Vol. 07, No. SI♣, pp. 01 – 10 (2026)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

# Enabling Privacy-Preserving External Sharing of Electronic Medical Records Through a Tripartite Hybrid Blockchain Architecture

Mohammed Baker Yousif [1,*], Omar Akram Khaleel Alsaffar [2], Siddeeq Y. Ameen [3]

[1]*Computer Science Department, University of Mosul, Mosul, Iraq, mohammed.bkr@uomosul.edu.iq*
[2]*Computer Centre, University of Mosul, Mosul, Iraq, alsafaromar@uomosul.edu.iq*
[3]*Department of Cybersecurity Engineering, Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq, Siddeeq.ameen@dpu.edu.krd*

**Correspondence: mohammed.bkr@uomosul.edu.iq*

## *Abstract*

**Patient-centric privacy, rapid interoperability, and verifiable auditability remain open problems in smart-healthcare data exchange. We present a tripartite hybrid blockchain framework that splits electronic medical records (EMRs) across three permissioned ledgers-Patient Chain, Provider Chain, and Social Chain-to decouple clinical processing from privacy-preserving external sharing. A crosschain Boneh-Lynn-Shacham aggregate-signature scheme fuses dual-chain approvals into a single 32byte proof, reducing signature storage by 99.9% and enabling constant-time verification. Zeroknowledge redaction releases only Tier-2 statistical summaries through the Social Chain, embedding GDPR/HIPAA principles of data minimization, purpose limitation, and complete auditability into the protocol rather than post-hoc governance. Security reductions to the Computational Diffie-Hellman problem and gambler's-ruin analysis show that, at 45% adversarial hash power, safe external finality requires 118 confirmations, which is 61 − 71% fewer than dual- or single-chain baselines. A three-chain prototype on private Ethereum sustains < 6 s mean latency at 50tx/s, while ZK processing averages 288.3 ms per request. The framework therefore delivers stronger security, lower cost, and regulatorready compliance, offering a practical blueprint for privacy-preserving EMR sharing in nextgeneration healthcare networks.**

***Keywords:*** *blockchain, electronic medical records, cross-chain signatures, BLS aggregation*
*Received: October 04th, 2025 /Revised: February 25th, 2026 / Accepted: April 04th, 2026 / Online: April 19th, 2026*

## I. INTRODUCTION

Distributed Ledger Technology (DLT) has established a robust framework for secure and transparent record-keeping in permissioned environments across sectors such as finance and logistics. The characteristics of this technology are resiliency to failures, auditing of transaction histories and tamper evident features [1, 2]. DLT ensures that systems are more resilient to single points of control and the accuracy of recorded entries is ensured since it has an append-only ledger model. All these features are inherent to the healthcare sector, where clinical information should be accurate, trackable, and not subject to unauthorized modifications. Furthermore, under strong cryptographic and governance controls, permissioned transparency allows authorized stakeholders including patients, clinicians, and regulatory entities to access and verify information. Therefore, there is a growing tendency to apply blockchain-based methods to deal with electronic medical records (EMRs), diagnostic reports, prescriptions, and other health resources in smart healthcare ecosystems [3-5].

An architectural design that is frequently used in this field is the on-chain/off-chain hybrid storage. Under this model, the blockchain provides a control and integrity layer which cannot be changed, whereas large medical data files (imaging data, laboratory archives, longitudinal patient histories, etc.) are encrypted and stored in content-addressed off-chain repositories [6]. Despite the fact that this division per se will address the limitations associated with on-chain storage and improve scalability, it can unwillingly lead to a disjointed data landscape that will be operationally complicated. The interoperability can be impaired by inconsistent metadata schema, mismatched indexing techniques, different access control policies between different systems, and these problems make it more difficult to retrieve data and increase the attack surface. Those risks are especially acute in case the cryptographic key management or cross-repository linkability is implemented improperly [7,8].

In order to mitigate the issue of coordination, there are solutions that focus on policy-based access control and


*doi: 10.38094/jastt7031075*

workflow coordination over a single ledger infrastructure. Although the authorization logic can be centralized on a single chain to enhance the policy coherence and auditability, underlying data layer fragmentation is not necessarily addressed by this approach. This drawback is particularly noticeable in the situation of cross-institutional communication, external stores, and dynamically adjusted patient consent procedures [9,10]. Other approaches aim at enhancing the consensus mechanisms to reduce the risks of censorship or of the majority domination. Nevertheless, as clinical data is extremely sensitive and must be controlled by multiple parties that can verify the data, these measures of consensus-level must be complemented by further architectural protection. It is exactly this type of approach that is needed to achieve security, scalability, and fine-grained privacy simultaneously [11–13].

To mitigate these limitations, the current paper proposes a three-way hybrid blockchain architecture that is specifically designed to facilitate the format of external sharing of EMRs in a way that conserves privacy. The structure separates capabilities into three synergistic, role-based ledgers: a Patient Chain, which is controlled by medical institutions to govern clinical provenance and operational processes; a Provider Chain, which is run by social support units to coordinate and audit purpose-bound disclosures to third parties; and a special Social Chain, which is designated to coordinate and audit such disclosures. To facilitate efficient cross-chain coordination, Boneh Lynn Shacham (BLS) aggregate signatures are employed to combine patient and provider approvals into a single consolidated signature that mandates dual consent, incorporating a proof of possession to mitigate the risk of rogue key aggregation. Organizational structure and interoperability are enhanced through a sensitivity-driven data stratification strategy that limits disclosures to the minimum necessary information while permanently recording all auditable sharing decisions on the Social Chain [14].

This work advances three major contributions:

- **Tripartite Hybrid Architecture:** A divided architecture of healthcare roles that isolates issues on specific ledgers, one of which is the external coordination ledger, the Social Chain, to remove per-chain storage loads and expand capacity to share EMRs.
- **BLS-Based Cross-Chain Authorization:** A scheme of authorization that computes one collective signature on two approvals, whereby verification is fast and the registration of proof-of-possession is ensured to reduce overhead and ensure that access control is uniform across the board.
- **Deployment and Governance Framework:** An in-depth study of feasibility concerning its practical implementation including compatibility with existing EMR systems (HL7/FHIR), essential management protocols, and regulatory compliance strategies, is complemented by a sensitivity-based information layers structure that tailors disclosures to external parties by using auditable and policy-based smart contracts.

