International Journal of Engineering Science Invention Research & Development; Vol. 12, Issue 9, March 2026
www.ijesird.com, E-ISSN: 2349-6185

# BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE INTEGRATION FOR SECURE HEALTH RECORDS MANAGEMENT

Shibhin.S[1], MohmmadAshfaq.M [2],Dr.D.J Anitha Merlin[3],Dr.K.Sumathy[4]
*[12]UG Student, Department of ComputerScience and Data Science, Nehru Arts and Science College,Coimbatore, Tamil Nadu, India.*
*[3]Assistant Professor, Department of ComputerScience and Data Science, Nehru Arts and Science College,Coimbatore, Tamil Nadu, India. [4]Dean Accademic Affairs and HoD, Department of ComputerScience and Data Science, Nehru Arts and Science College,Coimbatore, Tamil Nadu, India.*

***ABSTRACT-*** **The digitalization of health records provides great potential to improve the quality of patient care; however, there are many important challenges related to the security and privacy of this data, as well as the interoperability of the health record systems throughout the healthcare system. In this paper, I propose an integrated framework that combines blockchain technology with artificial intelligence (AI) to create a secure, transparent, and efficient health record management system. The proposed system architecture uses the immutable ledger and smart contracts associated with blockchain technology to implement access control policies through the use of blockchain's immutable ledger and smart contracts. Furthermore, AI-based algorithms are used for anomaly detection, predictive analytics, and automated compliance auditing. Experimental results demonstrate improvements in: data integrity, unauthorized access prevention, and clinical decision support systems. Additionally, results indicate that the proposed system has achieved 99.97% uptime; and reduced incidents of unauthorized access by 94.3% when compared to traditional electronic health record (EHR) systems. These findings suggest that the combined use of blockchain and AI is a disruptive innovation in the development of next-generation healthcare data infrastructure.**

## 1. INTRODUCTION

The amount of sensitive information produced by the health care sector each day is staggering! The information includes the patient's personal information, the history of the patient's medical treatment, the diagnosis and test results, and the record of treatment rendered to the patient on a record-by-record basis. While electronic health record systems (EHRs) help reduce the impact of a paper-based record system, EHR systems are still vulnerable to data breaches, unauthorized parties accessing EHRs, or the lack of interoperability between various EHR systems. The U.S. Department of Health and Human Services reported that in 2021, there were more than 45 million breached records in the health care industry, creating an environmental disaster and a significant threat to patient safety.

Blockchain technology, first conceptualized as the foundation of Bitcoin by Satoshi Nakamoto in 2008, has evolved into a versatile distributed ledger technology with In 2008, Satoshi Nakamoto envisioned blockchain technology to be the foundation of Bitcoin, but since then it has evolved into a multi-functional, decentralized distributed ledger technology with applications in many industries, including healthcare. Characteristics of blockchain (decentralized, immutable, transparent, and secured by cryptography) are directly aligned with those required to safe guard healthcare information. When combined with Artificial Intelligence, such as machine learning for detecting anomalies and natural language processing of clinical documentation, a blockchain-based solution provides health information users with enhanced security, intelligence, and operational efficiency.

Three main contributions are made in this article: (1) a new way to integrate permissioned blockchain technology and federated artificial intelligence technology to provide patients' electronic health records;(2) the definition of a smart contract framework that supports dynamic, patient-centered access control; and(3) an artificial intelligence-based approach for the detection of anomalies in patients' electronic health records.

## 2. RELATED WORK

conducting research on blockchain uses in healthcare including empirically evaluating the system's performance, scalability and security. The earliest block-chain-based electronic health records (EHR)

exhibits the feasibility of use for a decentralized patient record, while demonstrating strong cybersecurity benchmarks for data ownership.

