International Journal of Advanced Engineering Application (IJAEA)
Volume 3 Issue 5 May 2026
ISSN :3048-6807

Blockchain-Based Decentralised Electronic Health Record Management

Rahul Tiwari, Ananya Mishra. Vikram Singh Rajput
Department of Computer Science and Engineering, Harcourt Butler Technical University, Kanpur, Uttar Pradesh

Abstract

Electronic Health Records (EHR) fragmentation across multiple healthcare providers represents a critical systemic failure in India's health information infrastructure, resulting in unnecessary repeat diagnostic testing, medication errors from incomplete clinical histories, delayed emergency treatment due to inaccessible records, and significant patient burden from manual medical record transportation. The Ayushman Bharat Digital Mission (ABDM), launched in 2021, provides a regulatory and infrastructure framework for unified health ID-based EHR sharing, but the centralised Health Data Fiduciary architecture raises data sovereignty and single-point-of-failure concerns. This study presents the design, implementation, and performance evaluation of a permissioned blockchain-based EHR management system using Hyperledger Fabric 2.4 that enables patient-controlled, cryptographically auditable medical data sharing across a multi-provider consortium without relying on a central data authority. The architecture implements a three-channel design — patient demographics, clinical records, and consent management — with ABAC (Attribute-Based Access Control) enforcing granular patient consent at the data element level. Off-chain IPFS storage of large DICOM imaging files with on-chain content-addressed hash anchoring addresses the blockchain storage scalability limitation. Chaincode smart contracts implement ABDM FHIR R4 data exchange standards, enabling interoperability with existing hospital HMIS systems via REST API adapters. Performance benchmarking on a four-organisation Hyperledger Fabric network deployed on AWS EC2 instances demonstrates transaction throughput of 842 TPS (ENDORSEMENT + ORDERING + COMMIT) with 2.1-second end-to-end latency at 64 concurrent peer nodes, exceeding the 600 TPS minimum requirement for a district-level (500,000 patient) deployment scenario. Security analysis confirms resistance to Sybil attacks, 51% attacks (permissioned consensus), and DICOM file tampering via SHA-256 content addressing.

Keywords: *blockchain, electronic health records, Hyperledger Fabric, FHIR, interoperability, patient data sovereignty, ABDM, smart contracts, IPFS, healthcare informatics*

1. Introduction

India's healthcare delivery system, spanning over 25,000 public hospitals, 70,000 private hospitals, and 1.4 million registered physicians, generates an estimated 3.8 billion clinical encounters annually, each producing medical data of potential clinical value to subsequent healthcare providers. The overwhelming majority of this clinical data remains siloed within individual provider systems — paper records in rural primary health centres, proprietary HMIS databases in corporate hospitals, and portable digital files carried by patients on USB drives or WhatsApp-forwarded photographs. This fragmentation imposes a quantifiable clinical burden: a 2022 AIIMS New Delhi study estimated that 34% of specialist referral consultations require repeat laboratory investigations due to unavailability of existing results, at an estimated nationwide redundant testing cost of INR 11,800 crore annually.

The Ayushman Bharat Digital Mission's Health Account (ABHA) initiative provides a 14-digit Unified Health ID as the linking mechanism for distributed health records across consenting providers. While ABDM's Personal Health Records (PHR) architecture represents a significant policy advance, the proposed Health Data Fiduciary model — where a licensed centralised entity manages consent artefacts and record linkage — introduces a single point of failure for data sovereignty and privacy in a context where health data monetisation risks are significant. A decentralised architecture that preserves patient control over record sharing without a trusted central intermediary offers an alternative that aligns with the Supreme Court's right to privacy jurisprudence established in Justice K.S. Puttaswamy v. Union of India (2017) while achieving the interoperability goals of ABDM.

Permissioned blockchain platforms — particularly Hyperledger Fabric, with its configurable consensus mechanisms, channel-based privacy partitioning, and mature enterprise tooling — have been extensively explored for EHR management in the international literature. However, Indian deployment-specific requirements — ABDM FHIR R4 compliance, integration with HMIS systems from vendors such as Hims, Insta, and eVital, multilingual (Hindi/regional) patient interface, and performance adequate for district health authority deployments — have not been addressed in published systems. This study contributes an ABDM-compliant Hyperledger Fabric EHR architecture with demonstrated performance at district-scale load conditions.

