blockchain offers a immutable ledger, ensuring that EMHRs are secure, tamperproof, and accessible only to authorized parties.
2. **Data Interoperability:** Healthcare data is often stored in siloed systems that do not easily communicate with each other. Blockchain can enable seamless data sharing among different healthcare providers and systems, improving care coordination and patient outcomes.
3. **Data Integrity and Traceability:** In traditional systems, there is a risk of data being altered or deleted without a trace. Blockchain's transparent and immutable nature ensures that every transaction is recorded and can be traced back to its origin, enhancing data integrity and auditability.
4. **Patient Consent and Control:** Patients have limited control over their EMHRs in traditional systems. With blockchain, patients can own and manage their EMHRs, granting or revoking access to healthcare providers as needed, thus ensuring patient privacy and autonomy.
5. **Data Fragmentation and Duplication:** Healthcare data is often fragmented across multiple systems, leading to duplication and inconsistencies. Blockchain can provide a single source of truth for EMHRs, reducing duplication and ensuring data consistency.
6. **Regulatory Compliance:** Healthcare data sharing must comply with various regulations such as HIPAA. Blockchain can provide a framework for ensuring compliance with these regulations, facilitating secure and compliant data sharing.

IV. SYSTEM ARCHITECTURE

The architecture of Encrypted patient data sharing and appointment coordination System typically consists of several key components that work together to ensure the secure and efficient sharing of medical records. Here's an overview of the typical system architecture:

1. **Overview of System Architecture:**

   To understand the blockchain architecture let us use the following figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

   When a user initiates a transaction on the blockchain network, a new block is created to store the transaction. This block is then distributed to all connected nodes in the network. Each node maintains a complete copy of the blockchain, which helps in the verification process. The transaction, once placed inside a block, is broadcasted to all nodes, ensuring transparency and security.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

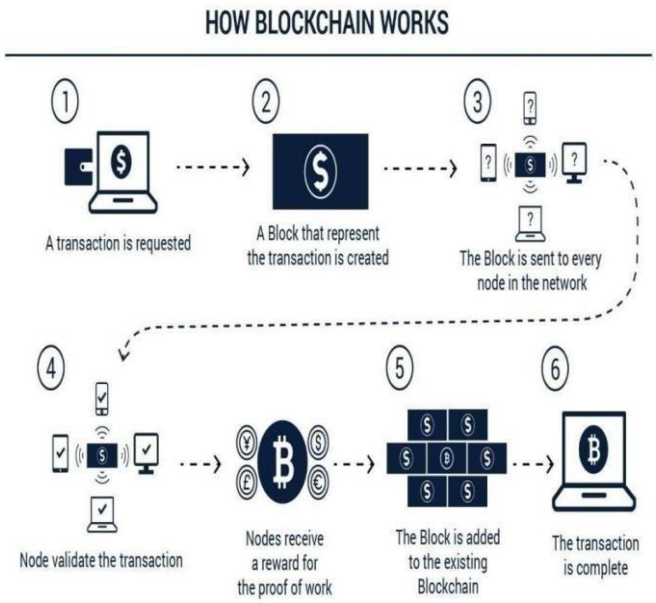

Figure 2: An Overview of Blockchain

Upon receiving the block, the connected nodes verify that it has not been tampered with. This verification process ensures that only legitimate transactions are added to the blockchain. If the block passes verification, each node adds it to its own copy of the blockchain, maintaining consistency across the network.

To determine which blocks are valid, nodes reach a consensus using cryptographic algorithms. These algorithms validate the transaction and confirm the sender's authenticity. The node that successfully performs this validation, known as a miner, is rewarded with cryptocurrency for its work. This process, called mining, ensures that only verified transactions are added to the blockchain.

Once the validation process is complete, the block is permanently added to the blockchain, finalizing the transaction. This decentralized approach makes blockchain highly secure and resistant to fraud, as each transaction must be validated before being recorded.

Blockchain technology offers significant advantages over traditional data storage systems. Its decentralized structure enhances security, ensuring that data remains tamperproof.

Additionally, blockchain provides better control and compliance measures while reducing the high costs associated with conventional data storage security. The distributed ledger system enables secure and costefficient data storage, making blockchain a superior alternative to traditional methods.

2. Blockchain Use Cases in Healthcare:

Blockchain technology has been widely adopted to enhance data storage and protect patient records in the healthcare industry. It ensures that the healthcare value chain remains secure and selfsustaining. Many industry leaders are actively exploring the full potential of blockchain,

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

developing innovative solutions that integrate it into the healthcare ecosystem. By understanding its holistic impact, blockchain can improve various aspects of healthcare, from billing processes to patient data management. It enhances security within the system, preventing data misuse while ensuring compliance with regulations. Additionally, blockchain provides greater control over information flow, helping to detect healthcare fraud and mitigate security threats.

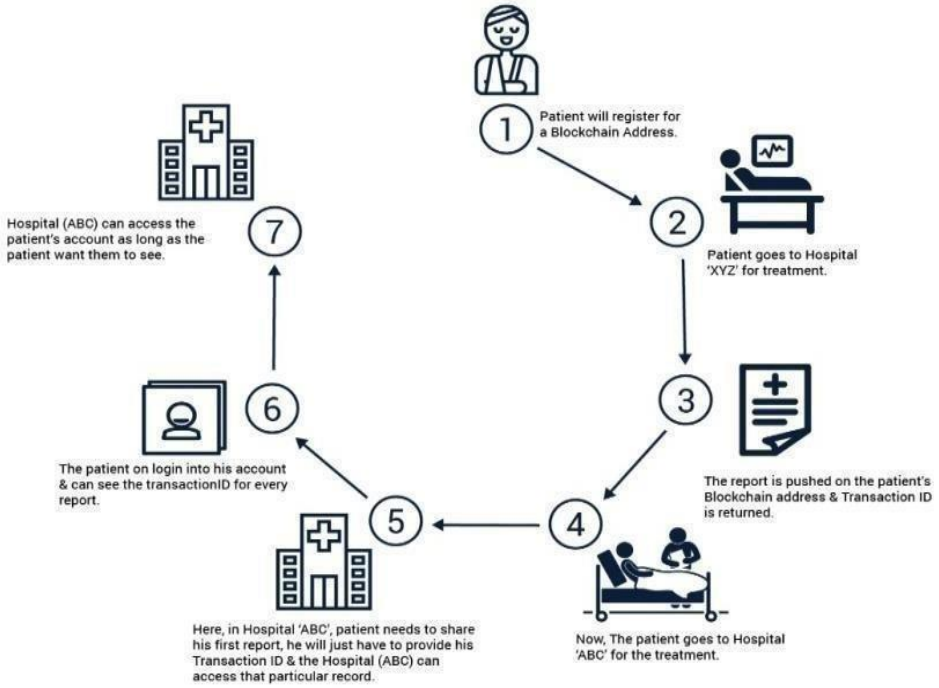

Figure 3: Blockchain to Increase Healthcare Security

One of the key advantages of blockchain is its ability to securely transfer patient data between different healthcare centers. As patients move from one facility to another, maintaining accurate and secure records becomes crucial. Blockchain creates a reliable and tamper-proof system that ensures seamless data sharing. Unlike traditional servers, blockchain does not rely on a single storage point, reducing the risk of data breaches. Its decentralized ledger structure enhances data integrity by distributing information across multiple nodes, ensuring that no single entity has complete control.

This approach strengthens security, promotes transparency, and contributes to the overall efficiency of healthcare data management.

3. Blockchain-based Healthcare Management Applications:

With the progress in electronic healthrelated data, cloud healthcare data storage and patient data privacy protection regulations, new opportunities are opening for health data management, as well as for patients convenience to access and share their health are immensely valuable to any datadriven organization, especially in healthcare where blockchain technology has the potential to resolve these critical issues in a robust and effective way.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

Figure 4 shows seven steps of healthcare data management workflow in blockchain, which are discussed below. Blockchain based applications in this category include data sharing, data management, data storage (e.g., cloud- based applications) and EHR, which are discussed in details below

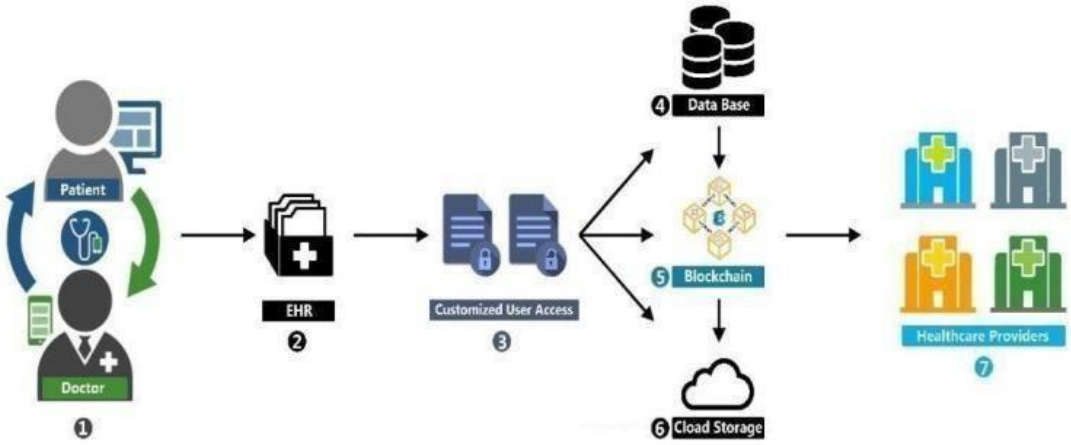

Figure 4: Healthcare Data Management in Blockchain

- **Step-1:** Primary data is generated by the interaction between a patient and their doctors and specialists. This data consists of medical history, current problem and other physiological information.
- **Step-2:** An EHR is created for each patient using the primary data collected in the first step. Other medical information such as those generated from nursing care, medical imaging, and drug history are also included in EHR.
- **Step-3:** Individual patient who has the ownership of sensitive EHR, and customized access control is given only to the owner of this property. Parties who want to access such valuable information must request permission which is forwarded to the EHR owner, and the owner will decide to whom access will be granted.
- **Step-4, 5, and 6:** These three steps are part of the core of the whole process including database, the blockchain, and cloud storage. Database and cloud storage store the records in a distributed manner and a blockchain provides extreme privacy to ensure customized authentic user access.
- **Step-7:** Healthcare providers such as ad hoc clinic, community care center, hospitals are the end user who wants to get access for a safe and sound care delivery which will be authorized by the owner. For example, no matter where you are treated in the globe, your health record will be available and accessible on your phone and validated through a distributed ledger such as blockchain, to which healthcare providers would continue to add to over time and unforgeability by using Merkle tree and order- preserving encryption.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

4. Data Management:

Even though many companies, especially healthcare institutions, are data driven, and the volume of data generated in this era or another era like the IoT is growing significantly, data security and privacy are continuously violated both unintentionally or by it users. A result, many institutions have experienced an enormous loss of reputation and capital. Different users of health data have different roles, and access to data should be governed by privileges allocated to these roles. Such mode of access can be ensured, in a seamless way, by blockchain technology. A new idea of reshaping the consent management in the healthcare system which mainly provides user to control the whole health record data by using blockchain was introduced. However, there is no authorization design and no access control in their implementation.

5. Health Education:

The primary use of the blockchain is a same mechanism for recording transaction of the Bitcoin digital currency, but this mechanism could be used in an education field too.The base of education is the exchange of knowledge as well as skills from multiple sources. It assumes the trustworthiness of all the parties involved. With the proliferation of online learning, it becomes challenging for regulatory agencies to control the alteration of knowledge in medical education. According to Funk et al. the health professions educators blockchain technology could potentially improve the quality of education and educational impact on multiple generations of learners. It can also help build a relative value of educational interventions. Additionally, any institution adopting blockchain technology would be able to provide certification on their own without any third party in between. Blockchain could also affect medical library management in many ways, including gathering, preserving, sharing authoritative information by creating timestamped, verifiable versions of journal articles.

V. PROPOSED APPROACH

The Proposed System aims to solve the health care sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding the third party accessing it without permission. EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger. A solution centered on the blockchain, can permit large-scale availability, data confidentiality, costeffectiveness, and belief in the information system.

1. Overview of Proposed Approach:

In the proposed healthcare data management system, healthcare providers first collect medical data from patients, including medical history, test results, and treatment records. This data is securely stored in hospital databases, ensuring that only authorized personnel can access it. To enhance security and maintain data integrity, a unique hash is generated for each data entry, acting as a digital fingerprint.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

These hashes are then sent to a blockchain, a decentralized and tamper-proof ledger, which adds an extra layer of security and transparency. Patients have complete control over their data, allowing them to grant or revoke access for specific stakeholders such as healthcare providers, insurers, or researchers. When an authorized party needs access to medical records, they query the blockchain, which verifies their request before granting access to the data stored in hospital databases. This secure and transparent system improves patient trust and protects sensitive information.

