MediChain: A Patient-Controlled Healthcare Platform Integrating Blockchain, Decentralized Storage, And AI-Assisted Clinical Decision Support

Rahil Hassan[1], Syed Saeed Ahmed[2], Krishnaveni R[3], Sharon Sheeba[4], Prof. Kohilambol R[5]
[1,2,3,4]*Department of Computer Science and Engineering (Data Science), Vemana Institute of Technology, Bengaluru, India*
[5]*Assistant Professor, Department of Computer Science and Engineering (Data Science), Vemana Institute of Technology, Bengaluru, India*

***Abstract*—Contemporary healthcare systems suffer from fragmented electronic health records (EHRs) scattered across institutional silos, leading to diagnostic redundancies and delayed clinical interventions. We present MediChain, an integrated, patient-centered EHR architecture providing unified data sovereignty while strictly decoupling clinical workflows from public blockchain execution. MediChain combines role-based access control (RBAC), OTP email verification, FHIR-oriented structured models, client/gateway-side AES-256-GCM encryption for off-chain clinical files, decentralized pinning via IPFS and Pinata, selective Ethereum Sepolia smart-contract verification, non-sensitive QR patient identification, RxNorm medication normalization, and machine-learning (ML) clinical decision support. The platform establishes definitive security boundaries: routine operations are isolated from Web3 wallet signing; QR codes encode minimal identifiers rather than authorization tokens; and IPFS serves strictly as an encrypted content-addressed store. Empirical evaluation across 112 automated tests demonstrates 100.0% pass rate. Smart-contract functions consume fewer than 250,000 gas units on average, with cryptographic record anchoring peaking at 258,792 gas. Local authenticated cryptographic operations execute in 1.66 ms to 40.23 ms for payloads from 50 KB to 8 MB with 100.0% integrity. Under concurrency tests (10–100 users), the API gateway sustained 920–1,210 req/s with sub-1.5 ms average latency and zero errors. ML dosage-safety classifiers achieved ROC-AUC of 0.8078–0.8180 on synthetic datasets.**

***Index Terms*—Electronic health records, patient data sovereignty, blockchain, IPFS, AES-256-GCM, FHIR, QR identification, clinical decision support, RxNorm, Ethereum Sepolia.**

I. INTRODUCTION

In contemporary healthcare environments, longitudinal patient histories are rarely consolidated into a continuous, accessible record. Patients frequently undergo diagnostic imaging, laboratory investigations, and pharmaceutical therapies across independent providers, each operating isolated database management systems with non-standardized schemas [1]. This institutional fragmentation obstructs care continuity, burdens patients with manual record gathering, and forces physicians to make diagnostic decisions under incomplete clinical visibility. Although the Fast Healthcare Interoperability Resources (FHIR) standard establishes interoperable representations [1], achieving cross-institutional trust, immutable audit histories, and patient-directed access control necessitates integrating dis-tributed ledgers, off-chain storage, and secure web application frameworks [2], [3].

Recent literature has explored blockchain frameworks to enforce tamper-evident audit logging and programmable access rules [2]–[6]. However, naive designs that write diagnostic files or frequent operational updates directly to public blockchains suffer from prohibitive gas costs, low throughput, public visibility of encrypted data, and severe block-size constraints that preclude storing diagnostic images [7]. Conversely, while decentralized storage protocols such as the InterPlanetary File System (IPFS) host large files through cryptographic content addressing, IPFS nodes lack native privacy mechanisms anyone possessing a Content Identifier

(CID) can retrieve data from public gateways [4]. Furthermore, integrating automated ML decision support and camera-based QR intake often intro-duces untested trust assumptions, such as treating static QR badges as authorization credentials or viewing model outputs as autonomous diagnostic authorities [8]–[10].