2. System Architecture and Design

2.1 Network Topology and Channel Design

The proposed Hyperledger Fabric network organises participating healthcare organisations (hospitals, diagnostic labs, pharmacies, insurance providers, and the district health authority) as Membership Service Provider (MSP) members of a permissioned consortium. Network governance — adding new organisations, updating chaincode versions, modifying channel configuration — is managed through Hyperledger Fabric's native channel configuration transaction mechanism with majority-rule signature policy across founder organisations. Three channels partition data by sensitivity: Channel A (Demographic) stores ABHA-linked patient identity and provider registration; Channel B (Clinical) stores FHIR R4 clinical resources (Observation, Condition, MedicationRequest, DiagnosticReport); Channel C (Consent) stores patient consent artefacts governing channel B access. This channel architecture ensures that insurance organisations, for example, have access only to diagnosis codes in Channel B with patient consent from Channel C, not to raw clinical notes or medication histories.

2.2 Off-Chain DICOM Storage via IPFS

DICOM imaging files (CT scans, MRI, X-rays) average 50-500 MB per study and cannot be stored on-chain without prohibitive storage costs and throughput degradation. The architecture implements an IPFS (InterPlanetary File System) cluster deployed at four geographic nodes (Delhi, Mumbai, Kolkata, Chennai) as the off-chain storage substrate. DICOM files are encrypted with the patient's AES-256 key prior to IPFS upload; the IPFS Content ID (CID) and encrypted AES-256 key (itself encrypted with the patient's RSA-2048 public key) are stored on Channel B as a DiagnosticReport FHIR resource. Authorised providers retrieve the DICOM file by resolving the CID from IPFS, decrypting the AES key using the patient's delegated key share, and decrypting the DICOM data. This pattern ensures that even IPFS node operators cannot access unencrypted imaging data.

2.3 Smart Contract (Chaincode) Design

Chaincode is implemented in Go (Hyperledger Fabric Node.js chaincode was evaluated but showed 30% lower throughput in preliminary testing). Three chaincode modules implement the core business logic: PatientRegistry chaincode manages ABHA identity verification and provider authorisation; ClinicalRecord chaincode implements FHIR R4 Create/Read/Update/Delete (CRUD) operations with integrated consent verification via cross-channel query to Channel C before permitting any record access; ConsentManager chaincode implements granular consent artefact creation, modification, and revocation with ABAC enforcement. All chaincode transactions are logged to an immutable audit trail on Channel B, enabling forensic reconstruction of complete record access history for regulatory compliance and breach investigation.

3. Implementation and Performance Benchmarking

The Hyperledger Fabric 2.4 network was deployed on AWS EC2 using a four-organisation topology (District Health Authority, Government Medical College Hospital, Private Tertiary Hospital, Diagnostic Chain) with two peers per

organisation (eight total peers), one orderer node per organisation (Raft consensus, four orderers), and a dedicated Certificate Authority per organisation. Each peer node ran on a t3.xlarge instance (4 vCPU, 16 GB RAM); orderer nodes on t3.medium instances. CouchDB was used as the state database to support rich FHIR resource queries (ABHA ID lookup, date-range clinical record retrieval). Network deployment and chaincode installation were automated via Ansible playbooks versioned in GitLab CI/CD.

Performance benchmarking used Hyperledger Caliper 0.5 with a synthetic workload comprising 60% read operations (FHIR record query by ABHA ID), 30% write operations (new clinical record submission), and 10% consent operations (consent artefact create/update). Benchmark results under varying concurrent transaction submission rates are shown in Table 1 and Figure 2. Peak throughput of 842 TPS is achieved at 64 concurrent clients with 2.1-second end-to-end latency (endorsement + ordering + commit). Throughput saturates above 64 clients due to orderer CPU contention — adding a second orderer per organisation in a 16-orderer configuration improves peak throughput to 1,240 TPS, adequate for state-level (5 million patient) deployment.

Concurrent Clients	TPS	Avg. Latency (s)	P95 Latency (s)	Error Rate (%)
4	112	0.4	0.7	0.00
8	218	0.5	0.9	0.00
16	421	0.8	1.4	0.00
32	638	1.2	2.1	0.00
64	842	2.1	3.8	0.01
128	834	4.2	7.6	0.08

Table 1. Hyperledger Fabric network performance benchmarks (Caliper 0.5, 4-organisation topology, mixed 60/30/10 read/write/consent workload)

3.1 Security Analysis

The system's security posture was evaluated against the OWASP Top 10 web application vulnerabilities, NIST SP 800-111 storage encryption standards, and blockchain-specific threat vectors including Sybil attack, 51% consensus attack, and chaincode vulnerability injection. The permissioned Raft consensus mechanism eliminates the 51% attack vector applicable to public blockchains: an adversary would need to compromise the private keys of a majority of orderer nodes — all operated by independently governed healthcare organisations — to manipulate the transaction ordering. Penetration testing using OWASP ZAP on the REST API gateway identified two medium-severity findings (insufficient rate limiting on the consent API and missing HSTS headers) that were remediated before pilot deployment. SHA-256 content addressing of IPFS-stored DICOM files provides cryptographic tamper detection: any modification to a stored imaging file changes the CID, rendering the on-chain reference invalid and triggering a data integrity alert.

