IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

Confidential Health Records of Stigma Diseased Patients using Blockchain Technology

Dr. Vikas Reddy S, Neha B R, S Tarun Tejas, Sai Sugun D R, Suprita
Department of Artificial Intelligence and Machine Learning
S J C Institute of Technology, Chikkaballapur, Karnataka, India

Abstract: *The abstract provides an overview of a proposed solution to create a secure and unchangeable platform for storing health records and related supplementary data. The solution aims to address concerns regarding the security of health records, user data ownership, and data integrity by leveraging blockchain technology. The system will incorporate precise access controls, empowering patients with greater authority over their electronic health records. To access the system, patients will need to register and generate a confidential key using their provided credentials. This design ensures that only authorised personnel can access patients' private health information, minimising the risk of unauthorised access and potential breach of confidentiality. Additionally, the utilisation of blockchain technology adds an extra layer of security by ensuring the immutability of data, thereby safeguarding the integrity of patients' records. Various blockchain- based systems have been proposed for managing electronic health records, and this solution carries significant implications for the healthcare industry.*

Keywords: Blockchain, digital health, stigma diseased patients, Cloud Computing, security, e-health data, secure communication, confidentiality

I. INTRODUCTION

Health holds a significant position in today's society, recognized as one of the utmost priorities for individuals. With the creation, storage, and repeated utilization of a vast amount of health- related data, the electronic health record (EHR) plays a pivotal role within the healthcare system. EHR and electronic medical record (EMR) systems bring about numerous benefits, including enhanced healthcare, improved clinical care and management, and simplified data analysis for research institutions. Nevertheless, challenges persist concerning the security of health records, ownership of user data, and data integrity. To tackle these issues, a proposed solution aims to establish a secure and unchangeable platform for storing health records and interconnected auxiliary data. EHRs are of great significance and sensitivity as they contain crucial information for diagnoses and medical treatments, shared among various parties such as hospitals, clinics, and private practices. The evaluation of a disease relies on advancements in medical knowledge, and any associated stigma primarily stems from the fear of depression associated with the condition rather than the name itself. Patients may seek medical attention at multiple hospitals or be transferred between facilities. According to laws1- 4, patients have the right to access their health information and can set rules and restrictions on who can view and retrieve their data. The emergence and continuous development of blockchain technology, along with the evolution of smart contracts and blockchain services like Ether and Hyper- ledger, have opened new possibilities. EHRs are indeed vital and influential, containing essential information for patient diagnoses and treatments, shared among different entities including hospitals, clinics, and personal practices. This information is aggregated to form a comprehensive patient medical history, requiring accuracy, confidentiality, up-to- dateness, and restricted access to authorized individuals only. Additionally, there should be assurance of availability even in challenging circumstances such as natural disasters or other disruptions that may lead to system failures or improper behaviour. In such exceptional scenarios, special EHR access and management policies may be temporarily waived, such as granting humanitarian organizations—both governmental and non- governmental— privileged access for rescuing and providing care on the ground. However, these exceptions must be documented for auditing and accountability purposes while preserving people's privacy and the security of their personal information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

II. REALATED WORK

In this section, we explore the domain of secure and shared health information using blockchain technology. It has become increasingly clear that the current models and systems designed to protect and share such information are inadequate in terms of functionality, accessibility, and user experience. Therefore, there is an urgent need to develop innovative solutions that can effectively overcome these challenges.

The proposed solution aims to address this issue by implementing precise access rules that empower patients to have greater control over their electronic health records. This approach also addresses the scalability problem often associated with blockchain technology. By leveraging blockchain, the proposed system has the potential to offer a practical solution to Electronic Health Record (EHR) standards.

An example of a blockchain-based solution for managing medical data is the Med-chain system developed by Daraghmi et al. This system seeks to enhance the functionality, security, and accessibility of medical records by utilizing time-based smart contracts to manage electronic health data and monitor transactions. This approach enables patients, healthcare providers, and other stakeholders involved in patient safety to securely access medical records.