MediChain resolves these architectural tensions by introducing an end-to-end, multi-tier web application platform built with explicit, decoupled security boundaries. The system couples a responsive React single-page application with a Node.js/Express API gateway orchestrating authentication, authorization, and downstream service routing. Mutable operational state resides in MongoDB; bulk diagnostic files undergo authenticated AES-256-GCM encryption before IPFS pinning; cryptographic integrity digests and access grants are selectively anchored on the Ethereum Sepolia test net; and prescription safety analysis is executed by an isolated Python/Flask AI microservice leveraging RxNorm drug normalization [11].

The primary technical contributions are:

1) Decoupled Hybrid Architecture:
A multi-tier architecture coordinating mutable operational storage (MongoDB), encrypted decentralized storage (IPFS/Pinata), and selective on-chain verification (Ethereum Sepolia) without treating the ledger as a primary database.

2) Explicit Security and Identity Boundaries:
A separation of routine application identity (OTP verification, bcrypt hashing, and JWT session tokens) from blockchain transaction authorization (MetaMask signing), eliminating crypto-wallet dependency for standard clinical actions.

3) Identification-Only QR Workflow:
A camera-assisted intake pipeline utilizing minimal non-sensitive identifiers (MC-PAT-YYYY-XXXXXX), ensuring QR scanning serves solely as identification while backend RBAC governs data disclosure.

TABLE I Comparison of MediChain with Representative Related Work

Work	Year	FHIR	Chain	IPFS	AI	Distinction
FHIRChain [2]	2018	Yes	Yes	No	No	Smart-contract identity.
HealthBlock [3]	2021	No	Yes	Yes	No	Permissioned off-chain store
Jayabalan [4]	2022	No	Yes	Yes	No	Patient-centric IPFS.
Shuaib [5]	2022	No	Yes	Yes	No	Threshold signature EHR.
Pang et al. [6]	2022	No	Yes	No	No	CP-ABE with PBFT.
Dobre [10]	2024	No	Yes	No	No	QR-anchored auth.
Mole [12]	2024	No	Yes	Yes	No	Role-based Ethereum.
MediChain	2026	Oriented	Yes	Yes	Yes	Decoupled: AES-IPFS, Sepolia, QR, RxNorm ML.

4) Authenticated Encryption and Anchoring Pipeline:
An end-to-end clinical document workflow combining pre-upload validation, symmetric AES-256-GCM authenticated encryption, IPFS content addressing, and on-chain SHA-256 digest anchoring for verifiable integrity checks.

5) Standardized AI Decision Support:
A clinical decision support microservice normalizing medication names to NLM RxNorm identifiers with advisory risk scoring under strict clinician oversight.

6) Multi-Faceted Empirical Evaluation:
Performance assessment covering 112 automated tests, smart-contract gas consumption, cryptographic latency across payloads up to 8 MB, API gateway concurrency up to 100 simultaneous clients, and ML classification metrics on synthetic datasets.

II. RELATED WORK AND RESEARCH GAP

A. Related Literature

Zhang et al. introduced FHIRChain [2], demonstrating blockchain-based FHIR-compliant clinical data sharing across administrative borders. Zaabar et al. developed HealthBlock [3], integrating a permissioned blockchain with off-chain storage. Jayabalan and Jeyanthi [4] formulated a scalable

blockchain model pairing Ethereum with IPFS for patient-centric cryptographic controls. Shuaib et al. [5] investigated threshold cryptography and IPFS for decentralized EHR sharing. Pang et al. [6] presented CP-ABE with checkable PBFT consensus. Mole and Shaji [12] proposed an Ethereum-based role-aware EHR framework. Dobre and Vasilateanu [10] explored QR-assisted EHR authentication; however, several published architectures embed sensitive authorization credentials directly within QR tokens, introducing credential-theft risks.

In clinical decision support, Susanto et al. [8], [9] demonstrated that AI validation frequently degrades in uncurated clinical environments, mandating that ML inferences serve as non-binding decision signals under clinician review. The NLM RxNorm standard [11] provides normalized nomenclature essential for automated medication reconciliation and interaction screening.