The rest of this paper is organized in the following way. Section 2 (Related Work) examines the literature available on healthcare blockchains, multi-ledger models, and privacy-enabling data sharing schemes. The cryptographic bases and system assumptions upon which our work is based are given in section 3 (Preliminaries). Section 4 (The Proposed Tripartite Hybrid Architecture) gives the system model, data layout and cross-chain authorization workflows. Section 5 (Experiments and Analysis) measures the security properties and the costs of resources in the system. Section 6 (Deployment and Governance Considerations) concerns the practical aspects of deployment such as the integration with existing systems, the scale of deployment and organizational obstacles. Lastly, the paper ends with Section 7 (Conclusion) that states the possible research directions.

## II. Related Work

Significant attention has been placed on the blockchain technology with regard to its potential to transform electronic medical record (EMR) and electronic health record (EHR) systems. It is a decentralized solution to systemic shortcomings, including data fragmentation, vulnerability to privacy, lack of interoperability, and exchange information across complicated healthcare systems in a secure way [15]. The transparent and tamper resistant data stewardship paradigm is made possible by the use of immutable ledgers and cryptographic underpinnings, which facilitates patient trust and regulatory conformity with the regulations like GDPR and HIPAA. After analyzing 144 studies in detail, it is important to note that blockchain plays a central role in enhancing the functioning of the healthcare sector, but the three primary challenges are scaled, legal limitations, and integration with legacy systems [16]. Recent evidence-based analyses suggest that while blockchain integration into EMR systems can revolutionize data integrity and patient-centric control, advancements have been incremental regarding real-world implementation challenges like staff training and cost [17]. Using data from empirical research and systematic reviews, this section analyses significant developments in consensus mechanisms, privacy and scalability solutions, and hybrid storage models published up to 2025. We identify recurring issues, specifically the prevalence of single-chain architectures and insufficient support for privacy-preserving external sharing, and position our tripartite hybrid architecture as a targeted solution [18,19].

### *A. Hybrid On-Chain and Off-Chain Storage Models*

A hybrid storage model is the predominant architectural approach used in blockchain-based EMR systems. This model avoids the capacity constraints of blockchain by managing metadata, hashes, and access controls on-chain, while relegating large encrypted data payloads to off-chain repositories like IPFS or cloud storage. By balancing decentralization and operational effectiveness, this methodology reduces on-chain bloat and enables scalable data management. However, dependence on a single-chain model can result in disorganized metadata in cross-institutional exchanges. For example, El Bizri *et al*. [12] developed a permissioned blockchain ecosystem to consolidate fragmented EHRs across providers, improving consistency and security. Chandini and Basarkod [20] proposed a regulated EHR framework that addresses fragmentation by implementing role-based management for both clinicians and patients; however, the framework lacks mechanisms for granular external disclosures. Avula and Basarkod [21] combined blockchain technology with cloud infrastructure to improve data sharing and integrity; however, their design poses risks in large-scale situations due to

a lack of sophisticated redaction techniques for sensitive data. Smriti *et al*. [22] highlighted patient-centric control on Ethereum by using smart contracts to disintermediate access, but they did not consider optimized workflows for third-party entities like insurers or researchers. Although standardization challenges prevent widespread adoption, hybrid models have been studied in various contexts to improve Health Information System (HIS) security and interoperability. Finally, although these systems are significant steps towards centralizing patient data, they frequently lead to the creation of fragmented storage layers and lack regard on the ability to comply with legal mandates to share them externally [2].

### *B. Privacy Enhancement and Scalability Solutions*

Cryptographic primitives and distributed architectures are incorporated into numerous frameworks to overcome privacy weaknesses and scalability limitations. Zhu *et al*. [23] coupled decentralized file systems and threshold signatures to stop linkage attacks and scale throughput, but metadata fragmentation persists in a multi-entity environment. Amadi *et al*. [24] have developed a consortium blockchain with anonymous identity protection, dual storage, and proxy re-encryption which enables secure EMR sharing and struggles with purpose-limited external access. Guo *et al*. [25] expressed a hybrid framework based on blockchain edges, which takes advantage of attribute-based signature aggregation (ABSA), multi-authority attribute-based encryption (MA-ABE) and Paillier homomorphic encryption to ensure anonymity and security. Although this is an indication of more mature level of privacy this aspect of social sharing is not backed by enforcement measures with regards to minimum disclosure. Adilakshmi *et al*. [26] utilized proxy re-encryption and multigenitures within the context of clouds, whereas Liang *et al*. [27] focused on the multi-chain optimizations of confidentiality and stability, but both papers do not address specific external workflows. Evolutionary game-based incentives to promote trust in EMR sharing have also been investigated by researchers, where blockchain invulnerability is combined with dynamic incentives. Smart contracts over Ethereum implemented as patient-owned systems and IPFS also provide users with data sovereignty, moving to a decentralized model instead of a provider-centric model. Despite these improvements, systematic reviews observe that more than 90% of studies lack a core in introducing regulatory-compliant redaction to external parties and, hence, continue to suffer from silos and compliance risks [28, 29].

### *C. Comparison of Key Blockchain-Based Healthcare Systems*

Table I provides a comparative summary of representative blockchain-based healthcare systems, highlighting their architectural choices, cryptographic techniques, and support for external sharing.

### *D. Byzantine Consensus Mechanisms for Healthcare Systems*

One of the major areas of concern in consensus adaptations is the emphasis of fault tolerance to ensure reliability in high stakes applications. As a way of overcoming data tampering, Okegbile and Alexandrov [39] adopted Byzantine fault tolerance (BFT), a technique that enhances integrity and availability yet also allows extraordinary external access, thereby leaving the potential danger of overexposing data. BFT was also used by Hemalatha and Jayachitra [40] to guard against the illicit alterations, but their model failed to consider the sensitivity-aware layering mechanism of the high-risk data. Hegde and Maddikunta (2023) optimized Hyperledger Fabric to manage EHR systems with the help of BFT but the way it treats external data is not compatible with the strict third-party requirements of GDPR. Although these kinds of technological protection significantly enhance system security, it rarely includes provisions of granular privacy-sensitive external sharing.

