IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

U-MEDCHAIN
A Blockchain Based System for Medical Records Access and Permissions Management

S. Farjana Farvin[1], R. Nithyashree[2], R. Sivanandhini[3], D. R. Subasri[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, Tamil Nadu, India
farzana@aamec.edu.in[1],nithyashreerameshkumar@gmail.com[2],
sivanandhini2210@gmail.com[3], subasri182009@gmail.com[4]

Abstract: *In recent years, the interest in using wireless communication technologies and mobile devices in the healthcare environment has increased. However, despite increased attention to the security of electronic health records, patient privacy is still at risk for data breaches. Thus, it is quite a challenge to involve an access control system especially if the patient's medical data are accessible by users who have diverse privileges in different situations. Blockchain is a new technology that can be adopted for decentralized access control management issues. In this work, blockchain based frame work Electronic Medical Records (EMR) is applied. The proposed frame work aims at providing interoperable, secure, and efficient access to EMRs by health providers, patients and third parties while maintaining the patient's privacy. We propose a timed-based smart contracts whose design meet the demands of EMRs. These contracts are employed in the blockchain for governing the transactions, monitoring the computations performed on the EMRs through the enforcement of the acceptable usage policies and managing the use of data after transmission. This work employs the blockchain technology with a collection of encryption techniques and hash functions. Sensitive information that are placed on the blockchain are encrypted to decrease the possibility of being accessed by unauthorized entity. Advanced cryptographic techniques are also adopted by the proposed framework for providing further security. The use of proxy re-encryption technique is employed to solve the problem of transferring encrypted messages among nodes with no need to share symmetric key. This adopts the distributed ElGamal re-encryption schema with distributed blinding technique. Our proposed framework employs the hashing method SHA-256, to ensure data integrity. The proposed system employs a new incentive mechanism integrated with the Proof of Authority (PoA) consensus algorithm for crating, validation, and appending new block. Now security and access control are maintained by the adoption of advanced encryption and authentication techniques throughout the blockchain. Interoperability, auditability, and accessibility are provided by the use of comprehensive logs. Our proposal gives efficient security and accessibility for medical records in an effective manner.*

Keywords: Blockchain, electronic medical records, smart contracts

I. INTRODUCTION

U - Medchain is a term used to describe the use of blockchain technology in the healthcare industry. Distributed ledger technology, known as blockchain, provides a secure and transparent method for storing and sharing data that is resistant to tampering. It has the potential to revolutionize the way healthcare data is managed, shared, and accessed. U - Medchain leverages the blockchain technology to provide a decentralized, secure, and transparent platform for managing medical records, clinical trials, drug supply chains, and other healthcare-related processes. The use of blockchain in healthcare can improve data security, increase transparency, reduce fraud, and enhance patient privacy.

The healthcare industry has traditionally faced challenges related to data management, interoperability, and privacy. Medical records are often fragmented and stored, making it difficult for healthcare providers to access and share patient

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

information. Moreover, healthcare data is often vulnerable to cyberattacks, which can compromise patient privacy and result in significant financial losses. By using blockchain technology, U - Medchain can address these challenges by creating a secure and decentralized system for storing and sharing medical records and other healthcare data. With a blockchain-based system, healthcare providers can easily access patient information across different healthcare organizations, while maintaining patient privacy and data security.

Additionally, U – Medchain can be used to manage clinical trials, ensuring that data is transparent, secure, and tamper-proof. This can help improve the accuracy and reliability of clinical trial data, ultimately leading to better patient outcomes. Finally, U – Medchain is a promising application of blockchain technology in the healthcare industry. By improving data management, enhancing patient privacy, and increasing transparency, blockchain has the potential to significantly enhance the overall quality of healthcare outcomes.

II. BACKGROUND

2.1 Blockchain

A blockchain is a shared ledger or distributed database that is accessible to all nodes on a computer network. Unlike traditional databases, blockchains use blocks to store data, which are then linked together using cryptography to form a chain. As new data is added, it is recorded in a new block, which is then chained to the previous block, resulting in a chronological chain of data. While blockchains can store different types of information, they are most commonly used as transaction ledgers. Immutable and decentralized, blockchains guarantee data fidelity and security, creating trust without the need for a third party. As information is added to the blockchain, it is stored in blocks, which have a limited storage capacity. Once a block is full, it is closed and linked to the previously filled block, forming a chain of data that is continuously updated with new information.

