A Secure Blockchain for Electronic Health Records

Jihad Qaddour
School of Information Technology
Illinois State University
Old Union Building, Box 5150, Normal, IL 61790, USA
jqaddou@ilstu.edu

Kanz Ul Eman)
School of Information Technology
Illinois State University
Old Union Building, Box 5150, Normal, IL 61790, USA
keman@ilstu.edu

Abstract—Blockchain technology has attracted considerable attention and has grown constantly since its introduction in 2008. It has emerged as a valuable tool in several industries, including healthcare, particularly regarding protecting and securing electronic health records. They contain sensitive patient data that is often vulnerable to cyberattacks. Blockchain's decentralized and immutable nature can help to protect EHRs from unauthorized access, modification, or deletion. This paper proposes a blockchain-based architecture for EHRs that incorporates Ethereum-based smart contracts, decentralized off-chain storage with the Interplanetary File System, and strong symmetric encryption. This architecture provides a robust solution that guarantees the security and scalability of EHRs. The paper also provides a thorough analysis of the framework's security merits and improves our knowledge and ability to use secure electronic health record systems.

Keywords—Blockchain; health data; electronic health records; security; decentralize; confidentiality.

I. INTRODUCTION

The healthcare industry generates and maintains a vast amount of data daily, including highly sensitive information such as medical records, diagnoses, vital signs, and drug regimens [1]. Electronic health records (EHRs) have become widely adopted in the healthcare industry due to significant technological advances. In fact, by 2017, 96% of non-federal acute hospitals in the United States had adopted EHR systems [2]. This adoption demonstrates the industry's understanding of the benefits of EHRs in improving data management and accessibility, optimizing workflows, and improving patient care.

EHRs and well-established health information exchange (HIE) systems work together to provide a number of benefits, including lower healthcare costs and higher care quality [3]. However, using digital technologies to transmit highly private and sensitive information raises concerns, particularly about privacy and security. When information is shared between different healthcare organizations, there is an increased risk of unauthorized access, making it vulnerable to potential hackers who could launch targeted attacks [4].

To address these concerns, it is essential to create strong security controls and privacy protections. Solutions such as encryption, access controls, secure authentication protocols, and data anonymization techniques can be used to preserve the confidentiality and integrity of shared data [4]. Secure sharing of health information can also be ensured through ongoing monitoring, frequent security assessments, and employee training. These measures can also help to mitigate risks.

This research proposes a novel decentralized approach to enhancing the security of electronic health records (EHRs). The proposed system provides a scalable and decentralized alternative for storing and distributing EHR data using the Ethereum blockchain and the Interplanetary File System (IPFS) [4]. This approach leverages the built-in security features of blockchain technology and the durability of IPFS to guarantee the integrity and privacy of private medical records. The project's focus on decentralization is coherent with the growing demand in the healthcare industry for secure and effective EHR storage and interchange.

The rest of this paper is organized as follows. Section II provides background and related work. Section III discusses the proposed model. Section IV concludes the paper with the future direction.

II. BACKGROUND AND RELATED WORK

The healthcare industry is facing a critical challenge in ensuring the security of information flow. Data breaches in the healthcare industry have affected millions of people in recent years, highlighting the need for strong security measures to safeguard sensitive healthcare data [5][6]. Blockchain technology is a promising solution for information exchange in the healthcare industry. Blockchain uses a distributed ledger to ensure that every participating node keeps an exact copy of the ledger, improving data integrity and transparency [6]. Blockchain is also decentralized and irreversible, which makes it ideal for secure data sharing [6]. While blockchain technology presents exciting possibilities for electronic health records (EHR) in the healthcare sphere, there are significant challenges to overcome. Scalability is a major challenge because the bulk of EHR data can be enormous, resulting in slower and longer transactions when stored on the blockchain [6]. Another issue is transparency, as all transactions on a blockchain are public, posing privacy issues for sensitive healthcare data [6]. Balancing the need for privacy while guaranteeing effective blockchain tracking and recordkeeping becomes a critical challenge [6].
There is a growing body of research on how to overcome the challenges of using blockchain technology in healthcare. Matos et al. [7] presented a system design that uses cloud services and granular access control to successfully administer EHR. The goal was to create a safe and scalable solution that allows patients and clinicians to access EHR from anywhere in the world. Intercloud storage was used, which entails joining separate clouds to form a bigger network, allowing for end-to-end anonymity and smooth data migration between providers. In their access control method, Matos et al. emphasized the need for authentication and permission checks. However, despite efforts to prioritize patient privacy, the system may still be open to exploitations that could allow unauthorized access to critical data [7].