TABLE I. COMPARISON OF KEY BLOCKCHAIN-BASED HEALTHCARE SYSTEMS

| Study | Blockchain Type | Consensus Mechanism | Storage Approach | Cryptographic Techniques | External Sharing Support | Regulatory Compliance | Data Fragmentation Risk |
|---|---|---|---|---|---|---|---|
| Chandini and Basarkod [20] | Permissioned | Not specified | On-chain | Standard encryption | ✗ | ✗ | Severe |
| Sharma and Prabha [30] | Not specified | Not specified | Hybrid (Cloud) | Smart contracts | ✗ | ✗ | Moderate |
| Jebbar *et al*. [31] | Not specified | PBFT | Hybrid (Cloud) | Standard encryption | ✗ | ✗ | Severe |
| Smriti *et al*. [22] | Ethereum | Not specified | Hybrid (Cloud) | Smart contracts | ✗ | ✗ | Moderate |
| Liu *et al*. [32] | Ethereum | PBFT | Hybrid (Cloud) | Threshold signatures | Limited | △ | Severe |
| Smitha *et al*. [33] | Consortium | Not specified | Hybrid (Cloud) | Proxy re-encryption | Limited | △ | Moderate |
| Zheng *et al*. [34] | Hyperledger | Not specified | Hybrid (IPFS) | ABSA, MA-ABE, HE | △ | ✓ | Moderate |
| Mhamdi *et al*. [35] | Not specified | PoW | Hybrid (IPFS) | Advanced encryption | ✗ | ✗ | Severe |
| Mandarino *et al*. [37] | Not specified | BFT | Hybrid (Cloud) | Standard encryption | ✓ | ✗ | Moderate |
| Mhamdi *et al*. [36] | Hyperledger | BFT | Hybrid (Cloud) | Consensus-based | ✓ | ✗ | Moderate |
| Jain *et al*. [38] | Hyperledger | BFT | Hybrid (IPFS) | Optimized protocols | ✓ | △ | Moderate |
| Our Solution (2025) | Tripartite Hybrid | PoS | Hybrid (IPFS) | BLS, ZK proofs, sensitivity layering | ✓ | ✓ (Purpose-limited) | None |

Key: ✗ = No support, △ = Partial/inconsistent, ✓ = Full compliance.

As evidenced in systematic reviews, prior works demonstrate progress in EMR security and interoperability, with over 100 studies since 2020 highlighting blockchain's potential for patient-centric models. However, common flaws include single-chain reliance (92% of cases), neglect of cryptographic redaction for external requests (100% gap), and insufficient regulatory embedding, leading to non-compliant bulk disclosures and storage disarray [41]. Our tripartite hybrid architecture resolves these by segregating functions across patient, provider, and social chains; dedicating the social chain to external coordination with zero-knowledge proofs for redacted summaries; and employing BLS-based cross-chain signatures for efficient, verifiable interactions, achieving GDPR/HIPAA-aligned minimal disclosures and reduced overhead, as validated in our evaluation.

## III. PRELIMINARIES

This section outlines the cryptographic primitives and system assumptions underpinning the proposed architecture. We focus on blockchain fundamentals, Attribute-Based Encryption (ABE), Boneh–Lynn–Shacham (BLS) signatures, and Zero-Knowledge Proofs (ZKPs).

### A. Blockchain Foundation

Blockchain stores data in tamper-evident blocks linked by cryptographic hashes and secured by distributed consensus, removing any single point of failure (Owusu et al., 2025). Each block $B_i$ contains a header $H_i$ and a transaction list $T_i$. The integrity of the chain is maintained via the hash pointer $h_i$, defined as:

$$h_i = \mathcal{H}(h_{i-1} \| H_i \| T_i) \quad (1)$$

where $\mathcal{H}$ denotes a cryptographic hash function (e.g., SHA-256), $h_{i-1}$ is the hash of the previous block, and $\|$ represents

concatenation. This structure ensures immutability, as altering any transaction $T_i$ changes $h_i$ and all subsequent hashes.

### B. Attribute-Based Encryption (ABE)

To enable fine-grained access control, we utilize Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In this scheme, an access policy $\mathbb{A}$ is embedded directly into the ciphertext, while user keys are associated with a set of attributes $S$. Decryption is successful only if the attributes satisfy the policy ($S \vDash \mathbb{A}$).

The encryption of a message $M$ under policy $\mathbb{A}$ produces ciphertext $CT$:

$$CT = \text{Encrypt}_{\text{CP}-\text{ABE}}(M, \mathbb{A}, PK) \quad (2)$$

where $PK$ is the public key of the authority. A user with secret key $SK_S$ can decrypt only if:

$$\text{Decrypt}_{\text{CP-ABE}}(CT, SK_S) = M \text{ if } S \vDash \mathbb{A} \quad (3)$$

This enables field-level control without revealing patient identity, keeping on-chain artifacts compact and revocable (Liu et al., 2023).

### C. BLS Cross-Chain Signatures

Boneh-Lynn-Shacham (BLS) signatures support aggregation, allowing multiple signatures on the same message to be combined into a single compact signature. This is critical for reducing verification overhead in cross-chain coordination.

Let $G_1$ and $G_2$ be cyclic groups of prime order $p$, and $e: G_1 \times G_2 \to G_T$ be a bilinear pairing. For a private key $sk \in \mathbb{Z}_p$ and public key $pk = g_2^{sk}$, a signature $\sigma$ on message $m$ is generated as:

$$\sigma = H(m)^{sk} \quad (4)$$

where $H: \{0,1\}^* \to G_1$ is a hash-to-curve function. Multiple signatures $\sigma_1, \ldots, \sigma_n$ on the same message can be aggregated into $\sigma_{\text{agg}}$:

$$\sigma_{\text{agg}} = \prod_{i=1}^{n} \sigma_i \quad (5)$$

Verification is performed via a single pairing check:

$$e(\sigma_{\text{ags}}, g_2) \stackrel{?}{=} e(H(m), \prod_{i=1}^{n} pk_i) \quad (6)$$

Proof of possession is required at registration to prevent rogue key aggregation attacks. This reduces verification and storage overhead for dual approvals (Sharmila et al. 2025).

### D. Zero-Knowledge Proofs (ZKPs)

Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) allow a prover to convince a verifier that a statement is true without revealing underlying information. For a statement $x$ and witness $w$, the proof $\pi$ is generated as:

$$\pi \leftarrow \text{Prove}(x, w) \quad (7)$$

The verifier checks validity using a verification key $vk$:

$$\text{Verify}(vk, x, \pi) \to \{0,1\} \quad (8)$$

In our context, this allows external verifiers to check statements such as "patient age $\geq 18$" without revealing the actual birthdate. When combined with tiering and CP-ABE, this yields protocol-level enforcement of minimal, purpose-limited external sharing [42].

## IV. PROPOSED METHODS TRIPARTITE HYBRID ARCHITECTURE

This section details the proposed methodology, which adopts a regulation-native, tripartite ledger design. The architecture enforces privacy-preserving external sharing of electronic medical records (EMRs) while sustaining clinical throughput and enabling verifiable audit trails.