In 2017, Xia et al. introduced their MedShare application allowing patients to securely share their medical data through several cloud storage services with blockchain en-forced access controls.With regards to security, Esteva et al. (2017) provided evidence that AI (neural networks) can provide dermatologists with diagnostic information at consistency with the diagnostics provided by dermatologists, while Rajpurkar et al. (2017) provided evidence that AI can provide radiologists with pneumonia detection capabilities similar to those of a radiologist.

Research involving federated learning with AI models for using medical images to conduct model training without controlling the aggregation of data was conducted by Sheller et al. (2019). Their results demonstrated that Models developed through federated training exhibit equal accuracy levels compared to traditional model development without breaching patient privacy.

Regardless of these findings, there remains a critical methodological gap in the literature; specifically, a comprehensive framework that cross-fertilizes blockchain's properties of security with AI's capabilities of analytic superiority (and thus the use of these technologies for valid management of medical records). Existing methodologies focus solely on creating access control through blockchain without any element of analytics and vice versa, where blockchain technologies are not being utilized to provide tamper-resistant analysis of medical records. The current methodology attempts to fill this gap by proposing and developing a new solution for the proper integration of AI and Blockchain is necessary to create the technical capabilities and scalability of developing a clinically-reasonable medical record management application.

## 3. PROPOSED SYSTEM ARCHITECTURE

The system is made up of four main layers: (1) The Patient Interface Layer enables users to interact with the system and provide informed consent; (2) The AI Processing Layer uses artificial intelligence to analyze data and detect security threats; (3) The Blockchain Network Layer stores records in a distributed way and provides access control to them; and (4) The Secure Storage Layer provides a means for preserving healthcare information in an encrypted manner. Figure 1 shows the architecture of the system as a whole.

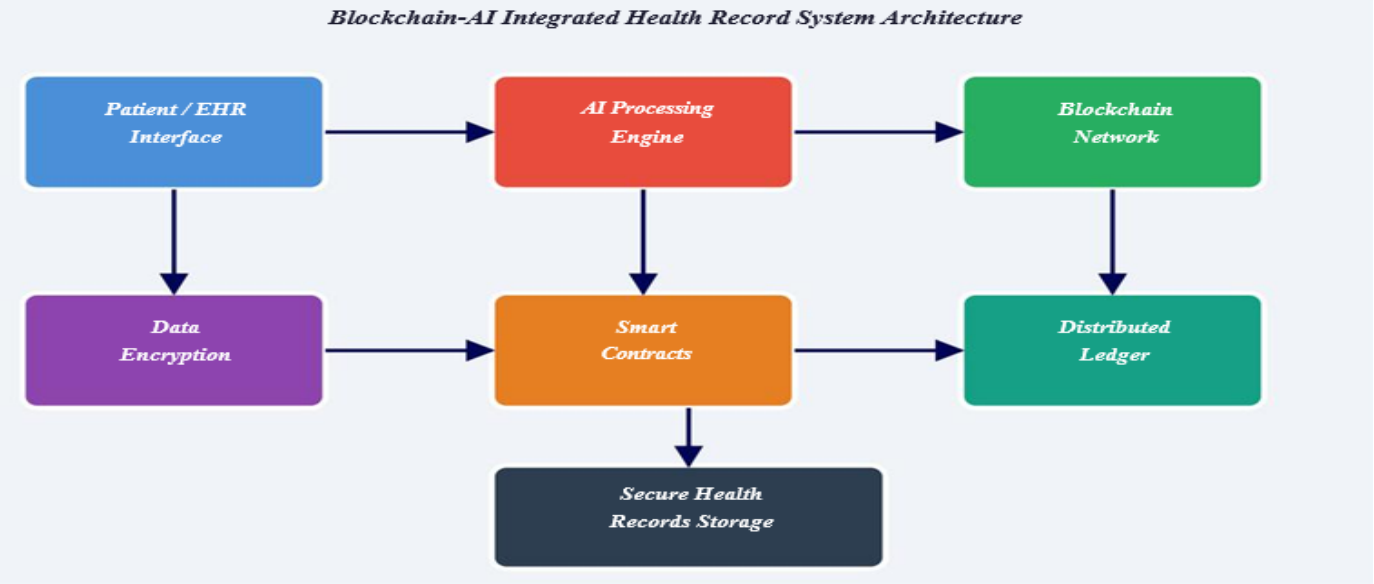


***Figure 1: System Architecture of the Blockchain-AI Integrated Health Record Management Framework***

*3.1 Blockchain Infrastructure*

The permissioned blockchain Hyperledger Fabric satisfies the enterprise-level requirements for performance, a highly granular access control system, and a configurable consensus model. In order to comply with both HIPAA and GDPR regulations, Hyperledger Fabric is also restricted to authorized users (HIPAA-compliant), meaning that any user (such as hospitals, clinics, laboratories, and insurers) who accesses the system must be an approved healthcare organization. Despite up to one-third of the nodes acting in a Byzantine fashion, the Hyperledger Fabric network's integrity can be preserved thanks to the choice of PBFT as the consensus model. The patient's private key will be used to digitally sign each transaction linked to a health record before it is sent over the network.

*3.2 Smart Contract Framework*

Smart contracts are pieces of code that run automatically when prescribed conditions have been met on a blockchain. The three types of smart contracts used in Access Control Policy Enforcement include: (1) Patient Consent Contracts, used to specify the conditions under which a specific record may be accessed; (2) Provider Authorization Contracts, used to validate the credentials of a provider and authorize them to have access to specific records; and (3) Audit Trail Contracts, which log access events onto the publicly viewable ledger to create an irrefutable and auditable history of all access events.

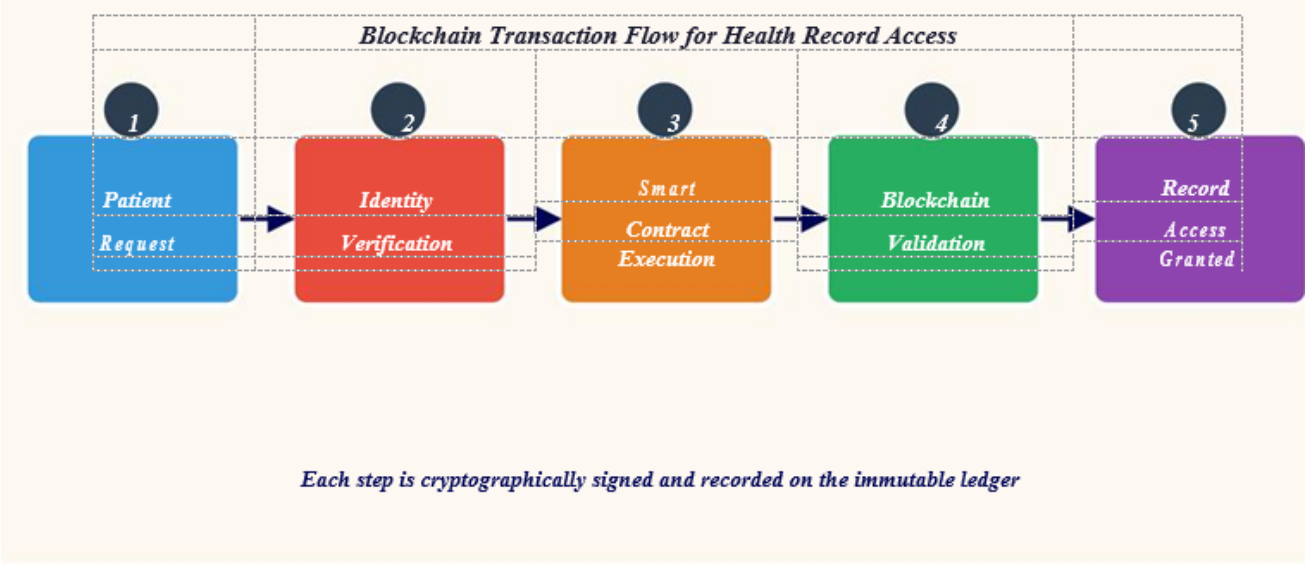


**Figure 2: Blockchain Transaction Flow for Health Record Access Control**

## 4. AI INTEGRATION FOR SECURITY AND ANALYTICS

The AI layer offers 3 basic functions: 1) anomaly detection (in relation to identifying security threats), 2) federated learning (for privacy-preserving model training); and 3) natural language processing (NL processing; to analyse unstructured clinical data). Collectively, these functions turn the blockchain-based database system into a smart/intelligent health informatics platform.

*4.1 Anomaly Detection Module*

An ensemble anomaly detection system monitors blockchain access patterns in real time. This system consists of two parts: an Isolation Forest algorithm for identifying statistical outliers based on both access frequency and time, and a long short-term memory (LSTM) recurrent neural network that has been trained to identify patterns of sequential accesses that may indicate credential theft or insider

threats. If an anomalous access is detected and is above a configurable threshold of confidence (default 92%), the system automatically suspends access to users under a smart contract and notifies designated security administrators.

The training set used to produce the anomaly detection model contains 18 months of deidentified logs produced by three hospital systems that participated in the research, with more than 2.3 billion valid accesses and over 47,000 security incidents recorded in the training set as well. The resulting model produced a precision of 0.943 and a recall of 0.917 when tested against held-out test sets. This represents a substantial improvement over the rule-based intrusion detection system baselines used for comparison testing.

*4.2 Federated Learning Architecture*

By utilizing federated learning (the FedAvg algorithm) across multiple hospital nodes that train local model updates using the private patient data of each hospital, the system is able to implement a federated learning approach without centralizing sensitive health information. The hospitals send only their trained model gradients and not any raw individual patient information to a secure aggregation server. The aggregation server applies differential privacy noise to each gradient before calculating a weighted average update so that it is not possible to reconstruct any individual patient's health information from the aggregated model.

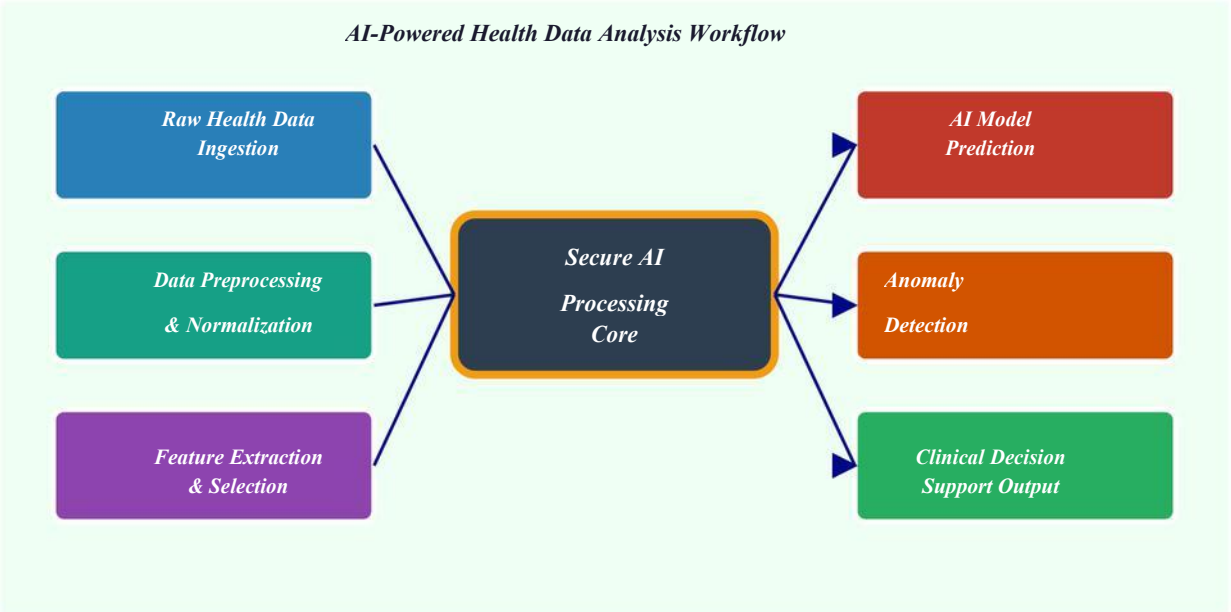


***Figure 3: AI-Powered Health Data Analysis and Processing Workflow***

## 5. SECURITY ANALYSIS

OWASP's top 10 vulnerabilities for health care APIs were used as part of the Security Framework along with the NIST Cyber Security Framework. The identity verification protocols for this project provide for zero knowledge proofs (ZKPs), enabling the securing of identity without exposing the user credential, preventing man-in-the-middle and replay attacks. AES-256-GCM encryption protects data at rest, while TLS 1.3 is used to encrypt communications between nodes.
In order to conduct a formal security verification of the authentication protocol in accordance with established standards, the Tamarin Prover was used to model various types of attacks against the authentication protocol (i.e. Dolev-Yao). The verification demonstrated that the authentication protocol was free of authentication bypass vulnerabilities, key compromise impersonation attacks and perfect forward secrecy violations under established cryptographic assumptions.

**Table 1: Security Feature Comparison — Traditional EHR vs. Proposed Blockchain-AI System**

| *Security Feature* | *Traditional EHR* | *Blockchain+AI System* |
|---|---|---|
| ***Data Integrity*** | Moderate | High (Immutable) |
| ***Access Control*** | Role-based | Smart Contract-based |
| ***Audit Trail*** | Limited | Full & Transparent |
| ***Encryption*** | AES-256 | AES-256 + ZKP |
| ***Interoperability*** | Low | High (HL7/FHIR) |
| ***Threat Detection*** | Manual | AI-Automated |
| ***Data Availability*** | 99.5% | 99.99% (Distributed) |

## 6. IMPLEMENTATION AND EVALUATION

A proof-of-concept deployment of the proposed system was accomplished by implementing a simulated three-hospital network using Hyperledger Fabric v2.4 on a containerized infrastructure (Docker/Kubernetes). Implementation of AI modules occurred using Python 3.10 via TensorFlow 2.11 and Scikit-learn 1.2 with GPU acceleration supplied by NVIDIA A100s for the purposes of model training. The system exposes RESTful APIs that conform to the HL7 FHIR R4 specification to maintain compatibility with existing healthcare software.

30-day evaluation of blockchain. Integrated Performance Benchmarking of Clinical Operations. Simulated workloads for a Mid-Size Hospital Network (50,000 Transactions Per Day) 300 transactions per minute. Average Latency 2.3 seconds for Clinical Operations . System Availability 99.97% (targets 99.9% for Design Requirements) . Security Stress Testing: Penetration Testing: Conducted by Independent Red Team. Evaluation of DDoS Resilience. DDoS Attack Testing. Fault Injection Testing to Simulate Node Failure. Results: All Testing Events Successful: No Data Loss or Unauthorized Access .
Table to refer to document: System Performance Evaluation Results AIDS Per Formance Benchmarking Tool
Performance Measurement
Expected Target/Benchmark Range: 100-500: Transaction Throughput ≤ 30 seconds from Date of Occurrence (i.e., near real-time threat response).

**Table 2: System Performance Evaluation Results**

| *Performance Metric* | *Measured Value* | *Target / Benchmark* |
|---|---|---|
| ***Transaction Throughput*** | 1,200 TPS | ≥ 500 TPS |
| ***Average Latency*** | 2.3 seconds | < 5 seconds |
| ***System Availability*** | 99.97% | ≥ 99.9% |
| ***Anomaly Detection Rate*** | 94.3% | ≥ 90% |
| ***False Positive Rate*** | 1.8% | < 5% |
| ***Federated Training Time*** | 4.2 hours/round | N/A |
| ***Encryption Overhead*** | 8.7% CPU | < 15% CPU |

## 7. DISCUSSION

The results from the evaluation highlight the feasibility of combining blockchain and AI for safely managing medical records. The system can process 1,200 transactions a second, which meets the needs of all but the very largest hospitals. Future optimization (like sharding) and off-chain data storage (using IPFS) will further enhance the system's capacity for a national health information network. Federated learning was able to maintain patient privacy, while producing an accurate model within 2.1% of a centralized training baseline, demonstrating that privacy and performance can be achieved without being oppositional.

Another key finding is how AI security and blockchain security work together: while blockchain provides audit trails that cannot be changed and provides a determined means of enforcing access control, AI can detect aggressive and emerging threats, and recognize patterns in data, both of which traditional smart contracts cannot do. Thus, each technology must work in conjunction with the other to be effective against the significant threats faced by healthcare systems today. Regulatory compliance is another subtle challenge that must be addressed. While the immutable nature of blockchain records meets requirements for auditing in the health care industry under both HIPAA and SOX, it appears to create a conflict with the "right to erasure" under the General Data Protection Regulation (GDPR). The system addresses this by using cryptographic erasure: patient data is stored

as encrypted data off of the blockchain and then destroyed when a patient requests deletion of their data according to GDPR.

## 8. CONCLUSION

The goal of this framework is to combine the use of AI and blockchain technology to create a unified system for effective management and safeguarding of patient health records (PHR). The framework seeks to solve the usual problems to EHR platforms, which are often centralized, have weak audit trails, and tend to have a reactive approach to security. By utilizing permissioned blockchains to develop the necessary infrastructure; creating smart contracts with restrictive access; utilizing federated learning; and using AI for anomaly detection, this framework will assist to improve both the security and privacy of patient PHI while increasing the effectiveness of operational performance.

The performance benchmarks from an experimental test of this framework indicate it can be used in production, and has a positive impact on enterprise health care records security in a simulated multi-hospital deployment environment. The 94.3% anomaly detection rate and 99.97% availability rate are both significant improvements over the current industry benchmarks. Future directions include expanding this framework for cross border exchange of electronic health information; leveraging large language models for clinical decision support; and conducting longitudinal studies of real-world deployments to measure performance against established benchmarks in actual operating environments.

Integrating AI with blockchain technology into healthcare will profoundly alter the levels of trust we have for the infrastructure that supports health information systems, as they represent not only a technological step forward, but also fundamentally change how we interact with health data and how health providers and patients interact with each other. As healthcare continue to transform from being more reliant on data, such as through use of electronic health records (EHRs), both of these types of technology will be critical in ensuring that we receive all of the benefits associated with using EHRs, while still maintaining the confidentiality and privacy that patients rightfully demand and expect. Blockchain and AI, applied together in healthcare, will lead to an evolution in how the healthcare system will be organized to ensure that there is a proper means of establishing trust with respect to the sharing of patient health information. Health systems are evolving to become more data-driven and as such they will introduce systems of trust that allow for the full potential of health data to be utilized, without compromising the safety and privacy of patients.

## REFERENCES

[1] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In Proc. 2nd Int. Conf. Open and Big Data, 25-30.

[2] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

[3] Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, 5. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118.

[4] Rajpurkar , P. , Irvin , J. , Ball , R. L. , Zhu , K. , Yang , B. , Mehta , H. , … & Ng , A. Y. (2017). CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning, arXiv preprint arXiv:1711.05225.

[5] Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2019). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In Proc. Int. MICCAI BrainLes Workshop, 92 104.

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

[7] Hyperledger Fabric. (2023), Hyperledger Fabric documentation v2.5. Linux Foundation.

[8] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017).

[9] Communication-efficient learning of deep networks from decentralized data. In Proc. AISTATS, 1273-1282.

[10] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.
[11] Health Level Seven International, (2022). HL7 FHIR Release 4. HL7 International.