

AN EFFICIENT DATA SECURITY IN MEDICAL REPORT USING BLOCKCHAIN TECHNOLOGY

Sathyanarayana S¹, Amruthesh², Dhruv G R³, H M Hemanth Nayak⁴, Hemanth C G⁵

¹Professor, ²Final year Student, ³Final year Student, ⁴Final year Student, ⁵Final year Student

Department of Computer Science and Engineering, Jawaharlal Nehru New College of Engineering, Shimoga

Abstract – The health care services industry is always showing signs of change and supporting new advancements and advances. One of the predominant requirements in today's health care systems is to protect the patient's medical report against potential attackers. Hence, it is basic to have secure information that can just approve people can get to the patient's medical report. So, it has proposed Block chain technology as a disbursed approach to grant security in accessing the medical report of a patient. It's composed of three phases: Authentication, Encryption and Data Retrieval using Block Chain Technology. For authentication – Quantum Cryptography.

Key Words: Block chain, Medical Report, Data Accessibility, Security, Encryption, Data Retrieval.

1. INTRODUCTION

The Block chain is the fastest growing technology through various applications in a secure manner. The various implementations make use of block chain technology among stakeholders. Banking, healthcare services, and supply chain management utilize this technology for its immense potential and secure data sharing management. Mainly, block chain technology plays a major role in the medical and healthcare system. Because of the decentralized and distributed technology, Block chain provides security services in healthcare.

Blockchain technology is a decentralized and transparent system that records transactions securely using cryptographic principles. It operates on a peer-to-peer network, ensuring no central authority controls the shared ledger. Transactions are grouped into blocks, linked through cryptographic hashes, forming an immutable chain. Its transformative potential spans beyond cryptocurrencies, impacting industries through decentralized applications.

2. RELATED WORKS

Siva Rama Krishnan S, Manoj M.K, Thippa Reddy Gadekallu, Neeraj Kumar, Praveen Kumar Reddy [2020]. The use of electronic medical records (EMRs) has simplified the processing of patient data because the patient does not need to carry documents and can simply show an identity card to retrieve a complete medical record history. This digitization has revolutionized the medical sector, but two major challenges exist with online records: security and trust. In this paper, a blockchain-based security framework is proposed to maintain the confidentiality of EMRs. This solution is also used to securely access the patient's records in any hospital—using the patient's public key as a universal identifier—and to obtain the medical record history of a patient much more quickly even during emergencies.

3. METHODOLOGY

There are mainly 6 steps:

- Patient Registration: New patients register with personal information to create a unique ID, public key, and privatekey. Existing patients can directly log in using their ID.
- Specialist Assignment: A specialist is assigned to the patient, and the doctor's information is registered in the system.
- Doctor Authorization: The assigned doctor is responsible for adding information to the patient's records and is authenticated using the AES algorithm.
- Data Update: If the doctor wants to add details, permission is obtained from the patient. The data is validated by the patient before updating the record.
- Data Encryption: The data is encrypted using the AES algorithm with a key provided by the patient.
- Data Storage and Retrieval: The encrypted data is stored in a private cloud with a timestamp, and the location address is stored in the Block chain.

4. PROPOSED SYTEM

The proposed system utilizes Block chain technology to ensure secure management of accessing medical records. It involves three key phases: Authentication using Quantum Cryptography, Encryption using AES algorithm, and Data Retrieval using SHA algorithm. Patients register with unique IDs and keys, doctors are authenticated before accessing or adding information to patient records, and data is encrypted and stored in a private cloud with timestamps. Authorized doctors can retrieve encrypted data from the Block chain, ensuring secure and efficient access to medical reports while maintaining privacy and integrity in the healthcare system.