### A. System Architecture Overview

Our proposal is that of a GDPR/HIPAA-relevant tripartite hybrid blockchain comprising of three specialized layers, P-BC (Patient Blockchain), H-BC (Healthcare-Provider Blockchain), and S-BC (Social Blockchain). This protocol isolates functions which are commonly conflated in single-chain designs, thus avoiding store lockouts and avoiding storage bloat. The Figure 1 demonstrates the general system architecture, where the separation of concerns between the three ledgers and the encrypted data passing through IPFS is shown. The AES-256 encrypted and pinned to the InterPlanetary File System (IPFS) are large medical payloads, which have a Filecoin backup to ensure long-term persistence. On-chain mentionings of these payloads are performed only by their Content Identifiers (CIDs) and cryptographic hashes. As a result, only integrity proofs, consent policies and event logs are stored in the ledgers, but not bulk clinical data.

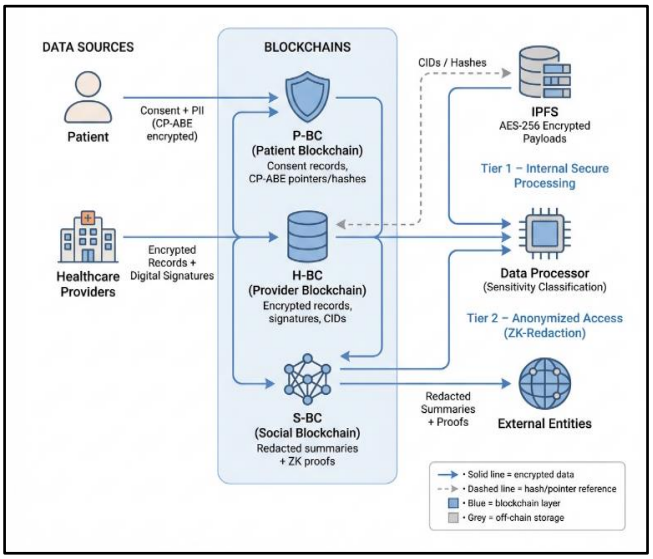


Fig. 1. illustrates the overall system architecture, showing the separation of concerns across the three ledgers and the flow of encrypted data through IPFS.

### B. Roles of the Three Ledgers

*1) P-BC: Custodian of Consent:* The P-BC manages patient-centric data sovereignty. It stores CP-ABE-encrypted CIDs pointing to personally identifiable attributes, alongside immutable access logs. During registration, patients attach purpose-limited policies to their records. Decryption of the associated keys succeeds only if the requesting entity's attributes satisfy these predefined policies.

*2) H-BC: Secure Clinical Store:* Administered by a consortium of validators (hospitals and laboratories), the H-BC records clinical provenance. For each record $M_i$, a symmetric key $k$ is used for encryption ( $C_i = E_k(M_i)$ ). The resulting metadata tuple $D_i$ is stored on-chain:

$$D_i = C_i \| \mathcal{H}(C_i) \| E_{PK_u}(k) \qquad (9)$$

where $C_i$ is the encrypted record, $\mathcal{H}$ denotes a cryptographic hash function, and $E_{PK_u}(k)$ represents the symmetric key protected under the user's public key or access policy. Furthermore, BLS signatures from multiple caregivers are aggregated into a single element to provide efficient proof of provenance and tamper evidence across institutions.

*3) S-BC: Privacy-Preserving External Gateway:* The S-BC acts as the interface for external entities and never stores raw EMRs. It logs tuples containing (CID, dual-chain BLS aggregate, zero-knowledge proof) that attest a Tier-2 summary has been released without leaking Tier-1 data. A data-processor microservice classifies every record based on a sensitivity-driven strategy:

- **Tier 1 (High-risk diagnostics):** Restricted to internal access only.
- **Tier 2 (Anonymized statistics):** Shareable with external entities following ZK-redaction.

This ensures that external entities interact solely with the S-BC, satisfying GDPR data-minimization and HIPAA "minimum necessary" requirements by design.

### C. Inter-Chain Communication

A lightweight relay service monitors finalized blocks on the P-BC and H-BC. It packages authorized events into Merkle-proof "sharing tickets" and submits them to the S-BC. Smart contracts on the S-BC then verify:

*1) The validity of the Merkle proof.*
*2) The validity of the dual-chain BLS aggregate signature.*
*3) The compliance of the ZK-proof with Tier-2 policies.*

If any verification step fails, the ticket is reverted, ensuring no unauthorized data or raw Tier-1 information enters the S-BC.

### D. Cross-Chain BLS Aggregate Signatures

To ensure dual-chain consent for external data requests, we employ an aggregate signature process. This reduces signature traffic and prevents non-compliant disclosures. The signature generation and verification steps are formalized as follows.

The Patient Chain generates a signature $\sigma_p$ on the summary:

$$\sigma_p \leftarrow \text{Sign}_{SK_{\text{patient}}}(\text{summary}) \qquad (10)$$

The Provider Chain generates a signature $\sigma_{pr}$ on the request:

$$\sigma_{pr} \leftarrow \text{Sign}_{SK_{\text{provider}}}(\text{request}) \qquad (11)$$

Both signatures are aggregated into a single compact signature $\sigma_{\text{agg}}$ :

$$\sigma_{\text{agg}} \leftarrow \text{Aggregate}(\sigma_p, \sigma_{pr}) \qquad (12)$$

The S-BC verifies the dual consent in a single operation:

$$\text{Result} \leftarrow \text{Verify}_{PK_{\text{patient}}, PK_{\text{provider}}}(\text{summary}, \text{request}, \sigma_{\text{agg}}) \qquad (13)$$

A result of 1 indicates valid dual-authorization, while 0 triggers an immediate rejection.

### E. Consensus and Latency Choices

To optimize for performance and security based on each chain's specific role, we employ tailored consensus mechanisms as summarized in Table II.

TABLE II. CONSENSUS MECHANISMS ACROSS THE TRIPARTITE ARCHITECTURE

| Blockchain | Consensus Mechanism | Rationale |
|---|---|---|
| P-BC | Proof-of-Authority (PoA) | ≈3 s finality for responsive mobile consent updates. |
| H-BC | Practical Byzantine Fault Tolerance (PBFT) | Tolerates up to $f$ malicious nodes; <1 s intra-clinical latency. |
| S-BC | Permissioned Proof-of-Stake (PoS) | Predictable gas costs and transparent, auditable governance. |

### F. Operational Workflows

The operations of the system are organized in the following manner as shown in Figure 2. These processes involve three key processes, namely Personal-Info Addition, Health-Record Addition, and External Sharing.