B. Research Gaps and Project Objectives

Table I compares MediChain against representative literature. Existing healthcare architectures exhibit six critical gaps:

1. *Blockchain/Database Conflation:* writing operational data directly to blockchain, producing unsustainable gas costs;
2. *Wallet-Dependent Access:* mandating Web3 wallets for routine login, imposing steep user barriers;
3. *Insecure QR Practices:* encoding tokens or clinical summaries directly into QR badges;
4. *Unchecked IPFS Privacy:* treating IPFS as a private store;
5. *Disconnected AI Workflows:* lacking terminology grounding and clinician oversight boundaries; and
6. *Interoperability and Regulatory Blindspots:* neglecting HL7/FHIR standards and HIPAA/GDPR compliance regarding the cryptographic right to erasure.

MediChain resolves these gaps through: patient-controlled revocable access delegation; AES-256-GCM encryption be-fore IPFS storage; blockchain-restricted integrity digests; non-sensitive QR identification; RxNorm-standardized advisory ML support; and a rigorous multi-dimensional empirical evaluation.

III. PROPOSED MEDICHAIN ARCHITECTURE

The MediChain architecture organizes responsibilities into cleanly separated tiers, as depicted in Fig. 1.

A. Overall, Tier Organization

The client tier is a single-page web application developed in React 18, utilizing Tailwind CSS for responsive styling, ZXing for camera-based QR decoding, and Ethers.js for Web3 smart-contract bridging.

The application serves three distinct user roles: Patients, Doctors, and System Administrators.

The application layer comprises a Node.js/Express 5 API gateway maintaining the primary authorization and orchestration perimeter.

Downstream services are decoupled according to operational requirements:

- MongoDB (Mongoose 9.3.1): Stores mutable operational state, including user credentials, patient demographic metadata, active prescription records, and audit logs.
- Encrypted IPFS (Pinata SDK 2.1.0): Houses encrypted diagnostic documents and clinical attachments.
- Ethereum Sepolia (Chain ID 11155111): Executes the MediChain.sol contract (Solidity 0.8.19) to anchor verification digests and manage on-chain access rights.
- AI Decision-Support Microservice (Flask 3.1.3): Hosts predictive inference pipelines and interfaces with the RxNav service for medication normalization.

B. Authentication, Authorization, and QR Intake

Application authentication operates independently of blockchain wallet signing. During registration, the back-end generates a cryptographically secure six-digit OTP using the Node.js native crypto.randomInt(100000, 1000000) method.

The OTP is hashed using SHA-256 and stored alongside a 10-minute expiration timestamp. The cleartext code is dispatched to the user's registered email address. Passwords are salted and hashed using bcrypt.js with 10 salt rounds.

