Secure Remote Healthcare Systems using Blockchain: Privacy Challenges and a Hyperledger Fabric–based Implementation

Ali M. A. Abuagoub
Department of Computer Engineering,
College of Computer Engineering & Sciences,
Prince Sattam bin Abdulaziz University, KSA

ABSTRACT
Remote healthcare systems have become integral to modern medical delivery, yet they continue to face persistent challenges related to privacy, security, interoperability, and trust. Centralized architectures expose sensitive clinical data to unauthorized access, manipulation, and single points of failure, underscoring the need for more resilient solutions. Blockchain technology provides a decentralized, tamper-resistant, and auditable foundation capable of mitigating these risks. This paper examines the core privacy challenges inherent in remote healthcare environments and presents a practical blockchain-based system implemented using Hyperledger Fabric, a permissioned enterprise-grade distributed ledger framework. The study synthesizes insights from contemporary blockchain applications—including electronic health records, pharmaceutical supply chains, clinical trials, and IoT-enabled monitoring—and integrates them into a working prototype featuring Go-based chaincode, a Node.js/Express backend, and a ReactJS frontend deployed within a Dockerized Fabric network. Functional and minimal-load testing demonstrate enhanced data integrity, transparent auditability, and secure remote access. The paper concludes with recommendations for future enhancements, including large-scale performance benchmarking, interoperability with hospital information systems, and cloud-based distributed deployment. The work contributes both conceptual and practical foundations for advancing secure, decentralized remote healthcare systems.

General Terms
Security, Privacy, Distributed Systems, Blockchain, Data Management, Telemedicine, Healthcare Informatics.

Keywords
Hyperledger Fabric, Remote Healthcare Systems, Electronic Health Records, Decentralized Health Data, Smart Contracts, Chaincode, IoT-Enabled Monitoring, Interoperability, Access Control, Auditability.

1. INTRODUCTION
Remote healthcare systems—including telemedicine platforms, remote diagnostics, and IoT-enabled patient monitoring—have expanded rapidly in response to global digital transformation and the growing demand for accessible medical services. As healthcare delivery increasingly extends beyond traditional clinical environments, ensuring the secure handling of sensitive patient information becomes essential. However, current remote healthcare infrastructures rely heavily on centralized databases and siloed information systems, making them susceptible to data breaches, unauthorized access, and operational disruptions. These weaknesses erode patient trust, compromise care quality, and complicate compliance with regulatory frameworks such as HIPAA and GDPR.

Blockchain technology has emerged as a promising foundation for addressing these challenges due to its decentralized architecture, immutability, cryptographic security, and transparent auditability. Recent studies demonstrate blockchain's applicability across multiple healthcare domains, including electronic health records (EHRs), pharmaceutical supply chain verification, clinical trial data management, genomics data sharing, and IoT-based monitoring. Despite these advancements, practical deployment within remote healthcare environments remains limited, particularly in areas such as role-based access control, logical deletion, interoperability, and user-friendly system interfaces.

Hyperledger Fabric, a permissioned blockchain framework developed under the Linux Foundation's Hyperledger Project, offers features well suited to healthcare applications, including identity-based access control, private channels, modular consensus mechanisms, and enterprise-grade scalability. This paper combines a sector-wide review of blockchain applications in healthcare with a practical Hyperledger Fabric implementation designed to secure remote medical data. The system incorporates Go-based smart contracts, a Node.js backend with JWT authentication, and a ReactJS frontend tailored for doctors, patients, and administrators. The implementation demonstrates how blockchain can enhance privacy, integrity, and trust in remote healthcare systems.

The remainder of this paper is organized as follows: Section 2 reviews related work and privacy challenges. Section 3 presents the system architecture and design. Section 4 describes implementation and testing. Section 5 discusses the results and evaluation. Section 6 concludes the study and outlines future work.

2. BLOCKCHAIN HEALTHCARE RESEARCH DOMAINS
Between 2020 and 2026, the rapid evolution of digital health ecosystems has generated extensive research exploring how blockchain, IoT, AI, and other decentralized architectures can enhance security, privacy, interoperability, and operational efficiency across healthcare domains. To capture this diversity, the literature is organized into eight thematic groups: (A) EHR security and interoperability, (B) pharmaceutical supply-chain traceability, (C) IoT/IoMT and digital-twin security, (D) AI–blockchain convergence, (E) telemedicine and remote healthcare, (F) healthcare insurance and financial systems, (G) adoption, governance, and policy, and (H) bibliometric and systematic reviews.

