iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56362

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 X Oct 2023- Available at www.ijraset.com

Leveraging Smart Contracts for Decentralized Healthcare Data Sharing

Prof. Sumit. S. Shevtekar[1], Sanket Chaudhari[2]
[1] *Assistant Professor,* [2]*Student, Department of Computer Engineering, SCTR's Pune Institute of Computer Technology,* Pune,India

Abstract: ***Healthcare data sharing is essential for enhancing healthcare service quality and efficiency. However, traditional healthcare data sharing systems are often centralized, opaque, and inefficient. This can pose security and privacy concerns, as well as delays and errors in data access.***
The integration of blockchain-based smart contracts into the healthcare sector has introduced a transformative paradigm for decentralized healthcare data sharing. This research paper explores the multifaceted landscape of leveraging smart contracts to enhance the security, efficiency, and accessibility of healthcare data sharing. By offering secure, transparent, and automated mechanisms, smart contracts address critical challenges in patient data management, consent verification, and interoperability across healthcare systems.
This paper delves into the architecture and practical implementation of smart contracts in healthcare, highlighting their potential to revolutionize electronic health records, streamline administrative processes, and ensure compliance with data privacy regulations. Through this exploration, we underline the pivotal role of smart contracts in reshaping the healthcare industry and fostering trust in the digital age.
Keywords: Smart Contracts, Decentralized, Healthcare, Data Sharing, Privacy, Security, Patient Data Management, Consent Verification, Interoperability, Electronic Health Records, Compliance, Patient-Centric Care, Data Integrity, Healthcare Industry, Trust.

I. INTRODUCTION

The healthcare industry is facing significant challenges related to data sharing, interoperability, and security. Traditional healthcare systems make accessing and sharing patient data across systems challenging for physicians. Furthermore, patient data is frequently held in centralized systems that are subject to cyber-attacks and privacy breaches.
Blockchain technology, which provides a decentralized trustworthy environment for data sharing and storage, has emerged as a viable answer to these difficulties.
Smart contracts, that are self-executing contracts in which the conditions of the buyer-seller agreement are explicitly put into lines of code, can improve the efficiency and openness of healthcare data exchange even further.
To begin with, we presume that the security of health records for patients and sensitive medical information is unavoidable. In an era rife with data breaches and privacy concerns, blockchain, with its immutability and encryption capabilities, offers a promising solution.
We also believe that interoperability, or the easy interchange of data among various healthcare systems and institutions, is critical. Another major assumption is achieving this while guaranteeing regulatory compliance, such as compliance of the Health Insurance Portability and Accountability Act (HIPAA).
Moreover, we assume that the principles of transparency and patient consent, when combined with the benefits of blockchain technology, can foster a healthcare ecosystem where patients have greater control over their data and who accesses it.

The proposed system is based on the following basic assumptions:

1) Patients own their private healthcare data and have the right to control how it is shared.
2) Healthcare providers and other authorized parties should only have access to the data they need to provide care or conduct research.
3) Data should be shared securely and efficiently, while protecting patient's privacy.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

II. LITERATURE SURVEY

This section compiles some of the prior research on smart contracts for data sharing. This survey is carried out in order to overcome the limitations of the already implemented systems and gain a brief overview on the secure data sharing in the healthcare industry.

No	Title	Findings
1.	A secure blockchain-based e-health records storage and sharing scheme	This research presents a secure blockchain-based scheme for storing and sharing e-health records, ensuring data security. However, the study may have limitations and communication overhead is also very high.
2.	A Blockchain-Based Smart Contract System for Healthcare Management	Khatoon's work focuses on a smart contract system tailored for healthcare management, enhancing efficiency and data security. However, the study may require further validation and real-world testing for practical implementation in healthcare systems. Not applicable for large datasets.
3.	A Decentralized Storage System Using IPFS, Attributed-based Encryption, and Blockchain	Pham et al. introduce B-Box, a decentralized storage system that combines IPFS, attributed-based encryption, and blockchain technology. This innovative approach ensures secure data storage and sharing. Limitation of this system is it lacks to provide confidentiality.
4.	A healthcare system based on IoT, Blockchain and IPFS for data management security	This research by Azbeg et al. explores "BlockMedCare," a healthcare system leveraging IoT, blockchain, and IPFS for enhanced data management security. The study highlights the potential of this innovative system in addressing data security and privacy challenges in healthcare. It lacks to offer data integrity.
5.	Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals	Jamil et al. investigate the development of an IoT-based blockchain integrity management platform for remote monitoring of patient vital signs in smart hospitals. This research aims to enhance patient care through secure and efficient data management. Lacks Cloud security.
6.	Blockchain-based privacy preserving e-health system for healthcare data in cloud.	The study by Zhang et al. explores a blockchain-based privacy-preserving e-health system designed to secure healthcare data in cloud environments. The research emphasizes data privacy and security in the cloud, however it cannot provide security against insider attacks.