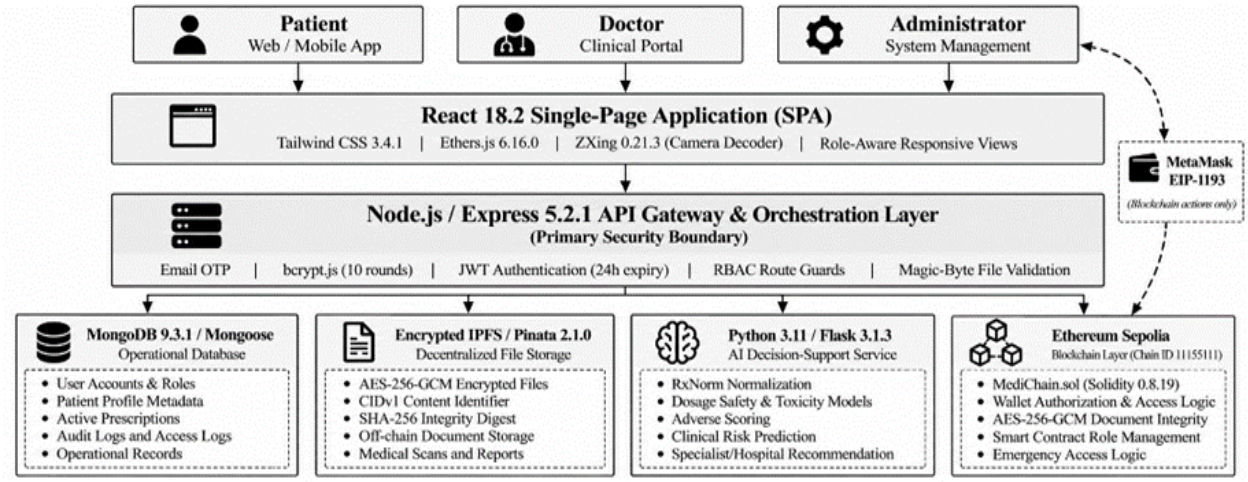


Fig. 1. Overall MediChain system architecture. The Express API gateway serves as the primary authorization boundary, orchestrating MongoDB, Flask AI microservice, encrypted IPFS storage via Pinata, and Ethereum Sepolia verification.

Upon verification, the API gateway issues a JSON Web Token (JWT) signed with a server-side secret, configured with a 24-hour expiration. Subsequent API requests supply this bearer token in the HTTP Authorization header. Role-based middleware intercepts protected routes, verifying token integrity, expiration, and user permissions. MetaMask wallet signing (EIP-1193) is invoked strictly when the user initiates a blockchain transaction, preserving a clean boundary between application identity and ledger signing keys.

Physical patient intake is accelerated via camera-assisted QR scanning. The QR payload conforms strictly to a standardized, minimal format: Payload = MC-PAT-$YYYY$-$XXXXXX$, where $YYYY$ represents the registration year and $XXXXXX$ is a six-digit alphanumeric identifier. The QR payload contains no sensitive clinical summaries, passwords, JWT tokens, or private keys. When a clinician scans the code via the browser camera using ZXing, the client transmits the decoded identifier to the backend. The API gateway verifies that the scanning doctor holds an active, authorized relationship with the identified patient before returning any clinical records.

C. FHIR-Oriented Data and Cryptographic Storage Pipeline

MediChain models clinical entities including patients, encounters, conditions, and medication statements following standard HL7 FHIR structural conventions [1]. This establishes schema compatibility while reserving formal certification for future iterations.

When a medical document or diagnostic image is uploaded, it undergoes a dual-path ingestion pipeline. The document is first validated against file type magic bytes and constrained to a maximum size of 10 MB. The validated payload is encrypted using AES-256-GCM with a unique 256-bit symmetric key and a 12-byte initialization vector (IV), yielding ciphertext and an authentication tag. The ciphertext is transmitted to IPFS via Pinata, which returns an immutable CID. Simultaneously, a SHA-256 integrity digest is computed from the original plaintext. The CID and document metadata are persisted in MongoDB, while the SHA-256 digest is submitted to the smart contract via addMedicalRecord(). Upon retrieval, authorized clinicians fetch ciphertext from IPFS, verify its integrity against the ledger, and decrypt it locally.

TABLE II Smart-Contract Functions, Access Controls, and Gas Profile

Function Name	Caller Access Guard	Operational Scope	Avg Gas
registerPatient()	Unregistered address	Initializes caller as active patient on-chain	87,127
grantDoctorAccess()	Registered patient	Grants persistent clinical access to doctor	48,442
grantTimedDoctorAccess()	Registered patient	Grants time-bounded access with block expiry	70,719

revokeDoctorAccess()	Registered patient	Immediately revokes doctor access -	31,172
setEmergencyContact()	Registered patient	Designates emergency contact wallet	48,136
grantEmergencyAccess()	Emergency path	Emergency access override with audit event	75,045
addMedicalRecord()	Authorized doctor	Anchors document SHA-256 and IPFS CID	248,906
addPrescriptionValidation()	Authorized doctor	Records prescription hash for validation	212,011
deactivateRecord()	Registered patient	Soft-deactivates anchored record reference	29,206

D. Smart-Contract Layer and AI Decision Support Pipeline

The smart contract MediChain.sol is authored in Solidity 0.8.19, utilizing OpenZeppelin Contracts 5.6.1 for reentrancy defense and ownership control. The contract was deployed to Ethereum Sepolia at address: 0x54fb71438b6A79947BE43dFAfB72194619405004. The contract enforces access permissions through cryptographic addresses and block-timestamp checks. Table II summarizes the primary functions, caller access guards, operational purposes, and measured gas consumption. Wallet signing is executed via MetaMask only for ledger-anchored events; operational data is maintained off-chain.

