iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51153

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Healthcare Management System Using Blockchain

G V Sairam[1], Sankalp Kumar[2], Shefali Gupta[3], Syed Sharique Haider[4]
[1, 2, 3, 4]*Department of Computer Science and Engineering Dayananda Sagar University Bangalore, India*

Abstract: ***The current healthcare system has traditionally relied on paper-based medical records or electronic medical records (EMRs) that are stored in centralized databases. This method, however, has shown to be ineffective and unreliable, causing major delays in patient care. Medical documents are frequently sent over email as a temporary fix; however, this approach is unsafe and unreliable. Data breaches or unauthorised access to sensitive patient information pose a serious danger and may have far-reaching repercussions for both patients and healthcare providers. Blockchain technology can provide a more secure, decentralized, and efficient way to store and share medical records. Blockchain offers a tamper-proof and auditable method to trace transactions while using cryptographic methods to secure the integrity and confidentiality of data, access to patient data and modifications. Patients, physicians, and hospitals may easily, anytime, anywhere, and with total safety and security, access medical records via a decentralised blockchain network. Patients have discretion over who gets access to their information and can allow healthcare professionals and organisations access to their medical records. We are employing a number of technologies, like MetaMask, Ganache, Web3JS, and Solidity, to develop a blockchain-based solution. Users may connect with blockchain networks via the browser plugin MetaMask, and a local blockchain development tool called Ganache offers a testing environment for blockchain-based apps. Programmers may interface with the Ethereum blockchain using Web3JS, a JavaScript framework, and Solidity, a language used to create smart contracts the blockchain of Ethereum. A centralised blockchain network that can safely store and distribute patient data is the predicted result of a blockchain-based system for medical record sharing. The system's interoperability and scalability may be ensured via integration with already-existing healthcare systems and databases. Medical record sharing may be automated with smart contracts, allowing for safe and auditable access based on predefined criteria and permissions.***

I. INTRODUCTION

Electronic Health Records (EHRs) have revolutionized the healthcare industry by enabling healthcare providers to access a patient's medical information from anywhere, at any time. Electronic medical records (EMRs) are kept in electronic health records (EHRs) and include a patient's medical diagnosis, allergies, history, treatments, and test results. This data exchange helps healthcare professionals to decide on a patient's treatment with knowledge, resulting in better results and a higher quality of life.

Sharing private medical information, however, might expose vital information if it is done in an unprotected manner. The existing methods of storing and exchanging data through EHR/EMR systems provide substantial issues in terms of data security and privacy. Maintaining interoperability among the numerous related identities is one of the crucial concerns.

The capacity of various healthcare applications and systems to share, understand, and use data is referred to as interoperability. Lack of interoperability across disparate healthcare systems can lead to erroneous or insufficient data, which can affect patient care and result in medical blunders. Since healthcare systems employ several standards for data storage and transmission, it is challenging to properly communicate information.

The security and privacy of data in EHR/EMR systems is a key issue. Sensitive information contained in electronic medical data must be shielded from unauthorised access, alteration, and disclosure. Lack of control over personal data can have negative effects, such as unauthorised users accessing or changing private medical information. Identity theft, financial loss, and reputational harm to healthcare organisations can all result from data breaches.

Healthcare providers must prioritise the accuracy, secrecy, and privacy of patient data while exchanging clinical data in order to meet these difficulties. This may be done by putting in place strong security measures including encryption, access limits, and frequent audits to check for regulatory compliance. The management of patient data, including data access, use, disclosure, and destruction, must be governed by rules and procedures that healthcare organisations must adopt.

In conclusion, EHR/EMR technologies have transformed the healthcare sector by making it simple for healthcare professionals to access and exchange medical data. To maintain patient safety and confidentiality, data security and privacy pose serious issues that must be resolved. Healthcare organisations may successfully share clinical data while ensuring the integrity and privacy of patient information by putting in place strong security measures and developing rules and processes for managing patient data.

