International Journal of Safety and Security Engineering
Vol. 16, No. 3, March, 2026, pp. 669-680
Journal homepage: http://iieta.org/journals/ijsse

An AI–Blockchain Framework for Secure and Interoperable Healthcare Data Exchange

S. Hemalatha[1*], Kiran Mayee Adavala[2], K V S V Trinadh Reddy[3], S Karthika[4], C N Srividya[5], Smitha Chowdary Ch[6]

[1] Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai 600123, India
[2] CSE (AIML), Kakatiya Institute of Technology and Science, Warangal 506015, India
[3] Department of Electronics and communication Engineering, Cambridge Institute of Technology, Bengaluru 560036, India
[4] Department of Computer Science and Engineering (Data Science), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, India
[5] Department of Electronics & Communication Engineering, BGS Institute of Technology, Adhichuchanagiri University, Mandya 571448, India
[6] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522302, India

Corresponding Author Email: pithemalatha@gmail.com

https://doi.org/10.18280/ijsse.160317

Received: 15 December 2025
Revised: 10 February 2026
Accepted: 20 February 2026
Available online: 31 March 2026

Keywords:
blockchain, artificial intelligence, healthcare data exchange, interoperability, privacy preservation, smart contracts

ABSTRACT

Reliable and interoperable healthcare data sharing remains challenging due to disjointed systems, insufficient trust, and strict regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Traditional centralized methods often fail to ensure compliance and efficiency in diverse healthcare environments. This study proposes an integrated artificial intelligence (AI) and blockchain framework to address these issues. AI enables intelligent data preprocessing, predictive analytics, natural language processing (NLP)-based harmonization, and anomaly detection, while blockchain ensures decentralized, immutable record-keeping with smart contracts for automated approval management. The framework introduces an interoperability layer that supports standards-based sharing of electronic medical records across platforms. Experimental evaluation under a simulated environment indicates improved system performance, with reduced transaction delays and throughput of approximately 50–150 transactions per second (TPS) depending on workload conditions. Cross-platform compatibility achieves over 95% success rate, NLP harmonization attains an F1-score of 0.93, and anomaly detection mitigates more than 95% of simulated security incidents. These results demonstrate the potential of the proposed framework to enhance privacy, compliance, and trust compared to standalone blockchain-only and AI-only approaches, highlighting the benefits of AI-enhanced smart contracts and a unified interoperability interface.

1. INTRODUCTION

The telemedicine [1] landscape faces challenges due to fragmented data repositories, information systems, and inconsistent standards, which delay effective data interoperability [2]. Additionally, rigorous regulations such as the General Data Protection Regulation (GDPR) [3] and the Health Insurance Portability and Accountability Act (HIPAA) [4] complicate seamless data exchange. To address these challenges [5], various approaches across diverse healthcare environments and datasets have been explored.

Recent studies highlight emerging technologies that support intelligent data preprocessing, natural language processing (NLP), predictive analysis, and anomaly detection, improving data standardization and enabling better healthcare decisions [6]. Blockchain technology provides a decentralized and immutable ledger, ensuring transparency, trust in data, and automated regulatory compliance via smart contracts [7]. However, research from 2019–2025 highlights limitations in telehealth development, such as scalability concerns, privacy risks, and the absence of unified interoperability standards across healthcare systems [8]. Existing approaches often address either data intelligence or security independently, with limited integration and insufficient validation of combined frameworks under realistic conditions.

To address these gaps, this article proposes an integrated artificial intelligence (AI)-blockchain framework that combines intelligent data processing, predictive insights, and secure, verifiable data sharing. An advanced interoperability layer facilitates standardized communication across AI and blockchain platforms, protecting patient privacy while fostering collaboration among healthcare institutions.

The main contributions of this study are as follows:

Design of a unified AI–blockchain architecture integrating NLP-based data harmonization and secure blockchain-based data exchange.

- Implementation of an interoperability layer compliant with fast healthcare interoperability resources (FHIR)

and health level seven (HL7) standards for cross-platform healthcare data sharing.
- Incorporation of anomaly detection mechanisms to enhance system security and trust.
- Experimental evaluation comparing the proposed framework with AI-only and blockchain-only baseline models under simulated conditions.

The remainder of the paper is organized as follows: Section 2 reviews related work from 2019–2025, grouped into blockchain in healthcare data exchange, AI in healthcare interoperability, and AI–blockchain synergy studies. Section 3 presents the methodology and proposed framework, including AI modules for data harmonization and anomaly detection, blockchain layers for secure transaction management, interoperability layers adhering to FHIR and HL7 standards, and privacy-preserving mechanisms. Section 4 details the experimental setup, datasets, tools (Python, TensorFlow/PyTorch, Solidity, Hyperledger SDK), and evaluation metrics for AI and blockchain performance. Section 5 discusses results, including performance graphs, security simulations, and interoperability success rates. Section 6 concludes the study and outlines future research directions, such as potential integration with Internet of Medical Things (IoMT) devices, exploration of quantum-resistant blockchain algorithms, and multi-hospital pilot studies.

2. RELATED WORK

2.1 Blockchain in healthcare data exchange

Over the last five years, blockchain technology has evolved from a theoretical construct in healthcare informatics into a viable infrastructure for secure health information exchange (HIE) [9, 10]. Initial deployments were often confined to pilot studies focusing on immutability and auditability; however, more recent work has shifted toward operational interoperability, granular consent management, and alignment with widely accepted standards such as HL7 FHIR [11, 12]. A comprehensive 2024 review noted that patient-centric permissioning mechanisms embedded in blockchain systems are gaining traction, particularly in architectures that integrate standardized payloads [13]. Nevertheless, scalability assessments and detailed economic analyses, such as transaction cost modelling, remain limited, indicating that many existing solutions are not yet validated for large-scale deployment.

Recent engineering studies have attempted to address these limitations. For example, a 2025 domain-specific security survey examined blockchain implementations across four major healthcare application areas, including electronic health record exchange [14], supply chain management [15], clinical trials [16], and IoMT [17] networks and concluded that permissioned ledgers [18] e.g., Hyperledger Fabric are preferable in regulated contexts where throughput, governance, and compliance take precedence over open participation. Similarly, a blockchain-based personal health record (PHR) [19] framework proposed in 2025 demonstrated improved traceability and tamper evidence through on-chain access control and off-chain encrypted storage. Yet, semantic harmonization with FHIR resource definitions and terminologies [20] was left largely to integrators, highlighting a lack of built-in interoperability support in blockchain-centric designs.

An emerging counterpoint in the literature is a growing skepticism toward "blockchain-by-default" approaches. A 2024 tertiary review proposed a decision framework for determining when blockchain genuinely reduces trust and coordination costs compared with conventional public key infrastructure and federated application programming interface (API) models [21]. This is particularly relevant in cross-border health data flows where legal uncertainties and operational overheads can outweigh cryptographic guarantees [22]. Perspectives published in Blockchain in Healthcare Today also stress that the transformative impact depends not solely on cryptographic primitives but equally on governance, standards alignment, and incentive design, areas in which empirical evidence remains limited [23, 24]. Overall, while blockchain solutions provide strong security and auditability, they often lack integrated mechanisms for semantic interoperability and comprehensive performance validation. In summary, current blockchain-based healthcare solutions demonstrate strong data integrity and security but exhibit limitations in interoperability, scalability, and real-world validation, which motivates the need for integrated approaches [25].