III. PROBLEM STATEMENT

There is a pressing need for a novel solution that can decentralize healthcare data sharing while maintaining data integrity and privacy. Leveraging smart contracts for decentralized healthcare data sharing aims to address these challenges, offering a secure and efficient way to manage patient data. This project seeks to develop a system that can enable seamless, privacy-compliant, and secure sharing of healthcare data across the industry. The challenge lies in designing a robust, scalable, and user-friendly platform that integrates smart contracts into healthcare data management, enhancing patient-centric care and regulatory compliance.

IV. PROPOSED SYSTEM

The proposed system is a decentralized healthcare Smart contract-based data sharing system. This technology enables people to control their own data and exchange it on a need-to-know basis with healthcare practitioners, researchers, and other authorized parties. The system also ensures that data is shared securely and efficiently, while protecting patient's privacy.

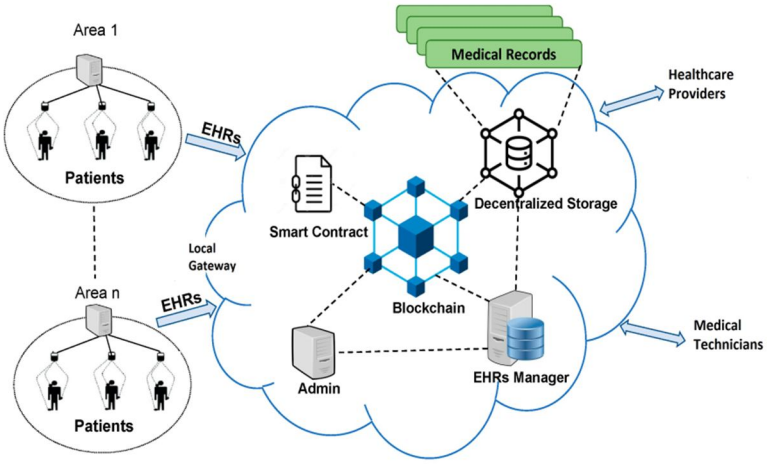


Figure 1: Architecture of Proposed System.

The system consists of the following components (Figure 1):

1) *Blockchain:* The system is built on a blockchain platform, such as Ethereum. The blockchain provides a secure and tamper-proof platform for storing and sharing data.
2) *Smart Contract:* To manage data exchange, the system employs a smart contract. The smart contract specifies the rules and circumstances for data sharing.
3) *Decentralized Storage:* The system uses decentralized storage, such as IPFS, to store data. Decentralized storage provides a secure and reliable way to store data without the need for a central server.

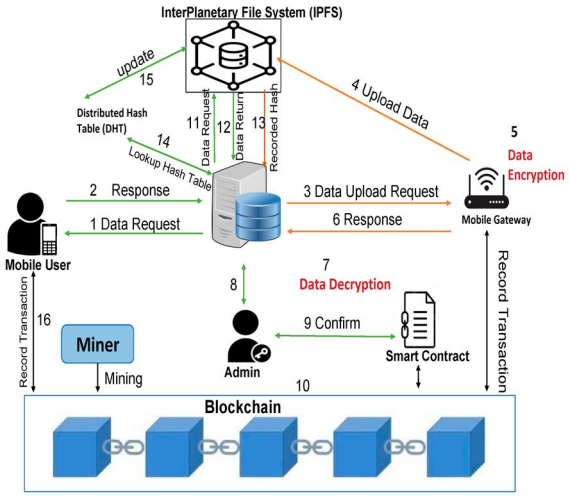


Figure 2: Design of Proposed System.

