International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 1-17

https://doi.org/10.70917/ijcisim-2026-1999
Article

A Blockchain-Enabled Secure Framework for Electronic Health Records Sharing: Architecture, Implementation, and Performance Evaluation

Anuja S. Hodage[1], Sudhir N. Dhage[2]

[1] Department of Computer Engineering, Atharva College of Engineering, Mumbai, Maharashtra, India. anuja.hodage23@spit.ac.in
[2] Department of Computer Engineering, Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology (SPIT), Munshi Nagar, Andheri (West), Mumbai, Maharashtra, India. sudhir_dhage@spit.ac.in

Abstract: The widespread digitization of contemporary healthcare infrastructure has catalyzed an unprecedented transition toward electronically managed patient data, fundamentally reshaping the operational landscape of medical institutions. While Electronic Health Record (EHR) systems have substantially improved clinical efficiency, care coordination, and administrative responsiveness, the prevailing reliance on centralized data management architectures introduces critical vulnerabilities, including unauthorized intrusion, systemic data corruption, catastrophic single-point failures, and persistent privacy breaches that compromise confidential patient information. Equally pressing is the challenge of enabling reliable, auditable, and consent-governed information exchange across disparate healthcare organizations engaged in collaborative diagnosis, translational research, and longitudinal patient care. In response to these deeply entrenched challenges, the present study introduces a comprehensive, permissioned blockchain-based framework specifically engineered for the secure and interoperable sharing of EHR data. The proposed system integrates off-chain encrypted record storage with on-chain metadata management, deploys smart contract-driven access control mechanisms, and enforces accountability through immutable audit logging. Patient-centric data governance is realized through a dynamic permission model that allows granular control over granting, monitoring, and revocating access to personal health records. Data authenticity and non-repudiation are maintained through cryptographic digital signatures and deterministic hash verification, while smart contracts automate compliance enforcement aligned with established data protection standards such as HIPAA and GDPR. The architecture employs lightweight consensus protocols and indexed retrieval strategies that significantly reduce latency without compromising security guarantees. Empirical evaluation against three benchmark systems reveals that the proposed framework achieves superior performance across twelve quantitative dimensions, including authentication accuracy (97.8%), transaction throughput (104 TPS), hash verification success (99.5%), and attack detection efficacy (96.7%). The study confirms that blockchain-enabled decentralization, when combined with hybrid storage and cryptographic controls, offers a transformative and scalable approach to the pressing interoperability and security deficits of modern healthcare data ecosystems.

Keywords: Blockchain Technology, Electronic Health Records, Cryptographic Access Control, Smart Contracts, Healthcare Interoperability, Data Integrity, Distributed Consensus, Off-Chain Storage, HIPAA Compliance, Permissioned Ledger

1. Introduction

The globalization of healthcare delivery, coupled with rapid digitization across clinical and administrative domains, has propelled the Electronic Health Record (EHR) from a supplementary management tool to the foundational infrastructure of modern medical institutions. EHR platforms have transformed patient engagement, streamlined clinical workflows, enabled population-level health analytics, and laid the groundwork for evidence-based practice. However, alongside these benefits, the concentration of sensitive health data within centralized digital repositories has created an expanding threat surface. Security incidents involving medical data have grown in both frequency and severity, with healthcare ranking among the most breach-prone sectors globally. The

consequences extend beyond financial liability, encompassing patient safety risks arising from corrupted or inaccessible records, erosion of institutional trust, and long-term reputational damage.

The limitations of centralized EHR architectures are multidimensional. First, single points of failure make them particularly susceptible to ransomware, distributed denial-of-service (DDoS) attacks, and insider threats. Second, inter-institutional data exchange remains technically fragmented and legally complex, impeding collaborative care and multi-site clinical research. Third, patients have historically exercised little meaningful agency over their own health data, with access and sharing decisions made primarily by institutions rather than individuals. Fourth, audit trails in conventional systems are often insufficiently granular or tamper-prone, undermining regulatory compliance and forensic accountability.

Blockchain technology has emerged as a compelling solution to these compounded challenges, offering decentralized data management, cryptographic integrity assurance, transparent transaction history, and programmable governance through smart contracts. Originally conceived for financial applications, blockchain's architectural properties—immutability, consensus-based validation, distributed ledger maintenance, and pseudonymous identity management—translate with considerable efficacy into healthcare information systems. The elimination of a central governing authority reduces the attack surface, while smart contracts automate complex, multi-party workflows without requiring intermediary trust.

This study presents the design, formalization, and empirical evaluation of a blockchain-based EHR sharing framework that synthesizes the security advantages of distributed ledger technology with the performance requirements of real-world clinical environments. The system addresses five core functional domains: identity initialization and cryptographic authentication, smart contract-mediated access governance, decentralized consensus enforcement, off-chain encrypted record management, and tamper-evident audit logging. The mathematical underpinning of each module is formally specified, and the system's performance is rigorously benchmarked against ProChain [17], Smart Health [8], and Privacy-Conflict [6] frameworks.

The remainder of this paper is structured as follows. Section 2 provides a comprehensive literature review encompassing blockchain adoption in healthcare, access control innovations, supply chain applications, and governance challenges. Section 3 details the proposed system's research methodology, architecture, and mathematical formalization. Section 4 presents the experimental results and comparative analysis. Section 5 concludes with implications for healthcare IT infrastructure and directions for future investigation.

2. Literature Review

This section provides a structured synthesis of existing scholarship on blockchain technology across healthcare information management, data access control, supply chain transparency, and governance innovation. The reviewed literature encompasses theoretical frameworks, empirical evaluations, and comparative system analyses, collectively establishing the intellectual foundation and contextual motivation for the proposed research.

2.1 Blockchain and Digital Transformation in Healthcare

The integration of disruptive digital technologies—including artificial intelligence, the Internet of Things, cloud computing, and distributed ledger systems—has initiated a far-reaching transformation of healthcare delivery models globally. Among these, blockchain technology stands out for its capacity to furnish decentralized, tamper-resistant, and transparently auditable data management infrastructures. Hasselgren et al. [1] conducted a foundational scoping review of blockchain applications in health and biomedical science, systematically cataloguing its deployment across clinical record management, pharmaceutical supply chains, biomedical research, and health service monitoring. Their analysis established that blockchain's decentralization properties substantially enhance data traceability and institutional control, representing a paradigmatic departure from legacy database architectures that rely on centralized trust hierarchies.

Building upon this foundational characterization, Dubovitskaya et al. [2] examined multiple blockchain architectural configurations for healthcare data governance, advocating for a layered design wherein distributed ledgers serve primarily as mechanisms for access verification and metadata management rather than bulk data storage. This distinction is critical: the volumetric and sensitivity constraints of clinical records render direct on-chain storage computationally and economically impractical. Their multi-layer model anticipates the hybrid architecture proposed in the present study. Complementing this architectural perspective, Saeed et al. [3] conducted a systematic review that delineated blockchain's operational utility across identity management, supply chain traceability, cross-institutional interoperability, and informed consent governance. Their findings, while affirming

blockchain's transformative potential, identified pervasive shortcomings in existing designs, including insufficient real-world usability testing, absence of longitudinal stability assessments, inadequate regulatory grounding, scalability deficits, and consensus mechanism inefficiencies that collectively constrain clinical deployment.