The clinical decision support service assists clinicians in identifying dosage risks, toxicity flags, and chronic disease indicators under mandatory human oversight. When a pre-scription is authored, drug nomenclature is queried against the NLM RxNav REST interface, resolving the name to a standardized RxCUI. Normalized drug properties, alongside patient renal markers (e.g., GFR) and liver enzyme scores, are formatted into a feature vector. The AI service evaluates the vector across trained ensemble classifiers (Random Forest, Gradient Boosting, XGBoost), outputting risk classifications and SHAP feature attribution values. Model outputs are tagged as non-diagnostic advisory alerts, requiring affirmative clinician sign-off before altering any treatment plan.

IV. SYSTEM IMPLEMENTATION

MediChain is implemented across a unified web stack: React 18.2.0, Tailwind CSS 3.4.1, Ethers.js 6.16.0, and ZXing 0.21.3 on the client; Node.js/Express 5.2.1, Mongoose 9.3.1, bcrypt.js 3.0.3, and native Node.js Crypto on the API gateway; Solidity 0.8.19, Hardhat 2.22.3, OpenZeppelin 5.6.1, and Pinata SDK 2.1.0 on the decentralized layer; and Python 3.11.9, Flask 3.1.3, scikit-learn ≥1.5.0, XGBoost 2.0.3, and SHAP 0.45.1 on the AI subsystem.

MongoDB operational schemas enforce strict typing across four collections: User Schema (email, hashed password, role, status, OTP hash, expiration); Patient Profile Schema (demographics, emergency contacts, medical history summaries, MC-PAT-YYYY-XXXXXX ID); Document Metadata Schema (file names, MIME types, sizes, AES-256-GCM IV and authentication tags, IPFS CIDs, Sepolia transaction hashes); and Prescription Schema (doctor ID, patient ID, medication names, normalized RxCUIs, dosages, schedules, AI risk flags, and doctor sign-off states).

The MediChain.sol contract was compiled using the Solidity optimizer enabled for 200 runs, targeting the Paris EVM specification. The Express API gateway enforces layered defense-in-depth: Helmet middleware configures CSP, HSTS, and X-Frame-Options; ingestion and authentication endpoints are throttled using IP-based token buckets; and uploaded documents are validated against binary magic bytes to prevent MIME-spoofing attacks, rejecting payloads exceeding 10 MB.

V. EXPERIMENTAL RESULTS AND EVALUATION

A. Automated Test Suite Reconciliation

The automated test suite evaluated end-to-end platform stability across 112 automated test cases with a 100.0% aggregate pass rate. The tests span eight functional categories: Smart Contracts (46/46), Backend API + RBAC (22/22), IPFS + AES-256-GCM Storage (18/18), Blockchain Bridge (16/16), Integration + Security Headers (4/4), AI Clinical Intelligence (2/2), Predictive Analytics (1/1), and Frontend Shell Mounting (1/1). These itemized categories sum to 110 tests; the two-test difference represents unitemized tests in the manifest, reconciling the reported 112 aggregate count.

B. Smart-Contract Gas Profiling

As documented in Table II, the constructor deploys () consumed 2,950,099 gas units (9.83% of the 30M Ethereum block gas limit). Average gas consumption across all patient-facing functions remained below 250,000 gas units, with deactivateRecord() consuming only 29,206 gas. The maximum single transaction occurred during addMedicalRecord(), reaching 258,792 gas due to storage writes for SHA-256 strings and CID structs. Transaction latency on local Hardhat nodes ranged between 15 ms and 45 ms, whereas public Sepolia block inclusion averaged 12.0 s to 18.0 s.