Working of Proposed System (Figure 2):

1) *Data Request by Mobile User:* The process begins with a mobile user initiating a data request. This request is transmitted to the system to fetch specific data based on user preferences or requirements.
2) *Response Generation:* Upon receiving the data request, the system queries the Distributed Hash Table (DHT) to locate the requested data. The located data is then transmitted back to the mobile user as a response.
3) *Data Upload Request to IPFS:* If the mobile user decides to upload data, it first gets encrypted via the mobile gateway. Post encryption, a data upload request is sent to the IPFS.

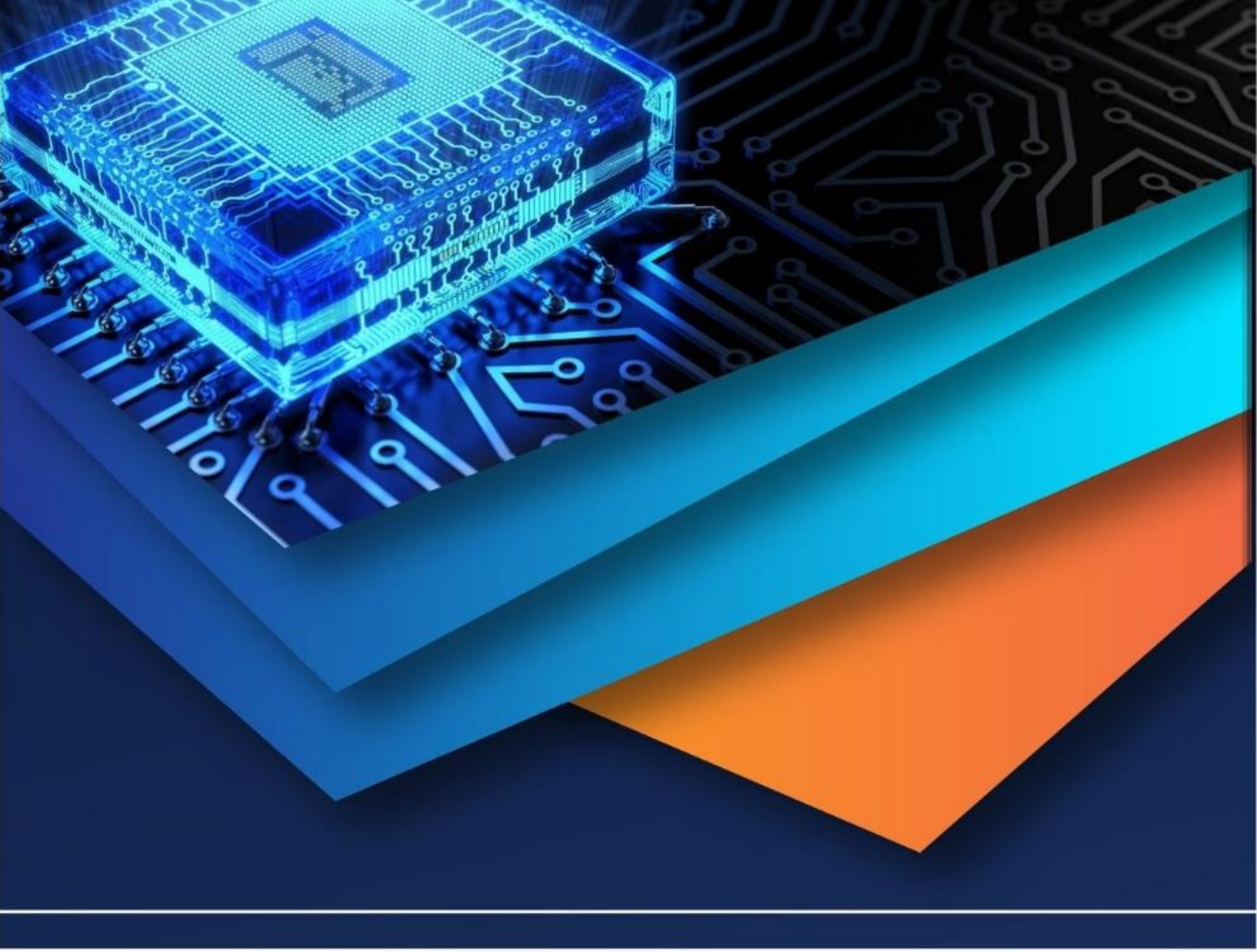
4) *Data Storage on IPFS:* The encrypted data is then uploaded and stored within the IPFS, ensuring decentralized and tamper-proof storage. A unique hash for the stored data is generated.
5) *Data Encryption through Mobile Gateway:* Prior to uploading, data passes through the mobile gateway where it undergoes stringent encryption processes to ensure security and privacy.
6) *Acknowledgment of Data Upload:* Once the data is securely stored on IPFS, an acknowledgment or response is sent back to the user confirming successful data upload.
7) *Data Decryption for Admin Review:* The admin, when needed, can retrieve and decrypt the stored data for verification or other administrative purposes.
8) *Admin Confirmation:* Post decryption and review, the admin sends a confirmation about the data's validity and integrity.
9) *Smart Contract Execution:* A smart contract, pre-coded with specific rules, triggers automatically upon receiving admin's confirmation, thereby ensuring the data's authenticity and facilitating its subsequent use or transaction.
10) *Blockchain Role in Data Validation:* Once the smart contract is executed, the data (or its related transaction) is recorded and validated on the blockchain, ensuring immutability and transparency.
11) *Data Retrieval on IPFS:* Data can be retrieved from IPFS using its unique hash. This ensures that even in a decentralized system, data retrieval remains efficient and swift.
12) *Recording of Hash in DHT:* For every data stored on IPFS, its unique hash is recorded in the Distributed Hash Table, enabling easy and quick lookups in the future.
13) *Update Mechanism:* The system supports updating the stored data. Any modifications to data would involve generating a new unique hash, ensuring the previous versions remain intact.
14) *Lookup in Hash Table:* When data needs to be fetched or verified, the system performs a lookup in the hash table using the unique hash, enabling swift data location.
15) *Data Update Confirmation:* Once data is updated on IPFS, a confirmation of the successful update is sent to the concerned parties or systems.
16) *Recording Transaction by Miners:* Miners play a crucial role in validating and recording data transactions on the blockchain, ensuring the data's integrity and authenticity at all times.

