
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

BLOCKCHAIN-BASED LOGGING TO DEFEAT MALICIOUS INSIDERS: THE CASE OF REMOTE HEALTH MONITORING SYSTEMS

[1] G Sudhakar, [2] Ch.Deepthi Reddy,[3] A.Anugnya,[4] N.Chithra Bhanu

[1]Associate Professor in Department of Information Technology, Bhoj Reddy Engineering College for Women

[2,3,4,]UG Scholars in Department of Information Technology, Bhoj Reddy Engineering College for Women

Abstract

In remote health monitoring systems, the secure management of sensitive patient data is a critical concern, particularly when such data is accessed by multiple stakeholders, including healthcare providers, patients, and remote monitoring devices. A significant challenge lies in preventing internal threats, such as malicious insiders, from tampering with or manipulating patient health records. To address this, the implementation of a secure, tamper-proof logging and data-sharing mechanism is essential. This paper proposes a blockchain-based framework that leverages the inherent properties of immutability and decentralization to safeguard the integrity, confidentiality, and privacy of patient health records. The proposed system ensures that every access or modification to health data is transparently logged and verifiable, mitigating internal threats and enhancing trust among stakeholders. Furthermore, the solution addresses critical issues such as data interoperability and information asymmetry by enabling secure and consistent sharing of medical records across institutions, while empowering patients with direct and controlled access to their personal health information.

I INTRODUCTION

The rapid advancement of remote health monitoring systems has revolutionized the delivery of healthcare services by enabling real-time tracking of patients' health conditions from remote locations. However, this progress also introduces significant security and privacy challenges, particularly concerning the management of electronic health records (EHRs). In traditional systems, patient data is often stored in centralized databases, which are susceptible to internal threats, including unauthorized access or manipulation by insiders such as healthcare staff and administrators. These threats compromise the integrity and trustworthiness of medical records, potentially endangering patient safety and breaching ethical standards.Moreover, the current landscape of healthcare data management suffers from poor interoperability between institutions and systems, leading to fragmented and insecure sharing of medical records. This lack of secure and standardized data exchange creates barriers to effective treatment and continuity of care. Additionally, information asymmetry persists, limiting patients' ability to access and control their own medical data.

To overcome these limitations, this paper proposes a blockchain-based solution designed to enhance the security and transparency of remote health monitoring systems. Blockchain technology offers a decentralized and immutable ledger that records every transaction in a tamper-evident manner. By integrating blockchain into healthcare data management, the proposed system ensures that all data access and modifications are securely logged, verifiable, and resistant to insider threats. It also facilitates secure interoperability between healthcare institutions and provides patients with greater visibility and control over their health information. The objective is to build a more trustworthy, patient-centered, and secure remote healthcare ecosystem.

II LITERATURE SURVEY

Blockchain technology was initially introduced by Satoshi Nakamoto (2008) as the foundation for Bitcoin, emphasizing its decentralized and immutable ledger system. These characteristics have since been applied beyond financial domains, particularly in healthcare, to ensure secure and tamper-proof logging of sensitive data. Ahmed et al. (2020) proposed the Blockchain-based Audit Log Security (BCALS) system, which leverages smart contracts to create immutable and auditable logs. While effective in ensuring data integrity, the system faces notable limitations in terms of high computational cost and scalability.

Insider attacks continue to pose serious threats to cloud-based and IoT-enabled healthcare infrastructures. A report by ObserveIT (2020) highlighted that over 60% of data breaches are attributed to insider activity, often involving individuals with privileged access who can bypass conventional logging systems. Kumar et al. (2021) addressed this issue by integrating blockchain into healthcare environments to record access logs and mitigate insider misuse. However, the solution also struggled with scalability due to the processing demands of blockchain technology.

In the context of remote health monitoring, Sengupta (2020) examined the use of biometric-based authentication schemes within IoT healthcare systems to enhance the protection of patient data. Despite improvements in access security, these systems lacked robust logging mechanisms necessary to detect and prevent insider tampering. Zhao et al. (2021) proposed a blockchain-based hierarchical processing method for IoT data logs, highlighting a clear trade-off between system throughput and the level of security achieved through logging.

Cloud Access Security Brokers (CASB), such as Bitglass CASB and Lookout CASB, have emerged as effective tools for enforcing access control and data encryption in cloud environments. These platforms are particularly adept at defending against external threats but are often insufficient in addressing insider threats unless coupled with a secure, immutable logging

framework. To bridge this gap, researchers like Ma et al. have explored hybrid models that integrate CASB functionality with blockchain-based logging. Such models aim to combine the real-time access control of CASBs with the tamper-proof logging capabilities of blockchain, offering a more comprehensive approach to securing healthcare systems from both external and internal threats.