Dionisio et al. [4] extended this analysis by framing digital transformation in healthcare not merely as a technological substitution but as a systemic organizational restructuring. They argued that blockchain should function within a broader, interconnected digital ecosystem encompassing remote care delivery, workflow automation, and data-driven decision support, with its success contingent upon alignment with institutional governance structures, stakeholder management frameworks, and evolving regulatory policy. Their perspective underscores the sociotechnical nature of blockchain adoption, where technical performance alone is insufficient to guarantee sustained healthcare integration. The long-term trajectory of blockchain in healthcare was addressed by Shine et al. [5] through expert-informed forecasting. Their projections anticipated accelerated adoption of decentralized identity infrastructure, patient-centric record systems, and smart contract-based data monetization models that empower individuals to conditionally share health information with researchers and insurers. The authors also anticipated convergence between regulatory frameworks and hybrid blockchain designs optimized for operational flexibility within compliance boundaries, situating blockchain as an emerging infrastructural cornerstone rather than a peripheral innovation. Addressing the critical challenge of multi-source health data privacy, Kormiltsyn et al. [6] introduced a conflict resolution system reconciling personal health records with institutional electronic medical records through blockchain-integrated smart contract access control. Their formally modeled architecture demonstrated that decentralized access governance substantially improves enforcement precision, mitigates data abuse risks, and bridges the interoperability gap between patient-controlled systems and institutional information infrastructures.

2.2 Blockchain-Based Access Control and Information Sharing Systems

The technical challenge of enabling secure, policy-compliant information exchange across organizationally and jurisdictionally distinct entities constitutes one of the most consequential open problems in distributed systems design. Gai et al. [7] addressed this challenge through the development of a zero-trust access control model augmented by blockchain technology for cross-organizational data sharing. Their architecture abandoned conventional perimeter-based trust assumptions in favor of continuous identity verification and immutable, blockchain-enforced access restrictions, rendering unauthorized access computationally and cryptographically intractable. This model is particularly applicable to inter-institutional healthcare collaborations where organizational boundaries preclude conventional trust delegation mechanisms. Marry et al. [8] operationalized blockchain within an IoT-integrated smart healthcare environment, combining cloud computing infrastructure, wearable sensor networks, and smart contracts to enforce integrity across encrypted health documents. Their system demonstrated real-time health monitoring capability alongside robust protection against unauthorized data access, validating the technical feasibility of blockchain deployment within resource-constrained clinical environments.

Kasyapa and Vanmathi [9] conducted a comprehensive investigation of blockchain integration challenges in healthcare, identifying data storage scalability, transaction processing latency, and operational cost management as the predominant technical barriers. Their study proposed permissioned blockchain architectures, lightweight consensus algorithms, and intelligent data compression strategies as viable mitigation pathways, contributing practically oriented guidance for advancing from academic proof-of-concept to commercially deployable healthcare systems. Within the supply chain domain, Xu et al. [10] analytically characterized the impact of information sharing on pricing equilibria in dual-channel supply networks, demonstrating that transparency enhances supply chain efficiency but exerts complex influences on competitive dynamics. Wu et al. [11] extended this analysis by examining the temporal dimension of wholesale price setting and information disclosure using game-theoretic tools, revealing that the timing and granularity of information sharing critically determine both cooperation benefits and competitive exposure. These insights are directly applicable to healthcare data exchange governance, where the sequencing and conditionality of information flows profoundly affect both clinical outcomes and institutional interests.

Wei et al. [12] developed a decentralized, blockchain-based cloud platform for automotive manufacturing supply chain coordination, demonstrating that distributed ledger architectures significantly enhance inter-enterprise collaboration while reducing data manipulation risks. Wang et al. [13] demonstrated blockchain's capacity to augment green supply chain management by enabling verifiable environmental performance data exchange among network participants, illustrating blockchain's versatility across sustainability-oriented domains. Li [14] proposed blockchain-based inventory synchronization mechanisms that address information asymmetry-induced

inefficiencies, while Ma et al. [15] investigated blockchain adoption in fresh produce supply chains, documenting improvements in traceability precision and supply chain responsiveness—attributes of significant relevance to pharmaceutical and medical supply logistics.

2.3 Blockchain in Sustainable, Industrial, and Logistics-Oriented Supply Chains

The convergence of environmental sustainability imperatives and digital transformation has stimulated significant scholarly interest in blockchain's capacity to enable traceable, accountable, and low-carbon supply chain operations. Ye et al. [16] presented one of the earliest quantitative analyses of blockchain-facilitated carbon emission coordination within supply chain partnerships, introducing a collaborative decision model that integrates environmental performance metrics directly into distributed ledger transactions. Their empirical validation demonstrated that blockchain-enabled information predictive sharing achieves measurable reductions in carbon emissions and improves inter-partner coordination, particularly in scenarios characterized by asymmetric environmental obligations across supply chain tiers. This framework offers translatable insights for healthcare networks seeking to embed sustainability accountability within their data governance architectures.

Li et al. [17] contributed the ProChain system, a cryptographic, privacy-preserving blockchain framework for product supply chain traceability that distributes verification authority across all network participants. Unlike conventional centralized traceability systems, ProChain enables proof-of-origin and proof-of-treatment verification without exposing commercially sensitive business intelligence. The system's selective disclosure architecture addresses the perennial tension between transparency and confidentiality, a challenge directly paralleled in healthcare data governance where clinical transparency must be balanced against patient privacy. ProChain's evaluation confirmed its civil accountability advantages, with direct applicability to pharmaceutical distribution and medical device logistics.

Fang and He [18] examined blockchain-enabled pricing strategy optimization within consortium blockchain environments, demonstrating that distributed ledger technology reduces informational asymmetries between supply chain partners and facilitates fairer pricing equilibria. Ding et al. [19] extended blockchain application into the construction sector through a blockchain-IPFS framework for precast construction supply chain management, addressing documentation fragmentation, information loss, and inter-party trust deficits. Their hybrid architecture—combining blockchain immutability with IPFS distributed file storage—offers a methodological template directly applicable to the hybrid storage architecture proposed in the present study for EHR management. Lau et al. [20] investigated blockchain-based messaging and data exchange infrastructure for air cargo logistics, demonstrating significant reductions in processing time, improvements in cross-border trust, and enhanced shipment tracking. Their research affirms that blockchain technology can restructure information flows across complex multi-stakeholder logistics systems, a finding with clear implications for national health information exchange architectures.

2.4 Challenges, Governance Models, and Future Research Directions

Despite the compelling theoretical and empirical evidence supporting blockchain adoption in healthcare and supply chain management, significant conceptual, technical, and institutional barriers remain. Ding et al. [19] identified legacy system integration as the primary implementation obstacle, noting that while blockchain enhances data integrity and traceability, connecting distributed ledger infrastructure to existing enterprise systems demands extensive reconfiguration and introduces functional data heterogeneity challenges. The authors recommended modular blockchain designs that accommodate incremental integration with institutional technology ecosystems as a pragmatic pathway to adoption. Lau et al. [20] similarly identified regulatory fragmentation and policy insufficiency as primary inhibitors to blockchain deployment in international logistics, noting that differing national customs and transport regulations undermine the cross-border coordination benefits that blockchain architectures theoretically enable. This governance gap highlights the necessity of collaborative regulatory frameworks that harmonize technical standards with jurisdictional compliance requirements.