Each group is synthesized through a narrative overview supported by structured summary tables detailing the objectives, contributions, and limitations of the referenced works. As illustrated in Fig. 1, these groups form concentric thematic layers—from core technological foundations such as EHR security and IoT integration to broader operational, governance, and evidence-based dimensions. The diagram emphasizes how blockchain-enabled healthcare research evolves hierarchically: beginning with privacy and data-integrity mechanisms, extending through system-level interoperability and AI-driven intelligence, and culminating in governance frameworks and meta-analytical evidence.

The following subsections elaborate on each thematic group, providing detailed synthesis and comparative insights that collectively define the research landscape of blockchain-enabled healthcare between 2020 and 2026.

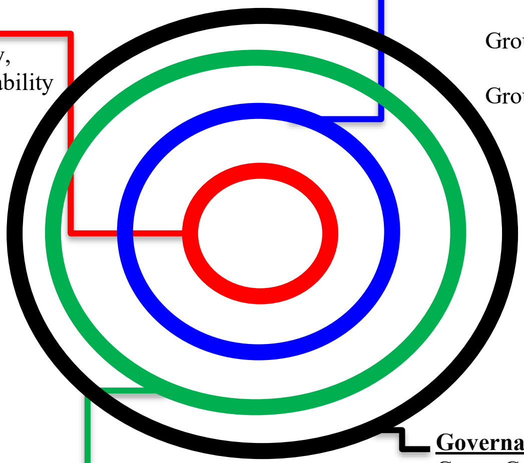

Fig. 1. Thematic relationship among related-work groups (2020–2026)

2.1 EHR Security, Privacy, and Interoperability

Blockchain-based EHR systems consistently strengthen confidentiality, provenance, and interoperability through decentralized architectures, permissioned ledgers, attribute-based encryption, self-sovereign identity, and hybrid on-/off-chain storage [1–14]. These mechanisms enhance auditability, reduce unauthorized access, and support cross-institutional data exchange. Recent work expands this foundation. Integrated ABAC–RBAC models with zero-knowledge proofs improve cloud-based access control [15]; decentralized HIE frameworks combining blockchain, IPFS, and HL7 FHIR compatibility enable scalable, patient-driven permissions [16]; permissioned Fabric-based designs increase confidentiality and throughput in controlled environments [17]; lightweight DLT architectures support trustworthy metadata management on constrained hardware [18]; and next-generation systems employing threshold cryptography and Avalanche consensus deliver high-performance, audit-ready EHR workflows [19]. User-centered evaluations also report strong acceptance of blockchain-enabled HIE platforms, with patients valuing granular access control, faster exchange workflows, and transparent permission management [20]. Despite these advances, challenges remain scalability limitations, key-management complexity, GDPR–immutability tensions, and integration barriers with legacy health IT infrastructures. Table 1 summarizes the main contributions and limitations of Group A studies.

Table 1. EHR Security & Interoperability

Ref	Subcategory	Contribution	Limitations / Challenges
[1]	Hybrid blockchain EHR	Public–private ledger; smart-contract consent; RBAC.	Integration complexity; scalability.
[2]	Smart contract EHR	Immutable logs; IPFS storage; decentralized access.	Regulatory alignment; limited deployment.
[3]	ABE-enabled EHR	Fine-grained ABE; tamper-resistant provenance.	ABE overhead; interoperability gaps.
[4]	Standards-aligned EHR	HIPAA/HL7-aligned decentralized exchange.	Legacy system integration.
[5]	Decentralized EHR	Cryptographic access policies; distributed storage.	Scalability; compliance encoding.
[6]	SSI-enabled EHR	SSI + adaptive access control; differential privacy.	SSI adoption complexity.
[7]	Blockchain EHR security	Privacy, integrity, secure access.	Scalability; legacy integration.
[8]	SSI-based EHR	Indy/Aries credentials; FHIR-based exchange.	SSI usability; interoperability.
[9]	BlockCare EHR	HIPAA/GDPR compliance; multisignature auth; FHIR/HL7 APIs.	Vendor integration barriers.
[10]	Clinical data management	Secure consent; audit trails; decentralized access.	Scalability; regulatory diversity.
[11]	U.S. EHR data sharing	Breach mitigation; tamper-resistant logs.	Fragmented U.S. ecosystem.