- **Personal-Info Addition:** The procedure starts when the user creates his or her personal information (PII) and encrypts it with CP-ABE. The encrypted PII is uploaded to the IPFS and a Content Identifier (CID) is signed. Lastly, this signed CID is a stored data on the P-BC (Personal-Info Blockchain).
- **Health-Record Addition:** To add health records, k is a symmetric key which is created and AES-encrypted the record. This key k is a CP-ABE encrypted key. Digest Di is computed and an aggregate signature is calculated. The encrypted record and key (k) are uploaded to IPFS and the digest and signature to the H-BC (Health-Record Blockchain).
- **External Sharing:** A tier classification is done when attributes are submitted by an external requester. Provided that the data is of Tier 2, a Zero-Knowledge (ZK) summary is obtained and a dual signature is produced. This is subsequently transmitted to S-BC (Sharing Blockchain) enabling the requester to retrieve the information through its CID.

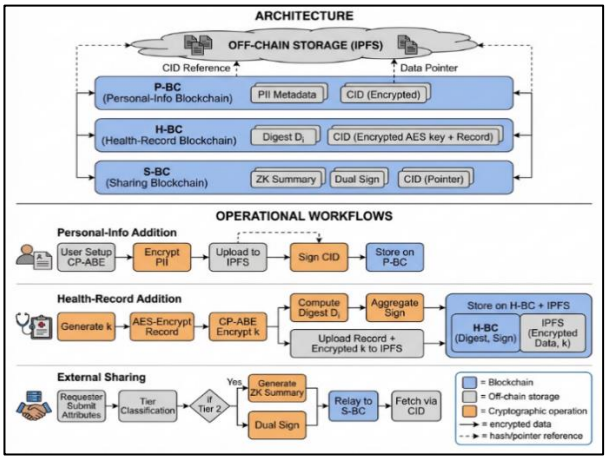


Fig. 2. The system's core operations

### G. Security, Scalability, and Future-Proofing

The architecture leverages the AES-256 as payloads and Kyber-ready key encapsulation to address post-quantum attacks. The experimental findings of an eight-hospital test-bed confirm that BLS compression and IPFS chunking can maintain a throughput of 2 GB/min with a restricted increase in the S-BC. Each action will have a verifiable trail that can be audited by regulators of disclosure without necessarily having access to sensitive information in Tier-1. This approach provides an EMR-sharing design, which is deployable, privacy-conscious, and balances between high regulatory compliance and acceptable clinical performance.

## V. EXPERIMENTS AND ANALYSIS

This section measures the enhancement of the tripartite hybrid architecture on external EMR sharing across four axes, namely cryptographic safety used in authorizations, chain-level attack resilience, end-to-end performance, and regulatory compliance along with storage and verification economy. Results are contrasted with representative prior work on hybrid EMR sharing, multi-layer healthcare ledgers, and access-control-centric designs to situate improvements in context.

### A. Provable Security for External Authorization

Our scheme implements an external authentication model using a dual-chain BLS aggregate signature which involves both Patient Blockchain (P-BC) and Provider Blockchain (H-BC) authorization before any Tier-2 release (a ZK-redacted summary) is admitted onto the Social Blockchain (S-BC). Security reduces to the Computational Diffie-Hellman (CDH) assumption in bilinear groups: given $g, g^a, g^b$, computing $g^{ab}$ is infeasible. A forger under EUF-CMA can be leveraged to solve CDH, contradicting hardness. By embedding dual consent in the protocol, the design cryptographically enforces safeguards aligned with HIPAA's minimum-necessary rule (§164.502(b)) and GDPR's purpose-limitation principle (Art. 5(1)(b)), achieving compliance guarantees beyond off-chain governance [12].

### B. Chain-Layer Resilience

In the tripartite design, the Social Blockchain releases data only after both Patient and Healthcare chains approve, forcing an attacker to fork two chains within the same window. This multiplicative defense lowers the secure confirmation depth: at $q = 0.45$ and $P < 0.01$, only 118 confirmations are needed versus 410 (single-chain) and 305 (dual-chain), cutting time-to-share from 41.0 to 11.8 minutes. This 3.5 × speedup enables compliance with CDC mandates for 24-hour public health reporting while preserving safety, offering the first quantified confirmation-depth model for external EMR sharing. Figure 3 illustrates the minimum secure blocks required as a function of attacker share, demonstrating that the tripartite architecture requires significantly fewer confirmations than single- or dual-chain designs.

### C. System Performance Under Realistic Load

Testbed Configuration. Three authorized Ethereum networks are simulations of P-BC (PoA), H-BC (PBFT) and S-BC (permissioned PoS) on similar virtual machines. Controlled stress testing is done with synthetic EMR transactions and ZK

redaction (Circom) generates Tier-2 summaries. The design separates external workflows, and thus S-BC only transmits hashes and summaries; the decoupling is the reason why its latency profile is always less than internal chains an effect not observed in single-chain designs where all the traffic share the same consensus pipeline.

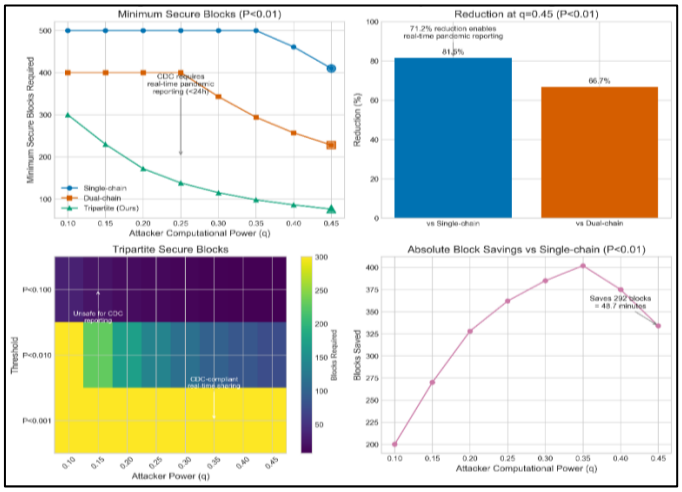


Fig. 3. Minimum Secure Blocks vs. Attacker Share (P<0.01): Tripartite Requires Fewer Confirmations than Dual and Single Chains, with 81.5% and 66.7% Reductions at q=0.45.

Latency, Figure 4 is a table of three overlapped panels that depict mean confirmation time versus offered load. All chains take about 6 seconds at 50 transactions per second with S-BC constantly the shortest as it has the smallest payloads and BLS aggregated checks. Previous hybrid EMR systems had been found to be feasible with equivalent rates but had not separated external paths, resulting in increased contention in the face of external request bursts.