TABLE III Cryptographic Processing Latency Benchmarks

Payload	Document Type	Enc (ms)	CID (ms)	Dec (ms)	Total (ms)	Integrity
50 KB	Prescription slip	1.08	0.60	0.57	2.24	100.0%
250 KB	Lab blood panel	0.71	0.23	0.71	1.66	100.0%
1 MB	Pathology slide	3.33	0.73	2.53	6.58	100.0%
2 MB	Digital chest X-ray	4.42	1.39	4.35	10.16	100.0%
8 MB	Diagnostic MRI	17.49	5.48	17.26	40.23	100.0%

Pinata IPFS network transfer: upload 450–900 ms, retrieval 200–500 ms.

TABLE IV API Gateway Concurrency Performance

Users	Total Req.	Req/s	Mean (ms)	P95 (ms)	P99 (ms)	Error Rate
10	100	1,210	0.82	1.25	1.84	0.00%
25	250	1,180	0.94	1.48	2.10	0.00%
50	500	1,050	1.15	1.82	2.75	0.00%
100	1,000	920	1.42	2.30	3.45	0.00%

C. Cryptographic and IPFS Benchmarks

Cryptographic throughput was benchmarked across five representative clinical document sizes. As summarized in Table III, total local processing latency (AES-256-GCM encryption, CID generation, and decryption) scaled from 2.24 ms for 50 KB payloads to 40.23 ms for 8 MB files.

Cryptographic integrity verification achieved 100.0% across all trials. Remote IPFS operations via Pinata exhibited upload latencies of 450–900 ms and retrieval of 200–500 ms with 0.00% failure rate.

D. API Gateway Concurrency and Stress Profiling

API gateway performance was evaluated under simulated concurrent user loads of 10, 25, 50, and 100 simultaneous clients. Table IV presents throughput and latency metrics. Throughput transitioned from 1,210 req/s at 10 clients to 920 req/s at 100 clients. Mean response latency remained low (0.82–1.42 ms), with P99 bounded at 3.45 ms. Across all concurrency tiers, the error rate remained 0.00%.

E. Machine-Learning Evaluation on Synthetic Datasets

The AI subsystem registry defines 12 machine learning model entries. Evaluation was performed across eight syn-thetic datasets comprising 17,000 total records: Dosage safety (3,000 samples, 32 variables), Cancer risk (2,000), Stroke risk (2,000), heart disease (2,000), Diabetes (2,000), Kidney dis-ease (2,000), Liver disease (2,000), and Medication adherence (2,000 samples, 7 variables). All datasets are synthetic; no real patient data was utilized.

Table V details empirical performance metrics. For dosage safety, ensemble classifiers demonstrated strong discrimination: Random Forest achieved ROC-AUC of 0.8180, XGBoost 0.8120, and Gradient Boosting 0.8078. However, classification accuracies (0.4733–0.4867) and F_1-scores (0.4503–0.4743) reflect severe multi-class imbalance in the synthetic feature set.

The binary toxicity and emergency models exhibited weak discriminative power (ROC-AUC 0.5191 and 0.4546). Because all training data are synthetic, these metrics evaluate algorithmic pipeline execution rather than clinical efficacy.

VI. SECURITY ARCHITECTURE AND THREAT ANALYSIS

MediChain adopts a defense-in-depth security model. Table VI details the threat matrix, delineating attack vectors and implemented mitigations. Application confidentiality is rooted in AES-256-GCM authenticated encryption, providing both data confidentiality and cryptographic authenticity via a 128-bit authentication tag.

