IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOCARE: Blockchain Based Health Record Management System

[1]G Manasa, [2]T Sri Pujitha, [3]P Sri Ram, [4]P Mallikharjuna

[1]Student, [2]Student, [3]Student, [4]Student,

[1234] Department of CSE- ATIFICIAL INTELLIGENCE AND MACHINE LEARNING,

[1,2,3,4] Aditya College of Engineering and Technology, Surampalem, Andhra Pradesh, India.

Abstract: The growing use of digital healthcare systems has sparked major worries about the security, privacy, and availability of Electronic Health Records (EHRs). Traditional centralized systems are prone to data breaches, lack transparency, and offer patients limited control. Moreover, they are susceptible to side-channel attacks that take advantage of indirect information leaks during cryptographic processes. This paper introduces CryptoCare, a healthcare management system built on blockchain technology and combined with cryptographic blinding methods to guarantee secure and privacy-focused data handling. The system implements a patient-focused approach that allows individuals to dynamically choose or switch hospitals, with automatic removal of access to prior hospitals to safeguard data privacy. Smart contracts implement role-based access control, enabling doctors to view records only when patients give their permission. A special emergency access system allows doctors to access patient records when the patient is not available, provided it is approved by a super administrator, and includes complete audit logs and notification to the patient. Medical records are kept secure through off-chain storage (IPFS), whereas the blockchain is used to keep unchangeable access logs and metadata. The suggested system improves data confidentiality, integrity, transparency, and accessibility, positioning it as a dependable and scalable solution for contemporary healthcare systems.

Index Terms - Blockchain, Healthcare Security, Electronic Health Records, Cryptographic Blinding, Smart Contracts, IPFS

I. INTRODUCTION

The healthcare industry has undergone quick digital changes, allowing for effective storage and exchange of patient information via Electronic Health Records (EHRs). Nevertheless, this progress has also created significant challenges concerning data security, privacy, and trust. Traditional centralized healthcare systems are very susceptible to cyberattacks, unauthorized access, and single-point failures, which can endanger sensitive patient data.

Furthermore, current cryptographic methods are not entirely secure against sophisticated threats like side-channel attacks, in which attackers use indirect data such as processing time or energy usage to gain unauthorized access. These weaknesses emphasize the importance of developing stronger and more secure methods that go beyond traditional encryption techniques. A major drawback of current systems is that patients do not have control over their own medical information. Patients frequently encounter challenges when managing access rights or transitioning between hospitals, resulting in privacy issues and inefficient operations.

To address these challenges, this paper introduces CryptoCare, a blockchain-based healthcare management system aimed at improving security and giving patients greater control. The system combines cryptographic blinding, decentralized storage, and access controls based on smart contracts. It allows patients to safely handle their records, manage who can access them, and protect their privacy while keeping transparency and trust intact in the healthcare system

II. EXISTING & PROPOSED SYSTEM:

Exisiting System

Current healthcare record management systems mainly depend on centralized databases managed by individual hospitals or organizations. These systems keep patient information in separate environments, resulting in weak compatibility and restricted data exchange between organizations. Because of their centralized nature, they are extremely susceptible to cyberattacks, data leaks, and single-point failures. While conventional encryption methods are employed, they are not enough to defend against sophisticated threats like side-channel attacks. Patients have limited control over their medical records, as access rights are generally handled by healthcare professionals.

Moreover, these systems do not allow for dynamic switching between hospitals, which complicates the secure transfer of patient records between different institutions. Access tracking is frequently unclear, which diminishes responsibility and confidence. In general, the current system is lacking in security, transparency, and control focused on the patient, which creates major difficulties in today's healthcare settings.

Proposed System

The suggested system, CryptoCare, presents a decentralized and secure framework for managing healthcare records through the use of blockchain technology. It allows for a patient-focused approach, enabling patients to choose or switch hospitals dynamically, with automatic removal of access from previously linked hospitals. The system uses role access control based on smart contracts, enabling doctors to view medical records only when given direct permission by the patient. All transactions and access records are stored on the blockchain, guaranteeing openness and permanence.

To improve security, encryption uses cryptographic blinding methods to guard against side-channel attacks and safeguard sensitive patient information. Medical records are kept secure through IPFS, and blockchain is used to keep track of hash references for verification purposes. In addition, there is an emergency access feature that allows doctors to request access in critical situations, but this must be approved by a super administrator, and it includes proper audit logs and notification to the patient.

