WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Patient-Centric Data Security: A Blockchain and CASB Approach for Remote Healthcare

Anneboina Krishna[1], *Nandelly Rahul*[2], *Himaja Nounuri*[3], *Kesaboina Sravan Kumar*[4], *Kondaparthy Tharun*[5]

[1]Asst Professor, Computer Science and Engineering (IOT) Guru Nanak Institutions, Technical Campus Telangana, India
[2,3,4,5] Computer Science and Engineering (IOT) Guru Nanak Institutions Technical Campus Telangana, India
[2]rahulchowdary82215@gmail.com, [3]nounurihimaja@gmail.com, [4] kesaboinasravan@gmail.com

DOI : https://doi.org/10.55248/gengpi.6.0625.2124

ABSTRACT

Remote healthcare monitoring, powered by IoT devices, offers vital support to patients unable to access clinical environments regularly. However, safeguarding the integrity and confidentiality of health data remains a critical challenge—especially against insider threats. Unlike external attackers, malicious insiders often have privileged access, enabling them to manipulate, erase, or exploit patient records without detection. Conventional audit logs stored in centralized cloud systems are insufficient, as they can also be tampered with by those same insiders. This research presents a novel solution that integrates a Cloud Access Security Broker (CASB) with a private blockchain network to create an immutable and transparent log management system. Every interaction with patient data—whether initiated by users or administrators—is recorded in a tamper-proof blockchain ledger accessible to patients through a secure interface. This design empowers data owners with visibility into how their data is used, while preventing unauthorized changes to logs. The implemented system consists of a web platform for health data collection, a CASB for secure access control and cloud storage, and a permissioned blockchain for real-time action logging. Performance and security evaluations confirm the system's resilience, low latency under load, and ability to deter insider attacks through cryptographic accountability. This architecture lays the foundation for trust-centric remote healthcare systems where patient data security is verifiable, enforceable, and decentralized.

Keywords Remote Health Monitoring, Insider Threat Detection, Blockchain Logging, Cloud Access Security Broker (CASB), Health Data Security, Immutable Audit Trail, IoT Healthcare Systems, Private Blockchain, Data Integrity, Patient-Centric Security

I. Introduction

The growing reliance on digital healthcare technologies, particularly remote monitoring systems enabled by IoT devices, is reshaping how patients receive medical attention. These systems are especially valuable for individuals with chronic conditions, limited mobility, or those who avoid hospital visits due to personal or public health concerns. By continuously collecting and transmitting biometric data—such as heart rate, blood pressure, or glucose levels—these platforms enable remote consultations and real-time medical decision-making.

However, the highly sensitive nature of health data demands robust security mechanisms that go beyond traditional confidentiality, integrity, and availability (CIA) principles. While current solutions focus on securing data during transmission or storage, one critical vulnerability persists: insider threats. Administrators and privileged users, who often have unrestricted access to both patient data and system logs, can exploit this access for unauthorized actions. These actions—ranging from data tampering to unauthorized disclosure—can occur without triggering alarms, especially if audit logs are also under their control.

Despite the deployment of advanced access control frameworks like Cloud Access Security Brokers (CASBs), most systems remain vulnerable to such internal threats. CASBs may monitor access and enforce encryption, but without tamper-proof logging, malicious insiders can erase or manipulate records to cover their tracks. Real-world incidents have demonstrated that insider-driven breaches can result in reputational damage, legal consequences, and loss of patient trust.

In response to this growing risk, this study proposes a secure architecture that integrates a CASB with a private blockchain network. The blockchain ensures that every data access event is recorded in a decentralized, immutable ledger. Unlike conventional systems, these logs cannot be modified or deleted—even by system administrators. Moreover, patients gain direct visibility into their data access history, promoting transparency and accountability.

This hybrid approach not only deters insider attacks but also enhances compliance with data protection standards by ensuring verifiable auditability. The system is practically implemented as a web application with integrated blockchain logging, evaluated under varying operational loads to validate both its performance and security robustness.

In the evolving landscape of digital healthcare, remote patient monitoring systems powered by IoT devices have become indispensable. These platforms enable the continuous collection and sharing of patient health metrics with medical professionals, facilitating timely interventions and improving outcomes. However, as the reliance on cloud infrastructure and remote data access grows, so too does the risk to the privacy, integrity, and security of sensitive health information.

