JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVOLUTIONIZING HEALTHCARE INFORMATIONMANAGEMENT: A COMPREHENSIVE REVIEW OF BLOCKCHAIN'S IMPACT ON PATIENT RECORDS, PHRS, AND EHRS

Chinnaswamy CN[1], Rampur Srinath[2], Akshay Goud T[3], Arya B[4], Keerthan Chandra M[5], Krupal M Urs[6]

[12]*Associate Professor, Department of Information Science and Engineering., NIE, Mysuru, Karnataka.*
[3456]*UG student, Department of Information Science and Engineering., NIE, Mysuru, Karnataka.*

ABSTRACT

This comprehensive review brings together insights from four research studies that together highlight the potential of blockchain technology to be brought into healthcare systems. The first paper addresses the challenges of electronic medical records and proposes a secure storage solution based on encryption based on an attribute of a cryptographic policy, InterPlanetary File System (IPFS) storage and blockchain, which provides anti-counterfeit traceability and optional protection against keyword attacks [1]. Another paper advocates patient-based electronic health record (EHR) sharing using cloud computing and blockchain, focusing on precise access control through attribute-based and multi-keyword encryption systems. A practical Byzantine fault-tolerant consensus algorithm controlled by node state is also presented to improve the resilience of the consortium blockchain network [2]. The third paper presents insights from a systematic literature review, classifies the benefits and challenges of blockchain in data-intensive healthcare, and proposes a framework for future research [3]. Finally, the fourth article discusses blockchain and its increasing visibility in health applications, highlighting its role in changing traditional medical practices, especially in the context of the Covid-19 pandemic. The paper recommends blockchain-based tracking systems to ensure secure and accurate data sharing to meet the information security challenges of the pandemic era [4]. This synthesis provides a comprehensive understanding of blockchain and its multifaceted implications for improving safety, efficiency and patient care in healthcare systems.

INTRODUCTION

The rapid development of information technology in the medical field has led to the widespread use of electronic information systems, resulting in the production of a wide variety of medical information, including

electronic medical records (EMRs), medical images and diagnostic reports [1]. The effective use of this wealth of medical information is essential for predicting infectious diseases, preparing for defense, and as legal evidence in medical disputes. However, the availability and potential misuse of shared medical information presents challenges to patient privacy, requiring urgent solutions to manage access rights. The proposed solution integrates attribute-based encryption (ABE) and blockchain technology to create a secure storage and operating system for EMRs in the InterPlanetary File System (IPFS) storage environment [1]. By encrypting medical data based on attributes and using the distributed IPFS storage platform, the system ensures secure content storage, verifiable keyword search and access control. Blockchain records the entire process and provides strong evidence of medical disputes and negligence [1].

Effective integration of medical devices and sensors, cloud computing, and Internet of Things (IoT) technology has revolutionized healthcare, especially through electronic health records (EHR) [2]. However, protecting EHRs during data sharing processes and considering the semi-trusted nature of cloud servers requires attribute-based encryption (ABE) and blockchain technology. The evolution of ABE to CP-ABE (Ciphertext-Policy Attribute-Based Encryption) facilitates fine-grained access control, while blockchain and the decentralized, tamper-proof nature of add an additional layer of protection [2]. A strategic combination of cloud computing and blockchain is needed to improve data storage and sharing, especially when managing large-scale, multidisciplinary health data [2].

The data-intensive nature of healthcare, where large volumes of data are produced, distributed, stored and used every day, has led to the exploration of blockchain technology as a possible solution to improve safe and efficient data transfer [3]. With the introduction of remote health monitoring and the growth of the Internet of Things, the healthcare for safe storage and transmission of medical data has become paramount. A systematic literature review in this area identifies the blockchain symbiosis in healthcare, highlights its benefits and challenges, and provides a framework for future research efforts [3]. The decentralized, traceable and programmable functions of Blockchain make it a promising technology to ensure the integrity of health data and contribute to the effective management of drug supply chains [3].

The popularity of Blockchain extends beyond financial applications and becomes a key technology to solve critical problems in healthcare, such as secure information sharing, medical information management and public health crises [4]. Blockchain's decentralized and decentralized nature offers advantages in secure data sharing and management, especially when dealing with sensitive and critical data in healthcare systems. Unexpected challenges caused by the Covid-19 pandemic highlight the importance of accurate and transparent reporting, making blockchain technology essential to streamline clinical processes, ensure data accuracy and facilitate successful decision-making [4]. From e-health to telemedicine, blockchain applications promote the secure and transparent distribution of patient data and address security, privacy and storage of sensitive health data [4]. The versatile integration of blockchain technology into healthcare sectors highlights its potential to disrupt the industry by providing secure, efficient and transparent solutions for managing and sharing medical information.