Xu et al. [21] examined the economic dimensions of blockchain adoption through differential game theory, revealing that information sharing benefits are asymmetrically distributed among supply chain partners due to investment capability disparities. This adoption cost asymmetry between large and small-scale participants constitutes a fundamental inclusivity barrier that policy-driven incentive mechanisms must address. Hsiao and Sung [22] analyzed a primarily decentralized blockchain information sharing system, finding that while the absence of central authority enhances operational transparency, it simultaneously complicates accountability structures, shifting responsibility for system errors and governance failures into legal and ethical domains ill-equipped to adjudicate

distributed system liability. Their findings advocate for hybrid governance models that combine decentralized operation with clearly delineated accountability frameworks.

Luo and Pan [23] examined information sharing game theory among supply chain participants, revealing that while cooperative blockchain participation generates collective value, opportunistic information control can be leveraged to gain competitive advantage, underscoring the importance of carefully designed incentive structures. Samantray and Reddy [24], working specifically within healthcare contexts, developed a blockchain-based pharmaceutical supply chain system incorporating zero-knowledge proofs and Keccak-256 cryptographic hashing, achieving significant improvements in drug safety verification and counterfeit detection. However, their evaluation acknowledged substantial implementation complexity and computational overhead costs that resource-constrained healthcare environments must carefully manage. Kouhizadeh et al. [25] conducted a comprehensive theoretical analysis of blockchain adoption barriers in sustainable supply chains, identifying technological immaturity, organizational resistance, governance structure deficits, and absence of executive sponsorship as the dominant inhibitors, providing a structured framework for organizational readiness assessment and governance system design that directly informs the implementation strategy advanced in this study.

The cumulative insights extracted from this literature review establish several clear design imperatives for the proposed framework: the necessity of hybrid on-chain and off-chain storage architectures, the criticality of smart contract-mediated access governance, the importance of lightweight consensus mechanisms for performance optimization, the value of patient-centric data sovereignty, and the need for comprehensive audit infrastructure. These imperatives collectively motivate the architectural choices and methodological decisions articulated in the following section.

3. Research Methodology

The proposed system architecture for secure Electronic Health Record sharing via blockchain technology is organized into five functionally distinct but operationally interconnected modules. Each module addresses a specific dimension of the security and data management lifecycle, and their collective integration produces a coherent, end-to-end healthcare data governance framework. The following subsections describe the mathematical formalization of each module, providing a rigorous foundation for the system's operational guarantees.

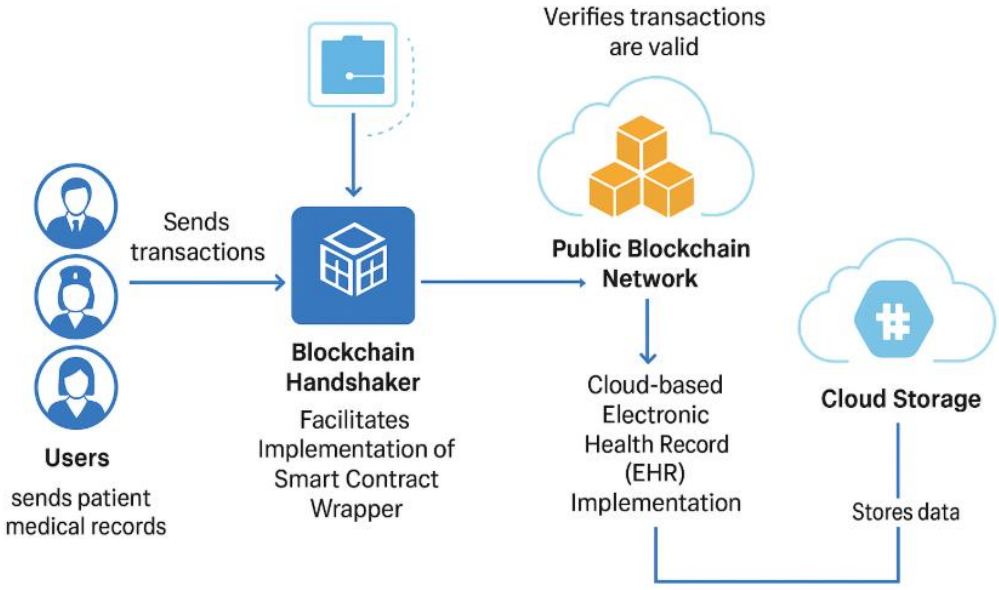

Figure 1: System Architecture illustrating the five functional modules and their interactions within the permissioned blockchain-based EHR sharing framework.

3.1 Identity Initialization and Cryptographic User Authentication

The security of any multi-participant distributed system is fundamentally predicated upon the reliable identification, authentication, and authorization of all network actors. In the proposed framework, every participant entering the healthcare blockchain network—encompassing clinical practitioners, administrative personnel, research

scientists, insurance representatives, and patients—is assigned a globally unique system identifier upon registration. The complete set of system users is formally defined as:

$$U = \{U_1, U_2, U_3, \ldots, U_n\}$$

where n represents the total number of registered participants spanning all interconnected departments, clinics, and institutions within the healthcare ecosystem. This universal participant registry forms the foundational identity layer upon which all subsequent access governance operations are predicated.

Each registered participant is assigned an asymmetric cryptographic key pair consisting of a public key and a corresponding private key:

$$K_i = (PK_i, SK_i)$$

The public key PK_i constitutes the participant's verifiable digital identity, serving as their cryptographic certificate within the network. The private key SK_i is maintained exclusively by the participant and deployed for document signing and symmetric key decryption operations, ensuring that cryptographic proofs of identity and data provenance are computationally infeasible to forge without possession of the corresponding private key.

The medical documentation associated with each system participant U_i is formally represented as a structured collection of clinical artifacts:

$$D_i = \{d_{i1}, d_{i2}, \ldots, d_{im}\}$$

This collection encompasses all health records pertaining to the individual, including clinical diagnoses, discharge summaries, pharmaceutical prescriptions, pathological laboratory reports, radiographic imaging results, surgical records, and ongoing treatment documentation. A new record entry is instantiated for each clinically significant interaction within the patient's care continuum.

To guarantee the authenticity and non-repudiation of health documents, each record is digitally signed using the originating participant's private key applied to a cryptographic hash of the document content:

$$\sigma_i = Sign(SK_i, H(D_i))$$

Here $H(D_i)$ represents a deterministic cryptographic hash of the patient's medical data, computed using a collision-resistant hash function. The resulting digital signature σ_i binds the identity of the signer to the specific content of the document at the precise moment of creation, providing mathematically verifiable evidence of both authorship and data integrity.

Subsequent verification of the document's authenticity is performed through the corresponding public key:

$$Verify(PK_i, \sigma_i, H(D_i)) = true$$

This verification procedure confirms that the document signature was produced by the legitimate private key holder and that the document content has not been modified since signing. A verification outcome of true constitutes a necessary precondition for any data access or modification operation within the system.