Moreover, the proposed blockchain- based health database provides additional measures and tools for patients to enhance record privacy. Patients can choose to grant access to their data to specific doctors, who are then only able to view a limited amount of information with the patient's consent. For example, a doctor may access the patient's health history, age, and allergies, while other fields remain inaccessible for viewing or editing. Various blockchain-based systems have been suggested for managing electronic health records. For instance, the MedRec system proposed by Azaria et al. adopts a modular structure to manage, authorize, and distribute system data among participants. Similarly, the Medblock system employs a hybrid architecture to secure EMRs, consisting of support doors, gate doors, and delivery doors. The architecture proposed by Conceicao et al. involves storing EHR data using blockchain technology, ensuring a secure and tamper-proof approach by tracking all blockchain activity. Yang and Li's blockchain-based DSE architecture also aims to prevent tampering and misuse of EHR. In conclusion, the use of blockchain technology in healthcare carries significant implications due to its disruptive nature. The proposed blockchain- based solutions offer numerous advantages, including secure access, tamper-proof management of electronic health records, and improved patient privacy and control. The development of such innovative solutions can profoundly impact the healthcare industry by enhancing the management, sharing, and accessibility of medical data.

III. LITERATURE REVIEW

The study conducted by Aishwarya L, Hariprasad N, Prathiksha P Desai, and Shashank D [1] explores the challenges encountered by medical establishments when converting ancient medical records to electronic health records. The study proposes a medical knowledge sharing theme that utilizes permissioned blockchains and ciphertext-based a t t r i but e e n c o d i n g t o e n s u r e confidentiality and access management of medical knowledge. The authors suggest using a polynomial equation to achieve absolute association of keywords while guaranteeing patient identity privacy. The proposed theme has keyword-in distinguishability against adaptive chosen keyword attacks and high retrieval efficiency.

The literature review by Adeoksang Lee and Minseok Song [2] discusses the benefits and challenges of health information exchange (HIE) and proposes MEXchange, a novel blockchain- based privacy-preserving HIE solution. The authors highlight the privacy issues caused by analyzing senders and receivers of transactions in existing blockchain-based HIE studies and suggest the use of smart contracts, ring signature, and stealth address to address these issues. The study evaluates MEXchange quantitatively and qualitatively using the requirements of the Office of National Coordinator for health Information Technology and compares it with existing solutions. MEXchange mitigates privacy and security issues among healthcare stakeholders and lowers barriers to the application of blockchain-based HIE systems.

Panwar et al. [3] propose a framework for managing personal health records (PHR) using blockchain technology and IBM cloud data lake. The authors highlight the challenges faced by the overcrowded healthcare system and the need for improved health record management. They suggest that blockchain technology can enhance the security, performance, and transparency of sharing medical records. The proposed framework aims to minimize the problem of latency and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

throughput and provides better results than existing techniques. The study concludes that the proposed system can effectively manage healthcare processes with high accuracy

Pilozzi and Huang[4] explore the burden of stigma faced by individuals with Alzheimer's disease (AD), which can lead to avoidance of diagnosis and treatment. They discuss the potential of information technology, specifically natural language processing (NLP), to analyze public sentiment surrounding AD on social media. The authors also address concerns about the security of medical data and suggest using decentralized and blockchain- based methods to give patients more control over their data, thus alleviating fears of discrimination.

Dubovitskaya et al. (2019) [5] discuss the potential of using blockchain technology for managing and sharing electronic medical records (EMRs) in healthcare. They argue that blockchain can provide a secure and trustable system for managing sensitive healthcare data, while enabling easy sharing between healthcare providers and researchers. The authors propose a framework for managing and sharing EMR data for cancer patient care, and present a prototype developed in collaboration with Stony Brook University Hospital. They conclude that their approach can improve decision- making, reduce turnaround time for EMR sharing, and lower overall costs.

The authors propose [6] a healthcare information security storage solution based on Hyperledger Fabric and Attribute-Based Access Control (ABAC) to address privacy and sharing issues in medical data. The scheme employs attribute-based access control, stores medical information in the blockchain, and uses IPFS technology to relieve blockchain storage pressure. The proposed solution ensures secure storage, integrity, and dynamic, fine- grained access to medical information, while demonstrating high throughput when accessing medical information.