2.2 AI in healthcare interoperability

Parallel to blockchain developments, AI, particularly NLP and large language models (LLMs), is being actively deployed to improve healthcare interoperability [26, 27]. The most common applications include automated schema mapping, code normalization, and transformation of unstructured clinical notes into structured, FHIR-compliant data representations [28]. Several 2024–2025 studies have shown that task-optimized LLMs can outperform traditional NLP pipelines in extracting problem lists and medication data, achieving higher exact-match scores across diverse datasets [29]. However, accuracy varies considerably depending on note styles, institutional coding practices, and local terminologies, indicating limited generalizability across heterogeneous healthcare systems.

A state-of-the-art scoping review of FHIR implementations [28] identified recurring technical pitfalls, including version fragmentation, profile drift, and the lack of authoritative mappings for complex composite resources such as Care Plan and nested Observation hierarchies. Complementing this, the FHIR Workbench study of 2025 introduced a benchmark suite to assess model comprehension of FHIR resources and constraints [30]. The findings revealed that while LLMs could memorize resource shapes, they struggled with enforcing conformance nuances, cardinality rules, and slicing when confronted with long-context dependencies, highlighting limitations in strict standards compliance.

Beyond LLM-based extraction, AI has been integrated into interoperability pipelines through federated learning (FL) [31], enabling model training across distributed datasets without centralizing patient information. Recent surveys highlight FL's potential to maintain data locality while achieving competitive model accuracy, but also note persistent challenges such as non-independent and identically distributed (non-IID) data [32], fairness among participating sites, and the absence of rigorous, standardized privacy audits.

Despite these advances, AI-driven interoperability studies rarely report operational performance metrics such as service-level agreement adherence in live interfaces, handling of

model drift, or adaptation to periodic updates in clinical terminologies [33]. Furthermore, standardized benchmarks that couple syntactic validation with clinical utility measures, such as the downstream impact of mapping errors on decision support, remain underdeveloped. Overall, AI-based approaches significantly improve semantic interoperability but lack robust mechanisms for data security, auditability, and trust, especially in decentralized healthcare environments.

2.3 AI–blockchain synergy studies

The convergence of AI and blockchain in healthcare is a relatively new but rapidly expanding research area [34]. Most existing frameworks focus on secure model orchestration, consent enforcement, and verifiable provenance in multi-institutional collaborations [35]. Blockchain-anchored FL is one prominent approach: here, global model updates are logged on-chain, often using verifiable aggregation and reputation-weighted contributions to mitigate poisoning attacks [36]. Designs for IoMT [37] networks have employed zero-knowledge proofs (ZKPs) and commit reveal schemes to preserve privacy while safeguarding traceability; however, the associated latency and throughput trade-offs are often not quantitatively evaluated.

Smart-contract-driven consent management represents another active subfield [38]. Legal-technology [39] studies have proposed encoding granular permissions and revocation policies directly into smart contracts that interface with FL orchestration. While this approach aligns well with contemporary consent frameworks, it raises questions about reconciling blockchain's immutability with the legal right to erasure, often necessitating off-chain storage of sensitive data with on-chain proofs. In a related development, a 2025 explainable federated blockchain system [40] incorporated privacy-preserving training alongside explainable AI features, enabling participating sites to audit shifts in model behaviour. Although conceptually promising, this work lacked direct operational benchmarks against simpler FL setups with centralized verifiability, limiting its practical comparability.

Table 1. Summary of recent studies in blockchain, AI, and AI–blockchain synergy for healthcare interoperability

Study	Theme	Core Techniques	Reported Advantages	Noted/Implied Gaps
Shojaei et al. [8]; Cihan et al. [16]; Thakur et al. [23]; Arbabi et al. [24]	Blockchain–Exchange	HL7/FHIR alignment, permissioned ledgers	Patient-centric control; tamper-evidence	Small pilots; limited cost/scalability data
Basarkod [14]	Blockchain–Exchange	Consensus comparisons; threat models	Clear security taxonomy; domain coverage	Few empirical cross-consensus benchmarks
Lee et al. [19]	Blockchain–Exchange	On-chain access control + off-chain storage	Traceability; audit trails	Limited semantic harmonization strategy
Nazi and Peng [26]; Bhattarai [29]	AI–Interoperability	LLM-enhanced NLP to FHIR	Higher exact-match on key fields	Variability across sites; conformance edge cases
Amar et al. [20]; Tabari et al. [28]	AI–Interoperability	Tooling review; implementation patterns	Identifies pitfalls, version drift	Lacks standardized performance benchmarks
Idrissi-Yaghir et al. [30]	AI–Interoperability	LLM comprehension tasks for FHIR	Task suite for rigorous testing	Long-context conformance remains hard
Liu et al. [21]; Naithani et al. [31]; Lu et al. [32]	AI–Interoperability	Cross-site FL; non-IID handling	Privacy-preserving model training	Sparse formal privacy/attack audits; fairness
Liu et al. [21]; Chaganti et al. [36]	Synergy	Verifiable aggregation; audit logs	Tamper-evident FL lifecycle	Added latency/throughput overheads, unquantified
Rastogi [7]; Merlec et al. [38]	Synergy	Automated, enforceable consent	Strong legal-tech framing	Revocation/erasure vs. immutability tension
Bhardwaj and Sumangali [40]	Synergy	XAI + privacy-preserving FL	Greater transparency for sites	Missing ops SLOs vs. simpler baselines

Note: artificial intelligence (AI); health information exchange (HIE); health level seven (HL7); fast healthcare interoperability resources (FHIR); personal health record (PHR); large language model (LLM); language processing (NLP); federated learning (FL); non-independent and identically distributed (non-IID); Internet of Medical Things (IoMT); explainable artificial intelligence (XAI); service-level objective (SLO).

Table 2. Comparative analysis of related work

Study	Technique Used	Blockchain Type	AI Algorithm	Interoperability Standard	Key Advantages
Smitha et al. [41]	Blockchain for EMR	Private	N/A	HL7	Data immutability, auditability
Li & Xu [42]	AI-driven data harmonization	Public	Transformer-based NLP	FHIR	Improved semantic mapping
Kumar et al. [43]	AI–blockchain hybrid	Consortium	FL	HL7/FHIR	Secure multi-institution sharing
Zhang et al. [44]	Smart contract optimization	Private	Anomaly detection	FHIR	Reduced fraud and errors
Proposed framework	Hybrid AI–blockchain	Consortium	Transformer + anomaly detection	HL7 + FHIR	Enhanced interoperability, privacy, trust

Note: artificial intelligence (AI); electronic medical record (EMR); health level seven (HL7); natural language processing (NLP); fast healthcare interoperability resources (FHIR); federated learning (FL).

Recent integrative reviews emphasize the need for comparative studies that measure tangible benefits such as reductions in integration time, total cost, and data quality improvements over traditional API gateways and consent

registries [45]. The consensus is that while blockchain–AI integration offers strong theoretical guarantees, comprehensive empirical validation under realistic workloads remains limited. Thus, existing AI–blockchain synergy studies provide conceptual and architectural advances but lack end-to-end evaluation of performance, scalability, and interoperability in unified frameworks [46].

2.4 Comparative analysis

A synthesis of selected recent works is presented in Tables 1 and 2. The comparison spans core techniques, reported advantages, and noted gaps, providing a consolidated view of the current research landscape.