III EXISTING SYSTEM

Remote health monitoring systems currently depend on traditional centralized databases and conventional access control mechanisms for tracking and logging user activities. These systems typically store sensitive health data and access logs on centralized servers, making them vulnerable to manipulation and unauthorized access, particularly from malicious insiders with privileged access rights. Although encryption and basic access control protocols are in place, ensuring the integrity and authenticity of data logs post-storage remains a significant challenge—especially when the server or database itself is compromised.

The existing infrastructure also suffers from several technical limitations. Data privacy is not adequately enforced, and there is a lack of reliability and security during the sharing of health records across cloud servers. Additionally, centralized systems pose a major risk of a single point of failure, which can lead to complete data unavailability in case of system crashes or server outages. Storage constraints further impact the efficiency of data retrieval processes, contributing to delays and reduced performance in critical healthcare scenarios.

Disadvantages

The centralized nature of current systems introduces several vulnerabilities, including the risk of total system failure from a single point of attack. Transparency is limited, as traditional logging mechanisms do not offer verifiable and traceable audit trails, making it difficult to determine who accessed or altered specific patient records. Logs stored on centralized servers are susceptible to tampering or deletion by insiders, thereby compromising data integrity. Furthermore, auditing processes are often manual and inefficient, lacking real-time detection of unauthorized activities. The absence of robust accountability mechanisms makes it challenging to trace insider threats or hold responsible parties accountable for data breaches or policy violations.

IV PROBLEM STATEMENT

Remote health monitoring systems have become increasingly essential in modern healthcare, enabling continuous observation and management of patient health outside traditional clinical settings. These systems involve multiple stakeholders, including healthcare providers, patients, and IoT-enabled monitoring devices, all of whom access and interact with sensitive patient data. However, the centralized architecture commonly used in current

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

implementations introduces significant security risks. In particular, internal threats—such as malicious insiders with authorized access—pose a serious challenge, as they may exploit their privileges to alter, delete, or misuse critical health information without detection.

Traditional logging and access control mechanisms often fail to provide tamper-evident records or real-time accountability, especially when the central server itself is compromised. Therefore, ensuring the integrity, authenticity, and traceability of all data access and modifications is a pressing concern. To address these challenges, a decentralized, tamper-proof logging framework is needed—one that guarantees secure, transparent, and immutable tracking of patient data activities. Blockchain technology, with its inherent immutability, transparency, and distributed consensus mechanisms, offers a promising solution for enhancing the security and accountability of remote health monitoring systems.

V OBJECTIVES

1. To ensure the **integrity, confidentiality, and privacy** of patient health records within remote monitoring environments.
2. To overcome the issue of **data interoperability** by enabling secure and standardized sharing of medical records across different healthcare institutions.
3. To eliminate **information asymmetry**, thereby empowering patients with improved visibility and control over their personal health information.

VI PROPOSED SYSTEM

The proposed system introduces a blockchain-based framework to enhance the security, transparency, and reliability of remote health monitoring systems. By leveraging blockchain technology, the system creates a decentralized and tamper-proof ledger that records every access or modification of patient data as an immutable transaction. This ensures that once a log entry is created, it cannot be altered or deleted, thereby safeguarding the integrity of electronic health records (EHRs) against internal threats such as malicious insiders.

Through the integration of blockchain's distributed ledger, real-time auditing becomes feasible, allowing stakeholders to verify and trace every interaction with patient data in a secure and transparent manner. Smart contracts further strengthen the system by enforcing automated, fine-grained access controls, enabling secure sharing of health records between patients and authorized entities such as hospitals, pharmacies, and healthcare providers. By embedding these contracts into the blockchain, the system ensures that data access policies are consistently applied and verifiable, ultimately building a trust-based healthcare environment.

This blockchain-enabled approach not only enhances data security but also addresses key issues such as unauthorized data manipulation,

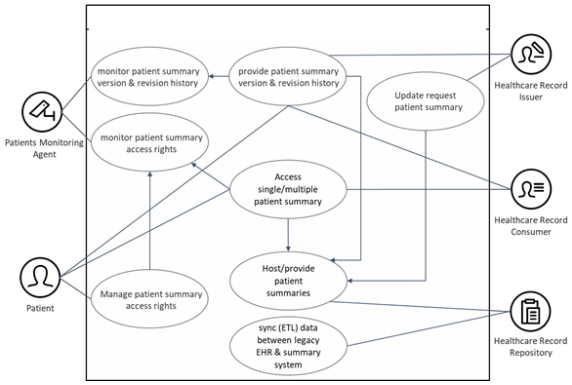
ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

lack of traceability, and inefficient auditing—problems commonly found in centralized healthcare systems.