The research project conducted by Prof. Rohini Hanchate, Samriddhi Garudik, Shruti Chavan, and Naisargi Bajpai focuses on [8] the potential of Blockchain in the healthcare industry. Electronic Health Records (EHRs) are currently used for storing and sharing medical records, but they are not very secure and accessible to patients and caregivers. The study suggests that Blockchain technology can improve health data protection and collaboration by placing patients in a centralized system. Blockchain provides cryptographic assurance of data integrity, security, privacy, and access, giving patients full control of their medical knowledge. The authors also outline the challenges that need to be addressed to implement this technology successfully.

The authors, Kianoush Kiania, Seyed Mahdi Jameii, and Amir Masoud Rahmani, [9] conducted a systematic literature review to analyze existing Blockchain-based approaches for improving privacy and security in electronic health systems. They highlighted weaknesses of traditional Electronic Health Records (EHR) due to their centralized architecture and how Blockchain technology can ensure privacy and security through encryption and decentralization. They reviewed 51 papers published between 2018 and Dec 2022 and discussed the main ideas, type of Blockchain, evaluation metrics, and used tools of each paper.

Finally, they discussed future research directions, open challenges, and some issues in the field.

In this literature review, Filippo Boiani [10] discusses the importance of electronic health records (EHRs) in emergency situations caused by natural disasters and how the use of permissioned blockchain implementations can provide a more failure-resistant solution for managing EHRs. Through the design and implementation of a prototype using Hyperledger Fabric and simulation tests based on the Haiti earthquake of 2010, the benefits and tradeoffs of the system were discussed, including performance parameters such as throughput, latency, memory, and CPU usage. The results showed that the system allowed for sharing and access of EHRs while preserving privacy and confidentiality, making it an interesting alternative for healthcare networks to ensure continuity of treatment in extreme situations.

IV. DESIGN

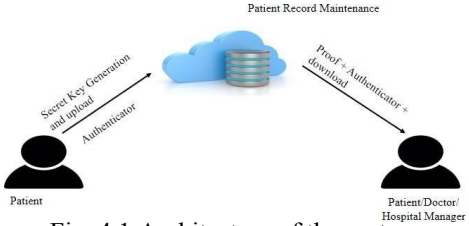

Fig. 4.1 Architecture of the system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

The design of the confidential health record system for stigma patients is unique as it utilizes blockchain technology. The system requires patients to register and generate a secret key using their provided credentials. Upon successful registration, the patient can then log in to the system using their credentials and secret key. In addition, a cloud login will also be generated to facilitate the storage of data.

When a doctor needs to access a patient's record, they must obtain the secret key from the patient. The patient will then verify and authenticate the access in the cloud. This design ensures that only authorized personnel can access the patient's confidential health information, thereby reducing the risk of unauthorized access and potential breaches of confidentiality.

Furthermore, the use of blockchain technology in this system provides an added layer of security through the immutability of the data. Once data is entered into the system, it cannot be altered or deleted, thereby ensuring the integrity of the patient's health record. This feature is particularly important for stigma patients as it ensures that their confidential health information remains secure and cannot be tampered with.

Overall, the unique architecture of this system ensures the confidentiality and security of stigma patients' health records while also allowing authorized healthcare providers to access the necessary information to provide effective treatment.

V. IMPLEMENTATION

Registration

It is a process of enrolling or being enrolled into the cloud. To utilize the cloud documents, every healthcare provider should enroll. During this process your basic information like email, contacts etc., are collected and stored in the Cloud. The cloud id for a particular user will get automatically generated during the registration.

Cloud ID

Every user should create a Cloud ID and use it to identify something with near certainty that the identifier does not duplicate one that has already been, or will be, created to identify something else. Information labelled with Cloud ID by independent parties can therefore be later combined into a single database, or transmitted on the same channel, without needing to resolve conflicts between identifiers.