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

1) *Jeyakumar Samantha Tharani, Mukunthan Tharmakulasingam and Vallipuram Muthukkumarasamy "A blockchain-based database management system" | May 2020 Cambridge University press*
The article explains how blockchain technology may be applied as a database management system. Blockchain is a distributed ledger that securely, transparently, and irrefutably records transactions. The advantages and difficulties of utilising blockchain for database administration are discussed by the writers, including data integrity, immutability, decentralisation, and transparency. Additionally, they go through the application of blockchain to guarantee data privacy, security, and interoperability. The authors underline the necessity for a flexible architecture that can handle various use cases and needs in their framework for creating a blockchain-based database management system. Overall, the essay makes the case that blockchain has the power to transform database administration and presents a viable method for safely and openly maintaining and exchanging data.

2) *Alevtina Dubovitskaya, Author Orcid, Furqan Baig, Zhigang Xu, Rohit Shukla, Pratik Sushil Zambani, Arun Swaminathan and others "ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care" | August 2020 JMIR Publications*
This paper proposes a permissioned blockchain-based system for EHR data sharing and integration. The article describes the development of a patient-centric, blockchain-based Electronic Health Record (EHR) system called ACTION-EHR, in collaboration with Stony Brook University Hospital. The system was created for cancer patients undergoing radiation therapy and was constructed using the open-source, permissioned blockchain technology Hyperledger Fabric. The solution communicates with hospital EHR systems using the HL7 Fast Healthcare Interoperability Resources standard and leverages chain code to implement data exchange transactions. Patients and users may safely access and manage their EHR data using a web interface. Using deidentified patient data, the system was evaluated in a distributed setting. Overall, the study emphasises the value of patient-centric design in EHR systems and the promise of blockchain technology for safe and transparent data sharing in healthcare.

3) *Ayesha Shahnaz, Usman Qamar; Ayesha Khalid "Using Blockchain for Electronic Health Records" | October 2019 Institute of Electrical and Electronics Engineers*
The paper suggests a blockchain-based method for managing and exchanging Electronic Health Records (EHR) in healthcare institutions in a safe manner. The authors contend that the management and exchange of EHR data may be done securely and transparently using blockchain technology, as opposed to the ineffective, error-prone, and opaque techniques now used. They suggest using smart contracts to automate access control and data exchange on a private, permissioned blockchain network to store and manage EHR data.
The Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR) standard is used to link the system with current EHR systems. The paper also discusses the limitations and challenges of blockchain technology in healthcare and suggests future research directions for improving the scalability, privacy, and security of blockchain-based EHR systems. Overall, the article suggests that blockchain has the potential to transform EHR management and offers a promising solution for addressing the challenges of data sharing in healthcare.

4) *Jack Huang, Yuan Wei Qi, Muhammad Rizwan Asghar, Andrew Meads, Yu-Cheng Tu "MedBloc: A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data" | October 2019 Institute of Electrical and Electronics Engineers*
This paper built a system Medbloc for sharing and accessing Medical Data. This system is built on permissioned block chain which restricts access to participants who have been authorized by the system administrator. The system architecture includes a smart contract layer for access control, which enables the creation of rules for data access and ensures that only authorized entities can view or modify data. MedBloc also includes a data layer that stores medical records in an encrypted format. By encrypting data while it is in transit and at rest, the encryption module adds an extra degree of protection, preventing unauthorised access to patient data.
The use of encryption, according to the authors, improves system privacy by making sure that patient data is safe even if the blockchain is hacked. The authors suggest that the system has the potential to improve the quality of healthcare by providing a secure and seamless mechanism for healthcare providers to access patient data, leading to more effective diagnoses and treatments.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

5) *Ansar Sonya, Ganesh Kavitha "An effective blockchain-based smart contract system for securing electronic medical data in smart healthcare application" | October 2022 Wiley Online Library*

The paper suggests a new Medical Cloud (BC-MedCl) infrastructure built on Blockchain for safe EMR (Electronic Medical Records) exchange between patients and physicians. The framework employs IoT devices to regularly gather patient health-related data, which is then encrypted and saved in cloud storage. The hash values are then added to the blockchain. To increase system security, a decentralised selective smart contract-based access control mechanism is created. With a greater accuracy ratio of 98.7% and a lower latency ratio of 25% when compared to existing systems, the suggested framework is shown to be more efficient in handling EMR in real-time healthcare systems. This evaluation was conducted using the Ethereum platform. The article discusses the problems that existing healthcare data management systems have with data availability, reliability, confidentiality, and security and offers a solid solution to the issue.