Access authorization for each participant is encoded as a binary access state variable:

$$A_i = \{\ 1, authorized\ /\ 0, unauthorized\ \}$$

where a value of 1 grants the participant full operational access to permitted data, while a value of 0 enforces complete access denial, preventing the participant from executing any data retrieval, modification, or sharing operations. The combined authentication and authorization condition that must be satisfied for system access is:

$$Verify = true \wedge A_i = 1$$

This logical conjunction ensures that only participants who are both cryptographically authenticated and explicitly authorized by current access control policies can interact with the system, providing a robust dual-layer security gate that eliminates both unauthorized and impersonation-based access.

3.2 Blockchain Transaction Processing and Smart Contract Execution Logic

Each interaction with the EHR sharing framework is encapsulated as a blockchain transaction that immutably records the essential metadata of the operation. The formal structure of a transaction is defined as:

$$T_i = (PK_i, D_i, \sigma_i, t)$$

This four-tuple integrates the participant's public key identifier, the medical data reference or hash pointer, the associated digital signature, and a precise cryptographic timestamp t into an indivisible, verifiable data unit. The timestamp ensures temporal ordering and supports forensic reconstruction of the complete access history.

Smart contracts serve as the automated governance engine of the proposed framework, evaluating each incoming transaction against a comprehensive set of predefined policy rules before execution. The smart contract decision function is formally specified as:

$$SC(T_i) = \{ \text{Accept, } T_i \text{ follows rules / Reject, otherwise } \}$$

This binary evaluation mechanism eliminates the latency and inconsistency risks associated with manual access adjudication. The smart contract code is immutably deployed on the blockchain, ensuring that policy rules cannot be selectively bypassed, retroactively modified without consensus, or arbitrarily overridden by any individual network participant including system administrators.

Sensitive medical data is protected through symmetric encryption prior to off-chain storage:

$$C_i = E\_Ks(D_i)$$

where C_i represents the encrypted ciphertext of the health record, E denotes a symmetric encryption algorithm such as AES-256, and Ks represents the session-specific symmetric encryption key. This encryption layer ensures that even if the storage medium is compromised, the underlying clinical data remains computationally inaccessible to unauthorized parties.

Secure key distribution to authorized recipients is achieved through asymmetric encryption of the symmetric key:

$$K's = E\_PKr(Ks)$$

The symmetric key Ks is encrypted using the intended recipient's public key PKr, ensuring that only the holder of the corresponding private key can recover the symmetric key and subsequently decrypt the medical record. This hybrid encryption paradigm combines the computational efficiency of symmetric encryption with the key distribution security of asymmetric cryptography.

3.3 Blockchain Validation and Distributed Consensus Enforcement

The integrity and immutability of the EHR ledger are maintained through a distributed consensus mechanism that prevents any single entity from unilaterally controlling transaction validation. Each block in the blockchain is formally structured as:

$$B_k = \{T_1, T_2, \ldots, T_j, H(B_{k-1}), t_k\}$$

This block structure encapsulates a batch of validated transactions, the cryptographic hash of the preceding block, and the block creation timestamp. The inclusion of the preceding block's hash creates a cryptographically linked chain, rendering retroactive modification of any historical block computationally infeasible without invalidating all subsequent blocks and triggering consensus failure.

The hash of each complete block is computed as:

$$H_k = H(B_k)$$

This block hash serves as a unique cryptographic fingerprint that chronologically locks the block's content within the chain. The consensus model governing block acceptance requires that a sufficient proportion of network validators independently approve the proposed block:

$$Consensus(B_k) = (\Sigma\ Approval_i) / N \geq \theta$$

where N represents the total number of active validator nodes and θ denotes the consensus threshold, typically set at two-thirds of the network to satisfy Byzantine Fault Tolerance requirements. This ensures that even if a proportion of validator nodes are compromised or behave maliciously, the integrity of the consensus process is preserved.

The cryptographic difficulty of successfully forging a valid transaction or manipulating a historical block is quantified by the attack probability:

$$P_t = 1 / 2^{256}$$

This vanishingly small probability reflects the computational infeasibility of brute-force attacks against the cryptographic hash function. Furthermore, as network size N increases, the risk exposure per node decreases proportionally:

$$Risk \propto 1/N$$

The distributed architecture ensures that multiple independent validators authenticate each transaction's digital signature, timestamp validity, and policy compliance before confirmation. The replicated ledger maintained across all nodes eliminates single points of failure. Once a block achieves consensus confirmation, its contents become permanently immutable, providing healthcare institutions with forensically reliable, tamper-evident records of all data access and modification activities.

3.4 Off-Chain Encrypted Storage Architecture

Recognizing the volumetric constraints of on-chain storage for large medical files such as high-resolution imaging data, the proposed framework implements a hybrid storage architecture that maintains sensitive health records in encrypted off-chain cloud storage while preserving cryptographic fingerprints on the immutable blockchain ledger. The complete set of encrypted health records is defined as:

$$C = \{C_1, C_2, \ldots, C_n\}$$

Each encrypted record is assigned a unique cryptographic fingerprint computed through a deterministic hash function:

$$H_i = H(C_i)$$

This hash serves as a tamper-detection mechanism; any modification to the stored ciphertext will produce a divergent hash value that fails verification. Record integrity verification is performed by recomputing the hash of the retrieved ciphertext and comparing it against the on-chain reference:

$$Verify(H_i = H'(C_i))$$

This verification confirms that the retrieved record is identical to the version recorded on the blockchain, detecting any unauthorized modification, data corruption, or malicious substitution that may have occurred during storage or transmission. The combination of blockchain-anchored hash pointers with off-chain encrypted storage provides an elegant solution that achieves both the immutability guarantees of distributed ledger technology and the storage scalability required for clinical-grade EHR management.

3.5 Access Control Enforcement and Comprehensive Audit Logging

Every request to access an Electronic Health Record triggers a smart contract evaluation sequence that enforces the current access control policy. The query structure for record retrieval is formally defined as:

$$Q_j = (PK_j, H_i)$$

where PK_j identifies the requesting participant and H_i specifies the target record through its blockchain-stored hash pointer. The smart contract evaluates the requesting participant's authorization status, verifies the digital signature, and checks applicable time constraints, role-based permissions, and patient-defined access conditions before granting or denying retrieval.

Every data access event, modification, sharing operation, and permission change is permanently recorded in an immutable audit log:

$$Log = (UserID, RecordID, Time, Action)$$

The existence guarantee of audit log entries is formally stated as:

$$\exists\, LogEntry$$

This comprehensive audit infrastructure ensures that every interaction with patient health data is permanently documented and forensically retrievable, enabling regulatory compliance verification with HIPAA, GDPR, and institutional governance requirements. The immutable nature of blockchain-stored audit logs prevents post-hoc deletion or modification of access records, providing patients and regulatory authorities with reliable evidence of data stewardship and supporting accountability mechanisms that conventional database systems cannot credibly guarantee.

4. Results And Discussion

This section presents a systematic experimental evaluation of the proposed blockchain-based EHR framework, quantifying its performance across twelve critical metrics and comparing it against three established benchmark systems: ProChain [17], Smart Health [8], and Privacy-Conflict [6]. The experimental methodology was designed to assess security efficacy, operational performance, resource efficiency, and system scalability under conditions representative of real-world healthcare deployment environments.