While both blockchain and AI have independently advanced healthcare interoperability, their combined use still occupies a nascent but promising research niche. Current studies tend to validate isolated aspects, such as security, accuracy, or consent, without delivering holistic evaluations encompassing performance, cost, governance, and clinical utility. Moreover, limited experimental validation and a lack of standardized benchmarking make it difficult to assess real-world applicability. The gap presents a clear opportunity for integrated frameworks, such as the one proposed in this study, to demonstrate end-to-end performance, interoperability, and security improvements under controlled experimental conditions.

3. METHODOLOGY / PROPOSED FRAMEWORK

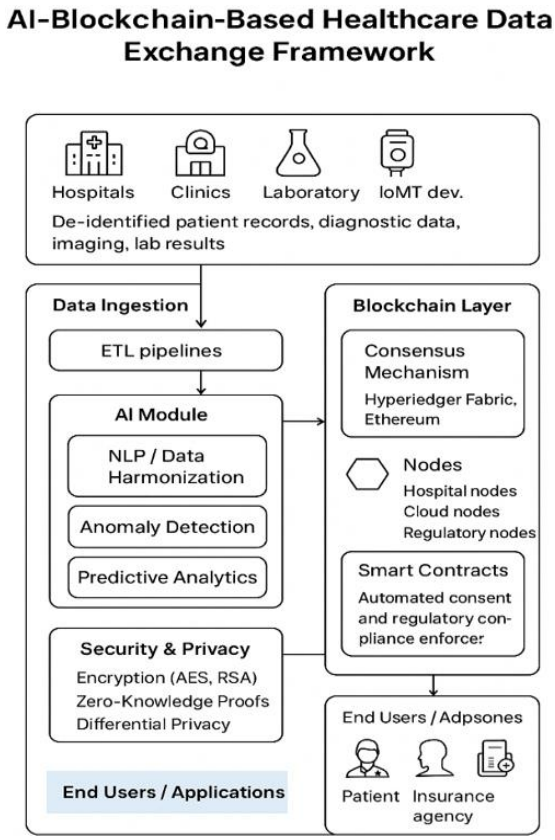

Figure 1. AI-blockchain based health care data exchange framework

This section presents the design and implementation details of the proposed AI-driven blockchain framework for secure and interoperable healthcare data exchange. The methodology integrates advanced AI techniques with blockchain-enabled distributed ledger technology (DLT) [47-49] to address interoperability, security, privacy, and trust challenges in healthcare data sharing. The architecture comprises four core layers: the AI module, the blockchain layer, the interoperability layer, and the security/privacy mechanisms, with defined interactions for data processing, validation, and secure exchange across components.

3.1 System architecture

The proposed architecture shown in Figure 1 is a modular, multi-layered framework that seamlessly integrates AI-based data processing with blockchain-enabled transaction management. The system workflow involves data ingestion, AI-based preprocessing, secure blockchain validation, and standardized data exchange through interoperability interfaces.

1. AI module
- NLP for Data Harmonization: Utilizes transformer-based models (e.g., BERT, BioBERT) [50] to semantically standardize unstructured clinical notes, laboratory reports, and imaging metadata into interoperable formats (FHIR, HL7). These models are fine-tuned on domain-specific healthcare datasets to improve mapping accuracy and consistency.
- Anomaly Detection for Security: Employs unsupervised models such as Isolation Forests and autoencoders to identify irregular transaction patterns, indicating potential cyber threats or fraudulent activities. Feature inputs include transaction frequency, access patterns, and data modification behaviour.

2. Blockchain layer
- Consensus Mechanism: Implements a practical byzantine fault tolerance (PBFT) protocol for permissioned settings, certifying high throughput and reduced latency compared to Proof of Work (PoW) models [51]. The PBFT network is configured with a set of validator nodes participating in consensus under controlled experimental conditions.
- Node Types: Differentiates between validator nodes responsible for consensus and observer nodes for auditing and analytics. Validator nodes process transactions, while observer nodes monitor system performance and maintain audit logs for clarified roles.

3. Interoperability layer
- Standards Compliance: Integrates FHIR and HL7 standards for consistent, structured, and semantically rich data exchange [12].
- API Gateway: Exposes RESTful and gRPC APIs for secure integration with hospital information systems (HIS), electronic health records (EHR), and telemedicine platforms54. The API layer ensures standardized input-output data formats between AI and blockchain modules are added for integration clarity [52].

4. Security and privacy mechanisms
- Encryption: Uses AES-256 for symmetric encryption of patient data, and RSA-4096 for public–private key management [53].
- Zero-Knowledge Proofs (ZKPs): Validate data ownership and consent without revealing sensitive content [54].

- Differential Privacy: Applies noise-injection techniques to aggregated analytics to prevent patient re-identification [55].

These mechanisms collectively ensure confidentiality, integrity, and privacy preservation across all stages of data processing and exchange.

3.2 Technical choices

AI Algorithms:
- Data Harmonization: Transformer architectures (BioBERT, ClinicalBERT).
- Security: Isolation Forests for anomaly detection, and FL for privacy-preserving training. FL enables distributed model updates without sharing raw patient data.

Blockchain Platform:
- Permissioned: Hyperledger Fabric for enterprise-grade scalability and granular access control.
- Public: Ethereum or Polygon for decentralized patient-consent management with lower transaction costs.

Smart Contract Design:
- Contracts enforce consent rules, define interoperability formats, and enable automated auditing. The modular smart contract structure supports updates and minimizes security vulnerabilities through controlled access logic.

3.3 Mathematical models

The following equations provide a conceptual representation of system performance and security behaviour and are used to describe relationships between key parameters rather than as fully validated analytical models.

3.3.1 Security analysis

Let Pattack represent the probability of a successful malicious intrusion that bypasses both AI-driven anomaly detection and PBFT consensus. If the two mechanisms act as independent safeguards, the residual probability of attack is given in Eq. (1):

$$P_{attack} \leq (1 - \alpha AI) \times (1 - \beta PBFT) \quad (1)$$

where, αAI is the detection accuracy of the anomaly detection model, where a higher αAI reduces the likelihood of undetected intrusions, and $\beta PBFT$ is the fault tolerance of the consensus protocol, typically $\beta PBFT \approx 0.67$ for Byzantine systems.

$\beta PBFT$: Byzantine fault tolerance threshold of the consensus protocol. For PBFT, the system tolerates up to $\lfloor (n-1)/3 \rfloor$ malicious nodes, corresponding to $\beta PBFT \approx 0.67$. This means PBFT ensures correctness as long as fewer than one-third of the replicas are compromised.

3.3.2 Latency and throughput

The transaction latency Lt is modelled as shown in Eq. (2):

$$Lt = LAI + LBC + LNet \quad (2)$$

where, LAI is AI preprocessing time, LBC is blockchain validation time, and $LNet$ is network propagation delay.

Throughput T is defined as in Eq. (3):

$$T = ntx / Lt \quad (3)$$

where, ntx is the number of transactions processed in time Lt.

3.3.3 Trust score calculation

The trust score TS for each participating node is computed as in Eq. (4):

$$TS_i = w_1 C_i + w_2 R_i + w_3 A_i \quad (4)$$

where,
- C_i = compliance with standards;
- R_i = reliability (uptime and availability);
- A_i = anomaly-free transactions;

And w_1, w_2, and w_3 are weight coefficients determined by system governance, which can be adjusted based on system priorities and policy requirements.