6) *Pronaya Bhattacharya, Sudeep Tanwar, Umesh Bodkhe, Sudhanshu Tyagi, Neeraj Kumar "BinDaaS: Blockchain-Based DeepLearning as-a-Service in Healthcare 4.0 Applications" | December 2019 Institute of Electrical and Electronics Engineers*

The paper proposes a blockchain-based deep learning as-a-service (DLaaS) platform for healthcare applications, called BinDaaS. The paper presents various use cases for BinDaaS, including disease diagnosis, drug discovery, personalized medicine, and predictive analytics. The paper discusses the technical architecture of the platform, including the use of smart contracts for data access and sharing, and the integration of off-chain storage for improved scalability. The writers also point out the platform's drawbacks and difficulties, such as the requirement for regulatory compliance, data privacy issues, and security issues. Overall, BinDaaS presents a viable method for healthcare institutions to use deep learning while maintaining the privacy and security of patient information.

III. OBJECTIVES

1) Have different roles such as Hospital, Doctor, Patient
2) Only authorized person with a role can perform certain task.
3) Hospital can register doctors
4) Doctors/hospital can update Test Results.
5) Patient can only view their Test Results

IV. REQUIREMENTS

A. *Non-Functional Requirements*

1) Keeping the data size minimum
2) Low Gas Fees

B. *Software Requirements*

1) MetaMask 10.21.1
2) Ganache
3) Web3JS
4) React
5) Solidity
6) Any OS such as Windows, Mac, Ubuntu

V. METHODOLOGY

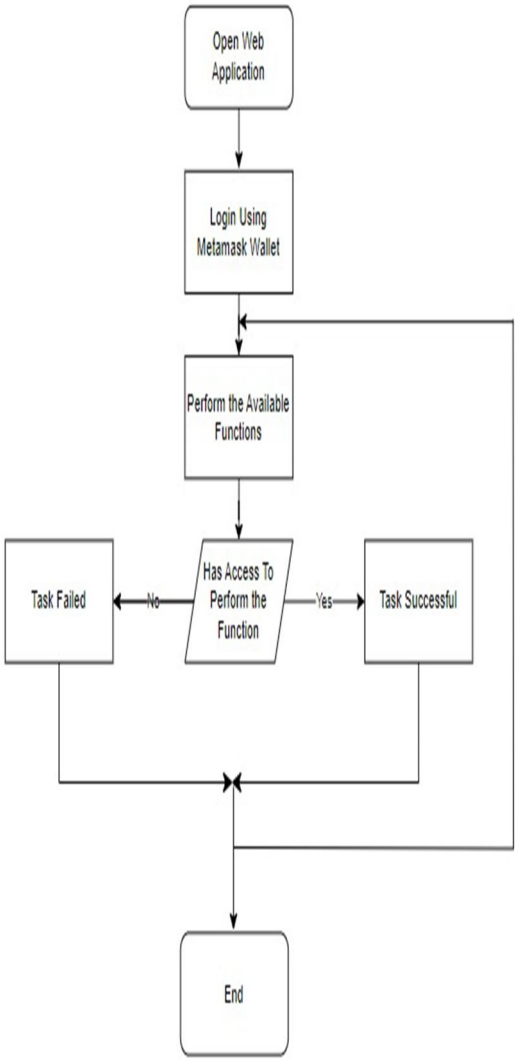
1) Create a MetaMask account for the patient, the doctor, and the admin: A popular browser plugin called MetaMask enables users to engage with applications built on the Ethereum network. All users of the healthcare system, including patients, physicians, and administrative staff, must create their own MetaMask accounts in order to use the system.
2) Fund the accounts with ether: The native cryptocurrency used on the Ethereum blockchain is called ethers. Each participant will require some ether to be added to their MetaMask account in order to access the blockchain-based healthcare system. Ethereum may be obtained by mining or bought on cryptocurrency exchanges.
3) Hospitals, physicians, and patients may all be registered with the use of smart contracts: Self-executing contracts known as "smart contracts" are kept on the blockchain. Smart contracts will be developed at this stage in order to register hospitals, physicians, and patients. Each participant's name, address, and medical history will be stored in these smart contracts along with other pertinent data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4) The owner and holder of all administrative rights is the person who initially deploys the contract: The first individual to install a smart contract on the blockchain takes ownership of that contract. The individual who deploys the smart contract for registering hospitals, physicians, and patients will become the owner of the healthcare system and be granted administrative powers to run it.