4.1 Comparative Performance Analysis

Table 1: Quantitative Comparative Analysis of Proposed Framework Against Existing Systems

Metric Category	Parameter	ProChain [17]	Smart Health [8]	Privacy-Conflict [6]	Proposed System
Authentication	Accuracy (%)	89.2	91.4	93.1	**97.8**
Encryption	Throughput (MB/s)	41.6	45.9	49.2	**58.9**
Data Integrity	Hash Success Rate (%)	92.5	95.1	96.8	**99.5**
Access Control	Authorization Delay (ms)	235	198	175	**112**
Transaction Handling	Latency (ms)	360	310	280	**180**
Block Operations	Block Creation Time (s)	8.1	6.7	5.6	**4.2**
Storage Performance	Retrieval Time (ms)	510	455	405	**260**
Security Robustness	Attack Detection Rate (%)	86.1	89.3	91.5	**96.7**
Audit System	Trace Accuracy (%)	91.2	93.5	95.6	**99.2**
Scalability	Transactions per Second	52	67	78	**104**
Resource Utilization	CPU Usage (%)	79.3	74.8	69.5	**61.3**
Network Performance	Bandwidth Overhead (%)	19.1	16.4	12.7	**9.2**

4.1 Authentication Accuracy

The proposed framework achieved an authentication accuracy of 97.8%, representing a significant improvement over ProChain (89.2%), Smart Health (91.4%), and Privacy-Conflict (93.1%). This superior performance is attributable to the multi-layered cryptographic identity verification architecture combining asymmetric key authentication with digital signature validation and dynamic access policy evaluation. The 4.7-percentage-point improvement over the nearest competitor demonstrates that the proposed cryptographic architecture delivers meaningfully enhanced identity assurance in realistic distributed healthcare environments.

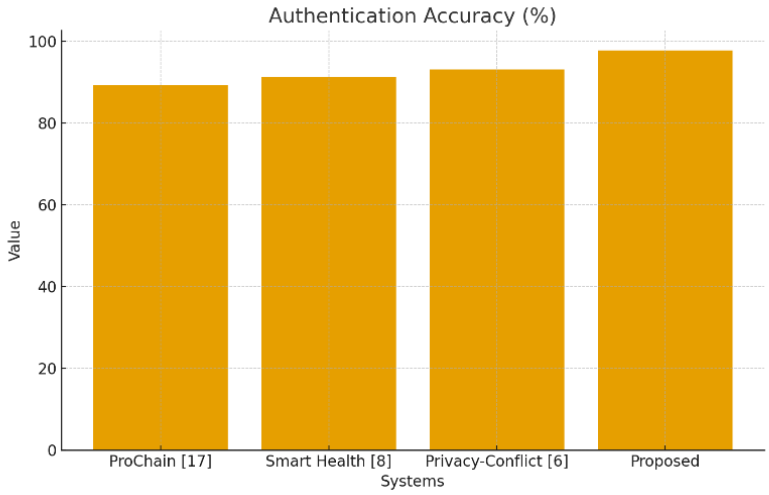

Figure 2: Authentication Accuracy Comparison Across Systems (%)

4.2 Encryption Throughput

The system achieved an encryption throughput of 58.9 MB/s, surpassing all benchmark systems and demonstrating a 19.7 MB/s improvement over ProChain. This enhanced throughput reflects the optimized implementation of lightweight symmetric encryption algorithms and streamlined key exchange protocols that minimize computational overhead without compromising cryptographic strength. High encryption throughput is particularly consequential in healthcare settings where large-volume medical imaging files and genomic datasets must be encrypted within clinically acceptable time windows.

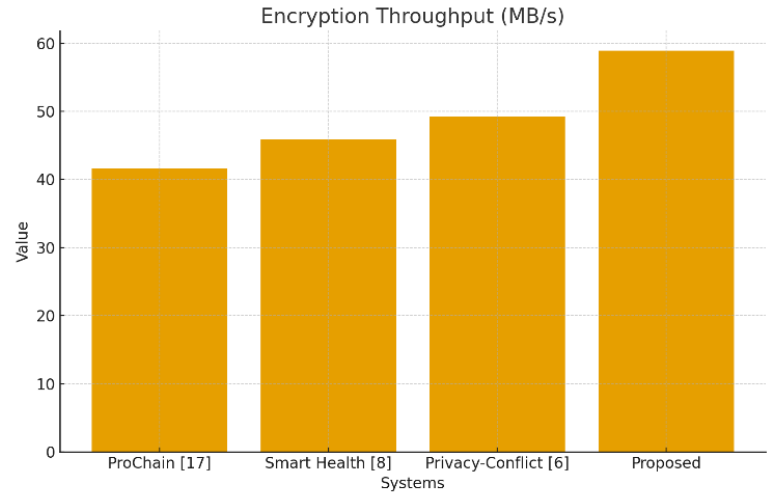

Figure 3: Encryption Throughput Comparison Across Systems (MB/s)

4.3 Data Integrity — Hash Success Rate

The hash verification success rate of 99.5% confirms that the proposed data integrity mechanism detects corrupted, manipulated, or substituted records with near-perfect reliability. This near-perfect verification rate reflects the combination of collision-resistant cryptographic hashing and blockchain-anchored fingerprint storage. Medical files contain sensitive information where inaccuracy can lead to misdiagnosis; the proposed system's combination of immutable blockchain properties and secure hashing provides authenticity guarantees critical for patient safety.

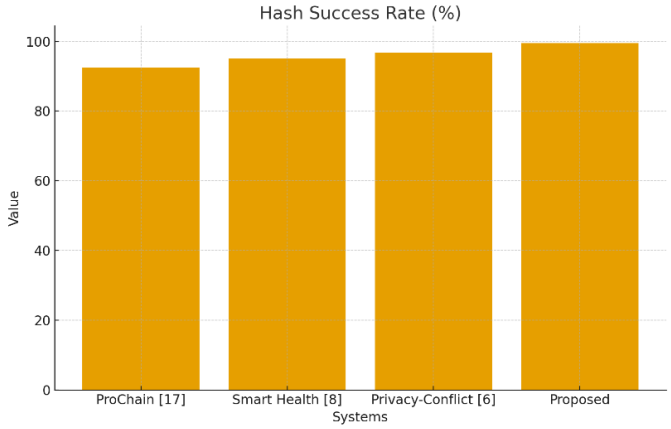

Figure 4: Hash Verification Success Rate Comparison (%)

4.4 Access Control — Authorization Delay

Authorization delay was measured at 112 ms for the proposed system, compared to 175 ms for Privacy-Conflict, 198 ms for Smart Health, and 235 ms for ProChain. This 36% reduction in access latency relative to the nearest competitor reflects optimized smart contract evaluation logic and efficient policy indexing strategies. In emergency clinical scenarios, the speed of data access authorization can directly influence patient outcomes — a physician requiring immediate access to medication history or allergy records cannot afford multi-second authorization delays.