III. RELATED WORKS

Significant research has focused on improving security and transparency in healthcare data management with digital technologies. Traditional healthcare systems mainly use centralized databases to store and manage Electronic Health Records (EHRs). While these systems make it easier to access and share data, they are at risk of data breaches, unauthorized access, and failures at a single point. They also lack proper audit trails and give patients limited control over their own medical data.

Blockchain technology offers a promising way to tackle these problems. It provides a decentralized and unchangeable ledger for storing healthcare records. Several studies have shown that blockchain can enhance data integrity, allow secure data sharing among different parties, and provide clear audit trails. It removes the need for a central authority and makes sure that all transactions are verifiable and resistant to tampering. However, most current blockchain systems mainly focus on backend security and do not fully address usability and patient-centered features.

Recent progress has also looked at using decentralized storage solutions like IPFS to manage large medical data efficiently. Smart contracts help enforce access control policies and automate secure data sharing. Despite these innovations, many systems do not protect against advanced threats such as side-channel attacks and lack flexible features like dynamic access control or emergency access. The CryptoCare system fills these gaps by combining blockchain, cryptographic blinding, and patient-focused access methods to offer a secure and effective healthcare solution.

IV. METHODOLOGY

The suggested CryptoCare system is built with a modular and layered structure, intended to provide secure, transparent, and patient-focused management of healthcare records. The framework combines patient registration, hospital selection, decentralized storage, blockchain-based access control, cryptographic security, and emergency access management into a single, cohesive process. Each module within the system carries out a particular role, guaranteeing scalability, dependability, and smooth communication between stakeholders like patients, physicians, and super administrators.

The design allows patients to securely handle their medical records and adjust access permissions as needed. Patients have the option to choose or switch hospitals whenever they want, and the system automatically removes access from their previous hospitals to ensure privacy. Medical records are

encrypted and kept in a decentralized storage system, with blockchain used to keep permanent logs and manage access rights to ensure transparency and the ability to audit.

Smart contracts are used to enforce role-based access control, enabling doctors to view records only when approved by the patient. Furthermore, an emergency access feature is included, allowing doctors to request access in critical situations, provided it is approved by the super administrator, with appropriate logging and notification to the patient. The modular structure enables each system component to be upgraded individually without impacting overall performance, providing a secure, efficient, and scalable solution for managing healthcare data.

4.1 System Architecture Overview

The CryptoCare architecture is made up of several functional layers, such as patient registration, hospital management, decentralized storage, blockchain-based access control, and cryptographic security. Patients sign up using a web-based interface and securely submit their medical records. These records are kept in a decentralized storage system, with their encrypted hash stored on the blockchain to guarantee data integrity. Smart contracts implement role-based access control, enabling doctors to view records only when authorized by the patient. Patients can dynamically choose or switch hospitals, and the system automatically removes access from previously linked hospitals. A mechanism for emergency access is available, allowing doctors to request access during critical situations, which is approved by the super administrator with appropriate logging. Patients are informed about this access as well as the reason behind it.