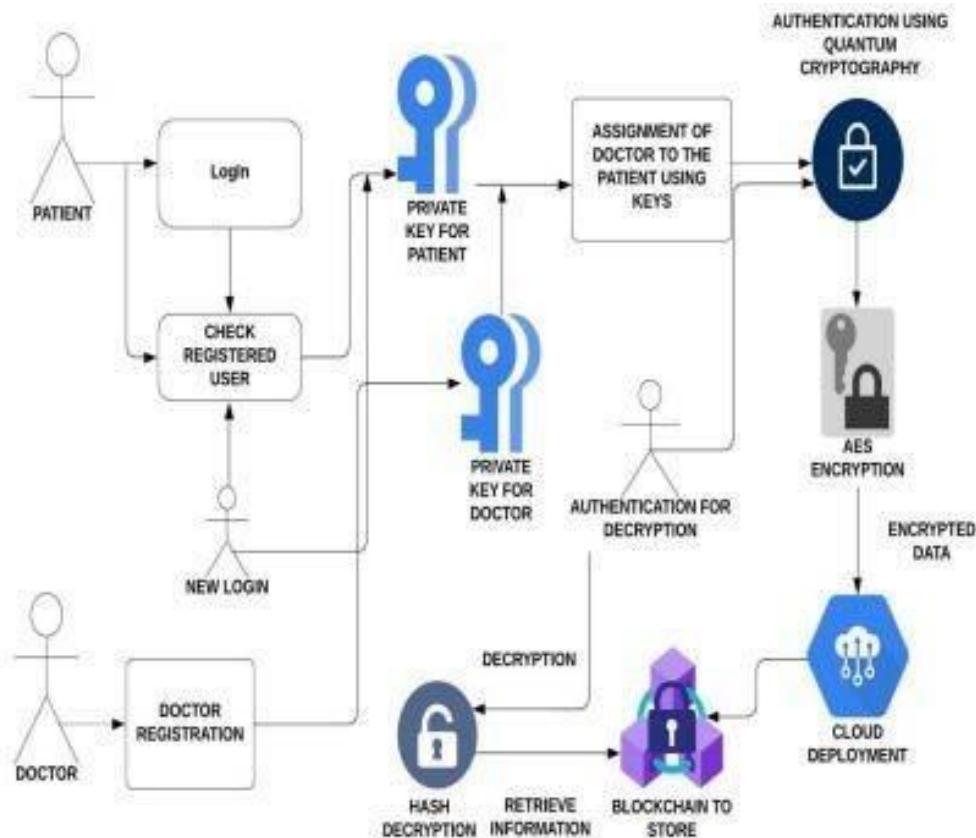


FIG 4.1 SYSTEM ARCHITECTURE

5. Registration of a new patient

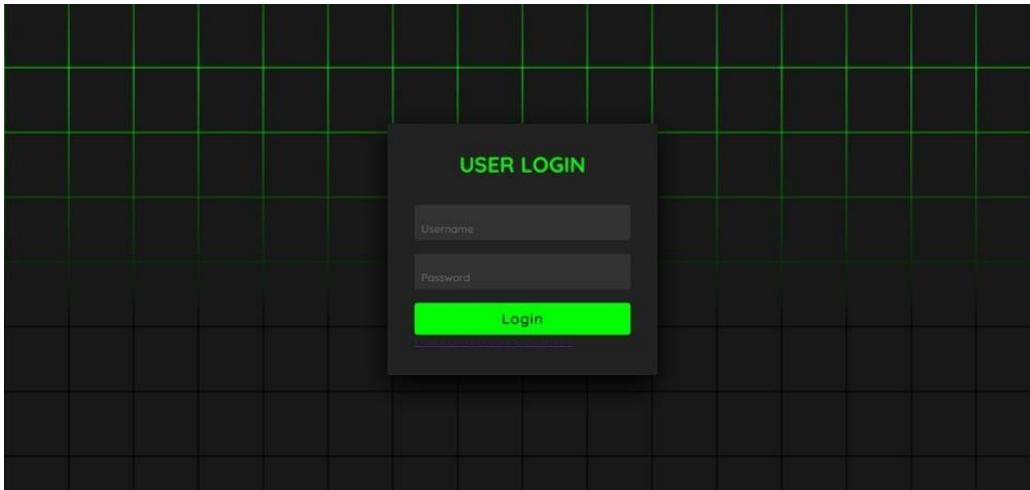
The Registration of a Patient is a pivotal process designed to uphold the confidentiality and integrity of sensitive medical information. Leveraging blockchain's decentralized architecture, each patient is assigned a unique cryptographic identifier that serves as a secure anchor for their comprehensive medical records. This decentralized architecture, each patient data is not only resistant to tampering but also accessible only to authorized entities. The use of smart contracts further optimizes the registration process, automating verification steps and facilitating a seamless, secure exchange of patient information within the blockchain network. This innovative approach not only enhances the efficiency of patient registration but also establishes a robust foundation for maintaining the security and privacy of medical reports throughout the healthcare ecosystem.