While traditional security models focus on protecting data from external threats using encryption, access control, and authentication mechanisms, they often overlook a more dangerous and insidious risk—**insider threats**. Administrators and privileged users, by virtue of their roles, possess extensive access rights and deep knowledge of the system's architecture. This privileged access allows them not only to view or manipulate sensitive patient data but also to alter or delete audit trails that could otherwise reveal malicious activity.

Existing audit systems typically store logs in centralized or semi-centralized repositories. These can be modified or purged by insiders, leaving no evidence of unauthorized access or data tampering. Even advanced solutions such as Cloud Access Security Brokers (CASBs), while capable of enforcing access policies, still suffer from this vulnerability when their logging mechanisms are not independently verifiable or tamper-resistant.

This creates a critical gap in the current healthcare cybersecurity infrastructure: the **inability to guarantee the immutability, transparency, and auditability of data access records**, especially in the face of internal misuse. As a result, patients remain unaware of unauthorized interactions with their data, regulatory compliance is weakened, and system trustworthiness is compromised.

Addressing this issue requires a paradigm shift in how audit logs are generated, stored, and accessed. There is an urgent need for a decentralized, tamper-proof logging mechanism that operates independently of system administrators and provides real-time visibility to data owners. Such a solution must not only detect and deter insider threats but also scale effectively across healthcare environments with high user concurrency and large volumes of data transactions.

The primary aim of this research is to design and implement a robust, blockchain-enhanced logging system integrated with a Cloud Access Security Broker (CASB) to mitigate insider threats in remote health monitoring environments. This system focuses on ensuring the immutability, visibility, and verifiability of all data access events, thereby protecting patient information from unauthorized internal misuse.

The specific objectives of this research are as follows:

To design a secure architecture that integrates a CASB with a permissioned blockchain network to log all actions performed on patient health records in a tamper-proof and decentralized manner.

To ensure data transparency and traceability by allowing patients and authorized parties to monitor access patterns to their health information using blockchain-based tracking IDs.

To prevent log manipulation by administrators or insiders by eliminating centralized storage of audit trails, thereby enhancing log immutability through distributed consensus.

To implement a real-time logging mechanism that captures every critical data interaction—such as viewing, uploading, modifying, or deleting patient data—and immutably stores it on the blockchain ledger.

To evaluate the performance and scalability of the system under varying user loads and transaction volumes, ensuring low-latency operation without compromising security.

To develop a patient-accessible interface for reviewing blockchain-logged actions, thereby increasing user trust and system accountability.

II. LITERATURE REVIEW

The rapid growth of IoT-powered remote health monitoring systems has introduced significant advancements in patient care, especially for those with restricted mobility. These systems allow continuous collection and transmission of physiological data to healthcare providers, facilitating timely diagnosis and intervention. However, due to the sensitive nature of medical data, securing these systems from insider threats remains a critical concern.

To address data tampering and unauthorized access by privileged users, researchers have explored various blockchain-based logging and access control mechanisms. Blockchain's inherent properties—immutability, decentralization, and transparency—make it a promising candidate for safeguarding audit logs against manipulation.

Nakamoto's introduction of Bitcoin in 2008 marked the beginning of blockchain as a decentralized ledger for digital transactions. Since then, its utility has extended beyond cryptocurrencies, notably into healthcare data security, owing to its immutable and verifiable record-keeping capabilities.

Kumar et al. proposed a healthcare data framework where encrypted patient information is stored on the cloud while its hash is secured on a permissioned blockchain. This model ensured controlled access but still depended on off-chain components, limiting the immutability guarantees of the system. Similarly, Sahai et al. developed the "Verity" framework, embedding cryptographic hashes of SQL operations into a blockchain to detect tampering. While effective for traditional databases, it lacked direct integration with IoT-driven health monitoring.

In the domain of supply chain transparency, Cueva-Sanchez et al. implemented a cloud-based blockchain for forestry data integrity. Although the context differs, the underlying concept of immutable audit trails is directly applicable to healthcare. Zieglmeier et al. proposed a pseudonym-based system where metadata is anchored to a blockchain, but sensitive data remains off-chain—posing challenges in re-identification and audit completeness.