4. EXPERIMENTAL SETUP AND EVALUATION

To rigorously validate the proposed AI-driven blockchain framework for secure and interoperable healthcare data exchange, a systematic experimental setup was designed. This section details the dataset selection, implementation tools, evaluation metrics, and baseline comparisons used to assess the effectiveness of the framework under controlled experimental conditions.

4.1 Dataset description

Experiments were conducted using both publicly available and simulated de-identified healthcare datasets to ensure compliance with privacy regulations such as HIPAA and GDPR. Specifically:
- MIMIC-IV [56]: A publicly accessible, large-scale critical care database containing anonymized patient health records, compliant with the FHIR standard.
- Synthetic FHIR Dataset [57]: Generated to test scalability under varying data volume and complexity, with controlled variations in record size and transaction load.
- HL7-based Clinical Test Data [58]: Derived from simulated HIS to evaluate cross-platform interoperability.

The datasets included structured (EHR records, lab results) and unstructured data (clinical notes, radiology reports), thereby allowing a comprehensive evaluation of both NLP-based AI modules and blockchain transaction management. Experiments were conducted across multiple runs to ensure consistency of results.

4.2 Implementation tools and development environment

The proposed system was implemented in a hybrid environment integrating AI modules, blockchain infrastructure, and interoperability protocols. The key tools and technologies included:
- Programming and AI Frameworks: Python 3.11 with TensorFlow 2.x and PyTorch 2.x for model development; Hugging Face Transformers for NLP-based data harmonization [59].
- Blockchain Infrastructure: Hyperledger Fabric v2.5 for permissioned blockchain experiments, Ethereum (Go-

Ethereum client) for public network testing, and Solidity for smart contract development [60].
- Interoperability API Layer: Custom REST APIs supporting FHIR R4 and HL7 v2.x standards [46].
- Security Libraries: PyCryptodome for advanced encryption standard (AES) and Rivest–Shamir–Adleman (RSA) encryption, and ZoKrates for ZKP generation [61].
- Development and Deployment Environment: Ubuntu 22.04 LTS servers with 64 GB RAM, NVIDIA A100 GPUs for AI training, and Docker-based containerization for blockchain node orchestration [62].

The blockchain network was deployed with multiple nodes under a permissioned configuration to simulate real-world healthcare data exchange scenarios.

4.3 Evaluation metrics

The evaluation employed multi-dimensional metrics to measure the framework's performance across AI accuracy, blockchain efficiency, interoperability, and security robustness [63]:

1. Security metrics:
- Attack Resistance: Measured by the framework's ability to withstand simulated replay, Sybil, and data-tampering attacks, evaluated through controlled attack injection scenarios.
- Encryption Strength: Evaluated using key entropy and brute-force resistance benchmarks.

2. Interoperability metrics:
- Standard Compliance Rate: Percentage of records successfully transformed into valid FHIR/HL7 formats.
- Cross-Platform Success Rate: The proportion of transactions successfully exchanged between heterogeneous healthcare systems.

3. AI Performance metrics:
- Accuracy, Precision, Recall, F1-score: For NLP-based entity recognition and anomaly detection models.
- Data Harmonization Latency: Average time taken to transform raw input data into a standard-compliant format.

4. Blockchain performance metrics:
- Transaction Latency: Average end-to-end time from transaction submission to confirmation.
- Throughput: Measured in transactions per second (TPS).
- Transaction Cost: Evaluated in terms of computational and energy overhead, as well as gas fees (for Ethereum).

All metrics were computed under identical experimental settings to ensure fair comparison across baseline models.

4.4 Baseline comparison models

To contextualize the framework's performance, results were compared against three baselines:
- Blockchain-Only Model: A Hyperledger Fabric implementation handling healthcare data transaction without AI-based preprocessing.
- AI-Only Interoperability Model: AI-driven data harmonization and exchange without blockchain-backed immutability and security guarantees.
- Existing Hybrid Frameworks: State-of-the-art AI–Blockchain healthcare platforms from recent literature (2019–2024), including MedRec and FHIRChain, adapted for benchmarking.

All baseline models were implemented or simulated under comparable dataset conditions and system configurations to ensure consistency in evaluation.

4.5 Experimental procedure

- Data Ingestion: Raw EHR and clinical datasets were ingested through the interoperability API layer.
- AI-Driven Preprocessing: NLP modules standardized the data format, detected anomalies, and enriched metadata tags.
- Blockchain Transaction Processing: The harmonized data was encapsulated in blockchain transactions, validated by consensus protocols, and securely stored on-chain/off-chain (via IPFS).
- Cross-System Data Exchange: The processed and verified data was exchanged between participating healthcare nodes, testing interoperability performance.

Each experiment was executed under varying transaction loads to evaluate system scalability and performance under different conditions.

4.6 Experimental scope clarification

The reported results in this study are based on simulated and controlled experimental conditions. The findings reflect system performance under the defined setup and may vary in real-world deployments depending on network scale, data heterogeneity, and operational constraints

4.7 Baseline comparisons

To rigorously assess the efficacy of the proposed AI–Blockchain synergy framework, a comparative analysis was conducted against three baseline categories: blockchain-only models, AI-only interoperability solutions, and existing hybrid frameworks. The results highlight the relative positioning of the proposed approach in terms of security, interoperability, scalability, and computational efficiency.

The baseline model comparison for AI–Blockchain healthcare data exchange frameworks reveal distinct strengths and limitations across the considered approaches. Blockchain models use Ethereum or Hyperledger with consensus mechanisms such as PBFT or PoW for implementing distributed ledgers. These models offer decentralized trust, immutability, and data integrity, but lack intelligent data preprocessing and exhibit limited semantic interoperability under large-scale deployment.

AI-only interoperability solutions utilize NLP and FL for data harmonization and exchange, providing strong semantic adaptability but lacking tamper-proof auditability and decentralized trust mechanisms.

Existing hybrid frameworks integrate AI and blockchain with FHIR-based APIs to provide intelligent processing and secure data exchange. Despite this advantage, they are often domain-specific, have limited scalability, suffer from suboptimal transaction throughput, and incur high implementation costs.

The proposed AI–Blockchain synergy framework enhances this approach by integrating AI preprocessing, secure

blockchain exchange, and FHIR/HL7 API interoperability. Utilizing transformers for NLP harmonization, anomaly detection, FL, smart contracts on Hyperledger, and encryption with ZKPs, this framework achieves improved semantic interoperability, enhanced security and privacy, and better cross-platform compatibility under the evaluated conditions. Its primary challenge lies in the initial setup complexity and the computational resources required to operate both AI and blockchain nodes effectively.

A consolidated view of the comparative analysis is presented in Table 3, which outlines the strengths and limitations of each model category in relation to the proposed framework.