LITERATURE SURVEY

The accelerated development of the Internet of Things (IoT) has attracted more attention to the security and privacy of personal data, making electronic health records (EHR) a key element of modern medical services [2]. However, EHRs, considered a powerful tool to improve the quality of medical services and accelerate biomedical discoveries, struggle with privacy and security issues inherent in their information systems. In EHRs, current storage methods have a low level of security, making them vulnerable to potential data leaks [2]. The growth of cloud technology has greatly improved EHR storage methods, but they still face security issues, especially with cloud service providers. Various attribute-based encryption (ABE) schemes have been

proposed to address these issues, including encryption-based attribute-based encryption (CP-ABE), fine-grained flexible access control, and secure attribute-based signatures [2]. The purpose of these systems is to ensure that EHRs are encrypted, allowing only users with certain attributes to decrypt. Despite these advances, there is still room for improvement, encouraging the search for solutions such as the integration of blockchain technology with cloud storage to improve EHR data, ensure patient-directed access to information, optimize the effectiveness of encrypted text searches and improve. information sharing in general [2].

Blockchain technology has become a transformative force in healthcare, especially in the management of sensitive data such as COVID-19 data [4]. Governments in some countries, including Chile, Germany and the UK, have decided to issue immunity certificates via blockchain networks to people who have recovered from COVID-19 so they can return to work and school. This approach addresses the confounds of faking and engaging in social activities [4]. Blockchain networks play an important role in securely storing and authenticating information related to COVID-19 through distributed ledgers and smart contracts. Biometric authentication and contact tracing is facilitated by smart devices connected to blockchain networks, which improve privacy and help detect potential exposure to a virus [4]. In addition to government initiatives, private blockchains have found applications in healthcare information management. Platforms like BlocHIE use loosely coupled chains for electronic medical records (EMR) and personal health records (PHD) that use transaction compression algorithms to improve fairness and eliminate retention issues. It ensures secure data storage in the health sector [4]. Combining blockchain and cloud storage offers a promising opportunity to address issues related to information security, patient access and efficiency of information sharing in healthcare systems [4].

In summary, the evolving healthcare landscape requires innovative solutions to meet the challenges of data security, privacy and effective data sharing. EHRs are a critical component of modern medical services and require sophisticated cryptographic mechanisms, including attribute-based encryption systems, to ensure secure access and prevent unauthorized disclosure [2]. The integration of blockchain technology and cloud storage technology appears as a strategic approach to improve the security and efficiency of health information management, as evidenced by applications related to the sharing of information related to COVID-19 and the issuance of immunity certificates [4]. These advances underscore the transformative potential of emerging technologies to shape the future of healthcare by providing solutions that prioritize patient privacy, data security and effective information exchange.

PROPOSED SYSTEM:

Strengthening Healthcare Information Security with Advanced Blockchain Resources

In response to growing concerns about the security and privacy of health data, our proposed system integrates modern solutions to strengthen patient data protection. We strategically combine private blockchain implementation, interoperability proof consensus algorithm and multi-factor authentication to create a complete and secure health information management ecosystem.

1. Private Blockchain Implementation:

Our main goal is to create a secure and private space for health information on a private blockchain network. This implementation ensures that access to data is strictly controlled, and only authorized individuals can enter. A centrally stored private blockchain is accessible only to authorized personnel, reducing potential privacy and security risks associated with broaderdata.

2. Proof of Interoperability Consensus Algorithm:

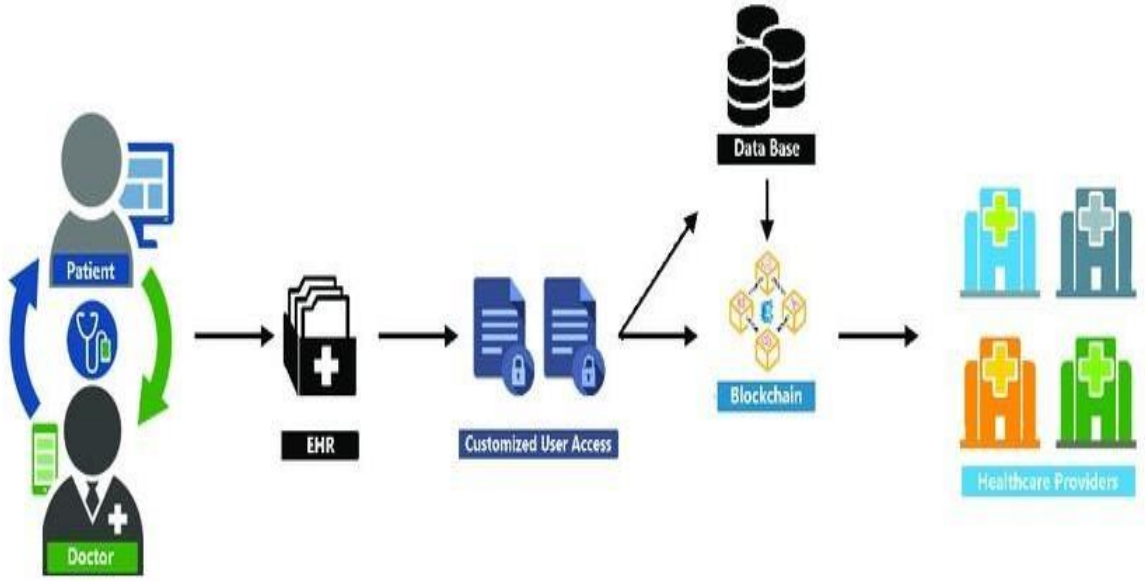
The proposed consensus algorithm focuses on increasing the transaction efficiency of healthcare applications