Building an electronic medical health records (EMHR) system using blockchain requires a well-planned approach. First, key stakeholders including healthcare providers, patients, and regulators—must be identified to understand their requirements, such as secure data sharing, privacy protection, and compliance with regulations. The next step is designing the blockchain architecture, selecting a suitable platform (e.g., Ethereum or Hyperledger Fabric) based on factors like scalability, privacy features, and security. The system must comply with healthcare regulations such as HIPAA and GDPR while ensuring smooth integration with existing electronic health record (EHR) systems. Smart contracts are developed to manage access control and record sharing, and privacy-enhancing techniques like zero-knowledge proofs may be implemented to protect sensitive data.

Strong identity verification methods, including digital signatures and biometric authentication, are used to confirm the identities of patients and healthcare providers. APIs and data exchange standards are created to enable seamless integration with third-party applications. Security measures such as encryption, multi-factor authentication, and regular audits ensure data protection. Before full deployment, the system undergoes thorough testing in a controlled environment with a pilot program. Once launched, it is continuously monitored, and feedback is gathered to refine and optimize its performance.

2. SHA-1 Algorithm:

The SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function that produces a fixedsize hash value (160 bits) from input data of arbitrary size. It is designed to be a one-way function, meaning it is computationally infeasible to reverse the hash value back to the original input data. SHA-1 is commonly used in various security applications, such as digital signatures, message authentication codes, and checksums, to ensure data integrity and authenticity.

In the SHA-1 algorithm, the input data is processed in blocks of 512 bits. The algorithm performs a series of logical operations, including bitwise operations such as AND, OR, and XOR, as well as rotations and additions modulo 2^32. These operations are applied to the input data in multiple rounds to generate the final hash value. The algorithm also includes a series of constant values and functions that are used in each round to introduce non-linearity and ensure the security of the hash function.

One of the key benefits of the SHA-1 algorithm is its cryptographic strength, which means it is highly resistant to collision attacks. A collision occurs when two different inputs produce the same hash value. While SHA-1 has been deprecated due to vulnerabilities discovered in its collision

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

resistance, it is still widely used in legacy systems and applications. However, for new applications, it is recommended to use more secure hash functions, such as SHA-256 or SHA-3, which offer higher levels of security and resistance to collision attacks.

Algorithm:

A] Convert the message "hello" to its binary representation: 01101000 01100101 01101100 01101100 01101111.

B] Add Padding: 01101000 01100101 01101100 01101100 01101111 1 00000000 ... 00000000 00000101 11000000 (total length is 512 bits).

C] Divide the message into 512-bit blocks: [01101000 01100101 01101100 01101100 01101111 10000000 ...], [00000000 ... 00000101 11000000].

D] Initialize the SHA-1 hash buffer: A = 0x67452301, B = 0xEFCDAB89, C = 0x98BADCFE, D = 0x10325476, E = 0xC3D2E1F0.

E] Process each block following the SHA-1 algorithm's steps.

F] The final SHA-1 hash for the message "hello" is 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c.

Steps of SHA-1 Algorithm:

- Padding: Append padding bits to the message so that its length is congruent to 448 modulo 512. The padding starts with a single 1-bit, followed by zeros, and ends with a 64-bit representation of the original message length.
- Dividing into Blocks: Divide the padded message into blocks of 512 bits (64 bytes).
- Initialization: Initialize the SHA-1 hash buffer (5 32-bit words, often represented as A, B, C, D, E) with the hash values from the SHA-1 standard.
- Processing Blocks: For each block, extend the 512-bit block into an 80word array of 32bit words. For words 16 to 79, apply a function to mix the words.
- Initialize Variables: Initialize variables for this chunk: a = A, b = B, c = C, d = D, e = E
- Main Loop: Perform 80 iterations of a compression function. In each iteration, update the variables a, b, c, d, and e using bitwise operations and logical functions.
- Update Hash Buffer: After processing each block, update the hash buffer by adding the current hash values to the computed values of a, b, c, d, and e.
- Output: The final hash value is the concatenation of the five 32-bit words in the hash buffer, typically represented as a 160bit hexadecimal number.

Needs of SHA-1 Algorithm:

SHA-1 (Secure Hash Algorithm 1) is a cryptographic function that generates a 160bit hash value from any input data. It is commonly used for digital signatures, data integrity checks, and password storage. For example, when downloading a file, its SHA1 hash can be compared to the original to detect tampering. Similarly, in password storage, only the hashed version is stored, ensuring security.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

Despite its known vulnerabilities to collision attacks, SHA-1 can still be useful in encrypted patient data sharing and appointment coordination. It can help verify the integrity of medical records stored on a blockchain or cloud, ensuring they remain unaltered. Additionally, SHA-1 can streamline appointment coordination by securely hashing patient details, allowing for efficient authentication without exposing sensitive data. However, for enhanced security, newer hash functions like SHA256 are recommended.

3. UML Diagram:

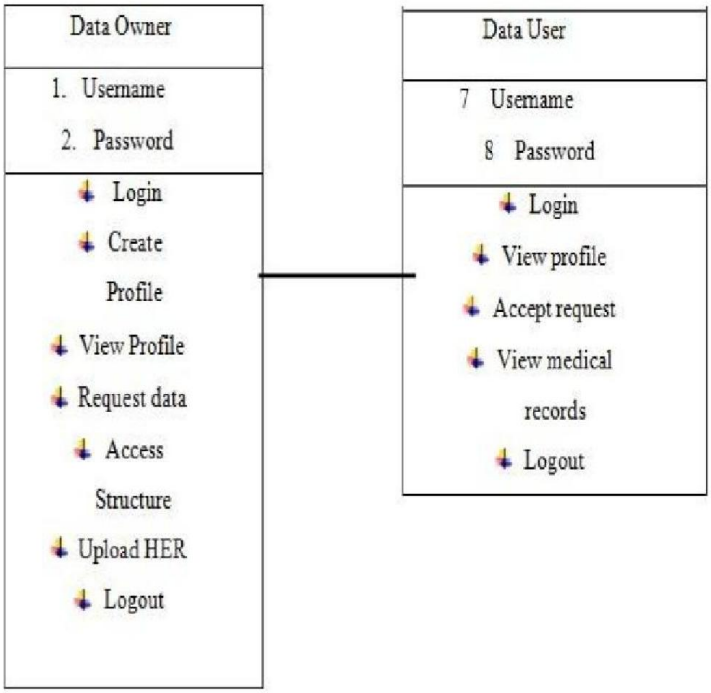

Figure 5: UML Diagram

4. Use Case Diagram:

A use case diagram is a behavioral diagram defined and created from a Use- case analysis. Its purpose is to represent a graphical overview of the functionality provided by a system in terms of actors and any dependencies. The main purpose of a use case diagram is to show how system functions are performed for which actor. Roles of the actors in the system can be depicted as below.

- **Data User :**
  Data user are the patients by login in they can view profile and medical record as well as accept the request if its necessary.
- **Data Owner:**
  Data owner the persons from hospitals who can create profile and requests patients and then view their history if any and if required create new case.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

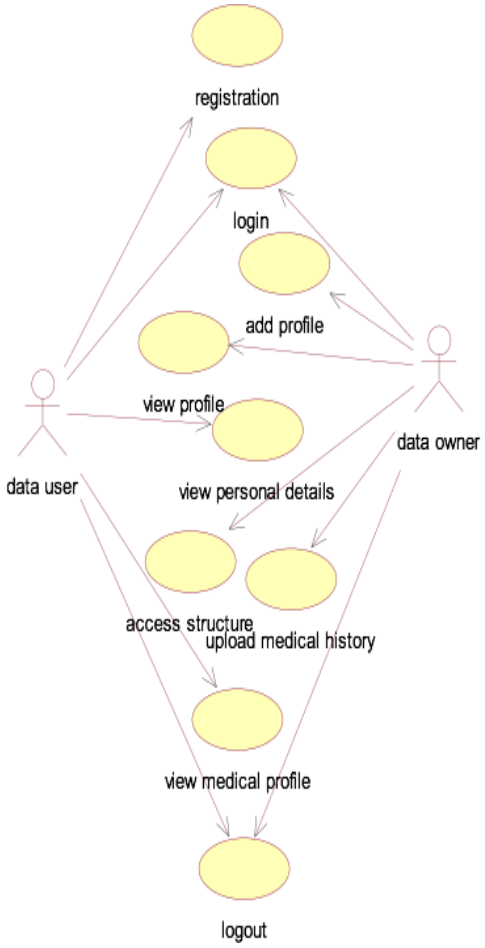

Figure 6: Use Case Diagram

VI. EXPERIMENTAL RESULTS AND DISCUSSION

This chapter introduces the Experimental setup that includes the hardware and software requirements for the "A System for Electronic Medical Health Records Sharing based on Blockchain". This chapter also introduces the experimental results that involved description of datasets and the screenshots of working system.

1. **Experimental Setup:**

Hardware Requirements

- System : Dual Core & more 2.4 GHz
- Processor Hard Disk : 500 GB.
- Ram : 2 GB

Software Requirements

- Operating System : Windows 7
- Technology Used : PHP,HTML,CSS,JAVASCRIPT, BOOTSTRAP
- Database Used : MySQL,XAMPP

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

2. Implementation and Results:

Blockchain is great for creating a single patient registry (Electronic health records). In fact, there will be a single base with a high level of security, stable operation and access from anywhere. Having such an infrastructure, the patient does not need to worry about data synchronization. Any doctor can review the medical history and prescribe treatment, of course only after the patient's permission. All data will be recorded in the general register, regardless of whether it is a private reception or health insurance application.

After all, often, a private doctor's appointment is not displayed anywhere in the patient's history. This will make it possible to see a clearer picture of the patient's illnesses. Our company, Mere head, is developing a web application in the healthcare, the interaction of doctors and patients and we believe that this is what is missing in the healthcare industry - the consolidation of patient data in one place based on reliable distributed technology.

This approach will significantly reduce the cost of hardware clinics. The data will be updated in real time, and the processing will be reduced several times. Within a few seconds, the doctor can find out blood group, chronic diseases, allergic reactions, etc. Thus, there is no need to do repeated tests. This will save time and increase the speed of treatment.

But there is a problem, the standardization of data. It is very important that all data is stored in one format and not lead to confusion. In addition, all information should be recorded according to preestablished standards. It may take several years. The data must be reliable and confirmed by the patient himself.Another problem is the reliability of the diagnosis. A wrong diagnosis can lead to wrong treatment. This will be displayed in the list of Electronic health records and may affect the following doctors decisions. A blockchain is a growing list of records, called blocks, that are linked together using cryptography Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it.

Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks. Although blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Blockchain technology is an effective way to provide security to the medical records where it is also known as distributed ledger technology, where it requires no third party to organize, maintain, manage data in the records the implementation is done in the steps :

- **Building a Record:**

  Structure and how patients and physicians can access the data Here patients information must be keep secured and how data users can access thedata is also important the structure is built how data is inserted and how data isretrieved. Here, the structure is built with two

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

users data owner and data user and howthere profile creations and problem description for data owner and tests, results, other information is added and how the data owner can access that information is built.

- **Webpage:**

  Is designed based on the record structure where the code is written for index page, registration. Data owner, data user ,and their profiles, problem description. Here data owner will not provide access to everything stored in the block chain provides only specific and required information for data user. If data user wants to view more information from the data owner he needs to gain access again from the data owner. This is why it is more secure this can be written using smart contract functionality.

3. Screenshots:

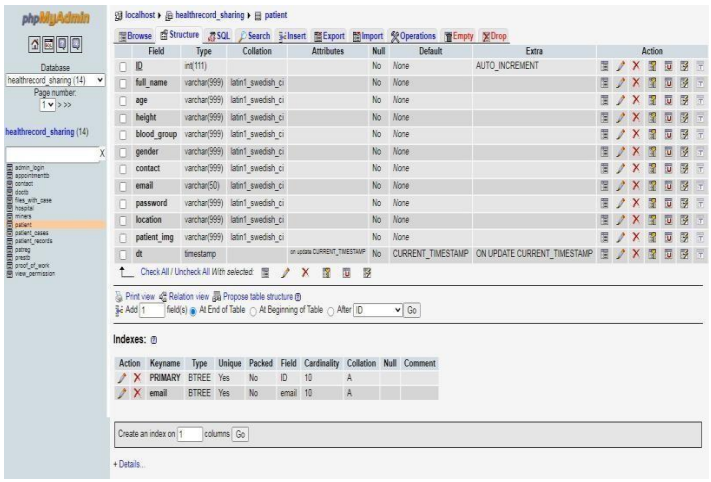

Figure 6: Patient Table

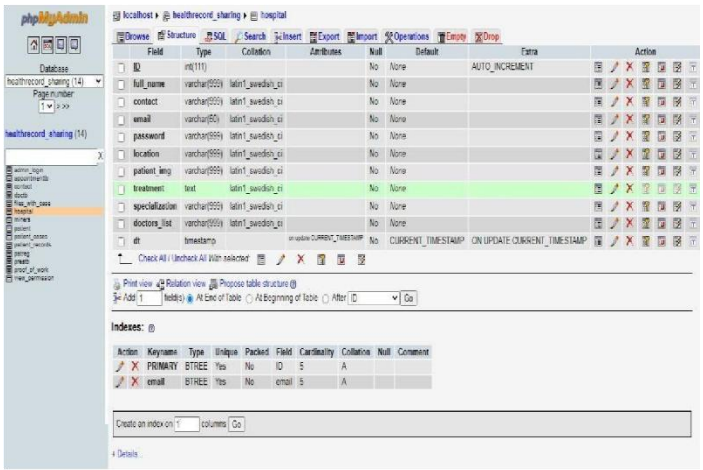

Figure 7: Hospital Table

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

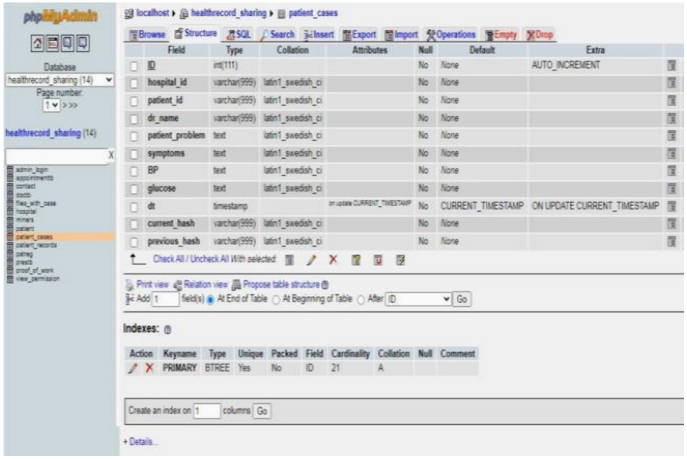

Figure 8: Patient_Cases Table

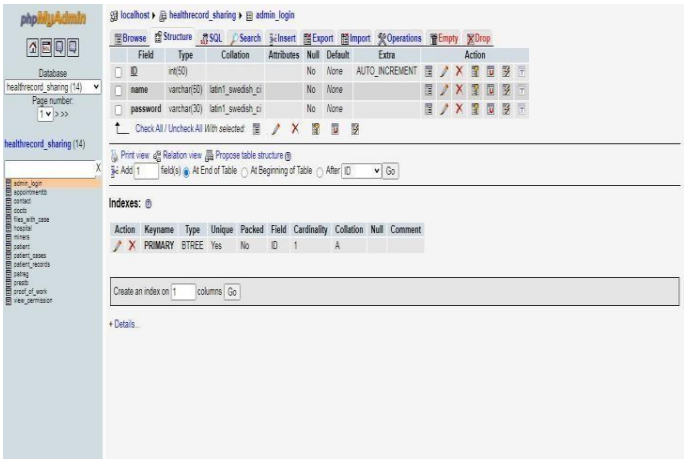

Figure 9: Admin Table

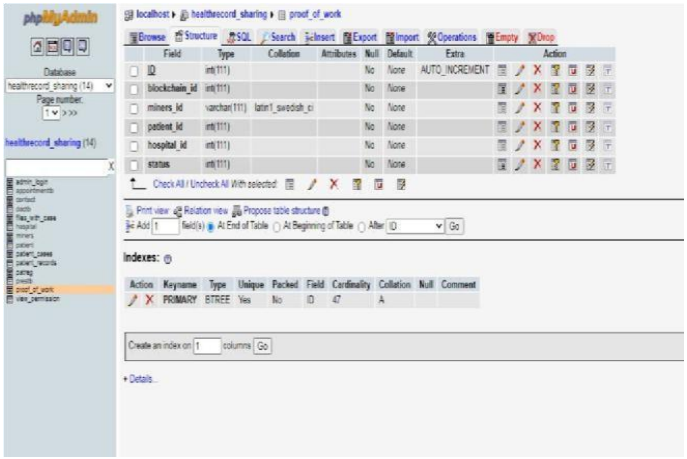

Figure 10: User table

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

Figure 11: Home Page

Figure 12: Main Navigation Links of Home Page

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

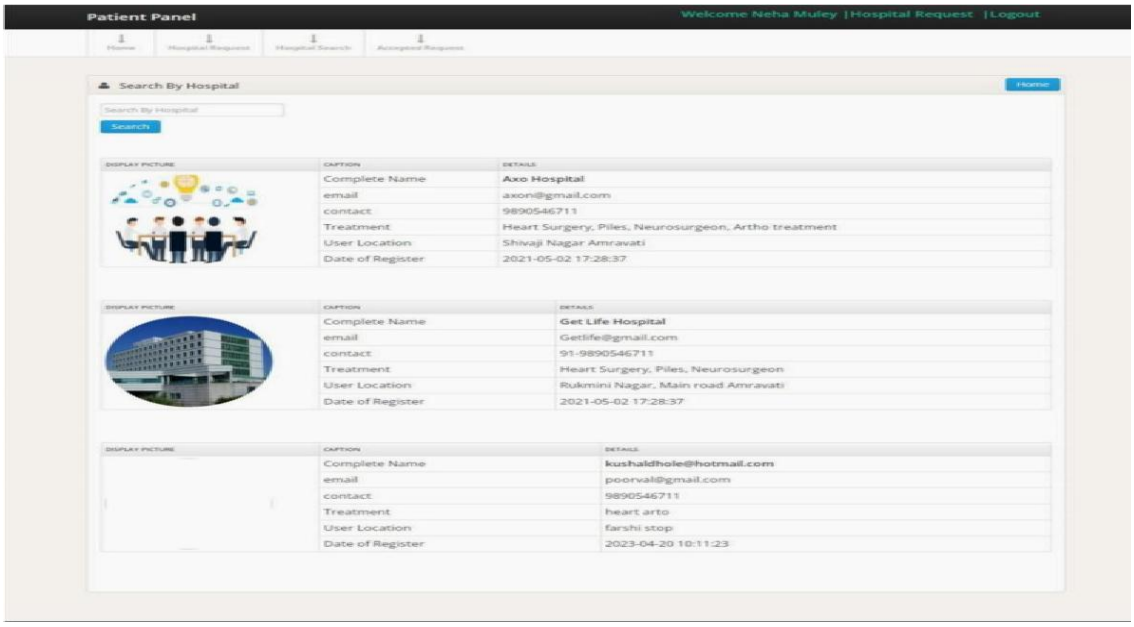

Figure 13: Hospital Search Page

VII. CONCLUSION AND FUTURE SCOPE

This chapter introduces the conclusion and future scope of A System for Electronic Medical Health Records Sharing based on Blockchain.

1. **Conclusion:**

   The blockchain technology is gaining significant attention from individuals, as well as organizations of nearly all kinds and dimensions. Despite the advancement in healthcare sector and technological innovation in EHR systems they still faced some issues that were addressed by this novel technology, i.e., blockchain. Our proposed framework is a combination of secure record storage along with the granular access rules for those records. It creates such a system that is easier for the users to use and understand. Also, the framework proposes measures to ensure the system tackles the problem of data storage as it utilizes the offchain storage mechanism of IPFS. And the role-based access also benefits the system as the medical records are only available to the trusted and related individuals. This also solves the problem of information asymmetry of EHR system.

2. **Future Scope:**