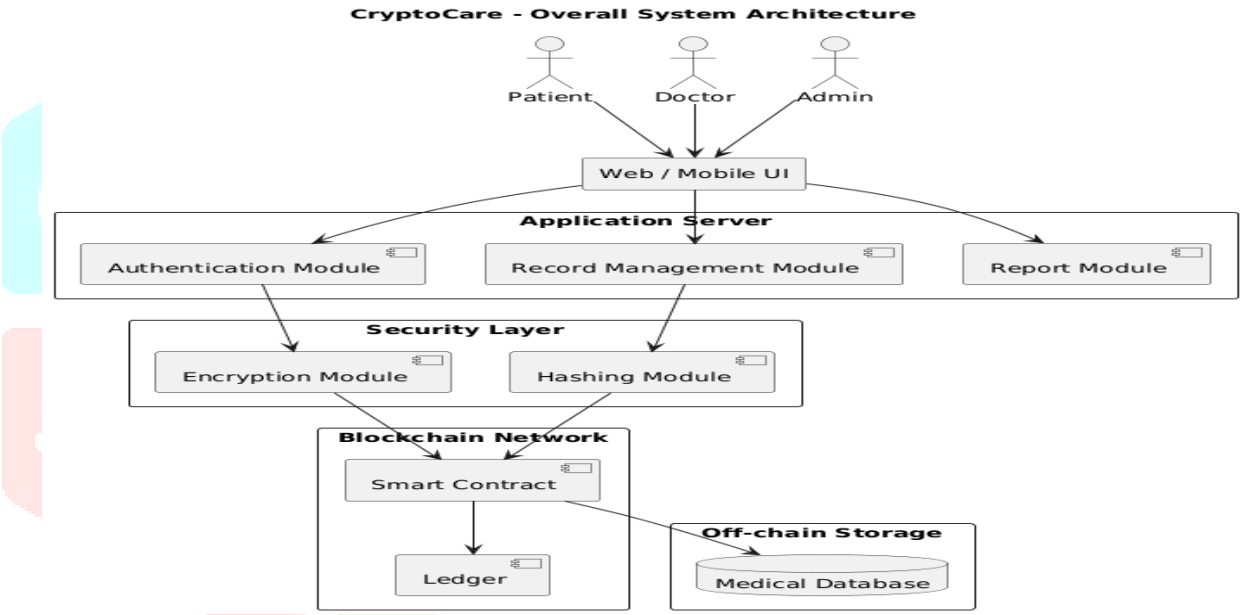

Figure 1: CryptoCare System Architecture

4.2 Authentication and User Management Module

This module acts as the system's main access point, allowing users such as patients, doctors, and administrators to securely register and log in. It uses role-based authentication to make sure that each user can only access the functions that are assigned to their specific role. Patients handle their profiles and choose hospitals, while administrators manage system users such as hospitals and doctors. The module provides secure identity confirmation and manages access to the system.

4.3 Medical Record Management Module

This module is responsible for creating, uploading, and managing patient medical records. Patients can safely upload reports, prescriptions, and diagnostic information via the app's interface. The system organizes and checks the data prior to processing. Patient records are connected to the individual and can only be accessed by authorized personnel, allowing for controlled viewing and updates of the information. sumers to confirm that the metadata retrieved is the same content uploaded in the first place.

4.4 Security Module (Encryption and Hashing)

The security module safeguards data confidentiality and integrity through the use of encryption and hashing methods. Medical records are encrypted prior to being stored in order to safeguard sensitive

information. Hashing algorithms create unique identifiers for each record, allowing the detection of alterations. Moreover, cryptographic blinding is used to safeguard critical operations against side-channel attacks, thereby improving security during data handling.

4.5 Blockchain and Smart Contract Module

This module oversees the blockchain network, utilizing smart contracts to enforce access control and ensure the security of transaction records. All access permissions, updates, and activities are logged on the blockchain ledger, guaranteeing immutability and transparency. The module ensures that only approved users can view medical records and stops any unauthorized changes.

4.6 Off-chain Storage Module

Medical records are kept in off-chain storage systems to enhance scalability and minimize the burden on the blockchain. The encrypted data is kept in a medical database, with only the hash reference being stored on the blockchain. This method guarantees effective storage, quicker access, and verification of data accuracy while keeping sensitive information secure.

4.7 Algorithm

Procedure SECURE_HEALTH_RECORD_MANAGEMENT (User U, Record R)

1. Register and verify user U (Patient, Doctor, or Admin).
2. The patient submits medical record R via the interface.
3. Encrypt record R and apply cryptographic blinding.
4. Keep encrypted data in external storage.
5. Create a hash for the record and save it on the blockchain.
6. Use smart contracts to grant access permissions.
7. If a patient switches hospitals, cancel their previous access.
8. For emergency access:
9. a. A physician requests access
10. b. An administrator verifies and approves the request
11. c. The access is recorded on the blockchain
12. d. The patient is informed of the reason
13. Retrieve and confirm the record using the blockchain hash.
14. End the Procedure

V. RESULTS & DISCUSSION

A. Evaluation of the System Workflow.

The CryptoCare system was tested by simulating real-time healthcare processes including patient registration, hospital selection, uploading medical records, granting access, and managing emergency access. Various user roles, such as patients, doctors, and administrators, were verified through secure login methods to ensure proper role-based access. The system made sure that all record transactions and access activities were securely logged on the blockchain and synchronized with off-chain storage, showing efficient and dependable healthcare data management.