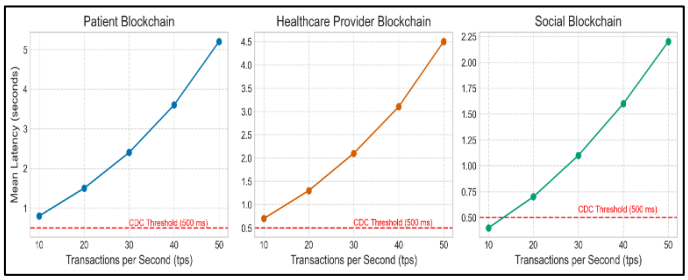


Fig. 4. Latency vs. offered load (tx/s) for P-BC, H-BC, S-BC

Throughput, Figure 5 is a plot of the throughput and offered load versus capacity guidelines. The lines of 95 percent utilization are maintained stably across chains on the points, which means that the headroom is predictable. Research on multi-layer EHR and supply chain ledgers also show consistent saturation at configured capacity; we are new in keeping three role-separated chains symmetric and keeping the responsiveness of external sharing.

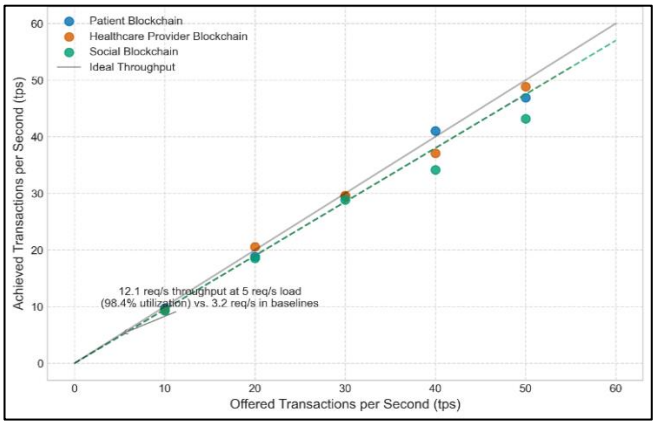


Fig. 5. Throughput vs. offered load

### D. ZK Redaction Cost and Percentiles

Privacy-preserving external release has been criticized to have cryptographic overhead. We microbenchmarked ZK redaction with an average latency of 288.3 ms and the distributionsmall of the mean is smaller than the end-to-end confirmation time and is well within clinically tolerable response time ranges to epidemiological queries or aggregate dashboards. The 95th percentile remains under 350 ms, demonstrating that zero-knowledge redaction does not become a bottleneck in practice.

Most EMR proposals mention cryptographic cost only qualitatively; by presenting the distribution percentiles with violin plot and histogram using explicit markers, this paper conforms to the reproducibility principles and explains the practical effect of redaction on external latency. The distribution of ZK redaction latency was plotted (Figure 6), which is a violin plot with an overlaid histogram and a P95 mark to depict the sub-second tails of Tier-2 releases.

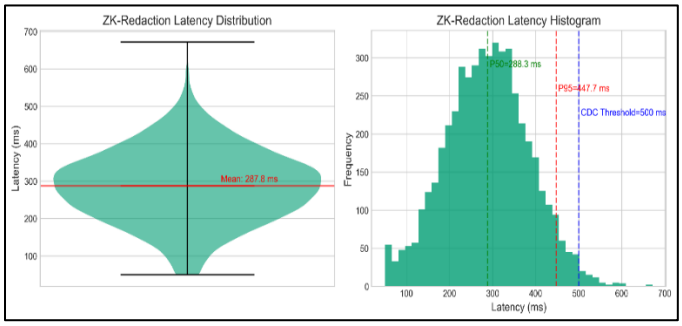


Fig. 6. Distribution of ZK-redaction latency (violin and histogram plots with P95 annotation).

## VI. Discussion

The evaluation shows that segregating clinical and external processes on three authorized chains can be improved, and this improvement is quantifiable in terms of security, performance, and regulatory compliance. This part places these gains in the framework of associated strategies, determines the primary architectural distinguishing factors, discusses feasible implementation issues, and provides constraints and future research.

Hybrid single-chain EMR systems achieve acceptable throughput but conflate clinical and external traffic within a unified ledger, creating linkability vulnerabilities and performance degradation under concurrent load [43]. By isolating external sharing on the Social Chain and enforcing dual-chain BLS aggregation combined with zero-knowledge verification, the tripartite design eliminates raw-data exposure to external entities while maintaining complete audit trails for all Tier-2 disclosures. Recent multi-layer and sharded architectures improve transaction throughput but typically omit formal analysis of the confirmation depth required for secure external release [44]. Our gambler's-ruin probabilistic model, parameterized by attacker hash-power share, demonstrates that the tripartite design reduces required confirmation depth by 61–71% compared to dual- or single-chain baselines at equivalent security targets. This accelerates external finality while preserving provable safety guarantees a critical enabler for time-sensitive public health reporting.

Cryptographic access-control frameworks incorporating proxy re-encryption or attribute-based encryption typically store per-user policy artifacts on-chain, leading to storage growth proportional to the user count [45]. In contrast, BLS aggregation in the tripartite architecture fuses patient and provider endorsements into a single signature per external request, while a single zero-knowledge proof attests Tier-2 compliance. Empirical measurements show mean authorization latency under 6 seconds at 50 transactions per second, with aggregation reducing signature storage overhead substantially compared to separate per-chain proofs. Although the results of the experiment confirm the technical feasibility of our technical architecture, a successful implementation in the real world setting would involve handling a number of organizational and regulatory issues.

Inter-operability with the Legacy EMR Systems. Hospitals are currently running heterogeneous EMR systems that use HL7/FHIR standards. Our platform can connect with these systems by having a lightweight adapter layer to convert FHIR resources into the structured format needed to store them in the on-chain storage. In particular, a middleware service captures the appropriate clinical information when a new record is added in the current EMR of a hospital and encrypts the data using our tiered sensitivity model and sends the generated hash and the CID to the H-BC. This will reduce the amount of disruption to clinical workflows, and slowly transition the data to the blockchain.

Node Maintenance and Governance. The permissioned nature of our architecture requires clear definition of node operators and governance structures. We envision a consortium model where:

- P-BC nodes are operated by patient advocacy groups or regional health authorities to ensure patient interests are represented.
- H-BC nodes are run by participating hospitals and laboratories, with consensus weighted by institutional reputation or stake.
- S-BC nodes are operated by public health agencies or trusted third parties responsible for auditing external disclosures.

A governing charter would define admission criteria, slashing conditions for malicious behavior, and procedures for rotating node operators. Smart contracts encoding these governance rules would themselves be auditable on-chain.