   The scope of Blockchain in healthcare looks super up-and-coming and promising as it helps to solve some of the pressing issues afflicting the industry. As Blockchain is decentralized unlike the majority of the healthcare records that are centralized, we envision a progressive future. A future where blockchain acts as an element of a system in which patients will become stewards of their own medical data, in place of relying on a central source. Of Course, the application of blockchain comes with its own set of technical challenges.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 2 | Issue 6 | December 2023

www.ijirid.in

REFERENCES

[1] S. Nakamoto, "Bitcoin: A PeertoPeer Electronics Cash System," pp. 1–9, 2008.

[2] W. J. Gordon and C. Catalina, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient Driven Interoperability," Computer. Struct. Biotechnology. J., vol. 16, pp. 224– 230, 2018.

[3] J. Eberhardt and S. Tai, "On or Off the Blockchain? Insights on Off- Chaining Computation and Data," Smart SOA Platforms Cloud Comput. Archit., no. October, pp. 11–45, 2014.

[4] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and Ethereum: A brief overview," 2018 17th Int. Symp. INFOTEHJAHORINA, INFOTEH 2018 - Proc., vol.2018Janua, no. March, pp. 1–6, 2018.

[5] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," IEEE Intel. Veh. Symp. Proc., vol. 2018-June, no. Iv, pp. 108–113, 2018.

[6] T. T. Kuo, H. E. Kim, and L. OhnoMachado, "Blockchain distributed ledger technologies for biomedical and health care applications," J. Am. Med. Informatics Assoc., vol. 24, no. 6, pp. 1211– 1220, 2017.

[7] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Comput. Struct. Biotechnology. J., vol. 16, pp. 267– 278, 2018.

[8] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, "Sharing Medical Questionaries based on Blockchain," Proc. - 2018 IEEE Int. Conf. Bioinforma. Biomed.BIBM 2018, pp. 2767–2769, 2019.

[9] M. S. Sahoo and P. K. Baruah, "HBasechainDB -- A Scalable Blockchain Framework on Hadoop Ecosystem," in Supercomputing Frontiers,2018, pp. 18–29.

[10] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K. and Tzovaras, D.,2018, August.