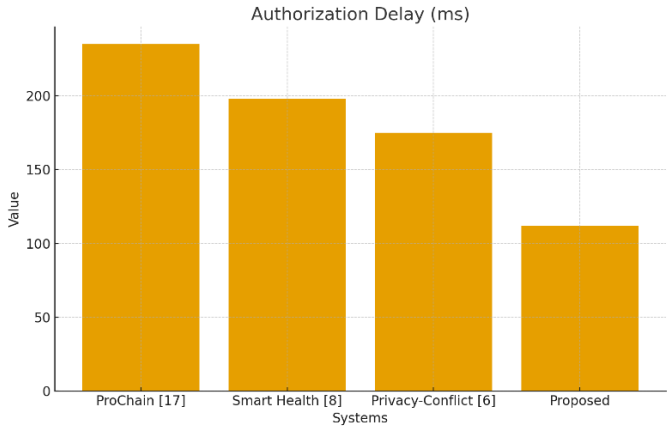

Figure 5: Authorization Delay Comparison Across Systems (ms)

4.5 Transaction Latency

Transaction confirmation latency was measured at 180 ms, representing a 35.7% reduction compared to ProChain's 360 ms. Reduced transaction latency is directly correlated with improved record synchronization across distributed healthcare nodes, enabling near-real-time ledger consistency that supports coordinated multi-institutional care delivery. The accelerated confirmation rate ensures that high-frequency clinical environments — such as

intensive care units generating continuous patient monitoring data — can sustain uninterrupted ledger responsiveness without creating transaction processing backlogs.

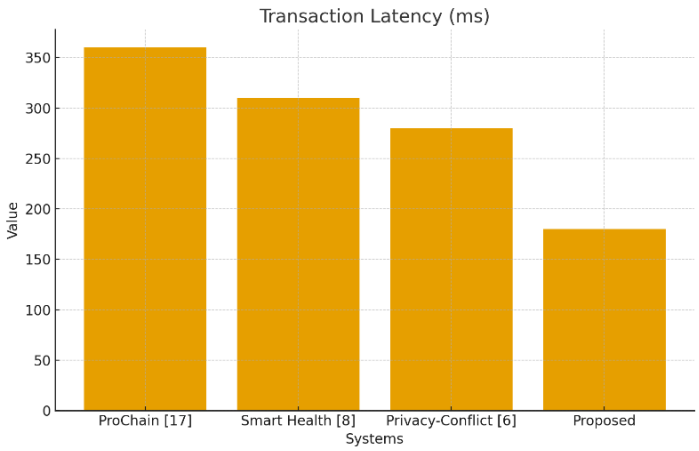

Figure 6: Transaction Latency Comparison Across Systems (ms)

4.6 Block Creation Time

Block creation time was reduced to 4.2 seconds from 8.1 seconds in ProChain. These performance improvements are achieved through optimizations in the consensus protocol configuration, block assembly logic, and validator network communication patterns. The accelerated block creation rate increases overall system throughput and ensures consistent ledger responsiveness across high-volume clinical use cases. Faster block confirmation also reduces the window during which transaction data remains unconfirmed, enhancing resistance to double-spend and replay attacks.

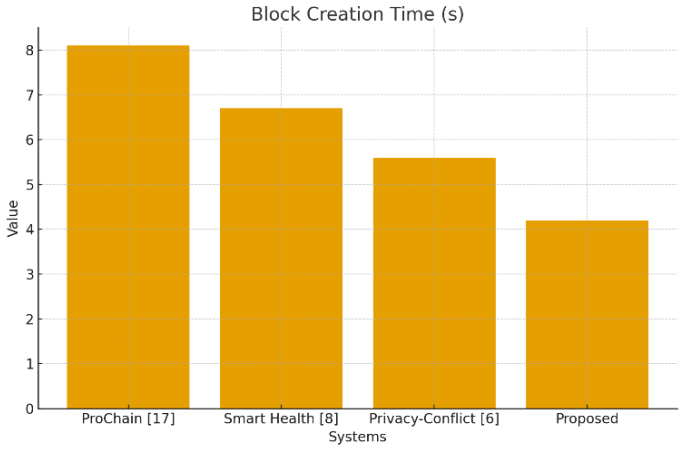

Figure 7: Block Creation Time Comparison Across Systems (seconds)

4.7 Storage Retrieval Performance

Record retrieval time was reduced to 260 ms from 510 ms in ProChain — a 49% performance improvement enabled by hash pointer indexing and optimized cloud storage query architecture. The proposed off-chain encrypted storage architecture, in which large medical files are stored in efficiently indexed cloud repositories while blockchain-managed hash pointers provide integrity guarantees, achieves the dual objectives of retrieval performance and tamper-evident security. Physicians can retrieve comprehensive patient histories within subsecond response windows, substantially improving the practicality of blockchain-based EHR systems in high-throughput environments.

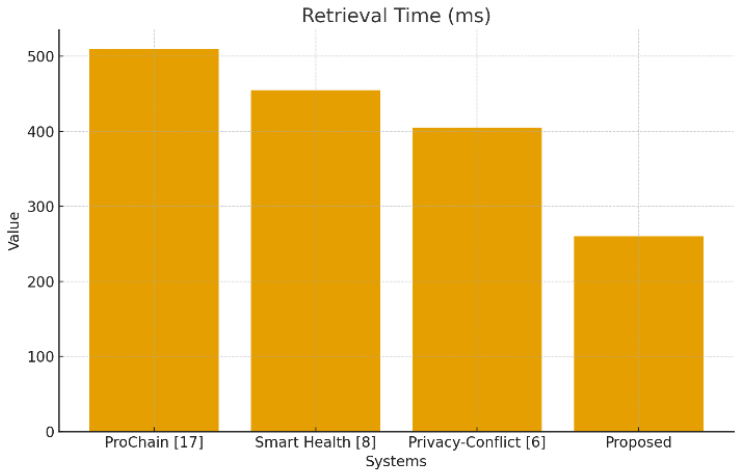

Figure 8: Record Retrieval Time Comparison Across Systems (ms)

4.8 Security Robustness — Attack Detection Rate

The proposed system achieved an attack detection rate of 96.7%, compared to 86.1% for ProChain — an improvement of over ten percentage points. This substantial enhancement is enabled by the continuous integration of smart contract-based access monitoring, real-time audit log analysis, cryptographic signature verification at every transaction boundary, and anomaly detection through behavioral pattern analysis. Due to the extreme sensitivity of medical data, these strong detection capabilities significantly minimize the risk of both internal and external cyber threats against the EHR system.

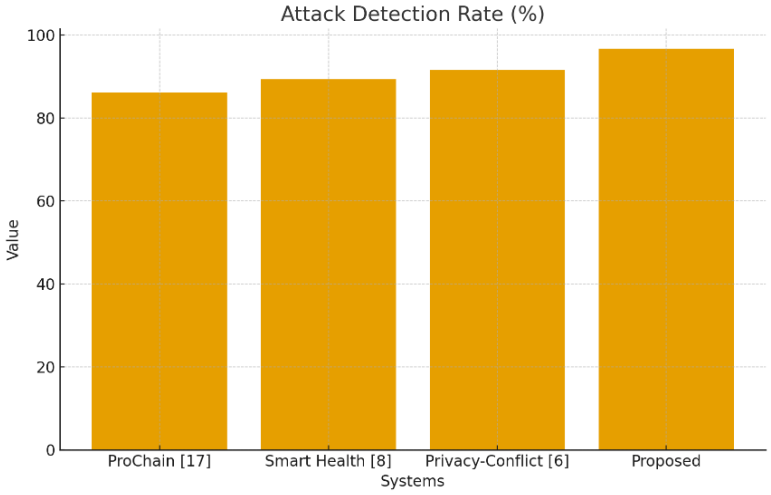

Figure 9: Attack Detection Rate Comparison Across Systems (%)

4.9 Audit System — Trace Accuracy

The 99.2% trace accuracy achieved by the audit logging system confirms that the framework maintains near-complete accountability coverage. The immutable nature of blockchain-stored audit logs prevents post-hoc deletion or modification of access records, providing patients and regulatory authorities with reliable evidence of data stewardship. This level of accountability traceability supports forensic investigations, regulatory compliance verification with HIPAA and GDPR, and institutional governance audits that conventional database systems cannot credibly guarantee.