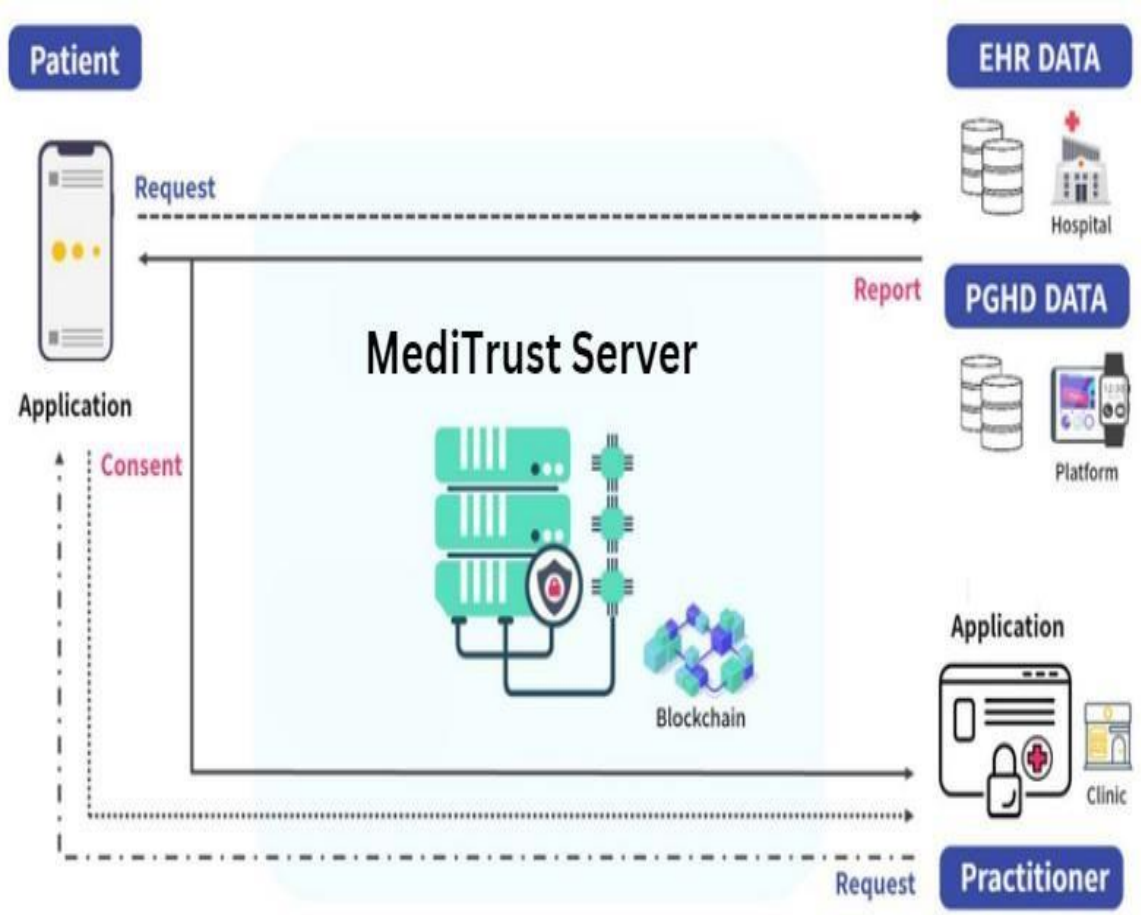
through the interoperability of participants. This approach greatly improves interoperability because it operates on a three-tier architecture, including an online platform for patient communication, a cloud-based middleware for data content, and a blockchain management node manager. By dividing blockchain functionality into multiple levels, we aim to optimize transaction processes and overall system performance.

3. Multi-factor authentication:

To strengthen participant authentication and minimize the risk of fraudulent activity, our system includes multi-factor authentication. This ensures that changes or additions to blockchain data require authentication by the majority (51%) of participants. By implementing strong user control measures, the proposed system protects against potential fraud and preserves the integrity of health data.