Adlam et al. leveraged Hyperledger Fabric alongside zero-knowledge proofs to protect electronic health record logs. Despite offering enhanced privacy, this approach relied on multichain configurations and off-chain data anchoring, which can weaken overall system transparency. Ma et al. addressed log indexing efficiency within blockchain systems but similarly used a hybrid approach that compromised full-chain immutability.

Researchers like Chistiakov introduced Directed Acyclic Graph (DAG)-based blockchain structures to enhance timestamping and concurrency in logging. While innovative, DAG architectures add complexity and demand synchronized operation—factors that may hinder real-time health monitoring systems. Rakib et al. proposed a blockchain framework emphasizing query and audit capabilities, though their design still revolved around public blockchains and lacked patient-driven access transparency.

Another notable contribution comes from Zhao et al., who tackled blockchain throughput limitations via hierarchical processing layers. Hsu et al. built an autonomous log management system combining access control and blockchain, but both approaches depended on the Proof of Work (PoW) consensus—impractical for healthcare due to high energy and computational demands.

Ahmed et al. designed BCALS, a blockchain-based audit logging framework ensuring immutability and decentralization. However, the system employed a Proof-of-Concept consensus, which, while functional in testing, is unsuitable for production environments. Mendon et al. introduced an audit chain using Proof of Existence (PoE), wherein only file hashes were stored on-chain, again relying on off-chain storage that weakens verifiability.

Jadidi et al. integrated blockchain logging with anomaly detection for industrial systems using Byzantine Fault Tolerance and proof of capacity. While their model emphasized anomaly detection, the chosen consensus algorithm suffers from scalability limitations and is vulnerable to Sybil attacks. Yenugunti et al. introduced a trust-score-based consensus to identify malicious insiders, assigning scores from 1 to 100 based on node behavior. Although novel, this model struggles with trust inaccuracies in dynamic environments.

Klinkmüller et al. offered a lightweight Ethereum-based logging solution using cost-optimized smart contracts. However, they stored logs in cloud-hosted JSON files, risking tampering and reducing system integrity. Tuan et al. and Lu et al. extended the discussion by incorporating encryption techniques such as Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and homomorphic encryption into blockchain log management. While this enhanced data confidentiality, they also introduced computational overhead and complexity in access.

Upon examining these studies, several limitations emerge. Many solutions use **off-chain storage**, which undermines the fundamental goal of **immutability**. Others depend on **multichain or PoW-based architectures**, making them resource-intensive and unsuitable for scalable, low-latency healthcare systems. Moreover, **real-time patient visibility and traceability of data access** remain under-addressed, and **smart contract automation** is often missing in off-chain hybrid systems.

In light of these gaps, this research proposes a blockchain-anchored CASB framework that:

- Ensures tamper-proof, on-chain logging of user actions,
- Enables patients to track and audit access to their health records,
- Avoids off-chain dependency by committing all essential audit data directly to a permissioned blockchain,
- Utilizes lightweight consensus mechanisms suitable for healthcare-grade scalability.

III. METHODOLOGY

Our proposed solution is built on the necessary background technologies and related concepts described in this section. Cloud access security broker and block chain are two technologies we cover here.

A. BLOCKCHAIN

Blockchain is a powerful decentralized and distributed ledger that meticulously records transactions or data within its blocks. The most renowned application of this groundbreaking technology is Bitcoin, introduced by Satoshi Nakamoto in 2008. Its robust security is ensured through a cryptographic hash function that links each block to the previous one, maintaining data integrity and authenticity via hash chaining. This process involves hashing a block with a cryptographic hash function and appending the resulting hash to the next block. Importantly, new blocks are strictly added to the end of the blockchain—never at the centre or beginning. The genesis block stands as the initial block without a preceding hash value; however, every subsequent block's header includes critical information such as its number, previous block's hash, NCE value, total transaction count, and transaction hashes within it. In Bitcoin's network, blocks undergo rigorous verification through mining—a process demanding complex mathematical problem-solving and adherence to consensus rules for validating transactions and headers. Once recorded on the blockchain, data remains immutable—unalterable and indelible—underscoring blockchain's unrivalled reliability in safeguarding information.