B. Dashboard Validation Based on Roles.

Role-specific dashboards were evaluated to check the visibility and operational access for patients, doctors, and administrators. Each user was restricted to the functions assigned to their role, which stopped them from performing unauthorized actions. This provided strict access control and enhanced operational clarity within the system.

C. Integrity and Storage of Medical Records.

The procedure for uploading and keeping medical records was evaluated by encrypting the data and connecting it to blockchain hash references. The system effectively preserved data integrity during retrieval, guaranteeing that records stayed untampered after being stored.

D. Access Control and Verification.

The process of verifying access was tested by letting doctors view patient records only after getting the patient's consent. The system made sure that all access requests and approvals were securely documented, showing good control over confidential medical information.

E. Enforcement and Security of Smart Contracts.

Unauthorized access attempts were deliberately carried out to evaluate the system's security. In every instance, smart contracts limited unauthorized actions, guaranteeing safe data access and preserving a trustworthy record of all activities.

F. Tracking Records and Activity Timeline.

The system was tested to monitor record access and changes in a time-ordered sequence. Blockchain timestamps guaranteed precise ordering of events, enabling users to track access history and identify any anomalies.

G. Performance Observations.

The system's performance was evaluated using transaction confirmation time, data retrieval speed, and response time for access. Most operations were finished in seconds, depending on network conditions, and repeated data access was improved by using effective storage methods**.**

H. User Interaction and Usability Testing.

The usability testing revealed that the system's interface was easy to use and friendly for both patients and doctors. Features like restricted access, hospital switching, and emergency access enhanced the user experience and made the system simple to use without requiring technical knowledge.H. User Interaction and Usability Testing.

I. Comparison with Traditional Healthcare Systems.

Compared to conventional centralized systems, CryptoCare offers improved security, openness, and greater patient control. Blockchain technology provides secure, unalterable records, and decentralized storage enhances the system's ability to scale. The system decreases reliance on central authorities and enhances confidence in the management of healthcare data.

VI.FiguresandTables

ID	Scenario	Result
TC-01	User registration and secure login (Patient/Doctor/Admin)	Pass
TC-02	Identification of the user's role on the patient dashboard	Pass
TC-03	Identification of the user's role on the doctor dashboard	Pass
TC-04	Patient selects a hospital and completes profile setup	Pass
TC-05	Upload and encryption of medical records	Pass
TC-06	Secure storage of records in an off-chain database	Pass
TC-07	Generation and storage of blockchain hashes	Pass
TC-08	Doctor granted access with patient consent	Pass
TC-09	Switching hospitals with automatic revocation of access	Pass
TC-10	Emergency access request and admin approval	Pass
TC-11	Notification to the patient after emergency access is granted	Pass

Table 1: Functional Validation of CryptoCare Workflow

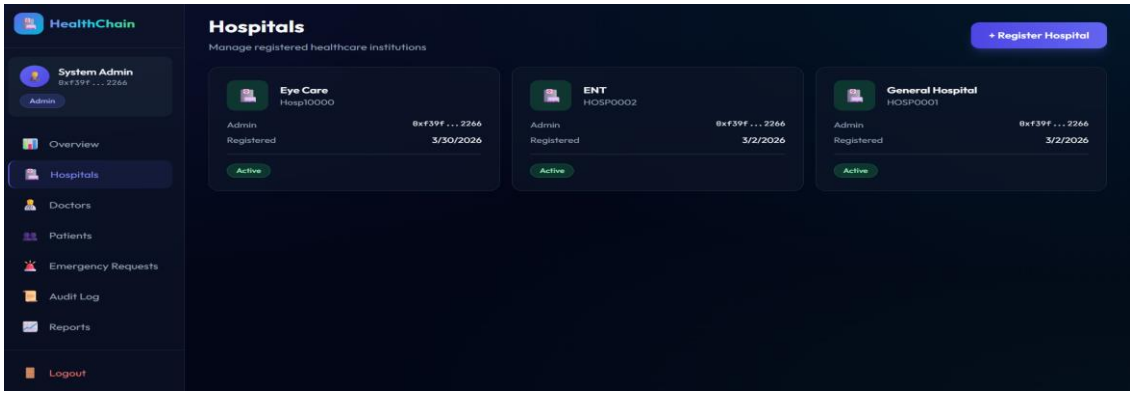

Figure 2: Admin dashboard consisting

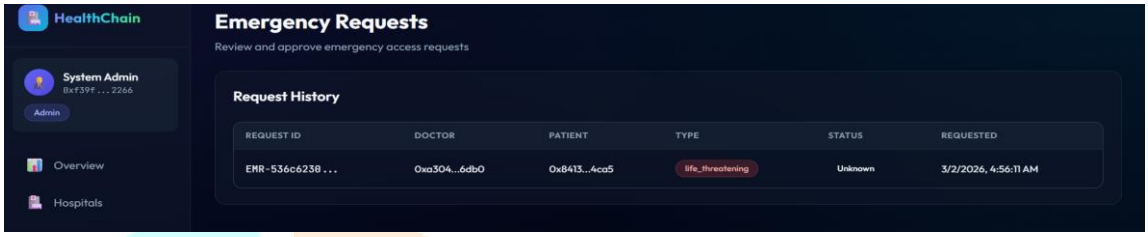

Figure 3: Emergency Requests history that are approved in Admin Dashboard.

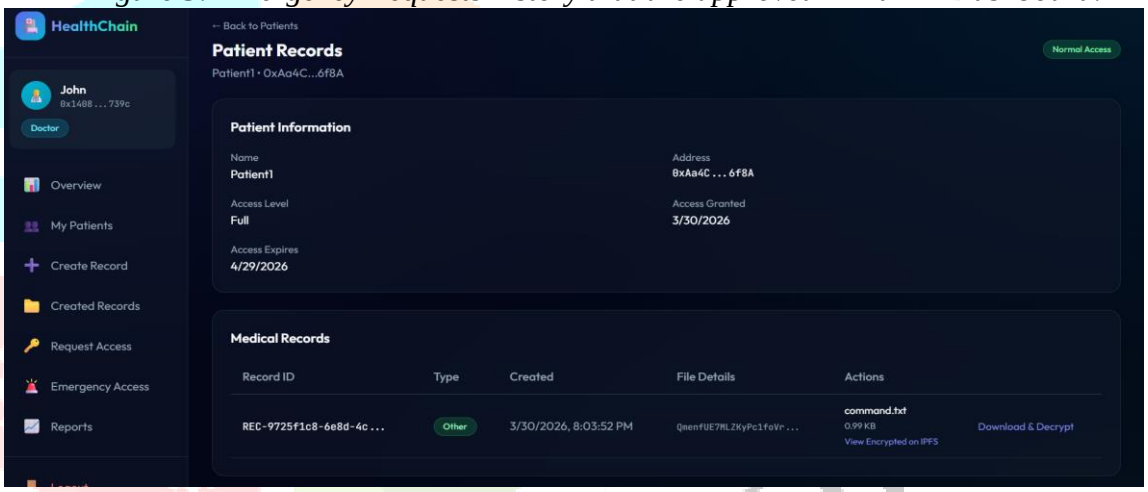

Figure 4: Doctor dashboard to view patients records by decrypting

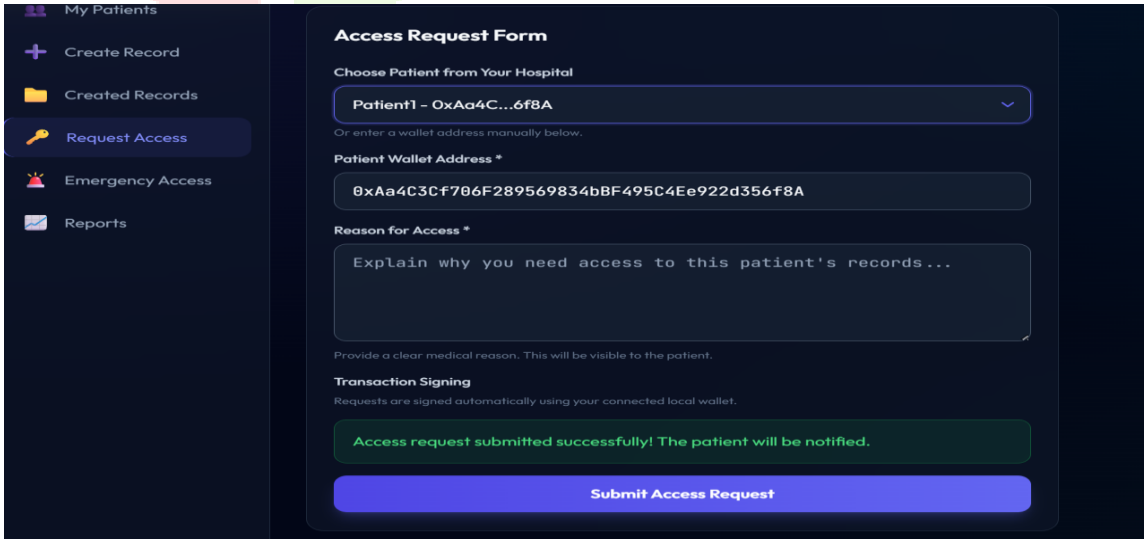

Figure 5: Doctor Request form to request patients records

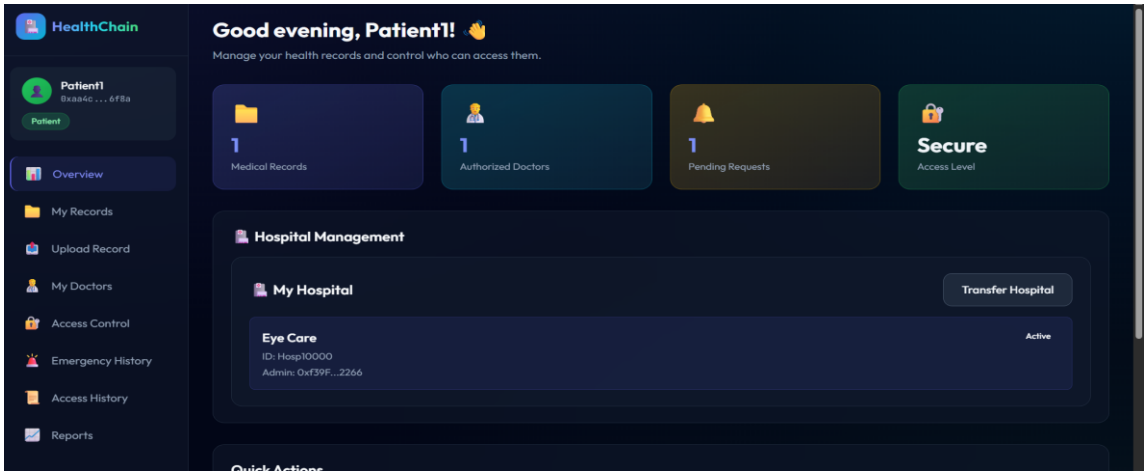

Figure 6: Patient Dashboard

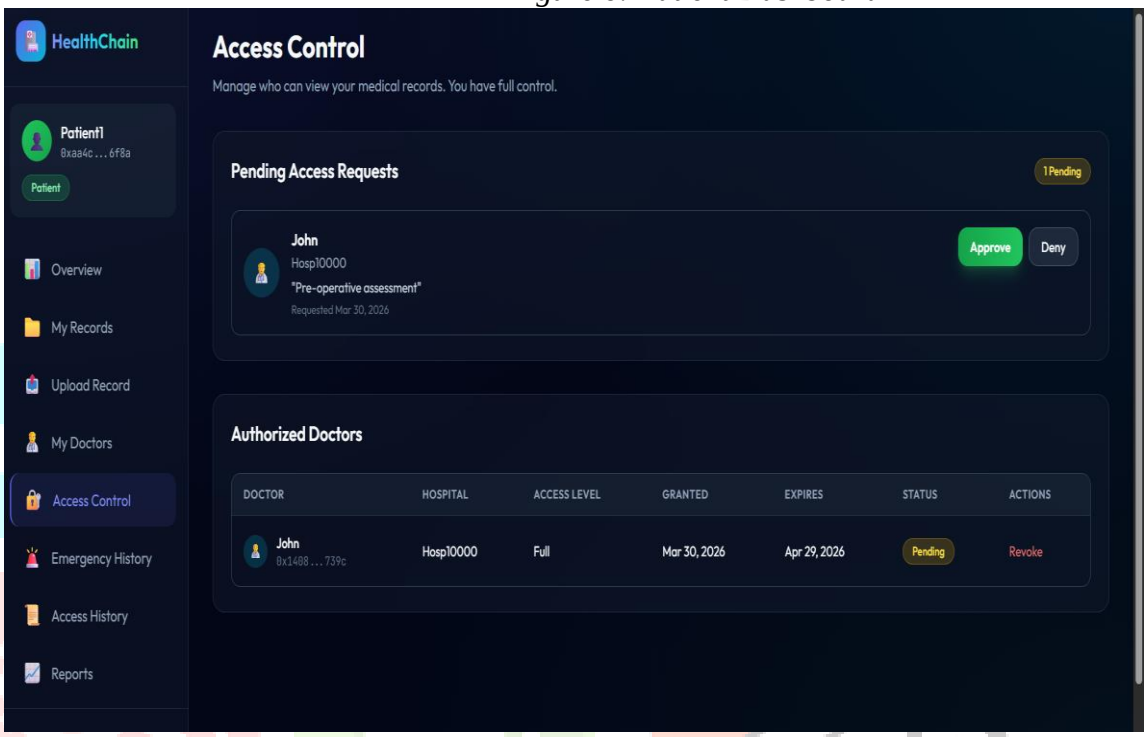

Figure 7: Patients Access Control to give permission for doctors.

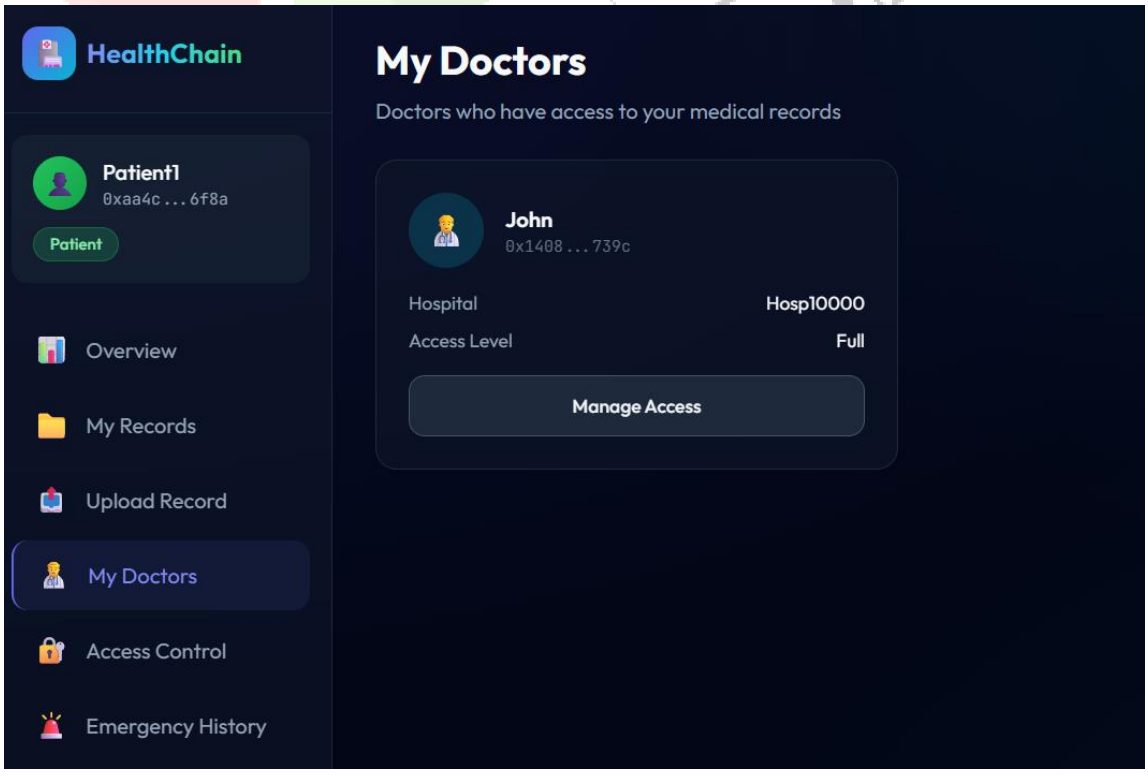

Figure 8: Doctors list which are being treated by patient.