TABLE V Empirical Machine-Learning Performance From Project Manifest

Model Identifier	Algorithm	Prediction Target	ROC-AUC	$F1$	Accuracy
dosage_safety_rf	Random Forest	Risk level class	0.8180	0.4503	0.4867
dosage_safety_gb	Gradient Boost	Risk level class	0.8078	0.4622	0.4733
dosage_safety_xgb	XGBoost	Risk level class	0.8120	0.4743	0.4867
dosage_toxicity	XGBoost	Drug toxicity flag	0.5191	0.0435	N/A
dosage_emergency	XGBoost	Emergency flag	0.4546	0.3577	N/A
xgb_cancer	XGBoost	Oncological risk	0.6567	0.3826	N/A
Pending: xgb_heart, xgb_diabetes, xgb_stroke, xgb_kidney, xgb_liver, adherence.					

TABLE VI Security Threat Matrix and Defensive Mitigations

Threat Category	Attack Surface	Implemented Defensive Mitigation
Unauthorized clinician	Patient clinical APIs	Backend RBAC guards and active grant checks.
Account compromise	Auth endpoints	6-digit OTP, 10-round bcrypt, 24-hr JWT tokens.
Stolen QR badge image	Optical scan intake	Minimal ID (MC-PAT-YYYY-XXXXXX); RBAC enforced.
Malicious file upload	Ingestion endpoint	Magic-byte format checks; strict 10 MB size limit.
IPFS data exposure	Public IPFS nodes	Symmetric A E S -256-GCM encryption with unique IVs.
Tampered medical file	Storage & database	Cryptographic SHA-256 di-gests anchored on Sepolia
Web3 wallet theft	Blockchain signing	MetaMask isolated to ledger events; no login power.
AI model manipulation	Inference endpoints	Strict schema checks; non-binding advisory role.
Third-party outage	Pinata / Sepolia	Exponential backoff retry logic and MongoDB caching.

The system enforces an explicit barrier between identification and authorization: scanning a QR badge yields only an opaque patient ID, while the backend cross-references the clinician's JWT identity against the patient-doctor grant table in MongoDB and blockchain state before returning protected health information.

VII. DISCUSSION, LIMITATIONS, AND FUTURE WORK

A central finding of this investigation is that healthcare platforms must decouple operational storage, decentralized archival, and immutable ledgers. MongoDB delivers sub-millisecond API queries for mutable state; IPFS provides content-addressed storage for large diagnostic files; and restricting Sepolia to verification hashes circumvents blockchain latency and cost. Empirical results confirm dramatic performance divergence: local cryptographic operations execute in 1.66–40.23 ms and API middleware responds in 0.82–1.42 ms, whereas Sepolia confirmation requires 12–18 s, validating that routine workflows must not block on public blockchain mining.

The ML evaluation underscores reporting balanced metrics. While ROC-AUC exceeded 0.81 for dosage safety, F_1-scores (0.45–0.47) reflect multi-class imbalance on synthetic distributions. The toxicity model failed to generalize ($F_1 = 0.04$), reaffirming that AI must operate strictly as advisory signals under clinician oversight. Addressing interoperability gaps requires certified FHIR R4 interfaces and adherence to HIPAA/GDPR frameworks, mandating no identifiable personal metadata on-chain while preserving the patient's right to data erasure through off-chain key disposal.

Limitations: (1) All eight datasets (17,000 records) are synthetic; (2) six of 12 registered models await clinical data; (3) test net gas dynamics do not fully reflect main net congestion; (4) data schemas are FHIR-oriented without formal certification; (5) security evaluation derives from automated suites rather than external penetration tests; (6) IPFS latency depends on Pinata gateway availability; and (7) 110 of 112 tests are itemized in the manifest.

Future Work: Future research will focus on: (1) implementing formal FHIR R4 REST endpoints with

SMART on FHIR authorization for hospital EHR interoperability (e.g., Epic, Cerner); (2) retraining predictive models on de-identified clinical datasets (e.g., MIMIC-IV) with explainable SHAP dashboards; (3) deploying federated learning to collaboratively train risk models across hospital boundaries without transfer-ring raw records, aligning with HIPAA/GDPR; (4) migrating smart contracts to a Layer-2 rollup (e.g., Arbitrum) for sub-2-second confirmation latency; (5) integrating Hardware Security Modules (HSMs) for envelope encryption and key custody; and (6) extending decentralized file ingestion to support DICOM-compliant medical imaging workflows.