B. CLOUD ACCESS SECURITY BROKER (CASB)

This paper, we propose a Cloud Access Security Broker (CASB) model that (a) logs every action performed on user data and (b) secures those logs by placing them in a private by the data owners (i.e., patients). Patients can query the blockchain, track their data's movement, and be alerted if their data has been accessed by an administrator or moved outside the cloud storage. In this work, we practically implement a web application that receives health data from patients, a CASB that securely stores the records in the cloud, and integrate a private blockchain that immediately logs all actions happening in the backend of the web application and CASB.

We evaluate the system's security and performance under varying numbers of patients and actions. The advantages from the proposed technology are (a) Faster transaction processing and lower costs due to reduced computational requirements. (b) Organizations maintain control over who can participate and how the network operates. (c) Better suited for scenarios where sensitive data needs to be protected from public view. So in this section let us discuss in detail regarding the background technologies that are being used, here mainly we are using two technologies, they are as follows

IV. RESULT

This section presents a detailed evaluation of the proposed blockchain-based logging system integrated with a Cloud Access Security Broker (CASB) for remote health monitoring. The results focus on validating system security, performance, and resilience against insider threats. Evaluations were conducted using a testbed simulating real-world hospital scenarios with varying numbers of patients, healthcare providers, and administrative users. Metrics are reported across five domains: system setup, functional correctness, logging integrity, insider threat detection, and system performance under different loads.

FUNCTIONAL VERIFICATION AND SCENARIO-BASED TESTING

To validate core functionality, the system was tested using real-world use cases:

- Patient registration and login
- Doctor assignment and appointment scheduling
- Medical report uploads
- Real-time doctor-patient consultation (via live message module)
- Prescription issuance and viewing
- Log queries from patient, doctor, or administrator dashboard

In each of these scenarios, the corresponding actions were hashed and committed to the blockchain log layer. Every event was accompanied by a timestamp, user ID, and action type. The logs were verified via blockchain queries and compared with expected values to ensure consistency.

LOGGING INTEGRITY AND TAMPER RESISTANCE

A core aspect of the system is its resistance to tampering—especially important in scenarios involving insider threats. Comparative experiments were conducted with two systems:

1. Traditional centralized SQL-based log storage
2. Proposed Ethereum-based blockchain log storage

The SQL system allowed logs to be accessed and edited directly via root access, demonstrating vulnerability. In contrast, the blockchain-based approach rendered logs immutable. Any attempt to modify even a single character in a transaction's metadata resulted in the entire chain hash invalidation, highlighting its tamper-proof nature.

Attempted Tampering	**SQL System Result**	**Blockchain Result**
Deleting login entries	Succeeded	Impossible
Changing timestamps	Succeeded	Block mismatch error
Falsifying doctor actions	Undetected	Transaction mismatch

Blockchain logs remained immutable with 100% success across all stress scenarios.

INSIDER THREAT SIMULATION AND DETECTION

We introduced controlled insider attack scenarios to evaluate the detection efficacy. These included:

- An administrator accessing patient records without patient request
- A doctor issuing a prescription without prior consultation

- Deletion of audit logs after unauthorized access

The CASB flagged these anomalies by cross-verifying access triggers. For example, any access not initiated by a patient or an assigned care flow was flagged. The blockchain audit trail allowed reverse querying to validate whether the chain of events complied with policy.

Attack Type	Detection Accuracy	Time to Detection
Unauthorized Data Access	100%	1.5 sec
Fake Prescription Entry	98.7%	2.1 sec
Log Deletion Attempt (SQL only)	0%	N/A
Blockchain Log Mismatch	100%	Instant

Notably, the system also allows patients to query their data logs and receive real-time alerts via blockchain-backed tracking IDs, thus placing log ownership in the user's hands.

PERFORMANCE METRICS

Performance testing was conducted under varying system load conditions, simulating simultaneous logins, report uploads, and data queries from users. Key metrics collected include blockchain transaction latency, CASB policy enforcement delay, and overall system response time.

Blockchain Logging Latency

Transaction latency remained under 1 second for up to 100 concurrent users and scaled linearly beyond that.

Users	Avg. Log Commit Time (ms)
10	180
50	320
100	620
200	980

CASB Processing Time

The CASB layer, which acts as an intelligent middleware, introduced negligible delay (~180ms average), while ensuring access rules were strictly enforced. Dynamic access control validation (e.g., patient-approved access) remained performant even with 200+ concurrent sessions.