In short, our comprehensive system aims to create a flexible and privacy-friendly information management environment. By combining the strengths of private blockchain, cloud storage, interoperability-focused consensus algorithms and multi-factor authentication, we aim to address existing vulnerabilities and raise security standards for health information systems. This integrated approach not only protects sensitive patient data, but also ensures efficient and secure data flow within the healthcare ecosystem.




Patient
EHR DATA
Request
Hospital
Report
PGHD DATA
MediTrust Server
Application
Platform
Consent
Application
Blockchain
Clinic
Request
Practitioner

EXISTING SYSTEM:

Challenges Addressed

1. Inefficiency of Manual Record Maintenance:

- Solution: Proposed system replaces manual record-keeping with an integrated Electronic Health Record (EHR) system, streamlining data entry and retrieval.

2. Difficulty in Records Transfer Between Hospitals:

- Solution: Proposed system offers Health Information Exchange (HIE) capabilities, enabling seamless sharing of patient records among different hospitals within the network.

3. Risk of Lost Records in Transfer:

- Solution: Proposed system ensures data integrity during transfers, minimizing the risk of lost records through secure and standardized data exchange protocols.

4. Challenges in International Records Transfer:

- Solution: The platform supports international data exchange standards, facilitating the secure transfer of patient records between healthcare institutions in different countries.

5. Risk of Manual Records Getting Lost:

– Solution: By digitizing records and ensuring their central storage, the proposed system mitigates the risk ofphysical records being lost or misplaced.

6. Concerns About Data Privacy and Security:

– Solution: Proposed system incorporates robust security measures, including encryption and access controls, safeguarding patient data from unauthorized access or potential sale.

Key Features:

– Unified Electronic Health Records: Proposed system provides a unified platform for storing and managing electronic health records, eliminating the need for manual paperwork.

– Health Information Exchange (HIE): Enables secure sharing of patient records among different healthcare entities, improving care coordination.

– International Standards Compliance: Adheres to international data exchange standards, facilitating interoperability and secure records transfer between countries.

– Data Security Measures: Implements encryption, access controls, and audit trails to ensure the privacy and security of patient information.

– Interoperability: Integrates with various healthcare systems, promoting interoperability and eliminating

silos in healthcare data.

– Real-time Access: Enables real-time access to patient records, reducing delays in healthcare decision-making.

– It stands as an example for an advanced healthcare information exchange platform that effectively addresses the inefficiencies associated with manual record maintenance, streamlining records transfer, and ensuring the privacy and security of patient data on a global scale.

CONCLUSION:

The integration of blockchain technology into healthcare systems offers a solid solution to critical issues related to data security, privacy and efficient data exchange. The proposal introduces a comprehensive encryption system that uses attribute-based encryption, blockchain and IPFS storage to ensure secure storage and controlled access to electronic medical records. Despite perceived shortcomings such as access rights and data timeliness, future improvements, including recall of attributes and smart contracts, aim to strengthen the system and its efficiency.

The transformative impact of blockchain on health information management. Healthcare applications have traditionally been vulnerable to various security threats and have been greatly improved thanks to blockchain and innovative security methods. The technology not only strengthens data security against data breaches, theft and alteration, but also transforms healthcare applications with clinical, biomedical and electronic health records (EHR). Finally, the importance of electronic health records (EHR) sharing systems in promoting accurate and comprehensive patient care. The proposed system uses a hybrid approach that stores data on both on-chain and off-chain platforms to ensure data authenticity and integrity. The inclusion of a multi-keyword searchable cryptosystem increases efficiency, while the improved Practical Byzantine Fault Tolerance (PBFT) consensus algorithm handles Byzantine node failures. While further optimizations are acknowledged, including restarting the network during consensus node changes, future efforts aim to improve the consortium blockchain and its dynamic adaptability. In addition, research into advanced cryptographic techniques such as proof-of-null and homomorphic encryption promises further advances in patient identity and EHR privacy. In short, the overall impact of blockchain technology in healthcare is its ability to enhance security, improve information and revolutionize traditional healthcare applications.

REFERENCES

[1] Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE access, 8, 59389-59401.

[2] Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. IEEE Access, 10,87803-87815.

[3] Kassab, M., DeFranco, J., Malas, T., Laplante, P. Destefanis, G.& Neto, V. V. G. (2019). Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing, 9(4), 1835-1852.

[4] Kaur, M., Murtaza, M., & Habbal, M. (2020, November). Post study of Blockchain in smart health environment. In 2020 5th International Conference on Innovative Technologies inIntelligent Systems and Industrial Applications (CITISIA) (pp. 1-4). IEEE.