6. Authenticate the doctor

Authenticating the doctor involves implementing a secure process to verify and validate the identity of healthcare professionals accessing patient records. Utilizing blockchain, a decentralized and tamper-resistant system, each doctor is assigned a unique cryptographic key or credential. This key, backed by the transparency and immutability of the blockchain, ensures that only authorized doctors can access patient information. Smart contracts may be employed to automate the authentication process, adding an additional layer of efficiency and security to verify the credentials of medical practitioners before granting access to sensitive medical data. This robust authentication mechanism enhances the overall security of the system, safeguarding patient confidentiality and trust in the healthcare environment.

7. Retrieve the medical report

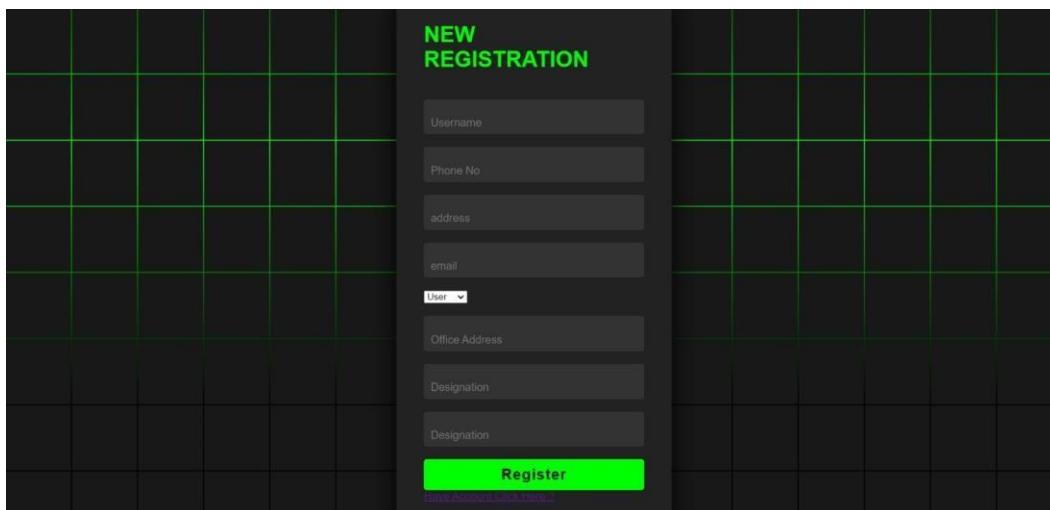
Retrieving a medical report involves a secure and streamlined process to access patient information. Authorized entities, such as healthcare professionals or the patients themselves, initiate a request to retrieve a specific medical report. Blockchain's decentralized architecture ensures the integrity and security of the retrieval process. When a request is made, smart contracts may be utilized to automate and validate the authorization, ensuring that only authenticated users can access the requested medical report. Once authorized, the decentralized nature of the blockchain allows for efficient retrieval, with the system securely accessing and presenting the relevant medical information. This approach not only safeguards patient privacy but also streamlines the retrieval process, contributing to the overall efficiency and security of accessing medical reports within the blockchain-based healthcare system.



A dark-themed login form titled "USER LOGIN" in green. It features two input fields for "Username" and "Password", and a bright green "Login" button. The background is a dark grid with green lines.