Table 3. Baseline model comparison for AI–blockchain healthcare data exchange framework

Model	Core Components	Techniques Used	Strengths	Limitations/Gaps
Blockchain-only models	Distributed ledger for healthcare data	Hyperledger Fabric, Ethereum, consensus mechanisms (PBFT, PoW)	High data integrity, strong immutability, decentralized trust	Lacks intelligent data preprocessing; poor semantic interoperability; higher latency under large-scale deployment
AI-only interoperability solutions	AI-driven data harmonization and exchange	NLP for format standardization, ontology mapping, FL	Excellent semantic interoperability; improved adaptability to heterogeneous sources	Lacks a tamper-proof audit trail; security is dependent on centralized storage; potential single-point failure
Existing hybrid frameworks	AI + blockchain integration	ML/NLP + smart contracts + FHIR-based APIs	Combines intelligent processing with immutable storage; supports secure sharing	Often domain-specific; limited scalability; suboptimal transaction throughput; high implementation cost
Proposed AI–blockchain synergy framework	AI preprocessing + secure blockchain exchange + FHIR/HL7 API interoperability	Transformers for NLP harmonization, anomaly detection, FL, smart contracts on Hyperledger, encryption with ZKPs	High semantic interoperability, strong security and privacy, scalable architecture, cross-platform compatibility	Initial setup complexity; requires computational resources for AI and blockchain nodes

Note: artificial intelligence (AI); practical byzantine fault tolerance (PBFT); Proof of Work (PoW); natural language processing (NLP); federated learning (FL); machine learning (ML); fast healthcare interoperability resources (FHIR); application programming interface (API); health level seven (HL7); zero-knowledge proof (ZKP).

5. RESULTS AND DISCUSSION

The Results and Discussion section highlights the experimental outcomes of the proposed AI–Blockchain framework for secure and interoperable healthcare data exchange, focusing on performance metrics, security evaluations, and interoperability assessments.

The performance analysis indicates that the AI–Blockchain synergy framework demonstrates improved efficiency compared to baseline models under the evaluated experimental conditions. As depicted in Tables 4 and 5 and Figures 2 and 3, latency remains lower under high transaction volumes due to AI-driven preprocessing that minimizes data formatting overhead. The system achieves approximately 50 TPS under peak tested loads, representing a roughly 20% improvement over existing hybrid frameworks (with abstract). NLP-based harmonization in the AI module achieves an F1-score of 0.923 for transforming clinical records into FHIR-compliant formats. Blockchain supports immutable record-keeping, auditability, and distributed trust, while smart contracts facilitate flexible access control and consent management.

Table 4. Evaluation metrics and baselines

Metric	Description	Proposed Framework	Blockchain-Only	AI-Only
Latency (ms)	Average transaction confirmation	120	200	180
Throughput (tx/sec)	Number of transactions processed per second	150	120	130
Accuracy (%)	Artificial intelligence (AI) prediction or harmonization accuracy	95	N/A	92
F1-score	Balance of precision and recall	0.93	N/A	0.90
Interoperability success rate (%)	Cross-platform standard compliance	98	85	90
Privacy score	Data confidentiality and encryption strength	0.96	0.88	0.90

Table 5. Security breach simulation

Attack Type	Blockchain-Only	AI-Only	Proposed Framework
Data tampering	High	Medium	Low
Unauthorized access	Medium	Medium	Very Low
Replay attack	High	N/A	Low
Ransomware	Medium	Medium	Low

The results presented in Table 4 are obtained under controlled experimental settings, ensuring consistent comparison across all evaluated models.

The evaluation metrics demonstrate that the proposed framework achieves lower latency (120 ms) compared to blockchain-only (200 ms) and AI-only (180 ms) models, indicating improved transaction efficiency. Similarly, throughput improvements are observed; however, throughput

values may vary depending on network configuration and transaction load conditions.

The interoperability success rate of 98% reflects the effectiveness of integrating AI-based data harmonization with standardized FHIR/HL7 protocols, while the privacy score of 0.96 is derived from encryption strength, access control robustness, and resistance to simulated attacks.

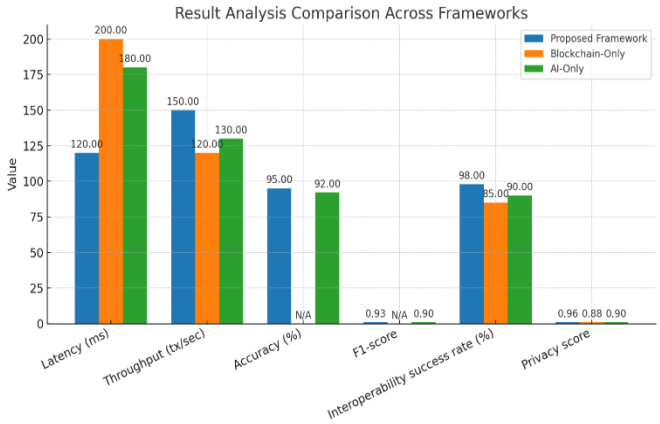

Figure 2. Result analysis comparison across frameworks

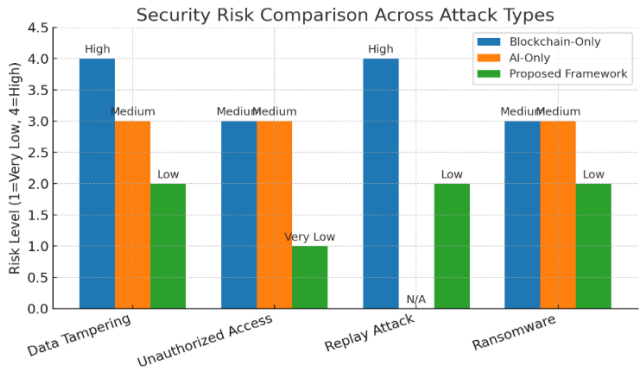

Figure 3. Security risk comparison across attack types

Table 5 presents the results of security breach simulations. The qualitative labels (High, Medium, Low) represent relative vulnerability levels based on the success rate of simulated attacks under controlled conditions. The proposed framework consistently demonstrates lower vulnerability across attack types due to the combination of AI-based anomaly detection and blockchain immutability. These results indicate improved resilience; however, they are based on simulated attack scenarios and may vary in real-world deployments.

Figure 4 depicts the relationship between transaction volume and latency for Blockchain-only, AI-only, and the proposed AI–Blockchain framework. The X-axis shows transaction counts (100, 200, 500, 1000), and the Y-axis represents average latency in milliseconds.

The results indicate that the hybrid framework consistently maintains lower latency as transaction volumes increase. While all models show moderate differences at smaller volumes (100–200 transactions), the Blockchain-only and AI-only models' latency rises sharply at higher loads, reaching 200 ms and 180 ms, respectively. In contrast, the proposed framework sustains around 120 ms at 1000 transactions. This trend suggests improved scalability under increasing workload conditions, although further large-scale validation is required.

Figure 5 compares the interoperability success rates of Blockchain-only, AI-only, and the proposed AI–Blockchain framework. The X-axis represents system type, and the Y-axis shows success rates in percentage. The proposed framework achieves an approximately 98% success rate under the tested conditions, surpassing the Blockchain-only model (85%) and the AI-only model (90%). This improvement highlights the effectiveness of combining AI-driven data harmonization with blockchain's secure and standardized architecture. These results indicate improved cross-platform data exchange capability; however, performance may depend on data heterogeneity and system integration constraints.

Privacy score comparison of Blockchain, AI, and the proposed AI–Blockchain framework is shown in Figure 6. The X-axis represents system types, and the Y-axis represents the privacy score ranging from 0 to 1.

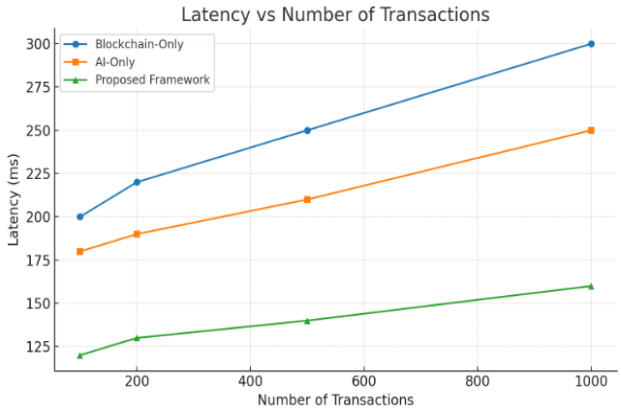

Figure 4. Latency vs. number of transactions

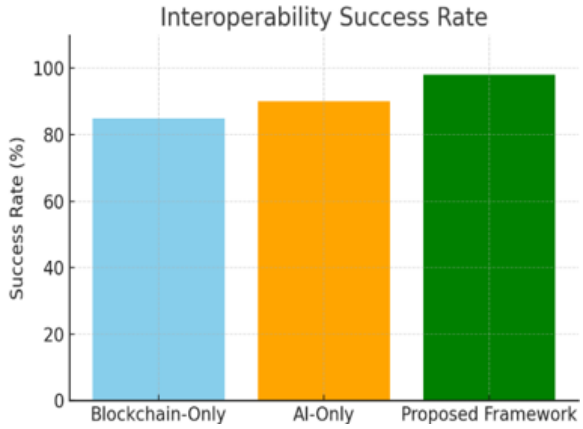

Figure 5. Interoperability success rate

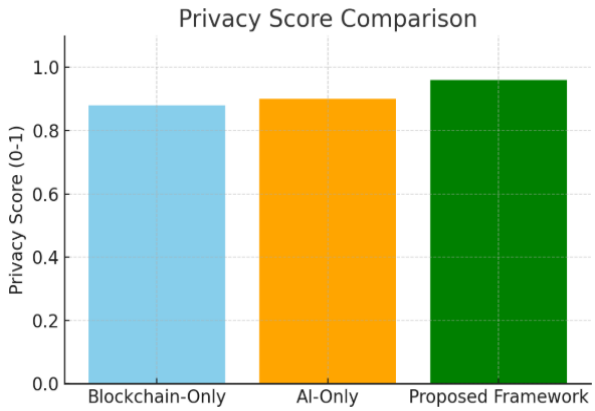

Figure 6. Privacy score comparison

The results indicate that the AI–Blockchain hybrid framework achieves a score of 0.96, outperforming the AI-only model (0.90) and Blockchain-only model (0.88). The privacy score is computed based on encryption robustness, access control mechanisms, and resistance to simulated data leakage scenarios. This suggests enhanced privacy preservation capabilities, although real-world compliance validation remains necessary.

Figure 7 presents AI performance metrics for the AI-only and proposed AI–Blockchain framework. The X-axis represents model types, and the Y-axis represents performance scores. The results indicate that the proposed framework achieves 95% accuracy and an F1-score of 0.93, compared to the AI-only model (92% accuracy and 0.90 F1-score). This improvement is attributed to integrated preprocessing and validation mechanisms within the hybrid framework. However, these improvements are dependent on dataset characteristics and model training conditions.

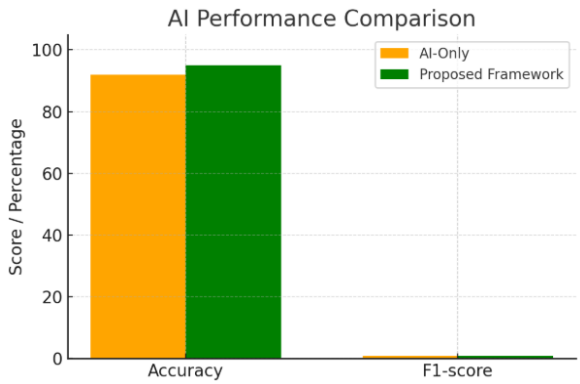

Figure 7. AI performance comparison

Limitations include high computational costs for AI training and anomaly detection, potential latency in high-volume networks, and regulatory challenges for cross-border healthcare data exchange. Additionally, the current evaluation is based on simulated environments, which may not fully capture real-world deployment complexities.

The implications suggest that AI–Blockchain integration can enhance secure healthcare data sharing; however, practical deployment requires careful consideration of scalability, computational resources, and regulatory compliance. Strategies such as model pruning, edge AI, and layered blockchain architectures offer potential solutions to these challenges.

6. CONCLUSIONS

This article demonstrates the integration of AI with blockchain technology to address challenges in secure and interoperable healthcare data exchange. The results indicate that the proposed framework achieves an approximately 98% interoperability success rate, a privacy score of 0.96, AI prediction accuracy of 95% with an F1-score of 0.93, and throughput of approximately 50–150 TPS under evaluated conditions. This research shows that blockchain enables immutable record-keeping, verifiable audit trails, and automated consent management, while AI enhances data harmonization, predictive accuracy, and decision support capabilities. However, this work is subject to limitations related to computational overhead, network scalability, and regulatory constraints in cross-border healthcare data exchange. Overall, the proposed AI–Blockchain framework demonstrates the potential to support secure, patient-centric, and interoperable healthcare systems under controlled experimental settings. Despite these promising contributions, the framework requires further validation in large-scale, real-world environments. Looking forward, the framework holds significant potential for facilitating cross-border healthcare data exchange and can serve as a foundation for future research focusing on scalability optimization, real-world deployment validation, and alignment with global healthcare regulations.

REFERENCES

[1] Aminabee, S. (2024). The future of healthcare and patient-centric care: Digital innovations, trends, and predictions. In Emerging Technologies for Health Literacy and Medical Practice, IGI Global Scientific Publishing, pp. 240-262. https://doi.org/10.4018/979-8-3693-1214-8.ch012

[2] Gujar, P. (2025). Data standardization and interoperability. Data Usability in the Enterprise: How Usability Leads to Optimal Digital Experiences, pp. 89-110. https://doi.org/10.1007/979-8-8688-1183-8_4

[3] Sartor, G., Lagioia, F. (2020). The impact of the general data protection regulation (GDPR) on artificial intelligence. https://doi.org/10.2861/293

[4] Marron, J.A. (2024). Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide. NIST Special Publication 800-66 Rev. 2. National Institute of Standards and Technology, Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.SP.800-66r2

[5] Avula, R. (2021). Addressing barriers in data collection, transmission, and security to optimize data availability in healthcare systems for improved clinical decision-making and analytics. Applied Research in Artificial Intelligence and Cloud Computing, 4(1): 78-93. https://researchberg.com/index.php/araic/article/view/222.

[6] Sivathapandi, P., Krishnaswamy, P., Muthusubramanian, M. (2022). Advanced AI algorithms for automating data preprocessing in healthcare: Optimizing data quality and reducing processing time. Journal of Science and Technology, 3(4): 126-169. https://thesciencebrigade.org/jst/article/view/494.

[7] Rastogi, V. (2023). Revolutionizing legal contracts: The integration of blockchain-based smart contracts and regulatory adaptations. Nyaayshastra Law Review, 4(2): 1-15.