VII.FUTURE SCOPE

The CryptoCare framework offers a solid basis for secure, patient-focused healthcare data management; nevertheless, several improvements could be made to enhance its scalability and practical implementation. Future research could involve implementing the system on Layer-2 blockchain networks to lower transaction costs and enhance processing speed, allowing for the effective management of large healthcare datasets. Connecting with IoT-based healthcare devices, like wearable sensors and remote monitoring systems, can enhance the automation of medical data gathering and minimize the need for manual involvement.

From a usability standpoint, enhancements can be achieved by creating mobile-friendly apps and streamlining login processes to make the system easier for non-technical users to access. Furthermore, advanced analytics and AI-driven models can be used to spot irregularities in patient data, recognize possible health threats, and improve decision-making processes. Another key area is ensuring compatibility with current hospital management systems and healthcare APIs, enabling smooth integration into existing medical infrastructures. Improving emergency access procedures through automated verification and multi-stage approvals can increase system reliability even more. These advancements will enhance the scalability, efficiency, and future adoption of blockchain-based healthcare systems.

VIII.CONCLUSION

This paper introduces CryptoCare, a healthcare management system built on blockchain technology aimed at improving data security, privacy, and patient autonomy. The system incorporates smart contracts to manage access based on roles, utilizes decentralized storage for effective data management, and employs cryptographic methods such as blinding to defend against sophisticated security threats. The suggested framework allows patients to handle their medical records, choose or switch hospitals as needed, and efficiently manage access rights. Introducing an emergency access system allows for the retrieval of essential medical information when needed, while ensuring transparency via audit trails and informing patients.

The system showed secure operations, dependable data accuracy, and effective access control when tested in simulated healthcare situations. Compared to conventional centralized systems, CryptoCare offers greater transparency, decentralization, and enhanced patient control. In general, the system provides a practical method for developing secure and reliable healthcare data management solutions in today's digital settings.

IX. REFERENCES:

[1] S. Alzahrani, T. Daim and K.-K. R. Choo, “Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems,” in *IEEE Transactions on Engineering Management (Volume: 70, Issue: 8, August 2023)*, 2022.

[2] Y. Chen, S. Ding, Z. Xu, H. Zheng and S. Yang, “Blockchain-Based Medical Records Secure Storage and Medical Service Framework,” *Journal of Medical Systems,* vol. 43, p. 5, 2019.

[3] E.-Y. Daraghmi, Y.-A. Daraghmi and S.-M. Yuan, “MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management,” *IEEE,* vol. 7, no. 10.1109/ACCESS.2019.2952942, pp. 164595 - 164613, 2019.

[4] D. V. Dimitrov, “Blockchain Applications for Healthcare Data Management,” *Healthcare Informatics Research,* vol. 25, no. 1, pp. 51-56, 2019.

[5] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah and S. A. Zabidi, “Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems,” *IEEE,* vol. 10, no. 10.1109/ACCESS.2022.3201878, pp. 94583 - 94615, 2020.

[6] H. M. M. A. K. Leila Ismail, “Performance Evaluation of a Patient-Centric Blockchain-based Healthcare Records Management Framework,” in *Association for Computing Machinery*, New York, NY, United States, 2020.

[7] A. A. Mamun, S. Azam and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," *IEEE,* vol. 10, no. 10.1109/ACCESS.2022.3141079, pp. 5768 - 5789, 2022.

[8] S. Mondal, M. Shafi, S. Gupta and a. S. K. Gupta, "Blockchain Based Secure Architecture for Electronic Healthcare Record Management," *GMSARN International Journal,* vol. 16, pp. 413-426, 2022.

[9] M. T. d. Oliveira, L. H. A. Reis, R. C. Carrano, F. L. Seixas, D. C. M. Saade and C. V. Albuquerque, "Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications," in *IEEE*, Shanghai, China, 2019.

[10] C. E. J. Pirtle, "Blockchain for Healthcare: The Next Generation of Medical Records?," *Journal of Medical Systems,* vol. 42, no. 10.1007/s10916-018-1025-3, p. 172, 2018.