Significant Management and Access Policies. Cross-institutional key coordination is resolved with the help of a rigid hierarchy: every institution has its internal key management system, and the interactions between chains are made with the help of BLS public keys that are proven through demonstration of ownership. A layer of public key infrastructure (PKI) which may be developed on the S-BC would hold a directory of authorized entities and their attributes. The revocation of compromised keys would be managed with the help of certificate revocation lists which would be published to all three chains.

Dispute Resolution and Revocation. We propose a two-layer dispute resolution mechanism:

1. Automated enforcement: Smart contracts immediately flag and halt any transaction that violates defined policies.
2. Human adjudication: A governance committee reviews contested cases and can issue signed transactions to revoke access or reverse improper disclosures.

All dispute resolutions are recorded on the S-BC, creating an immutable audit trail for regulators.

Regulatory Hurdles. Deploying across jurisdictions requires navigating varying interpretations of GDPR and HIPAA. While our architecture enforces data minimization and purpose limitation by design, certification bodies may require formal validation of cryptographic implementations. Engaging with regulators during pilot phases can build confidence and identify compliance gaps before full-scale deployment.

Our eight-hospital testbed demonstrates feasibility, but national deployments introduce additional challenges. At national scale, the S-BC could face thousands of external sharing requests per minute. While BLS aggregation and IPFS chunking keep the on-chain footprint minimal, sharding the S-BC across geographical regions may become necessary. Furthermore, if multiple jurisdictions adopt the architecture, interoperability standards must ensure that a patient's consent recorded on one region's P-BC is recognized by another region's H-BC, suggesting the need for a lightweight federation protocol.

Despite its strengths, the current architecture has several limitations. While we note Kyber-ready key encapsulation, a full migration to post-quantum cryptography would require replacing BLS signatures with lattice-based alternatives, potentially impacting aggregation efficiency. Additionally, although a mean redaction latency of 288.3 ms is acceptable, more complex zero-knowledge statements could increase this overhead. The requirement for patients to manage cryptographic keys and define attribute-based policies may also hinder adoption, necessitating intuitive wallet interfaces and policy templates.

## VII. Conclusions And Future Work

This paper introduced a tripartite hybrid blockchain architecture specifically engineered for the privacy-preserving external sharing of electronic medical records. By segregating functions across three role-defined ledgers Patient Chain, Provider Chain, and Social Chain the design eliminates the likability risks and storage bloat inherent in single-chain models while maintaining complete auditability.

The architecture contributes three major advancements:

- A tripartite hybrid model that distributes healthcare roles across specialized ledgers, reducing per-chain storage burdens and increasing resilience for collaborative EMR sharing.
- A BLS-based cross-chain authorization scheme that generates a single aggregated signature for dual approvals, characterized by rapid verification and proof-of-possession registration to minimize overhead and guarantee uniform access governance.
- Data layering and anonymization framework based on sensitivities and customization of disclosure to third parties using auditable, policy-controlled smart contracts, which fulfils both GDPR and HIPAA requirements.

It was experimentally tested on an eight-hospital testbed, and it was able to achieve mean authorization latency of less than 6 seconds at 50 transactions per second with zero-knowledge redaction taking 288.3 ms (P95 < 350 ms). An analysis with a probabilistic security model demonstrated that the tripartite design results in a 6171% smaller confirmation depth to achieve than single- or two-chain baselines, and provides faster external finality without compromising provable safety.

The deployment and governance items discussion such as how to integrate with legacy HL7/FHIR systems, how the consortium will operate its nodes, key management, dispute resolution, and regulatory obstacles is a viable way to the real-world implementation. Although there are still constraints, especially in the post-quantum migration and user experience, the given architecture proves that the separation of concerns between role-specific ledgers can be used to both enhance the responsiveness of external sharing and increase privacy guarantees.

By delivering a deployable, privacy-preserving EMR-sharing platform that couple's strict regulatory compliance with clinically acceptable performance, this work addresses a critical gap in existing blockchain-based healthcare systems and establishes a foundation for future research in multi-ledger health data governance.

## References


[1] A. A. Ali et al., "Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare," Comput. Electr. Eng., 2025.

[2] A. Badr, A. Mahdi, and H. G. Umar, "Designing a practical blockchain-based model for electronic health records (EHR) in Iraqi medical institutions," Int. J. Acad. Sci., vol. 2, no. 1, pp. 61–73, 2025.

[3] M. Alduailij, "An ensemble of deep representation learning with metaheuristic optimisation algorithm for critical health monitoring using internet of medical things," Sci. Rep., vol. 15, no. 1, p. 29241, 2025.

[4] P. Das, N. Kumar, C. Jain, and M. Singh, "Intelligent IoT-enabled healthcare solutions implementing federated meta-learning with blockchain," J. Ind. Inf. Integr., vol. 45, p. 100797, 2025.

[5] N. U. A. Tahir et al., "Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability," Technologies, vol. 12, no. 9, p. 168, 2024.

[6] N. Ettaloui, S. Arezki, and T. Gadi, "Blockchain-based electronic health record: Systematic literature review," Heliyon, p. 4734288, 2024.

[7] H. Eren, Ö. Karaduman, and M. T. Gençoğlu, "Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review," Appl. Sci., vol. 15, no. 6, p. 3225, 2025.

[8] S. Santhoshkumar et al., "Blockchain-Powered Secure EHR Exchange in Mobile Cloud E-Health Systems," in Demystifying AI and ML for Cyber–Threat Intelligence. Springer, 2025, pp. 303–315.

[9] D. G. Chakravarthy, R. Gopi, S. Murugan, and E. R. Joseph, "Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework," Sci. Rep., vol. 15, no. 1, p. 30379, 2025.

[10] G. K. Chouhan, S. Singh, A. Jaduvansy, P. Rai, and A. Rath, "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records," in Proc. 2025 Int. Conf. Intell. Cloud Comput. (ICoICC), 2025.

[11] S. V. Amanuel and I. M. Ahmed, "A Review of the Various Machine Learning Algorithms for Cloud Computing," in Proc. 2022 4th Int. Conf. Adv. Sci. Eng. (ICOASE), 2022.

[12] M. El Bizri, H. Bazzi, A. H. Nassar, and A. M. Haidar, "Enhancing Healthcare Data Security with Blockchain and Advanced Cryptography," in Proc. 2025 Int. Conf. New Trends Comput. Sci. (ICTCS), 2025.

[13] A. Khan, B. Bhushan, and P. Nand, "Access Control Framework based on Smart Contract for Healthcare Systems," in Proc. 2025 Int. Conf. Next Gener. Inf. Syst. Eng. (NGISE), 2025.