A. The Hyperledger Fabric blockchain

The Hyperledger Fabric blockchain, a private blockchain system, is used by the proposed framework, Action-EHR, presented by Dubovitskaya et al. [8] to improve authentication and authorization procedures. Hyperledger Fabric offers tighter control over node involvement and transaction visibility than open public blockchains. This system uses smart contracts to manage access control and preserve state variables pertaining to patient health records, much like the Ethereum network. Action-EHR intends to provide secure and auditable access to patient data by utilizing the smart contract logic. Fine-grained control over access permissions is made possible using Hyperledger Fabric and smart contracts, improving data privacy and security [8]. This strategy supports ongoing research into the effective and safe management of electronic health records using blockchain technology [8]. The misconception that blockchain technology was first developed for cryptocurrencies is a common one. However, the idea of blockchain was first proposed in 1991 [10]. The original concept behind blockchain was to create a system for digital document timestamping to prevent manipulation or backdating. This suggests that blockchain has applications beyond cryptocurrencies and can be used in various industries that require secure record-keeping and transaction tracking [10].

Distributed ledgers are used by blockchain technology to record and keep all transactions made on the network. An immutable hash signature is present in each block to which a transaction is added. Data manipulation within the blockchain is typically impossible due to the decentralized structure of the blockchain network and this hash, which assures that any unauthorized modifications to the blocks would be instantly identified and rejected [6].

B. Ethereum with Smart Contracts

Blockchain technology has made significant improvements since it was first used in Bitcoin. In 2015, Ethereum joined Bitcoin as a prominent cryptocurrency, building on the research report written by Vitalik Buterin two years prior [11]. A new blockchain was introduced by Ethereum that was comparable to Bitcoin's but distinguished itself by including smart contracts. Smart contracts allow logical code to be executed directly on the ledger, expanding the capabilities of the blockchain beyond basic transactions [11]. This innovation by Ethereum helped blockchain technology become more widely used and developed, making it a promising solution for information exchange in the healthcare industry.

C. IPFS: A Decentralized File Access and Storage Protocol

Interplanetary File System (IPFS)) is a peer-to-peer hypermedia protocol that provides a decentralized file access and storage system. IPFS differs from previous peer-to-peer protocols such as BitTorrent in that it uses a content-addressable addressing scheme. This means that data is divided into manageable portions, hashed, and assigned a CID (Content Identifier) value. This special addressing scheme ensures data integrity and reduces duplication, which enables efficient file retrieval on the IPFS network [12].

D. MedRec: A Blockchain-Based Electronic Health Records Platform

MedRec is a cutting-edge electronic health records (EHR) platform that is built on the Ethereum network. MedRec uses smart contracts written in Python to manage access to and permissions for EHR data. MedRec also features an innovative incentive system that rewards healthcare practitioners for contributing anonymized medical
data. This incentive system helps to build trust and facilitate access to valuable healthcare information [13].