End-to-End Response Time

The complete workflow from patient login → report upload → doctor access → log query was benchmarked.

Process	Avg. Response Time (ms)
Login Authentication	240
Upload Report	430
Doctor Record Access	360
Blockchain Log Query (By Patient)	500
Blockchain Log Query (By Admin)	480

System remained responsive under concurrent multi-user stress scenarios, confirming scalability and practical feasibility.

COMPARATIVE ANALYSIS

The proposed system was evaluated against existing solutions from literature:

Feature	Traditional System	Biometric IoT Model [1]	Proposed System
Tamper-Proof Logging	✗	✗	☑
Patient-Centric Log Access	✗	☑	☑
Real-Time Threat Detection	✗	✗	☑
Smart Access Mediation (CASB)	✗	✗	☑

Integration with Health Workflow	✗	☑	☑

The proposed model uniquely combines blockchain and CASB, addressing the core problem of insider data misuse with real-time logging, tamper-proof tracking, and auditable transparency.

Finally the proposed blockchain-integrated CASB system was rigorously evaluated and demonstrated strong performance across security, functionality, and scalability dimensions. The blockchain layer ensured 100% tamper-proof logging, outperforming traditional SQL-based systems. Simulated insider attacks were accurately detected with minimal latency, while access actions were transparently auditable by patients. Performance testing showed acceptable latency under high user loads, confirming the system's scalability for real-world healthcare environments. Overall, the results validate the solution's effectiveness in securing remote health data against malicious insiders while maintaining efficient and user-friendly operation.

REFERENCES

[1] S. Sengupta, ''A secured biometric-based authentication scheme in IoTbased patient monitoring system,'' in Emerging Technology in Modelling and Graphics, 2020, pp. 501–518.

[2] J. Sun, X. Yao, S. Wang, and Y. Wu, ''Blockchain-based secure storage and access scheme for electronic medical records in IPFS,'' IEEE Access, vol. 8, pp. 59389–59401, 2020.

[3] (2022). Bitglass CASB. [Online]. Available: https://www.bitglass. com/casb-cloud-access-security-broker

[4] (2022). Lookout CASB. [Online]. Available: https://www.lookout. com/products/casb-cloud-access-security-broker

[5] Cisco Cloudlock. https://www.cisco.com/c/en/us/products/security/ cloudlock/index.html

[6] Microsoft Cloud App Security. https://www.microsoft.com/enus/ security/business/siem-and-xdr/microsoft-defender-cloud-apps

[7] Cloud-Access-Security-Broker-CASB. [Online]. Available: https://www. techtarget.com/searchcloudcomputing/definition/cloud-access-securitybroker- CASB

[8] Casb. [Online]. Available: https://www.proofpoint.com/us/threatreference/ casb/

[9] ObserverIT Cost of Insider Threats Global Report 2020. [Online]. Available: https://www.proofpoint.com/us/products/informationprotection/ insider-threat-management

[10] The Colombia University Researchers Perform Survey in 2019. [Online]. Available: https://delinea.com/blog/insider-threats-in-cyber-security

[11] Real world Insider Attack Example. [Online]. Available: https://www.tessian.com/blog/insider-threats-types-and-real-worldexamples/

[12] Insider Threats at Hospitals. https://resources.infosecinstitute.com/topic/ insider-threats-at-hospitals/

[13] H. Halpin and M. Piekarska, ''Introduction to security and privacy on the blockchain,'' in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Apr. 2017, pp. 1–3.

[14] T. Yu, Z. Lin, and Q. Tang, ''Blockchain: The introduction and its application in financial accounting,'' J. Corporate Accounting Finance, vol. 29, no. 4, pp. 37–47, Oct. 2018.

[15] P. Gomber, Hinz-O. Nofer M. Schiereck D.,'Blockchain, vol. 59. Cham, Switzerland: Springer, 2017, pp. 183–187.

[16] M. Cinque, D. Cotroneo, and A. Pecchia, ''Event logs for the analysis of software failures: A rule-based approach,'' IEEE Trans. Softw. Eng., vol. 39, no. 6, pp. 806–821, Jun. 2013.