V. CONCLUSION AND FUTURE WORK

In this paper, we have presented a novel approach to decentralized healthcare data sharing using smart contracts. The suggested approach allows people to own their own data and exchange it on a need-to-know basis with healthcare practitioners, researchers, and other authorized parties. The system also ensures that data is shared securely and efficiently, while protecting patients' privacy. Future work consists addressing the regulatory challenges of using smart contracts for healthcare data sharing along with evaluating the scalability of the system.

REFERENCES

[1] H. L. Pham, T. H. Tran and Y. Nakashima, "A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract," 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644164.
[2] Shamshad, S.; Minahil; Mahmood, K.; Kumari, S.; Chen, C.-M. A secure blockchain-based e-health records storage and sharing scheme. J. Inf. Secur. Appl. **2020**, 55, 102590. [CrossRef]
[3] Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. Electronics **2020**, 9, 94. [CrossRef]
[4] Pham, V.-D.; Tran, C.-T.; Nguyen, T.; Nguyen, T.-T.; Do, B.-L.; Dao, T.-C.; Nguyen, B.M. B-Box—A Decentralized Storage System Using IPFS, Attributed-based Encryption, and Blockchain. In Proceedings of the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 14–15 October 2020; pp. 1–6. [CrossRef]
[5] Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egypt. Inform. J. **2022**, 23, 329–343. [CrossRef]
[6] Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. Sensors **2020**, 20, 2195. [CrossRef]
[7] Zhang, G.; Yang, Z.; Liu, W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput. Netw. **2021**, 203, 10858. [CrossRef]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY