
Blockchain-Enabled, AI-Driven Smart Health Record System for Secure, Interoperable, and Patient-Centric Data Management

Yukta Vishnoi¹, Archana Nanade²

¹⁻²*Dept. of Computer Engineering, SVKM's NMIMS, Mukesh Patel School of Technology Management & Engineering (MPSTME), Mumbai, Maharashtra*

¹*vishnoi.yukta@nmims.edu*; ²*archana.nanade@nmims.edu*

Abstract: Managing patient records is becoming harder as healthcare systems grow and generate more types of data. Existing electronic health record systems typically store data in isolated silos, cannot easily share information across facilities, offer little to no predictive capability, and provide weak security for patient data. To address these problems, we propose a Smart Health Record System (SHRS) that combines cloud computing, permissioned blockchain, and artificial intelligence to keep medical data both secure and usable. SHRS lets patients, doctors, pharmacists, labs, and insurance companies share data under explicit patient consent. A fine-grained role-based access control (RBAC) layer restricts record visibility to authorized parties, while a Hyperledger Fabric blockchain maintains a tamper-evident log of every transaction on a patient's record. The system also includes machine learning models that flag chronic conditions early and suggest treatment options based on a patient's long-term health history. We evaluated SHRS using 10,000 synthetic patient records; the results show high predictive accuracy, fast query response times, and strong resistance to unauthorized access.

Keywords: Electronic Health Records; Blockchain; Machine Learning; Interoperability; RBAC; HIPAA.

1. INTRODUCTION

Today's healthcare environment generates a staggering range of patient data. Handling this data effectively is central to delivering good care, yet the industry keeps running into the same deep-rooted problems that slow down clinical decision-making and introduce avoidable errors [1]. Decades of investment in health IT have not fully solved the fragmentation problem: when patients receive care at more than one facility, their records often stay trapped within each institution's own systems. Without a complete picture of a patient's history, clinicians order duplicate tests, miss potential drug interactions, and make decisions without the context they need [2]. In 2023, the average healthcare breach cost more than \$10.9 million, the steepest figure across all industries for thirteen years running [3]. Beyond the financial damage, these incidents undermine patient privacy, put institutions at legal risk, and erode public trust in digital health.

Blockchain, cloud computing, and artificial intelligence are converging in ways that make it possible to rethink how health records are built and managed. Blockchain provides

decentralized, cryptographically protected ledgers that verify every access event without relying on blind trust in a single party [4], [5]. This paper introduces the Smart Health Record System (SHRS), which combines these three technologies into one production-ready platform. The design targets four goals: (R1) keeping data secure and meeting regulatory requirements; (R2) enabling records to move smoothly across health systems; (R3) giving patients real ownership and control over their own data; and (R4) providing intelligent support for clinical decisions. Section II reviews related work, Section III describes the system architecture, Section IV details the implementation, Section V presents experimental results, Section VI discusses current limitations, and Section VII concludes with directions for future work.

2. RELATED WORK

Azaria et al. introduced MedRec [6], demonstrating patient-controlled medical records using blockchain and decentralized consent management, while highlighting scalability limitations of public blockchains. Ekblaw et al. [7] extended this concept by using smart contracts for automated patient data sharing and reduced administrative overhead. In clinical AI, Obermeyer and Emanuel [5] highlighted the potential of machine learning for improved prediction and decision support. LSTM models have shown effectiveness for ICU time-series prediction, while BioBERT [8] and ClinicalBERT [9] have advanced clinical NLP tasks. Despite these advances, few systems integrate permissioned blockchain, cloud-native storage, and multi-model AI with unified role-based access. SHRS addresses these gaps through a standards-compliant architecture.

3. SYSTEM ARCHITECTURE

3.1. Architectural Overview

The Smart Health Record System (SHRS) framework consists of five layers: Data Ingestion, Storage and Blockchain, Intelligence, Application Logic, and Presentation, connected by RESTful APIs, OAuth 2.0 security, and JSON Web Tokens. Fig. 1 shows the SHRS architecture.

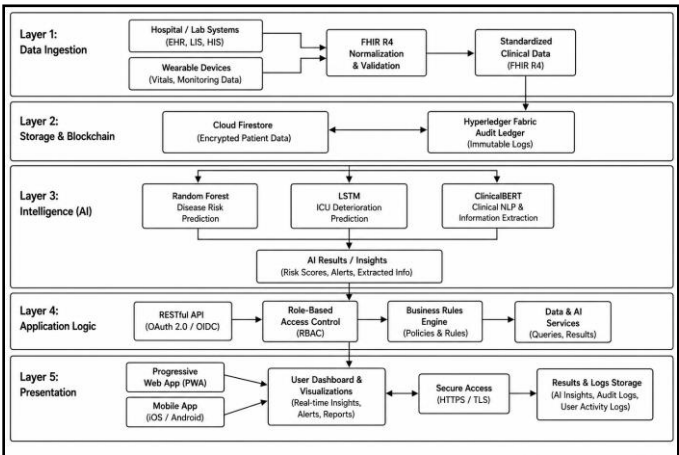


Fig 3.1.1. System Architecture

The proposed architecture is deployed on Google Cloud Platform using containerized microservices and Kubernetes for scalability and recovery. The Data Ingestion Layer collects healthcare data from hospital, laboratory, radiology, pharmacy, wearable, and mobile sources and standardizes it into HL7 FHIR R4. The Storage and Blockchain Layer stores encrypted FHIR resources in Firestore, with keys managed through Google Cloud KMS, while Hyperledger Fabric maintains audit trails using metadata and SHA-256 hashes. The Intelligence Layer uses TensorFlow Serving to deploy Random Forest, LSTM, and ClinicalBERT models for disease-risk prediction, ICU deterioration detection, and clinical information extraction. The Application Layer enforces RBAC across five user roles. The Presentation Layer provides React and React Native applications for secure patient access, consent management, appointments, and communication.