E. Ancile and BHEEM

In addition to MedRec, there are several other blockchain-based EHR platforms that have been proposed. These platforms share many similarities with MedRec, in that they all use blockchain technology to provide a secure and decentralized way to store and manage EHR data, including Ancile [14] and BHEEM [15]. Both frameworks use the Ethereum network/blockchain for access management and permissions while keeping health records off-chain in a local database. While Ancile uses two encryption techniques for record storage and distribution, BHEEM omits a specific description of the encryption method used. Asymmetric encryption and proxy re-encryption are used in the distribution encryption in the Ancile framework. This enables the restoration of fully encrypted messages using a user’s private key, even if the encryption was carried out using a different user’s public key [16].

![Figure 3](image-url). An example of proxy re-encryption [16].

F. Patient-centric framework for personal health records (PHR)

Madine et al. [17] developed a patient-centric framework for personal health records (PHR) using blockchain technology, specifically the Ethereum network. The framework uses smart contracts to create an access control system. IPFS and proxy re-encryption are used as complementary techniques to overcome scalability issues. Madine et al.’s [17] research included a thorough comparison between their blockchain-based PHR architecture and current cloud-based PHR solutions. The comparison focused on a number of factors, including provenance, immutability, trustworthiness, patient-centered approach, decentralized storage, decentralized execution, and privacy. A full comparison of the results is presented in Table 1 of their research.

<table>
<thead>
<tr>
<th>Table 1. Comparison of Blockchain-Based PHR Architecture with Cloud-Based PHR Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Factor</strong></td>
</tr>
<tr>
<td>Provenance</td>
</tr>
</tbody>
</table>
which is maintained and owned by the system developer. The administrator node is responsible for managing the system and connecting hospital nodes to the blockchain. Hospital nodes are responsible for issuing Ethereum addresses to patients and providers. Patient nodes store patient identifiers, such as gender and Ethereum address, as well as a mapping of which providers have access to the patient's EHR. Therefore, the patient is still in charge of keeping this mapping up to date, authorizing or denying access to providers as needed, and preserving control over their private medical data. Provider nodes store provider identifiers, such as Ethereum address and specialty. This node can create and edit health records, as well as access an existing patient's health record. However, it is the patient's obligation to add the provider to their access list, providing them permission to read and interact with the patient's health records.

The following are the steps involved in the operation of the proposed architecture:
1. The patient authorizes the creation of an EHR by a particular provider.
2. The authorized provider creates the patient's EHR.
3. The EHR is uploaded to the IPFS-distributed file storage system.
4. The EHR is encrypted using the Advanced Encryption Standard (AES) symmetric encryption algorithm.
5. The hash of the encrypted EHR is stored on the blockchain.
6. The patient or provider enters the hash to access the EHR.
7. Smart contracts are included in the framework to create the access control system. Only authorized parties can see and edit health records thanks to the execution of access control restrictions which are made possible by the incorporation of smart contracts.
8. Smart contracts can be created using Ethereum-specific programming languages such as Solidity programming or Python.
9. The encrypted EHR is downloaded using the hash.
10. The EHR is decrypted using the shared encryption key generated during the encryption process.
11. The encryption key is kept private and is only securely shared with the patient and authorized providers who need access to the EHR. The proposed architecture provides a secure and scalable mechanism for managing EHRs. It is patient-centric, giving patients full control over their data. It is also tamper-proof, ensuring that EHRs cannot be modified without the patient's consent.

The proposed architecture uses blockchain, smart contracts, and decentralized storage to improve the security, integrity, scalability, and access control of EHRs.

The proposed architecture has several advantages over traditional EHR systems, including:

- Security: Blockchain provides a high level of security for EHRs by making them tamper-proof and immutable.
- Integrity: Decentralized storage ensures that EHRs are not lost or corrupted.
- Scalability: The blockchain can be scaled to support many users and transactions.
- Access control: Smart contracts can be used to enforce access control policies for EHRs.

IV. Conclusion

In this paper, a framework for the blockchain-based management of electronic health records (EHR) is presented. The proposed architecture uses the Ethereum blockchain, smart contracts, and decentralized storage systems like IPFS to address the issues of privacy, security, scalability, and access control in the healthcare industry.