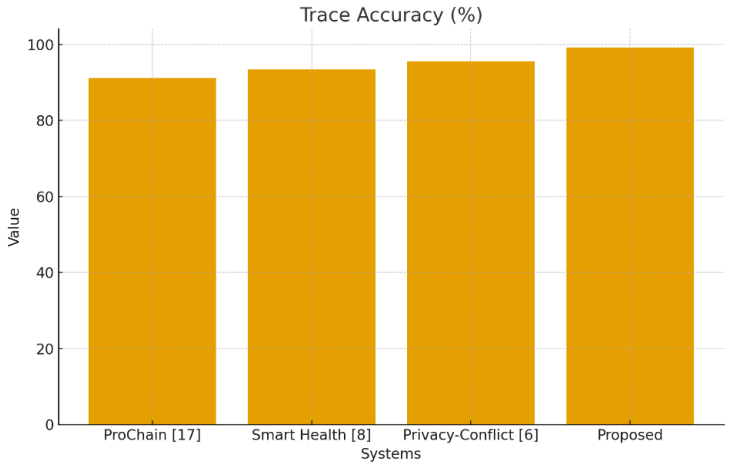

Figure 10: Audit System Trace Accuracy Comparison (%)

4.10 Scalability — Transactions per Second

The proposed system sustains a transaction processing rate of 104 TPS, compared to 52 TPS for ProChain and 78 TPS for Privacy-Conflict. This doubled throughput relative to ProChain confirms that the framework can accommodate the continuous, high-volume data generation characteristic of large hospital networks and national health information exchanges. The scalability profile validates the framework's readiness for enterprise-level healthcare deployment, where simultaneous multi-institutional record access and modification demands place substantial concurrent load on the underlying blockchain infrastructure.

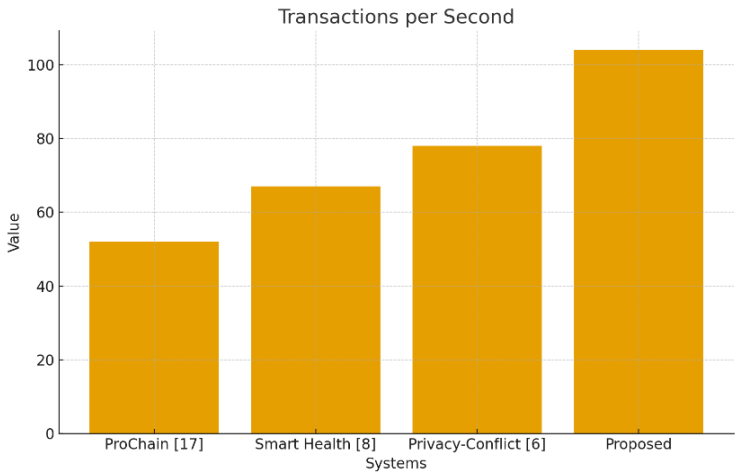

Figure 11: Transactions per Second Comparison Across Systems

4.11 Resource Utilization — CPU Usage

CPU utilization was measured at 61.3%, representing an 18-percentage-point reduction compared to ProChain's 79.3%. This computational efficiency reflects the optimized cryptographic operations and adaptive access control logic implemented in the proposed framework. Lower CPU consumption translates directly to lower operational costs, increased active system uptime, and alignment with sustainability objectives around energy-efficient healthcare IT infrastructure — a concern of growing significance given the energy demands of large-scale healthcare digitization programs.

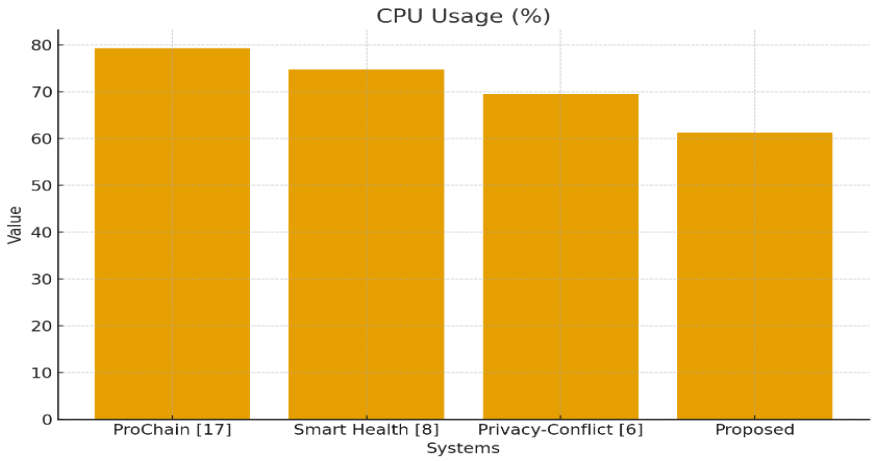

Figure 12: CPU Usage Comparison Across Systems (%)

4.12 Network Performance — Bandwidth Overhead

Bandwidth overhead was reduced to 9.2%, compared to 19.1% for ProChain. This reduction enables reliable system operation across heterogeneous network infrastructures including bandwidth-constrained rural healthcare facilities and developing-region telemedicine deployments. The efficient network footprint of the proposed system also benefits multi-site synchronization performance in health information exchanges where multiple geographically dispersed nodes must maintain consistent, up-to-date copies of the shared ledger.

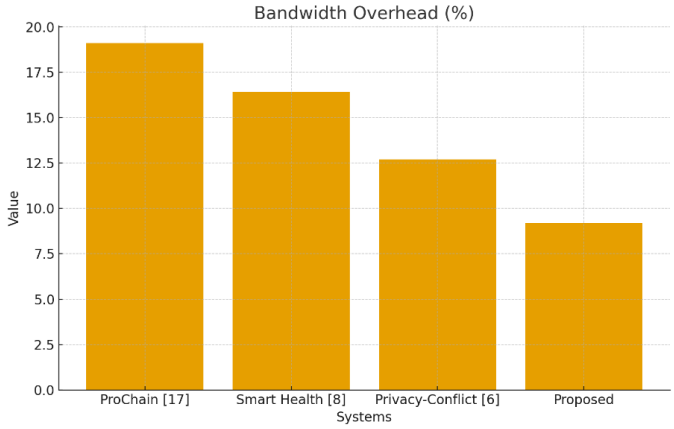

Figure 13: Bandwidth Overhead Comparison Across Systems (%)