2.2 Smart Contract

Smart contracts are utilized in tandem with blockchain technology by various applications, including decentralized finance (DeFi) platforms. Once finished, the transactions are irreversible and trackable. It enables trusted transactions and agreements to take place between disparate, anonymous parties without the need for a central authority, judicial system, or external enforcement tool. They are blockchain apps that ensure that each party of a transaction completes its portion. A smart contract, for example, could start a fund transfer with a third party to verify that the transfer occurred. A blockchain contains code for smart contracts that is capable of executing contract terms, but the execution takes place externally to the chain. It automates the actions that would otherwise be completed by the parties in the agreement, which removes the need for both parties to trust each other.

2.3 Ethereum

Ethereum is, at its heart, a decentralized global software platform based on blockchain technology. It is most famous for its national cryptocurrency, ether (ETH). Anyone can use it to build any secure digital technology. It has a token intended to compensate participants for work done in support of the blockchain, but it can also be used to pay for tangible goods and services if accepted. It is intended to be scalable, programmable, private, and distributed. It is the blockchain of choice for developers and businesses developing technology based on it to change the way many sectors function and how we live our lives. It natively supports smart contracts, an essential tool behind decentralized applications. Smart contracts are utilized in tandem with blockchain technology by various applications ,including decentralized finance (DeFi) platforms.

2.4 Wallet

Ethereum owners use wallets to store ether. A wallet is a digital interface that lets the user to access the ether stored on the blockchain. Wallet consists of address and private keys which is received for each ether and this key is essential for accessing ether.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

III. RELATED WORK

[1]This paper presents a comprehensive overview of the current state of research on blockchain in healthcare, highlighting the various functional use cases. However, despite the growing interest and research in this area, the majority of published studies are still in the conceptual, framework proposition, and experimental prototype stages, with limited real-world implementation or pilot projects. The analysis reveals that poor scalability, low general performance, and high costs continue to be significant barriers to implementing a scalable blockchain system in healthcare, as well as in other sectors.

[2]The paper presents a novel approach that utilizes blockchain technology to empower patients with control over their medical records in a decentralized and secure manner. The proposed solution leverages two Ethereum-based smart contracts to automate the defined events, ensuring traceability, reliability, and trustworthiness. To further enhance security, the proposed system is integrated with various technologies such as IPFS, proxy re-encryption, trusted oracles, and reputation systems. These integrations enable secure fetching, storage, and sharing of patients' medical records while maintaining their privacy and confidentiality.

[3]In this paper, a new system called SmartAccess is introduced as an Attribute-Based Access Control (ABAC) system designed for secure and efficient sharing of medical records across different organizations. The system allows organizations to reach a joint agreement over access policies, providing dynamic access control, transparency, and auditability. The proposed SmartAccess system implements the ABAC model by utilizing four smart contracts that mimic the granularity of the model. The system is applied to two healthcare use cases: access with explicit patient consent and access with implicit consent during acute care. Overall, the SmartAccess system provides a robust solution for secure cross-organization medical records sharing while maintaining privacy and security.