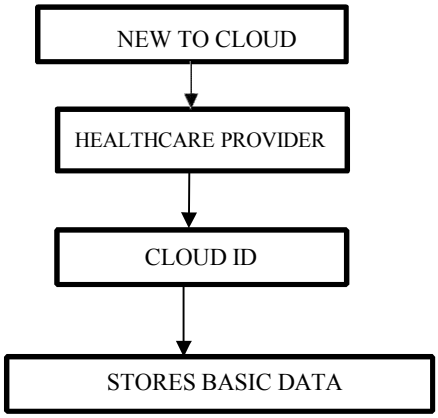

Fig. 5.3 Flow chart of the cloud architecture

- Healthcare Provider
- Load patient Records
- Key Generation
- Encrypt patient Records
- Block Creation
- Upload and Download Patient Records
- Data Selection and Loading

In this process, the health provider choose patient healthcare records for uploading and maintaining the dataset in the cloud.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

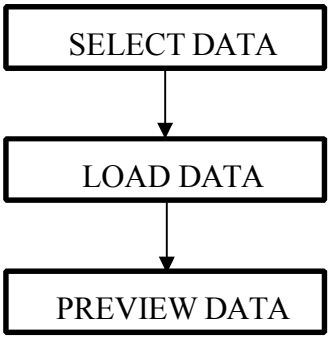

Fig. 5.4 Flow chart of the data selection and loading

Key Generation

The secret key is generated using cryptographic algorithm. This key is used for encrypting the dataset.

Encrypt Patient Records

The data is encrypted for secure maintenance. So that the unauthorized person cannot be able to access the data that are presented in the cloud.

Block Creation

- Each block contain patient record and it's timestamp.
- A blockchain, originally block is a growing list of records called blocks.

Upload and Download Patient Records

After creating the block, the healthcare provider will upload the records into the cloud. Suppose, if they want to retrieve an record from cloud, first the healthcare provider search the record. Based on the search it will show the results. After getting an approval and key from the cloud service provider the healthcare provider can download the data.

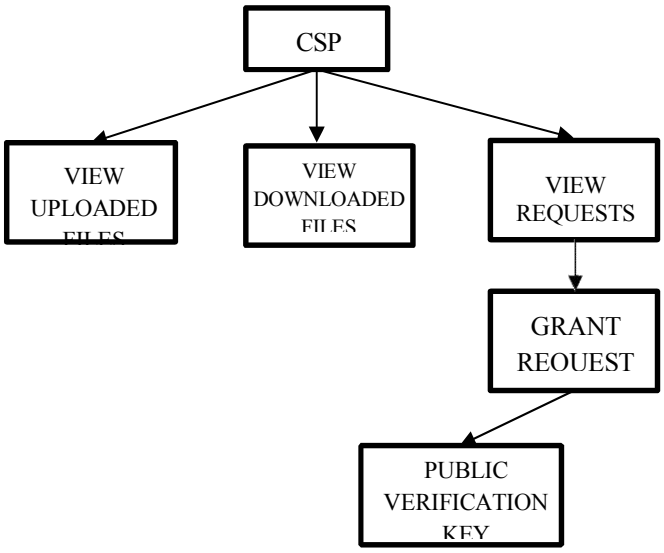

Fig. 5.10 Flow chart of Public Key Verification

Cloud Service Provider

The cloud service provider maintain all the patient records and also they can provide a permission to the user to access the data.

The Cloud Service Provider can view all the uploaded and downloaded documents in the Cloud. The CSP receives the document request from the Data User, verifies the authentication before granting permission. Then the CSP executes the query and returns the encrypted document according to the search token. And also returns an additional proof with the document, to verify the search result.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

Public Verification Key

Public verification key is a security measure designed to make sure that your document outsourced in cloud doesn't get hacked. By verifying public key, the Data Owner and the Data User adding another layer of protection to the documents or files in the cloud by confirming each other's identities.