4. Discussion

The 842 TPS peak throughput achieved on the four-organisation testbed exceeds the 600 TPS minimum requirement derived from district-level load modelling (500,000 registered patients, 2,000 daily clinical encounters, peak load factor 5x) by 40%, providing adequate headroom for load spikes during mass health campaigns. The 2.1-second end-to-end latency is acceptable for non-emergency record access scenarios (specialist referral, prescription dispensing) but may be marginal for emergency department applications requiring sub-second patient history retrieval. Future

optimisation will investigate Hyperledger Fabric's event-driven ledger pre-fetch mechanism, which can reduce perceived latency for frequently accessed patient records to below 500 ms by proactively pushing updated records to peer local caches based on scheduled appointment data.

Comparison with equivalent centralised SQL EHR database query latency (measured on AWS RDS PostgreSQL r5.xlarge) reveals that blockchain Channel B FHIR record queries are approximately 3.2x slower than centralised queries for single-record lookups, primarily due to the CouchDB state database's JSON document query overhead and multi-peer endorsement roundtrip. However, for multi-provider record aggregation queries — retrieving all FHIR Observations for a patient across four organisations — the blockchain architecture eliminates the centralised aggregation step entirely, yielding equivalent or faster response times versus centralised architectures that require inter-system API federation.

The ABDM FHIR R4 interoperability testing with four HMIS vendor systems (Hims, Insta, eVital, Practo) revealed that all four systems could exchange DiagnosticReport, MedicationRequest, and Condition resources via the REST API adapter without modification to the vendor HMIS, validating the adapter's translation layer design. The Observation resource — used for vital signs and laboratory results — required minor mapping customisation for each vendor's proprietary observation code system to the LOINC terminology mandated by ABDM FHIR profile.

5. Conclusion

This study presents the design, implementation, and comprehensive performance evaluation of a Hyperledger Fabric 2.4 blockchain-based EHR management system tailored to India's ABDM regulatory framework and multi-provider healthcare network context. The three-channel architecture with ABAC consent enforcement, IPFS off-chain DICOM storage, and FHIR R4 interoperability achieves 842 TPS throughput and 2.1-second end-to-end latency — adequate for district-scale deployment — while providing cryptographic data integrity assurance, immutable audit trail, and patient-controlled granular consent management absent from centralised EHR architectures.

The system's ABDM FHIR R4 compliance and demonstrated interoperability with four major HMIS vendor systems positions it for integration into India's National Digital Health Ecosystem. A pilot deployment covering 12 healthcare facilities in Kanpur district is planned for the second half of 2025 under the National Health Authority's ABDM Innovation Sandbox programme. Future research will address emergency access override mechanisms, zero-knowledge proof-based insurance claim verification, and federated machine learning on the privacy-preserved blockchain dataset for population health analytics.

References

[1] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. IOTDI 2016.

[2] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare. npj Digital Medicine, 1, 38.

[3] Ministry of Health and Family Welfare, Government of India. (2021). Ayushman Bharat Digital Mission — Operational Guidelines. New Delhi: MoHFW.

[4] Tiwari, R., & Mishra, A. (2022). Hyperledger Fabric for EHR management: Architecture and performance. Journal of Medical Systems, 46(8), 52.

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[6] Androulaki, E., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. EuroSys 2018.

[7] Rajput, V. S., & Bhatia, K. (2023). Patient data sovereignty in Indian digital health: Legal and technical perspectives. Journal of Health Informatics in Developing Countries, 17(1).

[8] HL7 International. (2019). FHIR R4 Specification. https://hl7.org/fhir/R4/

[9] Joshi, S. C., & Kumar, A. (2021). IPFS-based decentralised storage for healthcare imaging. IEEE Access, 9, 132145-132158.

[10] National Health Authority. (2022). ABDM Health Data Management Policy. New Delhi: NHA.

[11] Benet, J. (2014). IPFS — Content addressed, versioned, P2P file system. arXiv:1407.3561.

[12] OWASP Foundation. (2023). OWASP Top 10. https://owasp.org/top10