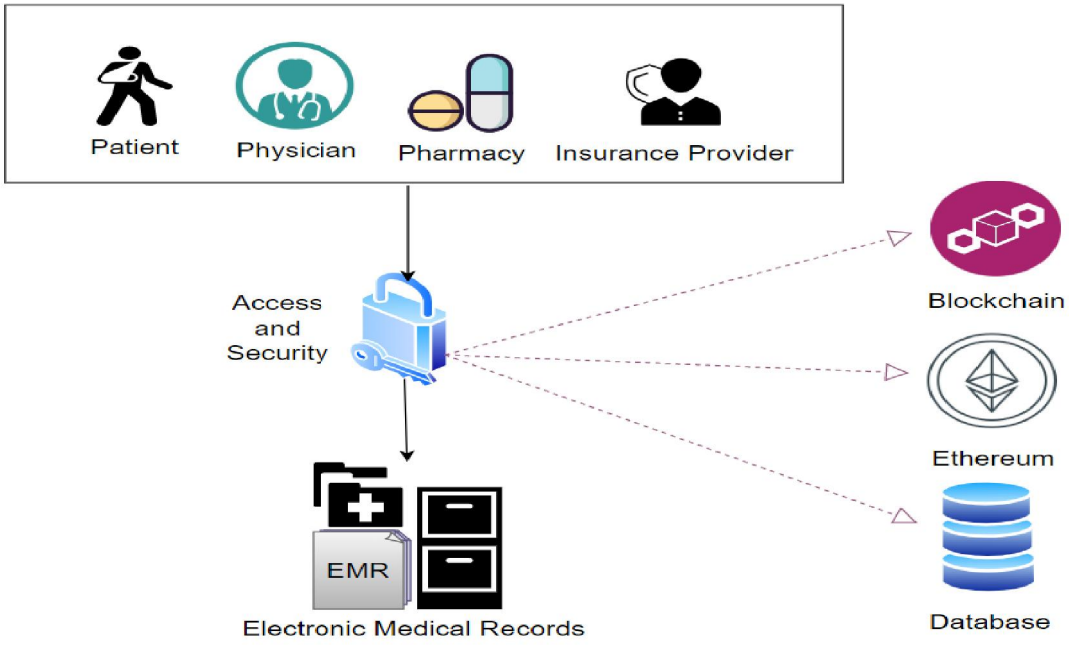

Figure.1 Overview of Architecture

[4]This paper proposes a lightweight medical data sharing scheme based on blockchain technology, which takes advantage of the decentralization and tamper-resistant features of blockchain to protect and share medical data securely. The proposed scheme utilizes proxy re-encryption technology to enable doctors to access patients' historical medical records securely, ensuring that the inquired information is transmitted in the ciphertext form to maintain confidentiality. The analysis results demonstrate that the proposed scheme satisfies various security requirements and has a low computational and communication cost. Overall, the proposed scheme presents a viable solution for secure and efficient medical data sharing using blockchain technology.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

[5]This study aims to provide insights into the current state of research on blockchain-based Electronic Health Record (EHR) management and future directions. The study findings indicate that Ethereum (private) and Hyperledger Fabric are the most prominent blockchain platforms for EHR management, as they meet most of the requirements for secure and efficient management of EHRs. However, the study also highlights the limitations of handling large-scale EHR data on blockchain, including limited storage capacity, computation cost, and communication cost. Overall, this study provides valuable insights into the current state of blockchain-based EHR management research and identifies potential future research directions.

[6]The proposed framework combines secure record storage with granular access rules to create a system that is user-friendly and easy to understand. Additionally, the framework includes measures to address the challenge of data storage by utilizing the off-chain storage mechanism of IPFS. This approach ensures that the system can store large amounts of data securely and efficiently, without compromising on performance. By combining secure storage with granular access rules and off-chain storage, the proposed framework presents a robust solution for managing sensitive data while ensuring accessibility and ease of use for users.

IV. PROPOSED WORK

U-Medchain uses blockchain technology to securely store health records and maintain a single version of the truth. The different organizations such as doctors, hospitals, laboratories, pharmacists and health insurers can request permission to access a patient's record to serve their purpose and record transactions on the distributed ledger. U-Medchain provides solutions to today's health record problems. The platform is built to securely store and share electronic health records. By digitizing health records and empowering users, we can leverage countless industry synergies. It is intended to be compatible with the existing EMRs databases. It enhances existing EMR management systems by ensuring security and ease of access. The creation , verification, and appending of new blocks is part of the U-Medchain protocol. It protects user's privacy by using timed-based smart contracts to control transactions. Adoption of advanced encryption and authentication methods ensures security and access control. Nodes Consensus Contract (NCC),Steward-relation History Contract (SRHC) ,Participants Records Contract (PRC),Logs Contract (LC),Access Control Contract (ACC), Proxy Re-encryption Contract (PReC) are the Smart Contracts involved in our system and algorithms used are:

A consensus algorithm is a process used to achieve agreement among multiple nodes or participants in a distributed system. It ensures that all nodes in the network have a consistent view of the system's state by facilitating agreement on a single version of the truth. In blockchain technology, consensus algorithms are used to validate transactions and create new blocks. There are various consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), each with its own advantages and disadvantages. Consensus algorithms play a critical role in ensuring the security, efficiency, and scalability of distributed systems.

Re-encryption schema is a technique used for secure transfer of encrypted messages between nodes without sharing sensitive credentials. It employs a proxy to re-encrypt a message in a way that allows another user to decrypt it via their private key, even if the associated public key is not used for encrypting the message. In this schema, each proxy node has a unique public/private key pair, and the public key is known to the other proxy nodes. The message is encrypted using a master public key, and the associated private key is distributed in pieces among the proxy nodes. Each proxy node then blinds the encrypted message, decrypts it using its private key, and un-blinds the result to create an obscured plaintext.