VI. FEATURE WORK

- **Interoperability:** Develop standards and protocols for seamless integration of blockchain-based systems with existing healthcare infrastructure. This would enable secure data exchange and interoperability between different healthcare providers, ensuring smooth coordination of care and improved patient outcomes.
- **Scalability:** Address the scalability limitations of blockchain technology to accommodate the large volume of healthcare data generated daily. Research and develop innovative solutions such as sharding, off-chain storage, or layer-2 solutions to ensure blockchain networks can handle the increasing demands of healthcare data without sacrificing performance or security.
- **Privacy-preserving techniques:** Explore privacy-enhancing technologies within the blockchain ecosystem to protect sensitive patient information. Techniques such as zero-knowledge proofs, homomorphic encryption, and secure multi-party computation can be leveraged to enable secure data sharing while preserving patient privacy.
- **Consent management:** Develop robust consent management frameworks on the blockchain to empower patients with granular control over their health data. Smart contracts can be utilized to define and enforce data access permissions, ensuring that data is only accessed or shared with explicit patient consent.
- **Data provenance and auditing:** Design mechanisms to track and verify the origin and integrity of healthcare data stored on the blockchain. Implement auditing tools that enable regulators and auditors to validate the accuracy and authenticity of healthcare transactions, ensuring compliance with regulations and standards.
- **Integration with emerging technologies:** Explore the integration of blockchain with other emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT). Combining blockchain with AI can enable secure and privacy-preserving machine learning models, while integrating blockchain with IoT devices can ensure secure and reliable data exchange between devices, healthcare providers, and patients.
- **Real-world implementation and adoption:** Conduct pilot projects and real-world deployments to assess the feasibility, effectiveness, and acceptance of blockchain-based healthcare systems. Collaborate with healthcare providers, regulators, and policymakers to identify and overcome barriers to adoption, such as legal and regulatory challenges, interoperability issues, and user acceptance.
- **Ethical considerations:** Address the ethical implications of blockchain technology in healthcare, including issues related to data ownership, consent, and algorithmic transparency. Develop frameworks and guidelines to ensure the responsible and ethical use of blockchain in healthcare, promoting equity, fairness, and inclusivity.
- **Education and awareness:** Promote education and awareness initiatives to inform healthcare professionals, policymakers, and the general public about the potential benefits and risks of blockchain technology in healthcare. Foster collaborations between academia, industry, and government to share knowledge, best practices, and lessons learned in implementing blockchain solutions.

By focusing on these future directions, researchers, practitioners, and policymakers can advance the application of blockchain technology in healthcare, ultimately contributing to a more secure, efficient, and patient-centered healthcare ecosystem.

VII. CONCLUSION

This paper introduces a novel approach that combines blockchain technology with an attribute-based access control model to leverage the benefits of b l o c k c h a i n f o r b r e a k i n g d o w n information silos in medical data and safeguarding the security and privacy of medical information. The utilisation of the interstellar file system is employed to alleviate the storage burden on the blockchain. The scheme adopts a distributed architecture to achieve dynamic fine-grained access control. Detailed descriptions of chain code deployment and invocation are provided, along with experimental evidence to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 11, May 2023

support the proposed approach. Furthermore, this paper explores various scenarios for applying blockchain technology in different healthcare settings, including primary care, medical data research, and connected health. It discusses the advantages of maintaining an immutable and transparent ledger to enhance the management of medical data by tracking all network events. The choice of permission blockchain technology is justified based on the specific constraints of the healthcare context. Additionally, an architecture framework is presented, tailored to the requirements of radiation oncology data sharing, and a prototype is implemented to ensure privacy, security, availability, and fine-grained access control over highly sensitive patient data.In the rapidly advancing technological landscape, blockchain technology has become pervasive and remains a prominent focus of research. Numerous works in this field strive to enhance performance and capabilities. Our proposed work is centered on leveraging blockchain technology in the domain of healthcare processing, contributing to this active research area.

REFERENCES

[1]. Confidential health record using blockchain. Aishwarya L, Hariprasad N, Prathiksha P Desai, Shashank.
[2]. MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address. DEOKSANG LEE AND MINSEOK SONG.
[3]. Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., & Gupta, G. (2021). A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake
[4]. Overcoming Alzheimer's Disease Stigma by Leveraging Artificial I n t e l l i g e n c e a n d B l o c k c h a i n Technologies. Alexander Pilozzi and Xudong Huang.
[5]. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2019). Secure and Trustable Electronic Medical Records Sharing using Blockchain.
[6]. A Blockchain-based Secure Storage Scheme for Medical Information. Zhijie Sun, Dezhi Han, Dun Li , Xiangsheng Wang , Chin-Chen Chang, Zhongdai Wu.
[7]. Hanchate, R., Garudik, S., Chavan, S., & Bajpai, N. (2021). Blockchain for giving patients control over their healthcare records. Journal of Medical Systems.
[8]. Kiania, K., Jameii, S. M., & Rahmani, A.M. (2021). Blockchain-based privacy and security preserving in electronic health: a systematic review. Journal of Medical Systems.
[9]. Boiani, F. (2021). Blockchain Based Electronic Health Record Management.