[17] S. Nakamoto, ''Bitcoin: A peer-to-peer electronic cash system,'' in Decentralized Business Review, 2008.

[18] F. Casino, T. K. Dasaklis, and C. Patsakis, ''A systematic literature review of blockchain-based applications: Current status, classification and open issues,'' Telematics Informat., vol. 36, pp. 55–81, Mar. 2019.

[19] T.-V.-L. T.-V. Le and C.-L.-H. T.-V. Le, ''A systematic literature review of blockchain technology: Security properties, applications and challenges,'' J. Internet Technol., vol. 22, no. 4, pp. 789–801, Jul. 2021.

[20] M. S. Kumar and V. Nagalakshmi, ''Secure transfer of robust healthcare data using blockchain-based privacy,'' Cluster Comput., pp. 1–17, May 2023.

[21] S. Sahai, M. Atre, S. Sharma, R. Gupta, and S. K. Shukla, ''Verity: Blockchain based framework to detect insider attacks in DBMS,'' in Proc. IEEE Int. Conf. Blockchain (Blockchain), Nov. 2020, pp. 26–35.

[22] J. J. Cueva-Sánchez, A. J. Coyco-Ordemar, andW. Ugarte, ''A blockchainbased technological solution to ensure data transparency of the wood supply chain,'' in Proc. IEEE ANDESCON, Oct. 2020, pp. 1–6.

[23] V. Zieglmeier and G. L. Daiqui, ‘‘GDPR-compliant use of blockchain for secure usage logs,’’ in Evaluation and Assessment in Software Engineering, 2021, pp. 313–320.

[24] R. Adlam and B. Haskins, ‘‘A permissioned blockchain approach to electronic health record audit logs,’’ in Proc. 2nd Int. Conf. Intell. Innov. Comput. Appl., Sep. 2020, pp. p1–7.

[25] S. Ma, Y. Cao, and L. Xiong, ‘‘Efficient logging and querying for blockchain-based cross-site genomic dataset access audit,’’ BMC Med. Genomics, vol. 13, no. S7, pp. 1–13, Jul. 2020.

[26] S. Akbar, S. Khan, F. Ali, M. Hayat, M. Qasim, and S. Gul, ‘‘IHBPDeepPSSM: Identifying hormone binding proteins using PsePSSM based evolutionary features and deep learning approach,’’ Chemometric Intell. Lab. Syst., vol. 204, Sep. 2020, Art. no. 104103.

[27] J. Eberhardt and J. Heiss, ‘‘Off-chaining models and approaches to off-chain computations,’’ in Proc. 2ndWorkshop Scalable Resilient Infrastructures Distrib. Ledgers, Dec. 2018, pp. p7–12.

[28] A. Ismailisufi, T. Popovic, N. Gligoric, S. Radonjic, and S. Šandi, ‘‘A private blockchain implementation using multichain open source platform,’’ in Proc. 24th Int. Conf. Inf. Technol. (IT), Feb. 2020, pp. 1–4.

[29] Y. Madhwal, I. Chistiakov, and Y. Yanovich, ‘‘Logging multi-component supply chain production in blockchain,’’ in Proc. 4th Int. Conf. Comput. Manage. Bus., Jan. 2021, pp. 83–88.

[30] M. H. Rakib, S. Hossain, M. Jahan, and U. Kabir, ‘‘Towards blockchaindriven network log management system,’’ in Proc. IEEE 8th Int. Conf. Smart City Informatization (iSCI), Dec. 2020, pp. 73–80.

[31] W. Zhao, S.Yang, and X. Luo, ‘‘Secure hierarchical processing and logging of sensing data and IoT events with blockchain,’’ in Proc. The 2nd Int. Conf. Blockchain Technol., Mar. 2020, pp. p52–56.

[32] C.-L. Hsu, W.-X. Chen, and T.-V. Le, ‘‘An autonomous log storage management protocol with blockchain mechanism and access control for the Internet of Things,’’ Sensors, vol. 20, no. 22, p. 6471, Nov. 2020.

[33] N. Shi, ‘‘A new proof-of-work mechanism for bitcoin,’’ Financial Innov., vol. 2, no. 1, pp. 1–8, Dec. 2016.