To guarantee data integrity, our proposed framework uses SHA-256 hashing methods. In order to access the EMR on the blockchain, U-MedChain maintains a hash value rather than the actual link, which will be created after the record's issuance. The encrypted query URL will be sent over HTTPS to the associated participant who has access rights in order to view a record. As a result, the hash value saved in the blockchain guarantees that no alterations were made outside the blockchain during the transfer because the hash value is unique to the original document.

V. PROPOSED METHODOLOGY

5.1 Adding New Health Provider

The proposed smart contract rules, the incentive system, the frequency of updating the blockchain network, and the procedure for generating, verifying, and appending a new block to the blockchain network must all be accepted by all

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

participating providers before a new health provider node can be added to the network. The process starts with the new provider node sending their ID, Ethereum address, and requested role to the NCC. Voters' nodes in the NCC validate and authenticate the request to ensure it is from a legitimate provider not previously registered. If the request is accepted and validated, the NCC updates its memory with the Ethereum address, ID, and role of the new node and creates a new SRHC for it. The address of the new SRHC is then sent to the new provider node.

5.2 Adding and Registering Patient

Adding a new patient node involves sending a request from a provider node to the NCC for validation of the patient's ID, Ethereum address and requested role. A new SRHC is created for the patient node by the NCC after it has updated its local memory following validation. The provider sends the patient's account information to the patient node, similar to creating a new online account. Registering a patient node requires the DB manager of the provider node to send the patient's Ethereum address and "patient" role to the NCC for verification. Upon confirmation, the provider node sends the patient information in a transaction to its SRHC, which requests to generate a new stewardship with the patient. The SRHC of the provider creates a new PRC for the new stewardship and fills in the patient's information. For future use, the PRC transmits the addresses of the provider and patient nodes to the SRHC.

5.3 Adding and Editing Record

To add a new record via a provider node, a stewardship needs to be established between the provider and patient nodes to have a shared Patient Record Cryptography (PRC). After internal encryption in the provider node, the new record is transferred to the DB Manager, which creates a query link and hashes it along with the medical record. The Cipher/Decipher Manager encrypts the record and link with a symmetric key, which is then encrypted with the public keys of the provider, patient, and proxies. The PRC stores the encrypted record and creates an access control chain (ACC) with permissions for the patient and provider. To edit a record, the provider node sends the patient's ID to retrieve the PRC address, then forwards the filename and Ethereum address to the PRC. The ACC checks permissions and forwards the symmetric key to the provider node for decryption and record modification, which creates a new hash value. The DB manager sends the new hash to the PRC for updating, and a log is created and encrypted for the LC.

5.4 Reading A Record

To read a record from a patient node, the patient node sends the provider's ID to its SRHC to retrieve the associated PRC address. The patient's Ethereum address and filename for the requested record are then sent to the PRC by the patient node. To determine whether the Ethereum address that was received has authorization to access the requested information or not, the PRC sends the request to the ACC. If so, the AAC forwards the patient's encrypted symmetric key to the PRC, which forwards it to the patient node. The DB manager of the patient's node then retrieves the encrypted EMR from the provider's database using the decrypted symmetric key, and creates an encrypted log of the process which is forwarded to the LC for addition to the blockchain.

VI. SYSTEM COMPARISON

Table 1. comparison between proposed frameworks for managing EMR's

Properties	Ref. [3]	Ref. [5]	U-Medchain
Blockchain based	✓	✓	✓
Access control	✓	✓	✓
Privacy preservation	X	X	✓
Scalability	X	X	✓
Smart Contracts	✓	✓	✓

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

Time based Smart contracts	X	X	✓
Performance Evaluation	X	X	✓
Incentive Mechanism	X	✓	✓

VII. CONCLUSION

The conclusion of the paper outlines the proposed design of a blockchain-based system, U-MedChain, which aims to improve the management of electronic medical records (EMRs) by providing secure and efficient access for health providers and patients while ensuring patient privacy. The system employs advanced techniques such as timed-based smart contracts, hashing, encryption, and authentication mechanisms to maintain privacy, security, and access control. It also offers interoperability, auditability, and accessibility through comprehensive logs. The paper presents an incentive mechanism that rewards the significance of providers in maintaining medical records and creating new blocks, ensuring fairness, equality, and sustainability of the system. Extensive experiments demonstrate the efficiency of U-MedChain in handling large datasets with low latency, making it a potential solution for managing EMRs in healthcare systems. Overall, U-MedChain offers an adaptable solution that can potentially enhance the management of electronic records and improve healthcare delivery

REFERENCES

[1]. "A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations"- Emeka Chukwu And Lalit Garg.