VIII. CONCLUSION

MediChain demonstrates an integrated, patient-controlled healthcare platform unifying role-based web application security, encrypted decentralized document storage, selective blockchain verification, camera-assisted QR identification, RxNorm medication normalization, and AI-assisted clinical decision support. By decoupling routine application authentication from Web3 wallet signing, restricting QR codes to minimal identifiers, and maintaining bulk clinical files off-chain via AES-256-GCM and IPFS, the architecture overcomes the security, cost, and latency barriers of monolithic healthcare blockchains. Empirical evaluation verifies 112 automated tests with a 100.0% aggregate pass rate, average smart-contract gas consumption below 250,000 gas for patient-facing functions, local cryptographic latency between 1.66 ms and 40.23 ms across payloads up to 8 MB, and API gateway throughput reaching 1,210 req/s with sub-2 ms latency. While the synthetic nature of the ML datasets and testnet execution represent clear development boundaries, the implemented system establishes a viable engineering foundation for decentralized, patient-mediated health data governance.

ACKNOWLEDGMENT

The authors acknowledge the guidance of Prof. Kohilambol R in the development and architectural review of the MediChain research project at the Department of Computer Science and Engineering (Data Science), Vemana Institute of Technology.

REFERENCES

[1] HL7 International, “FHIR Release 4: Fast Healthcare Interoperability Resources,” 2019. [Online]. Available: https://hl7.org/fhir/R4/. Accessed: 2026.

[2] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying blockchain to securely and scalably share clinical data,” Computational and Structural Biotechnology Journal, vol. 16, pp. 267–278, 2018.

[3] Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “Health-Block: A secure blockchain-based healthcare data management system,” Computer Networks, vol. 200, Art. no. 108500, 2021.

[4] J. Jayabalan and N. Jeyanthi, “Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy,” Journal of Parallel and Distributed Computing, vol. 164, pp. 152–167, 2022.

[5] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, “Secure decentralized electronic health records sharing system based on blockchains,” Journal of King Saud University Computer and Information Sciences, vol. 34, no. 8, pp. 5045–5058, 2022.

[6] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, “Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm,” IEEE Access, vol. 10, pp. 87803–87815, 2022.

[7] M. Shaikh, S. A. Memon, A. Ebrahimi, and U. K. Wiil, “A systematic literature review for blockchain-based healthcare implementations,” Healthcare, vol. 13, no. 9, Art. no. 1087, 2025.

[8] A. P. Susanto, D. Lyell, B. Widyantoro, S. Berkovsky, and F. Magrabi, “Effects of machine learning-based clinical decision support systems on decision-making, care delivery, and patient outcomes: A scoping review,” Journal of the American Medical Informatics Association, vol. 30, no. 12, pp. 2050–2063, 2023.

[9] A. P. Susanto, D. Lyell, B. Widyantoro, S. Berkovsky, and F. Magrabi, “How well do AI-enabled decision support systems perform in clinical settings?” in Proc. MEDINFO 2023, ser. Studies in Health Technology and Informatics,

vol. 310. IOS Press, 2024, pp. 279–283.

[10] Dobre and A. Vasilateanu, "Electronic health record authentication and authorization using blockchain and QR codes," Procedia Computer Science, vol. 239, pp. 1784–1791, 2024.

[11] U.S. National Library of Medicine, "RxNorm: Normalized Names for Clinical Drugs," 2024. [Online]. Available: https://www.nlm.nih.gov/research/umls/rxnorm/. Accessed: 2026.

[12] J. S. S. Mole and R. S. Shaji, "Ethereum blockchain for electronic health records: Securing and streamlining patient management," *Frontiers in Medicine*, vol. 11, Art. no. 1434474, 2024.