5) A hospital is added to a list after it registers. The same list is kept for patients and medical professionals: After a hospital, a physician, or a patient is registered on the blockchain, information about them is saved in the pertinent smart contract. Other system users have access to a list of the hospitals, physicians, and patients who have registered with the system.

VI. DESIGN



VII. RESULT

Electronic medical records (EMRs) can be safely stored and transferred using a blockchain-based system by creating MetaMask accounts for patients, physicians, and administrators and depositing ether into the accounts. Hospitals, physicians, and patients may all be registered using smart contracts, with the contract owner having complete administrative authority. Once registered, hospitals, physicians, and patients are added to the appropriate lists, making it simple to obtain medical data. Strong security measures like encryption and access controls can be used to preserve interoperability across diverse healthcare apps and systems. Healthcare providers should prevent problems with data security and privacy by prioritising the accuracy, confidentiality, and privacy of patient data while transmitting clinical data. This can be achieved by governing the management of patient data with rules and procedures that healthcare organizations must adopt.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

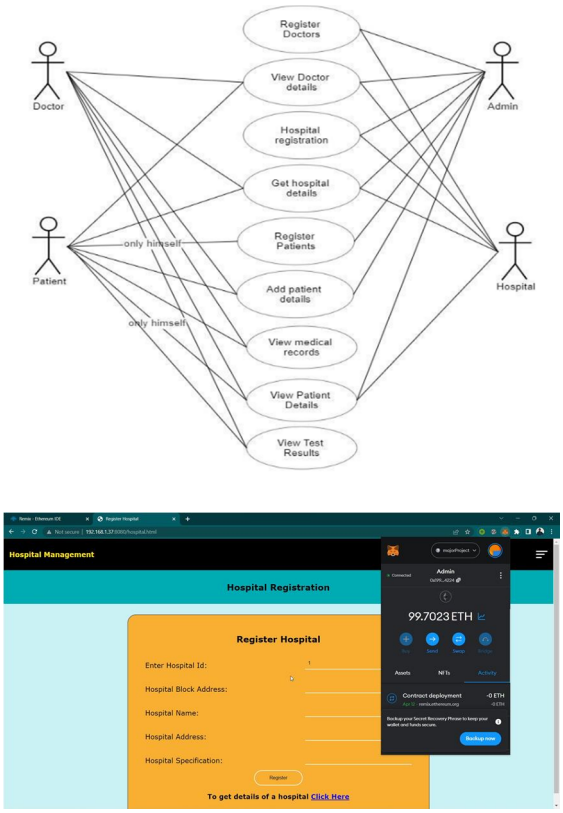
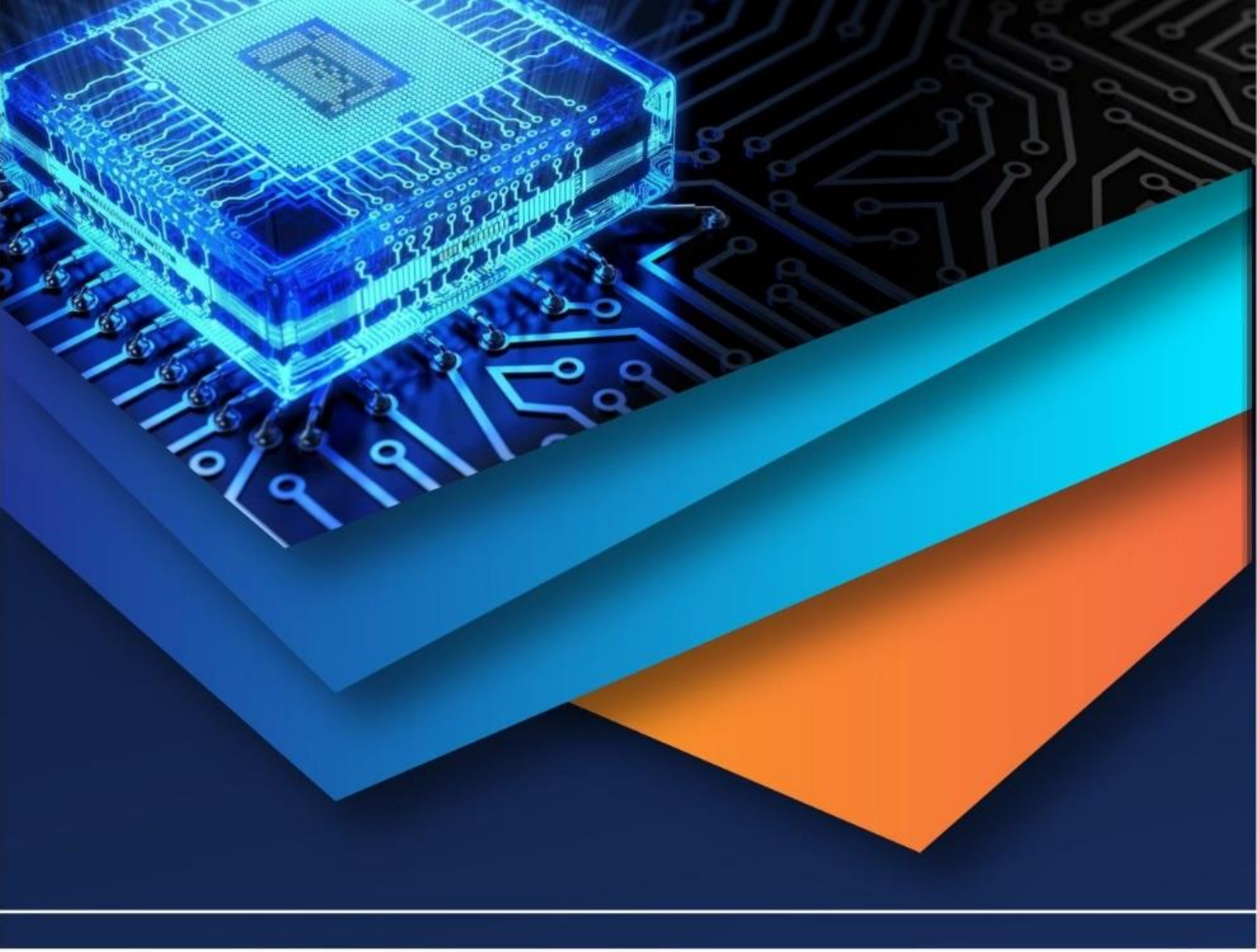


Fig 7.1

VIII. CONCLUSION

Healthcare practitioners may easily access and share medical data by deploying a secure blockchain-based system for the storage and exchange of electronic medical records, which will improve patient outcomes and quality of life. Healthcare providers may prevent problems with unauthorised access, modification, and disclosure of confidential medical information by placing a high priority on data security and privacy. Strong security measures may be put in place to do this, and policies and procedures for handling patient data can be created.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)