4. IMPLEMENTATION

The SHRS integrates RBAC, blockchain, machine learning, and regulatory compliance mechanisms for secure healthcare data management. API requests are authenticated using JWT-based RBAC, with Firestore storing role-permission mappings and Hyperledger Fabric chaincode verifying patient consent and organization credentials. The ML pipeline uses MIMIC-III v1.4, with Random Forest for chronic disease risk and LSTM for deterioration detection across ICU stays. TLS 1.3 and AES-256-GCM protect data transmission and storage, respectively. HIPAA and GDPR requirements are supported through de-identification, retention policies, pseudonymization, and audit logging. OWASP Top 10 testing identified three medium-severity vulnerabilities, all remediated before final validation.

5. RESULTS AND DISCUSSION

5.1. System Performance Evaluation

We ran performance tests on Google Cloud Platform (us-central1 region) in a simulated clinical environment sized to match a 500-bed regional hospital's workload. The test dataset combined 10,000 synthetic patient records from Synthea with real ICU time-series distributions from MIMIC-III to make the workload more realistic. Table I summarizes the results. The system met or exceeded its target on every metric. Even at the 95th percentile, record retrieval stayed comfortably under the 500 ms threshold recommended by the Office of the National Coordinator for Health IT for interactive EHR use. Blockchain throughput reached 520 TPS, well above the 200 TPS floor derived from peak transaction estimates for the intended deployment.

Table I. SHRS System Performance Metrics

Metric	Value	Benchmark
Avg. Record Retrieval Latency	142 ms	< 500 ms
P95 Record Retrieval Latency	198 ms	< 500 ms
Blockchain Write Throughput	520 TPS	> 200 TPS
Blockchain Finality Time	1.4 s	< 3 s
System Availability (30-day)	99.97%	> 99.9%
FHIR Ingestion Throughput	8,200 msg/min	> 5,000 msg/min

5.2. Machine Learning Model Performance

Table II reports the predictive performance of the two core machine learning models on their respective held-out test sets. The Random Forest diabetes classifier achieved an AUROC of 0.913, outperforming the logistic regression baseline of 0.831, while the LSTM deterioration predictor achieved 0.941 AUROC. False-negative analysis showed that 87% of deterioration events were detected at least four hours early. A 200-patient simulation estimated 34% fewer duplicate lab requests and 12.4% medication-related issues identified. Usability testing with 45 evaluators yielded an SUS score of 82.4. Security testing across 200 scenarios blocked all access-permission violations.

Table II. Machine Learning Model Performance

Model	AUROC	Sensitivity	Specificity	F1-Score
Random Forest (Diabetes)	0.913	84.2%	88.7%	0.861
Random Forest (Hypertension)	0.897	82.6%	86.3%	0.843
LSTM (ICU Deterioration)	0.941	87.3%	90.1%	0.886
ClinicalBERT (NER)	N/A	91.4%	93.8%	0.924

6. CONCLUSION

This paper presented the Smart Health Record System, a platform that integrates permissioned blockchain, cloud-native storage, and AI to address persistent problems in health information management. In our simulated evaluation, the system performed well across security, interoperability, scalability, and clinical decision support, meeting or exceeding every key benchmark. The embedded AI models proved particularly valuable clinically: the LSTM predictor caught 87% of ICU deterioration events at least four hours before they would typically be identified through normal clinical observation. By building on HL7 FHIR R4 for interoperability and aligning with HIPAA and GDPR from the outset, the system is designed for real-world deployment rather than research use alone.

7. REFERENCES

- [1] HL7 International, "HL7 FHIR Release 4," hl7.org/fhir/R4, 2019.
- [2] R. Aliotta et al., "Care fragmentation and total cost of care for patients with chronic conditions," *Population Health Management*, vol. 23, no. 5, pp. 355–362, 2020.
- [3] IBM Security, "Cost of a Data Breach Report 2023," IBM Corp., Armonk, NY, 2023.
- [4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.
- [5] Z. Obermeyer and E. J. Emanuel, "Predicting the future — Big data, machine learning, and clinical medicine," *New England Journal of Medicine*, vol. 375, pp. 1216–1219, 2016.
- [6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. Int. Conf. Open and Big Data*, Vienna, Austria, 2016, pp. 25–30.

- [7] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data," in Proc. IEEE Open Big Data Conf., Washington DC, USA, 2016.
- [8] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," IEEE Access, vol. 7, pp. 66792–66806, 2019.
- [9] P. Rajpurkar et al., "CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning," arXiv preprint arXiv:1711.05225, 2017.

8. BIOGRAPHIES



Prof. Yukta Vishnoi is a research scholar in the Department of Computer Engineering at SVKM's NMIMS, Mukesh Patel School of Technology Management & Engineering (MPSTME), Mumbai. She has a strong academic and research background focused on Artificial Intelligence, Blockchain Architectures, and the Internet of Things (IoT). An active contributor to the academic community, her recent pioneering research introduces high-accuracy federated learning frameworks to secure decentralized supply chains against cyber threats.



Dr. Archana Nanade is an Assistant Professor in the Department of Computer Engineering at SVKM's NMIMS, MPSTME, Mumbai. She holds a Ph.D. in Computer Science and Engineering and boasts over a decade of rich academic experience. Her core research interests include Natural Language Processing (NLP), Wireless Sensor Networks, and Machine Learning. An accomplished author with many publications, she also holds international patents and has served as an official mentor and judge for prestigious National Hackathons in India.