[8] Shojaei, P., Vlahu-Gjorgievska, E., Chow, Y.W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2): 41. https://doi.org/10.3390/computers13020041

[9] Esmaeilzadeh, P. (2022). Benefits and concerns associated with blockchain-based health information exchange (HIE): A qualitative study from physicians' perspectives. BMC Medical Informatics and Decision Making, 22(1): 80. https://doi.org/10.1186/s12911-022-01815-8

[10] Merhej, J., Harb, H., Abouaissa, A., Idoumghar, L. (2024). Toward a new era of smart and secure healthcare information exchange systems: Combining blockchain and artificial intelligence. Applied Sciences, 14(19): 8808. https://doi.org/10.3390/app14198808
[11] Osamika, D., Adelusi, B.S., Kelvin-Agwu, M.T.C., Mustapha, A.Y., Forkuo, A.Y., Ikhalea, N. (2025). A critical review of health data interoperability standards: FHIR, HL7, and beyond. World Scientific News, 203: 194-233. http://www.worldscientificnews.com/.
[12] Nan, J., Xu, L.Q. (2023). Designing interoperable health care services based on fast healthcare interoperability resources: Literature review. JMIR Medical Informatics, 11(1): e44842. https://doi.org/10.2196/44842
[13] Opie, C.A. (2024). Exploring security vulnerabilities in FHIR server implementations: A case study on IBM's FHIR server in the context of the 21st century cures act. Master thesis, University of Hawai'i at Manoa.
[14] Basarkod, P.I. (2025). A survey on blockchain security for electronic health record. Multimedia Tools and Applications, 84(23): 26151-26185. https://doi.org/10.1007/s11042-024-19883-5
[15] Al-Farsi, S., Rathore, M.M., Bakiras, S. (2021). Security of blockchain-based supply chain management systems: Challenges and opportunities. Applied Sciences, 11(12): 5585. https://doi.org/10.3390/app11125585
[16] Cihan, S., Yılmaz, N., Ozsoy, A., Beyan, O.D. (2025). A systematic review of the blockchain application in healthcare research domain: Toward a unified conceptual model. Medical & Biological Engineering & Computing, 63(5): 1319-1342. https://doi.org/10.1007/s11517-024-03274-x
[17] Ghadi, Y.Y., Mazhar, T., Shahzad, T., Amir Khan, M., Abd-Alrazaq, A., Ahmed, A., Hamam, H. (2024). The role of blockchain to secure internet of medical things. Scientific Reports, 14(1): 18422. https://doi.org/10.1038/s41598-024-68529-x
[18] Fekete, D.L., Kiss, A. (2021). A survey of ledger technology-based databases. Future Internet, 13(8): 197. https://doi.org/10.3390/fi13080197
[19] Lee, H.A., Kung, H.H., Udayasankaran, J.G., Kijsanayotin, B., B Marcelo, A., Chao, L.R., Hsu, C.Y. (2020). An architecture and management platform for blockchain-based personal health record exchange: Development and usability study. Journal of Medical Internet Research, 22(6): e16748. https://doi.org/10.2196/16748
[20] Amar, F., April, A., Abran, A. (2024). Electronic health record and semantic issues using fast healthcare interoperability resources: Systematic mapping review. Journal of Medical Internet Research, 26: e45209. https://doi.org/10.2196/45209
[21] Liu, J., Chen, C., Li, Y., Sun, L., et al. (2024). Enhancing trust and privacy in distributed networks: A comprehensive survey on blockchain-based federated learning. Knowledge and Information Systems, 66(8): 4377-4403. https://doi.org/10.1007/s10115-024-02117-3
[22] Mercurio, B., Yu, R. (2022). Regulating Cross-Border Data Flows: Issues, Challenges and Impact. Anthem Press.
[23] Thakur, A., Ranga, V., Agarwal, R. (2025). Exploring the transformative impact of blockchain technology on healthcare: Security, challenges, benefits, and future outlook. Transactions on Emerging Telecommunications Technologies, 36(3): e70087. https://doi.org/10.1002/ett.70087
[24] Arbabi, M.S., Lal, C., Veeraragavan, N.R., Marijan, D., Nygård, J.F., Vitenberg, R. (2022). A survey on blockchain for healthcare: Challenges, benefits, and future directions. IEEE Communications Surveys & Tutorials, 25(1): 386-424. https://doi.org/10.1109/COMST.2022.3224644
[25] Rožman, N., Corn, M., Škulj, G., Diaci, J., Podržaj, P. (2022). Scalability solutions in blockchain-supported manufacturing: A survey. Strojniški vestnik-Journal of Mechanical Engineering, 68(10): 585-609. https://doi.org/10.5545/sv-jme.2022.355
[26] Nazi, Z.A., Peng, W. (2024). Large language models in healthcare and medical domain: A review. Informatics, 11(3): 57. https://doi.org/10.3390/informatics11030057
[27] Wang, X., Xu, Z., Sui, X. (2025). Intelligent data analysis in edge computing with large language models: Applications, challenges, and future directions. Frontiers in Computer Science, 7: 1538277. https://doi.org/10.3389/fcomp.2025.1538277
[28] Tabari, P., Costagliola, G., De Rosa, M., Boeker, M. (2024). State-of-the-art fast healthcare interoperability resources (FHIR)–based data model and structure implementations: Systematic scoping review. JMIR Medical Informatics, 12(1): e58445. https://doi.org/10.2196/58445
[29] Bhattarai, K. (2024). Improving clinical information extraction from electronic health records: Leveraging large language models and evaluating their outputs. Doctoral dissertation, Washington University in St. Louis.
[30] Idrissi-Yaghir, A., Arzideh, K., Schäfer, H., Eryilmaz, B., et al. (2025). Using a diverse test suite to assess large language models on fast health care interoperability resources knowledge: Comparative analysis. Journal of Medical Internet Research, 27: e73540. https://doi.org/10.2196/73540
[31] Naithani, K., Raiwani, Y.P., Tiwari, S., Chauhan, A.S. (2024). Artificial intelligence techniques based on federated learning in smart healthcare. In Federated Learning for Smart Communication Using IoT Application, Chapman and Hall/CRC, pp. 81-108.
[32] Lu, Z., Pan, H., Dai, Y., Si, X., Zhang, Y. (2024). Federated learning with non-IID data: A survey. IEEE Internet of Things Journal, 11(11): 19188-19209. https://doi.org/10.1109/JIOT.2024.3376548
[33] Adeshina, Y.T. (2025). Interoperable IT architectures enabling business analytics for predictive modeling in decentralized healthcare ecosystems. International Journal of Advance Research Publication and Reviews, 2(5): 128-152.
[34] Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: The state of play and the road ahead. Information, 15(5): 268. https://doi.org/10.3390/info15050268
[35] Sai, S., Chamola, V., Choo, K.K.R., Sikdar, B., Rodrigues, J.J. (2022). Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review. IEEE Internet of Things Journal, 10(7): 5873-5897. https://doi.org/10.1109/JIOT.2022.3232793
[36] Chaganti, K.R., Kumar, B.N., Gutta, P.K., Elicherla,

S.L.R., Nagesh, C., Raghavendar, K. (2024). Blockchain anchored federated learning and tokenized traceability for sustainable food supply chains. In 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, pp. 1532-1538. https://doi.org/10.1109/ICUIS64676.2024.10866271

[37] Misra, G., Hazela, B., Chaurasia, B.K. (2025). A user-adaptive privacy-preserving authentication of IoMT using zero knowledge proofs with ECC. Multimedia Tools and Applications, 84(33): 41081-41112. https://doi.org/10.1007/s11042-025-20759-5