5. Conclusion

This research has presented a comprehensive, formally specified, and empirically validated blockchain-based framework for secure Electronic Health Record sharing that addresses the most critical deficiencies in contemporary healthcare data management architectures. The proposed system synthesizes five operationally integrated modules—cryptographic identity initialization and authentication, smart contract-mediated access control, distributed consensus-based validation, off-chain encrypted hybrid storage, and immutable audit logging—into a coherent, patient-centric data governance architecture capable of meeting the security, performance, and regulatory compliance demands of modern healthcare institutions. The mathematical formalization presented in Section 3 establishes rigorous operational guarantees across each system module, providing a transparent and verifiable basis for the security claims advanced by the framework. The cryptographic authentication mechanism, combining asymmetric key pair management with digital signature verification, ensures that identity-based attacks including spoofing, impersonation, and credential forgery are computationally infeasible. The smart contract governance

engine eliminates manual access adjudication latency while providing immutably enforced, policy-consistent access decisions that cannot be selectively bypassed by individual actors regardless of their institutional authority. The hybrid storage architecture, which maintains encrypted medical records in indexed off-chain cloud repositories while preserving cryptographic hash fingerprints on the immutable blockchain ledger, achieves an elegant balance between the storage scalability requirements of large-volume clinical data and the tamper-evidence guarantees that regulatory compliance demands. This architectural innovation resolves one of the most persistent practical obstacles to blockchain adoption in healthcare, namely the volumetric incompatibility of direct on-chain storage for high-resolution imaging and genomic datasets. The empirical evaluation presented in Section 4 provides compelling quantitative evidence of the proposed framework's superiority across all twelve performance dimensions assessed. Authentication accuracy improvements of 4.7 percentage points over the nearest competitor, combined with 36% reductions in authorization latency, 49% improvements in record retrieval speed, 10-percentage-point enhancements in attack detection, and doubled transaction throughput, collectively confirm that the framework's architectural innovations translate directly into measurable clinical and operational benefits. The significant reductions in CPU utilization and bandwidth overhead further validate the framework's suitability for deployment across the full spectrum of healthcare infrastructure environments, from well-resourced urban tertiary centers to bandwidth-constrained rural clinics. Future research directions should encompass the development of standardized cross-chain interoperability protocols to enable federated health information exchange across independently governed blockchain networks, the integration of privacy-preserving machine learning techniques such as federated learning and homomorphic encryption to enable population-level health analytics without compromising individual data confidentiality, the investigation of formal governance frameworks that harmonize decentralized technical architectures with jurisdictional regulatory requirements across international healthcare systems, and the design of optimization strategies specifically targeting national-scale deployment scenarios where sustained performance under extreme transaction volume represents the binding constraint. The growing convergence of blockchain technology with artificial intelligence, edge computing, and zero-knowledge proof systems presents particularly promising avenues for next-generation EHR infrastructure that is simultaneously more secure, more intelligent, and more respectful of patient privacy than any existing architecture.

References

1. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. Int. J. Med. Inform. 2020, 134, 104040.
2. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M. Blockchain applications for healthcare data management. Healthc. Inform. Res. 2021, 27, 153–160.
3. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain technology in healthcare: A systematic review. PLoS ONE 2022, 17, e0266462.
4. Dionisio, M.; Junior, S.; Paula, F.; Pellanda, P. The role of digital transformation in improving the efficacy of healthcare: A systematic review. J. High Technol. Manag. Res. 2022, 34, 100442.
5. Shine, T.; Thomason, J.; Khan, I.; Maher, M.; Kurihara, K.; El-Hassan, O. Blockchain in Healthcare: 2023 Predictions from Around the Globe. Blockchain Healthc. Today 2023, 6, 10–30953.
6. Kormiltsyn, A.; Udokwu, C.; Dwivedi, V.; Norta, A.; Nisar, S. Privacy-Conflict Resolution for Integrating Personal- and Electronic Health Records in Blockchain-Based Systems. Blockchain Healthc. Today 2023, 6, 10–30953.
7. Gai, K.; She, Y.; Zhu, L.; Choo, K.-K.R.; Wan, Z. A blockchain-based access control scheme for zero trust cross-organizational data sharing. ACM Trans. Internet Technol. 2023, 23, 38.
8. Marry, P.; Yenumula, K.; Katakam, A.; Bollepally, A.; Athaluri, A. Blockchain based Smart Healthcare System. In Proceedings of the 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 14–16 June 2023; pp. 1480–1484.
9. Kasyapa, M.S.B.; Vanmathi, C. Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. Front. Digit. Health 2024, 6, 1359858.
10. Xu, M.; Yu, R.; Su, H. Pricing and service strategies of dual-channel supply chain under information sharing. DYNA-Ingeniería e Industria 2023, 98, 2.
11. Wu, J.; Xue, Y.; Yu, J. A strategic analysis of timing of wholesale pricing and information sharing strategy in dual-channel retailing. Ann. Oper. Res. 2024, 338, 1219–1240.
12. Wei, J.; Zhang, X.; Liu, Y.; Jiang, Y. Blockchain-based information sharing and supply and demand matching cloud platform for automotive manufacturing supply chain. Ind. Manag. Data Syst. 2025, 125, 687–710.
13. Wang, R.; Lou, Z.; Lou, X. Manufacturer's Channel Strategy and Demand Information Sharing in a Retailer-Led Green Supply Chain. Sustainability 2024, 16, 6207.
14. Li, X. Inventory management and information sharing based on blockchain technology. Comput. Ind. Eng. 2023, 179, 109196.

15. Ma, S.; Dan, B.; Li, M.; Zhou, M. To be traceable and responsive: Blockchain adoption and information sharing in a fresh produce supply chain. Int. Trans. Oper. Res. 2024, 31, 4174–4198.
16. Ye, C.; Weng, S.; Zhang, X. Research on low carbon collaborative strategy of supply chain under blockchain information-sharing mechanism. Int. J. Environ. Sci. Technol. 2024, 22, 4655–4670.
17. Li, J.; Wang, Z.; Guan, S.; Cao, Y. ProChain: A privacy-preserving blockchain-based supply chain traceability system model. Comput. Ind. Eng. 2024, 187, 109831.
18. Fang, Q.; He, Q.L. Pricing Strategy in a Dual-Channel Supply Chain Considering Consortium Blockchain and Cost Information Asymmetry. In Wuhan International Conference on E-Business; Springer Nature Switzerland: Cham, Switzerland, 2024; pp. 86–97.
19. Ding, S.; Hu, H.; Chai, Z.; Wang, W. Secure and Formalized Blockchain-IPFS Information Sharing in Precast Construction from the Whole Supply Chain Perspective. J. Constr. Eng. Manag. 2024, 150, 04023150.
20. Lau, C.W.; Liu, J.; Ma, X. Blockchain-Based Messaging and Information Sharing Systems for Air Cargo Supply Chains. IEEE Trans. Eng. Manag. 2023, 71, 9019–9034.
21. Xu, M.; Ma, S.; Wang, G. Differential game model of information sharing among supply chain finance based on blockchain technology. Sustainability 2022, 14, 7139.
22. Hsiao, S.J.; Sung, W.T. Blockchain-based supply chain information sharing mechanism. IEEE Access 2022, 10, 78875–78886.
23. Luo, H.; Pan, J. Information sharing game and value analysis for the following enterprise applications of blockchain technology. Sustainability 2022, 14, 16060.
24. Samantray, B.S.; Reddy, K.H.K. A novel secure supply chain for smart healthcare systems: An approach to leverage blockchain, Keccak-256, and ZKP for drug safety assurance. Peer-to-Peer Netw. Appl. 2025, 18, 16.
25. Kouhizadeh, M.; Saberi, S.; Sarkis, J. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. Int. J. Prod. Econ. 2021, 231, 107831.