[2]. "Blockchain for Giving Patients Control Over Their Medical Records "-Mohammad Moussa Madine , (Member, IEEE), Ammar Ayman Battah , Ibrar Yaqoob , (Senior Member, IEEE), Khaled Salah , (Senior Member, IEEE), Raja Jayaraman , Yousof Al-Hammadi , SasaPesic , And Samer Ellahham.

[3]. " Smart Access: Attribute-Based Access Control System for Medical Records Based on Smart Contracts " - Marcela Tuler De Oliveira , Lúcio Henrik Amorim Reis , Yiannis Verginadis , Diogo Menezes Ferrazani Mattos , (Member, Ieee), And Sílvia Delgado Olabarriaga

[4]. "A Blockchain-Based Medical Data Sharing and Protection Scheme"- Xiaoguang Liu ,Ziqing Wang , Chunhua Jin , Fagen Li , (Member, IEEE), And Gaoping Li.

[5]. "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction"- Abdullah Al Mamun , Sami Azam , (Member, IEEE), And Clementine Gritti .

[6]. "Using Blockchain for Electronic Health Records"- Ayesha Shahnaz , Usman Qamar , And Ayesha Khalid, (Member, IEEE).

[7]. "Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test" Ye SeulBae ,Yujin Park , Seung Min Lee , Hee Hwa Seo, Hyeonji Lee ,Taehoon Ko, Eunsol Lee, Sang Min Park, And Hyung-Jin Yoon.

[8]. "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records" Mohammad Zarour, Md Tarique Jamal Ansari, Mamdouh Alenezi ,Amal Krishna Sarkar, Mohd Faizan, Alka Agrawal ,Rajeev Kumar And Raees Ahmad Khan (Member, IEEE).

[9]. "Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective" Yiying Liu, Guangxing Shan, Yucheng Liu, Abdullah Alghamdi ,IqbalAlam , And Sujit Biswas , (Member, IEEE).

[10]. "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems " Dinh C. Nguyen , Pubudu N. Pathirana, (Senior Member, IEEE),Ming Ding , (Senior Member, IEEE), And Aruna Seneviratne , (Senior Member, IEEE).

[11]. "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records" Mohammad Moussa Madine (Member, IEEE),Khaled Salah (Senior Member, IEEE), Raja Jayaraman ,Ibrar Yaqoob (Senior Member, IEEE), Yousof Al-Hammadi Samer Ellahham , And Prasad Calyam, (Senior Member, IEEE).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

[12]. "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records" Mohammad Zarour, Md Tarique Jamal Ansari, Mamdouh Alenezi ,Amal Krishna Sarkar, Mohd Faizan, Alka Agrawal ,Rajeev Kumar And Raees Ahmad Khan (Member, IEEE).

[13]. Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain " ShufenNiu , Lixia Chen , Jinfeng Wang , And Fei Yu.

[14]. "A Consent Model for Blockchain-Based Health Data Sharing Platforms" Vikas Jaiman AndVisaraUrovi.

[15]. "A Performant Protocol for Distributed Health Records Databases" MicaelPedrosa , Rui Lebre , And Carlos Costa.

[16]. "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System" Chun-Ta Li , (Member, IEEE), Dong-Her Shih , Chun-Cheng Wang,Chin-Ling Chen, And Cheng-Chi Lee.

[17]. VigilRx: A Scalable and Interoperable Prescription Management System Using Blockchain" Alixandra Taylor, Austin Kugler ,Praneeth Babu Marella,And Gaby G. Dagher .

[18]. "Practical Medical Files Sharing SchemeBased on Blockchain and DecentralizedAttribute-Based Encryption" Jiyu Tao And Li Ling.

[19]. "Revocable Attribute-Based Signature for Blockchain-Based Healthcare System" Qianqian Su , Rui Zhang , Rui Xue , (Member, IEEE), And Pengchao Li.

[20]. "SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities" ManafZghaibeh , Umer Farooq , Najam Ul Hasan ,And Imran Baig , (Senior Member, IEEE).

[21]. "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems "Alaa Haddad, Mohamed HadiHabaebi , (Senior Member, IEEE),Md. Rafiqul Islam , (Senior Member, IEEE),Nurul FadzlinHasbullah , (Member, IEEE),And Suriza Ahmad Zabidi, (Member, IEEE).