Advantages

1. **Enhanced Data Integrity**: The immutability of blockchain ensures that once an access or modification log is recorded, it remains permanent and cannot be altered, thereby preserving the authenticity and integrity of sensitive health data.
2. **Decentralization of Logs**: By distributing log storage across the blockchain network, the system eliminates the vulnerabilities associated with centralized databases, significantly reducing the risk of insider tampering or system-wide data breaches.
3. **Increased Accountability**: Every transaction on the blockchain is recorded with a precise timestamp and user identity, allowing for full traceability of actions. This ensures that all stakeholders can be held accountable for their interactions with patient data, thereby fostering transparency and trust in the system.

VII SYSTEM ARCHITECTURE



VIII IMPLEMENTATION

1. Blockchain Integration for Secure Logging: A permissioned private blockchain is deployed and integrated with the Cloud Access Security Broker (CASB) to securely log all actions performed on patient health data. The blockchain's inherent immutability guarantees that once a log entry is recorded, it cannot be modified or erased—even by privileged insiders. This continuous logging mechanism captures data access events in real-time, providing an up-to-date and tamper-proof audit trail that reflects every interaction with sensitive health records.

2. Patient Access and Monitoring: Patients are provided with the capability to query the blockchain ledger directly to monitor how their data is being accessed and by whom. This transparency empowers patients to stay informed and exercise greater control over their personal health information. The system is also configured to send alerts to patients if their data is accessed by administrators or moved beyond authorized cloud storage environments, thereby enabling timely detection of potential security breaches.

3. Enhanced Security Against Insider Attacks: By leveraging the blockchain to store audit logs, the system ensures that insiders with privileged access cannot tamper with or delete log records. This tamper-proof logging preserves the integrity of the audit trail and reinforces accountability within the healthcare ecosystem.

4. Data Access by Entering a Secret Key: Access to the sensitive data stored on the blockchain is protected by a secret keyword or key. Only users who enter the correct key are granted access to the storage server and the underlying data, ensuring that unauthorized parties cannot retrieve or manipulate patient health records.

IX RESULTS

The proposed blockchain-based remote health monitoring system successfully demonstrates enhanced security, transparency, and accountability in managing patient health records. The integration of a permissioned private blockchain with CASB ensured real-time, immutable logging of all data access events. Patient empowerment was achieved through queryable audit logs and timely alerts, providing greater visibility into data usage. The system effectively prevented tampering and deletion of audit logs by insiders, significantly improving the integrity of the healthcare data management process. Moreover, the secret key access mechanism reinforced confidentiality and restricted unauthorized data retrieval. Overall, the system addressed the critical limitations of centralized logging, improved interoperability, and fostered trust between patients and healthcare providers.

X CONCLUSION

a secure and efficient blockchain-based framework for logging and managing patient health records in remote health monitoring systems. By decentralizing audit logs on a private blockchain, the system mitigates risks posed by malicious insiders and centralized failures, ensuring data integrity and traceability. Patient-centric features, such as transparent data querying and alert notifications, enhance control over sensitive information and reduce information asymmetry. The use of smart contracts further strengthens access control mechanisms, enabling secure and interoperable sharing of electronic health records among healthcare stakeholders. Future work may focus on optimizing scalability and integrating advanced cryptographic techniques to further enhance privacy and performance in large-scale deployments.

REFERENCES

1. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. Ahmed, M., et al., “BCALS: Blockchain-based Audit Log Security for Cloud Environments,” *IEEE Access*, 2020.
3. ObserveIT, “Insider Threat Report,” 2020.
4. Kumar, R., et al., “Blockchain-Enabled Secure Healthcare System for Insider

Threat Prevention," *Journal of Medical Systems*, 2021.

5. Sengupta, A., "Biometric Authentication in IoT-based Healthcare Systems," *International Journal of Medical Informatics*, 2020.
6. Zhao, L., et al., "Blockchain-Based Hierarchical Processing for IoT Data Security," *IEEE Internet of Things Journal*, 2021.
7. Ma, Y., et al., "Hybrid CASB and Blockchain Models for Enhanced Cloud Security," *Computers & Security*, 2022.
8. Bitglass, "Cloud Access Security Broker (CASB) Solutions Overview," 2021.
9. Lookout, "CASB Security Framework for Cloud Data Protection," 2021.
10. Christidis, K., Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, 2016.
11. Kuo, T.T., et al., "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications," *Journal of the American Medical Informatics Association*, 2017.
12. Zhang, P., et al., "Blockchain Technology Use Cases in Healthcare," *Advances in Computers*, 2020.