Fig 7.1: Login

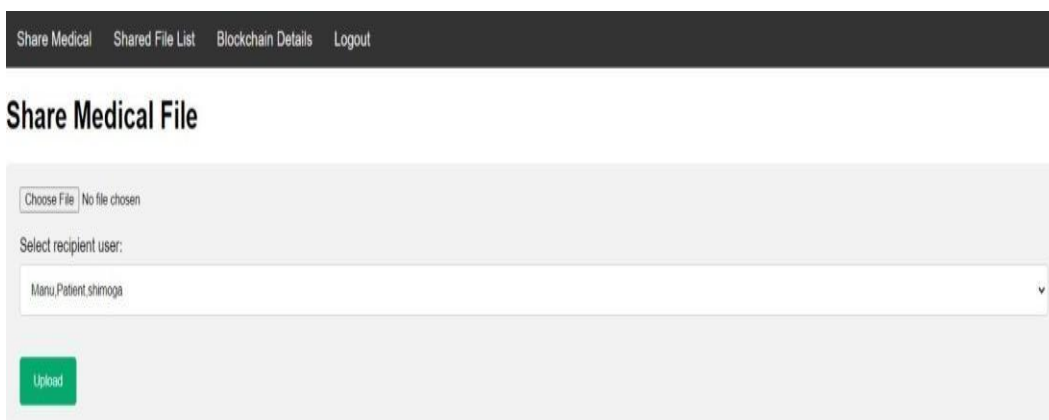
- This is login page where we are entering username and password. This is used for both patient as well as doctor login. Either patient or the doctor should enter the login credentials properly to enter next page.



A dark-themed registration form titled "NEW REGISTRATION" in green. It includes input fields for "Username", "Phone No", "address", "email", "User" (with a dropdown arrow), "Office Address", "Designation", and another "Designation" field. A bright green "Register" button is at the bottom. The background is a dark grid with green lines.

Fig 7.2 Registration

- This is registration page where a new patient or doctor are required to register here with the following details.



A web interface for sharing medical files. At the top, a dark navigation bar contains links: "Share Medical", "Shared File List", "Blockchain Details", and "Logout". Below, the heading "Share Medical File" is followed by a file upload section. It includes a "Choose File" button, the text "No file chosen", a "Select recipient user:" label, a dropdown menu showing "Manu Patient shimoga", and a green "Upload" button.

Fig 7.3: Shared Medical File

- This is the page where medical file is being shared either in pdf,png,jpeg,jpg formats. This is shared with doctor or patient



Shared Files

File ID	User	Timestamp	File Hash	Download
1	ravi	2024-04-25 23:25:47.114779	060b931f60804c4fabd80c7910bd5926a2d102298c221c59fe971c7d1a9f597b	Download
2	test	2024-04-25 23:45:12.179321	e5dd7b55bf97e652124658bb96aad8920023fd5a4adb684bb6979f5b9a678b3f	Download
3	Tejas	2024-04-26 00:02:47.109251	2b4fd97f37f91b9269a4247cb5e7b3180e3b05000dc1036a4f861661272a2e	Download
4	Tejas	2024-04-28 21:26:02.428663	a1d61ebbaa3376855db4ece8b08732c1c4649746348597f5ac5c54c3337e9c17	Download

Fig 7.4: Shared Files

- This page gives the details about the shared medical files with doctor as well as patient. It gives details about file ID, user, timestamp, file hash and download option to download the report.

Share Medical Shared File List Blockchain Details Logout

Blockchain Details

Block Index	Timestamp	Previous Hash	Transactions	Nonce
1	2024-04-25 23:25:47.125800	0	[{"user_id": 2, "filename": "ear.1.0.jpg", "timestamp": "2024-04-25 23:25:47.124811", "file_hash": "060b931f60804c4fabd80c7910bd5926a2d102298c221c59fe971c7d1a9f597b"}]	82968
2	2024-04-25 23:45:12.181097	0	[{"user_id": 1, "filename": "opencv.png", "timestamp": "2024-04-25 23:45:12.181097", "file_hash": "e5dd7b55bf97e652124658bb96aad8920023fd5a4adb684bb6979f5b9a678b3f"}]	7734
3	2024-04-26 00:02:47.110828	0	[{"user_id": 5, "filename": "heart_problem.png", "timestamp": "2024-04-26 00:02:47.110828", "file_hash": "2b4fd97f37f91b9269a4247cb5e7b3180e3b05000dc1036a4f861661272a2e"}]	26621
4	2024-04-28 21:26:02.445378	0	[{"user_id": 5, "filename": "20230624.jpg", "timestamp": "2024-04-28 21:26:02.445378", "file_hash": "a1d61ebbaa3376855db4ece8b08732c1c4649746348597f5ac5c54c3337e9c17"}]	93888