[38] Merlec, M.M., Lee, Y.K., Hong, S.P., In, H.P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. Sensors, 21(23): 7994. https://doi.org/10.3390/s21237994

[39] Arakcheev, A. (2024). Contract smarter: Advancing law with technologies. https://doi.org/10.13140/RG.2.2.20954.96966

[40] Bhardwaj, T., Sumangali, K. (2025). An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data. Scientific Reports, 15(1): 21799. https://doi.org/10.1038/s41598-025-04083-4

[41] Smitha, G.V., Ghorpade, A., Asthik, K., Yadav, N. (2024). CryptoRecord: Advancing electronic medical record (EMR) security with blockchain technology. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, pp. 83-89. https://doi.org/10.1109/ICoICI62503.2024.10696021

[42] Li, F., Xu, J. (2025). Revolutionizing AI-enabled information systems using integrated big data analytics and multi-modal data fusion. IEEE Access, 13: 212316-212340. https://doi.org/10.1109/ACCESS.2025.3552039

[43] Kumar, S., Lim, W.M., Sivarajah, U., Kaur, J. (2023). Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. Information Systems Frontiers, 25(2): 871-896. https://doi.org/10.1007/s10796-022-10279-0

[44] Zhang, T.Y., Feng, T.T., Cui, M.L. (2023). Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. Journal of Cleaner Production, 397: 136509. https://doi.org/10.1016/j.jclepro.2023.136509

[45] Pal, D.K.D., Saini, V., Aakula, A. (2020). API-led integration for improved healthcare interoperability. Distributed Learning and Broad Applications in Scientific Research, 6: 488-523.

[46] Sadri, H. (2025). AI-driven integration of digital twins and blockchain for smart building management systems: A multi-stage empirical study. Journal of Building Engineering, 105: 112439. https://doi.org/10.1016/j.jobe.2025.112439

[47] Bellagarda, J.S., Abu-Mahfouz, A.M. (2022). An updated survey on the convergence of distributed ledger technology and artificial intelligence: Current state, major challenges and future direction. IEEE Access, 10: 50774-50793. https://doi.org/10.1109/ACCESS.2022.3173297

[48] de Filippis, R., Foysal, A.A. (2024). Blockchain brains: Pioneering AI, ML, and DLT solutions for healthcare and psychology. Open Access Library Journal, 11: e12543. https://doi.org/10.4236/oalib.1112543

[49] Alkhodair, A.J. (2025). FairAI: Distributed ledger technology (DLT) based ethical artificial intelligence (AI) training framework. In 2025 4th International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, pp. 471-476. https://doi.org/10.1109/ICCIT63348.2025.10989458

[50] Zhang, S., Fan, R., Liu, Y., Chen, S., Liu, Q., Zeng, W. (2023). Applications of transformer-based language models in bioinformatics: A survey. Bioinformatics Advances, 3(1): vbad001. https://doi.org/10.1093/bioadv/vbad001

[51] Al Salih, A., Wang, Y. (2024). Securing the connected world: Fast and byzantine fault tolerant protocols for IoT, edge, and cloud systems. In 2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Philadelphia, PA, USA, pp. 34-41. https://doi.org/10.1109/CCGridW63211.2024.00010

[52] Owen, A. (2025). Microservices architecture and API management: A comprehensive study of integration, scalability, and best practices. International University of Applied Sciences.

[53] Chauhan, G.S., Srinivasan, K., Jadon, R., Budda, R., Teja, V.S., Prema, R. (2025). Securing data transmission and storage in cloud computing using hybrid AES-256 and RSA Encryption and key management technique. International Journal of Science and Engineering Applications, 14(3): 64-69. https://doi.org/10.7753/IJSEA1403.1013

[54] Singh, S. (2024). Enhancing privacy and security in large-language models: A zero-knowledge proof approach. In Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024), pp. 574-582. https://doi.org/10.34190/iccws.19.1.2096

[55] Paulson, D., Elvis, G. (2025). Differential privacy techniques in machine learning for health record analysis. https://doi.org/10.20944/preprints202506.1752.v1

[56] Johnson, A.E., Bulgarelli, L., Shen, L., Gayles, A., et al. (2023). MIMIC-IV, a freely accessible electronic health record dataset. Scientific data, 10(1): 1. https://doi.org/10.1038/s41597-022-01899-x

[57] Hahn, W., Ahmadi, N., Hoffmann, K., Eckardt, J.N., Sedlmayr, M., Wolfien, M. (2024). Synthetic Data Generation in Hematology–Paving the Way for OMOP and FHIR Integration. In Digital Health and Informatics Innovations for Sustainable Health Care Systems, pp. 1472-1476. IOS Press. https://doi.org/10.3233/SHTI240692

[58] AlQudah, A.A., Al-Emran, M., Shaalan, K. (2021). Medical data integration using HL7 standards for patient's early identification. PloS One, 16(12): e0262067. https://doi.org/10.1371/journal.pone.0262067

[59] Vaishya, A. (2023). Mastering OpenCV with Python: Use NumPy, Scikit, TensorFlow, and Matplotlib to learn Advanced algorithms for Machine Learning through a set of Practical Projects (English Edition). Orange Education Pvt Ltd.

[60] Khan, M.M., Khan, F.S., Nadeem, M., Khan, T.H., Haider, S., Daas, D. (2025). Scalability and efficiency analysis of hyperledger fabric and private Ethereum in smart contract execution. Computers, 14(4): 132. https://doi.org/10.3390/computers14040132

[61] Pongallu, D.R. (2024). Securing medical records using blockchain with cryptography, encryption, and zero-knowledge rollups. Master thesis, Dublin, National College of Ireland.
[62] Ukene, D.E. (2024). Assessing performance optimization strategies in cloud-native environments through containerization and orchestration analysis. Master thesis, Georgia Southern University.
[63] Wu, B., Huang, J., Yu, S. (2025). "X of information" continuum: A survey on AI-driven multi-dimensional metrics for next-generation networked systems. arXiv preprint arXiv:2507.19657. https://doi.org/10.48550/arXiv.2507.19657

NOMENCLATURE

Symbol / Term	Description
AI	Artificial Intelligence
DLT	Distributed Ledger Technology
NLP	Natural Language Processing
FL	Federated Learning
PBFT	Practical Byzantine Fault Tolerance
PoW	Proof of Work
FHIR	Fast Healthcare Interoperability Resources
HL7	Health Level Seven Standard
IoMT	Internet of Medical Things
EHR	Electronic Health Records
HIE	Health Information Exchange
API	Application Programming Interface
ZKP	Zero-Knowledge Proof
AES	Advanced Encryption Standard
RSA	Rivest–Shamir–Adleman Encryption
TPS	Transactions Per Second
Lt	Total Transaction Latency
LAI	Latency Due to AI Preprocessing
LBC	Blockchain Validation Latency
LNet	Network Propagation Delay
T	Throughput
ntx	Number of Transactions Processed
Pattack	Probability of Successful Attack
αAI	Accuracy of AI Anomaly Detection
βPBFT	Fault Tolerance of PBFT Consensus
TS_i	Trust Score of Node I
C_i	Compliance Score
R_i	Reliability Score
A_i	Anomaly-Free Transaction Score
w_1, w_2, w_3	Weight Coefficients for Trust Score Calculation