The architecture improves the security and integrity of EHR by utilizing blockchain's distributed ledger, immutable transactions, and cryptographic techniques. This makes it difficult for unauthorized parties to access or modify EHR data. Additionally, the architecture enables fast and transparent data sharing by allowing authorized parties to view and edit EHR data. This is made possible using smart contracts to enforce access control restrictions.

Decentralized storage solutions also increase data availability and lower the risk of data loss or tampering. This is because EHR data is stored on multiple nodes in the decentralized network, making it more difficult to lose or alter.

The patient-centric approach of the framework gives individuals control over their own health information. This includes the ability to store, view, and share their EHR data with authorized parties. The architecture works as follows:
1. Patients create their own EHRs and store them on the blockchain.
2. Providers can access patients' EHRs if the patient has granted them permission.
3. Access control is enforced using smart contracts.
4. EHRs are stored in a decentralized storage system, making them more secure and available.

The proposed architecture appears to be promising in terms of resolving the problems of traditional EHR systems. However, more research and evaluation are needed to demonstrate its effectiveness, scalability, and real-world applicability.

REFERENCES

def create_ehr(patient, provider):
    # Create a new EHR for the patient.
    # The provider must be authorized to create the EHR.
    ehr = {
        "patient": patient,
        "provider": provider,
    }
    # Upload the EHR to IPFS.
    ehr_hash = ipfs.upload_file(ehr)
    # Encrypt the EHR using AES.
    encrypted_ehr = encrypt_ehr(ehr, encryption_key)
    # Store the hash of the encrypted EHR on the blockchain.
    blockchain.store_hash(ehr_hash)
    # Create a smart contract to manage access to the EHR.
    smart_contract = create_smart_contract()
    # Add the patient and authorized providers to the smart contract.
    for provider in ehr["authorized_providers"]:
        smart_contract.add_user(provider)
    # Share the encryption key with the patient and authorized providers.
    patient.set_encryption_key(ehr["authorized_providers"]):
        provider.set_encryption_key(ehr["authorized_providers"])
    # Check if the patient is authorized to access the EHR.
    if not smart_contract.is_user_authorized(patient):
        raise UnauthorizedAccessError()
    # Download the encrypted EHR from IPFS.
    encrypted_ehr = ipfs.download_file(ehr_hash)
    # Decrypt the EHR using the shared encryption key.
    ehr = decrypt_ehr(encrypted_ehr, patient.get_encryption_key())
    # Return the EHR.
    return ehr

APPENDIX A

Simple outline for a secure Algorithm for Blockchain-Based Architecture for HER in Python

```python
def create_ehr(patient, provider):
    # Create a new EHR for the patient.
    # The provider must be authorized to create the EHR.
    ehr = {
        "patient": patient,
        "provider": provider,
    }
    # Upload the EHR to IPFS.
    ehr_hash = ipfs.upload_file(ehr)
    # Encrypt the EHR using AES.
    encrypted_ehr = encrypt_ehr(ehr, encryption_key)
    # Store the hash of the encrypted EHR on the blockchain.
    blockchain.store_hash(ehr_hash)
    # Create a smart contract to manage access to the EHR.
    smart_contract = create_smart_contract()
    # Add the patient and authorized providers to the smart contract.
    for provider in ehr["authorized_providers"]:
        smart_contract.add_user(provider)
    # Share the encryption key with the patient and authorized providers.
    patient.set_encryption_key(ehr["authorized_providers"]):
        provider.set_encryption_key(ehr["authorized_providers"])
    # Check if the patient is authorized to access the EHR.
    if not smart_contract.is_user_authorized(patient):
        raise UnauthorizedAccessError()
    # Download the encrypted EHR from IPFS.
    encrypted_ehr = ipfs.download_file(ehr_hash)
    # Decrypt the EHR using the shared encryption key.
    ehr = decrypt_ehr(encrypted_ehr, patient.get_encryption_key())
    # Return the EHR.
    return ehr
```