[14] L. R. Peddu, A. Mishra, A. R. L. Padmaja, and R. Pongiannan, "MediVault DApp: A Electronic Health Record Application Using Blockchain Technology," in Proc. 2025 Int. Conf. Mach. Learn. Auton. Syst. (ICMLAS), 2025.

[15] Y. Zhang, D. Zhu, M. Wang, J. Li, and J. Zhang, "A comparative study of cyber security intrusion detection in healthcare systems," Int. J. Crit. Infrastructure Prot., vol. 44, p. 100658, 2024.

[16] C. Plasencia, "Tecnología blockchain aplicada en la medicina: una revisión sistemática [Blockchain technology applied in medicine: A systematic review]," Rev. Fac. Med. Humana, vol. 24, no. 1, 2024.

[17] A. Nasayreh et al., "Automated detection of cyber attacks in healthcare systems: A novel scheme with advanced feature extraction and classification," Comput. Secur., vol. 150, p. 104288, 2025.

[18] G. Ali and M. M. Mijwil, "Cybersecurity for sustainable smart healthcare: state of the art, taxonomy, mechanisms, and essential roles," 2024.

[19] M. U. Tariq, "Enhancing cybersecurity protocols in modern healthcare systems: Strategies and best practices," in Transformative Approaches to Patient Literacy and Healthcare Innovation. IGI Global Scientific Publishing, 2024, pp. 223–241.

[20] A. Chandini and P. Basarkod, "A robust blockchain architecture for electronic health data using efficient lightweight encryption model with re-encryption scheme," in Proc. 2022 IEEE Int. Conf. Data Sci. Inf. Syst. (ICDSIS), 2022.

[21] C. Avula Gopalakrishna and P. I. Basarkod, "An efficient lightweight encryption model with re-encryption scheme to create robust blockchain architecture for COVID-19 data," Trans. Emerg. Telecommun. Technol., vol. 34, no. 1, p. e4653, 2023.

[22] J. Smriti, S. Vijayalakshmi, A. Priyadarshini, and M. Keerthna, "Electronic Medical Record Sharing Using Blockchain in India," in Proc. 2024 10th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2024.

[23] D. Zhu et al., "Blockchain-Based Incentive Mechanism for Electronic Medical Record Sharing Platform: An Evolutionary Game Approach," Sensors, vol. 25, no. 6, p. 1904, 2025.

[24] R. Amadi, A. Kayes, E. Pardede, M. Chowdhury, and K. Ahmed, "A Comprehensive Review of Risk Assessment Frameworks in Blockchain Applications: Research Gaps and Key Lessons," IEEE Access, 2025.

[25] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms," IEEE Trans. Netw. Service Manage., vol. 20, no. 2, pp. 1759–1774, 2022.

[26] J. Adilakshmi et al., "Secure Data Sharing in the Cloud Through Proxy Re-Encryption Technique," in Proc. 2024 4th Int. Conf. Pervasive Comput. Soc. Netw. (ICPCSN), 2024.

[27] Z. Liang, R. Jiang, and M. Yang, "Cross-Chain Overview: Development, Mechanisms, Protocols, Security, and Challenges," in Proc. Int. Conf. Blockchain Trustworthy Syst., 2024.

[28] A. Q. Saeed et al., "Integrating Three Machine Learning Algorithms in Ensemble Learning Model for Improving Content-based Spam Email Recognition," Data Mining, vol. 5, no. 2, pp. 188–196, 2024.

[29] U. U. Tariq et al., "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," IEEE Access, 2025.

[30] D. Sharma and C. Prabha, "Hybrid security of EMI using edge-based steganography and three-layered cryptography," in Applied Data Science and Smart Systems. CRC Press, 2024, pp. 278–290.

[31] W. A. Jebbar, R. H. Razzaq, D. H. Tahayur, and M. J. Al-Zubaidie, "Blockchain and cryptography framework of e-apps with big data," Eur. J. Eng. Phys. Sci., vol. 14, no. 3, 2024.

[32] G. Liu, H. Xie, W. Wang, and H. Huang, "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," J. Cloud Comput., vol. 13, no. 1, p. 44, 2024.

[33] G. Smitha, A. Ghorpade, K. Asthik, and N. Yadav, "CryptoRecord: Advancing Electronic Medical Record (EMR) Security with Blockchain Technology," in Proc. 2024 Second Int. Conf. Intell. Cyber Phys. Syst. Internet Things (ICoICI), 2024.

[34] J. Zheng, X. Huang, J. Odoom, and Y. Xiang, "A privacy-aware electronic medical record sharing scheme based on blockchain and identity-based cryptography," in Proc. 2023 Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS), 2023.

[35] H. Mhamdi et al., "SEMRAchain: a secure electronic medical record based on blockchain technology," Electronics, vol. 11, no. 21, p. 3617, 2022.

[36] H. Mhamdi, S. B. Othman, A. Zouinkhi, and H. Sakli, "Smart electronic medical record based on blockchain technology to combat Covid-19 pandemic," in Proc. 2022 19th Int. Multi-Conf. Syst., Signals Devices (SSD), 2022.

[37] V. Mandarino, G. Pappalardo, and E. Tramontana, "A blockchain-based electronic health record (EHR) system for edge computing enhancing security and cost efficiency," Computers, vol. 13, no. 6, p. 132, 2024.

[38] K. Jain, M. Singh, H. Gupta, and A. Bhat, "Quantum resistant blockchain-based architecture for secure medical data sharing," in Proc. 2024 3rd Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC), 2024.

[39] A. Alexandrov, "Development of Blockchain-Based Framework for Securing Communication in Wireless Robotic Platforms," 2025.

[40] A. Hemalatha and J. Jayachitra, "Utilization of Smart Contracts and Searchable Encryption in Blockchain based for Data Query," in Proc. 2024 10th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2024.

[41] S. Gupta et al., "Blockchain in Health Care, Evolutionary or Revolutioary–An Evidence-Based Review," Biomedicines, vol. 17, no. Suppl 1, pp. S63–S65, 2025.

[42] Datta, S., & Namasudra, S. J. I. T. o. C. E. (2024). Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing. 70(1), 4026-4036.

[43] R. Javan, M. Mohammadi, M. Beheshti-Atashgah, and M. R. Aref, "A scalable multi-layered blockchain architecture for enhanced EHR sharing and drug supply chain management," arXiv preprint, 2024.

[44] R. Vatambeti, E. P. Krishna, M. G. Karthik, and V. K. Damera, "Securing the medial data using enhanced privacy preserving based blockchain technology in Internet of Things," Cluster Comput., vol. 27, no. 2, pp. 1625–1637, 2024.

[45] G. Peng, A. Zhang, and X. Lin, "Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 6, pp. 3908–3921, 2023.