Fig 7.5: Blockchain Details

- This is the page where blockchain details are being displayed which shows the transaction logs with patient as well as doctor where the medical file is being shared.

8. CONCLUSION

Block chain in medicinal services frameworks has gotten gigantic open doors terms of not just giving secure and productive data putting away, sharing and access yet additionally creates a potential degree in the social insurance business for an assortment of partners. The principal center is to verify and effective information get to instrument for present day social insurance frameworks utilizing square chain innovation. Moreover, proposed plan can satisfy the prerequisites of trustworthiness, secrecy and validation in this medicinal services situation.

9. FUTURE SCOPE

As the healthcare landscape continues to evolve, blockchain presents a compelling solution for addressing critical challenges such as data integrity, privacy, and interoperability. Additionally, integrating smart contracts into blockchain-based systems can automate access control mechanisms, enforcing fine-grained access policies to safeguard sensitive medical information. Furthermore, the integration of blockchain technology with IoT devices opens up opportunities for securely storing and managing data generated by wearable sensors and remote monitoring devices, thus enabling data-driven healthcare decisions while maintaining patient privacy. Moreover, blockchain empowers patients by giving them greater control over their medical data, allowing them to selectively share access with relevant parties while maintaining ownership and sovereignty over their information. Future research can also focus on advancing privacy-preserving analytics techniques within blockchain-based medical record systems, enabling secure analysis of medical data without compromising patient confidentiality.

10. REFERENCES

- [1] Siva Rama Krishnan S, Manoj M.K, Thippa Reddy Gadekallu, Neeraj Kumar, Praveen Kumar Reddy “A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records” IEEE [2020]
- [2] Alisha Muhammed Shafi, Dr. Anita Brigit Mathew “Data Security in Health Reports using Blockchain Technology” Journal [2021]
- [3] Mary Subaja Christo, Anigo Merjora A, Partha Sarathy G, Priyanka C “An Efficient Data Security system in Medical Report using Blockchain Technology” IEEE [2021]
- [4] Xiaoguang Liu “A Blockchain based Medical Data Sharing and Protection Scheme” IEEE [2017]
- [5] Christian Esposito, Alfredo De Santis, Genny Totoro, Henry Chang, Kim-Kwang Raymond Choo “A Panacea for Healthcare Cloud Based Data Security and Privacy” IEEE [2018]
- [6] Vardhini B, Shreyas N Dass, Sahana R, Dr. R. Chinnaiyan “A Blockchain Based Electronic Medical Health Records Framework using Smart Contracts” Conference [2021]
- [7] Shwetha Ramachandran, Obu Kirthika O, Aishwaryavalli Ramsamy, Vanaja R, Saswati Mukherjee “A Review on Blockchain-Based Strategies for management of Electronic Health Records(EHRs)” IEEE [2020]

- [8] Koushik AS, Bhavya Jain, Nikitha Menon, Shilpa Choudhari, Vijaya Kumar BP, Divyansh Lohia “Performance Analysis of Blockchain based medical records management system” Conference [2019]
- [9] M N. Thippeswamy, Pawan R Tanksali, Pooja Rani Naik, Monica Hegde, B. Mohan Sai Kiran “Blockchain Based Medical Reports Monitoring System” Conference [2020]
- [10] B L Radhakrishnan, A Sam Joseph, S. Sudhakar “Securing Blockchain Based Electronic Health record using Multilevel Authentication” Conference [2019]