Ref	Subcategory	Contribution	Limitations / Challenges
[12]	DBHChain	MMPS + PoV consensus; high ledger integrity.	Multi-layer complexity; limited validation.
[13]	Secure data management	Transparent, interoperable exchange.	Organizational adoption barriers.
[14]	Scalable healthcare architecture	High-throughput ParallelChain; energy-efficient processing.	Integration complexity; consensus dependence.
[15]	Blockchain access control	ABAC–RBAC; multisignatures; ZKPs.	Policy complexity; signature overhead.
[16]	Blockchain-enabled HIE	IPFS storage; patient-driven permissions; FHIR compatibility.	Gas-cost sensitivity; legacy HIE integration.
[17]	Permissioned EHR sharing	Fabric + ABAC; AES-256 confidentiality.	Limited openness; encryption overhead.
[18]	Lightweight DLT workflows	Two-layer DLT; metadata-based privacy; low-resource deployment.	Limited scalability; metadata-only privacy.
[19]	Next-generation EHR architecture	Threshold cryptography; Avalanche consensus.	Key-management complexity; off-chain coordination.
[20]	HIE usability evaluation	High patient acceptance; strong access-control usability.	Narrow clinical sample; deployment challenges.

2.2 Pharmaceutical Supply Chain and Drug Traceability

Blockchain applications in pharmaceutical logistics consistently demonstrate improved drug provenance, serialization compliance, and counterfeit mitigation through tamper-proof ledgers, smart-contract automation, and decentralized verification [21–26]. These systems unify fragmented supply-chain workflows, enhance custody integrity, and accelerate recall operations by enabling secure, real-time authentication and interoperable tracking. Recent analyses also highlight adoption barriers, including limited technical expertise, high maintenance costs, and concerns over patient-related data security [27]. Broader challenges persist across the sector: regulatory fragmentation, heterogeneous data standards, high integration costs, and uneven organizational readiness. Table 2 summarizes the main contributions and limitations of blockchain-enabled pharmaceutical traceability.

Table 2. Pharmaceutical Supply Chain Traceability

Ref	Subcategory	Contribution	Limitations / Challenges
[21]	Drug authentication	Tamper-proof traceability; real-time authentication; decentralized verification.	Regulatory variation across regions.
[22]	Hyperledger Fabric supply chain	Continuous tracking; secure sharing; counterfeit detection.	Multi-country scalability.
[23]	FDA DSCSA Pilot	Serialized tracking; faster recall alerts.	Industry-wide interoperability.
[24]	MediLedger DSCSA	ZKP-enabled traceability; custody integrity.	Governance complexity.
[25]	PharmaChain	Fabric-based provenance; hybrid on/off-chain storage.	Confidentiality–transparency trade-offs.
[26]	Serialization regulations	Overview of 2025 global serialization requirements.	Harmonization challenges.
[27]	HSCM adoption barrier modeling	Identifies key adoption barriers via structured decision models.	Expert-driven results; limited real-world validation.

2.3 IoT, IoMT, Remote Monitoring, and Digital Twin Security

Blockchain-enabled IoT and IoMT systems enhance secure medical data streaming, device authentication, and trustworthy remote monitoring through decentralized architectures, lightweight cryptography, and edge/fog integration [28–32]. These approaches mitigate single points of failure, strengthen data integrity, and support continuous, verifiable sensor data exchange across distributed healthcare environments. Recent contributions extend these capabilities. Fog-enabled IoMT models integrate FB-ECC and GBCOA to provide low-latency sensor validation [33]; digital-twin security frameworks combine elliptic-curve cryptography with blockchain to ensure authenticated, resilient twin-based monitoring [34]; hierarchical ZKP-based authentication improves privacy and throughput in 5G-enabled edge settings [35]; and Hyperledger Fabric architectures incorporating Idemix deliver end-to-end anonymity and integrity for heterogeneous IoT ecosystems [36]. Across the literature, persistent limitations include device heterogeneity, latency overhead, energy constraints, and integration complexity within resource-constrained IoT environments. Table 3 summarizes Group C contributions and challenges.

Table 3. IoT / IoMT / Digital Twin Security

Ref	Subcategory	Contribution	Limitations / Challenges
[28]	IoT integrated EHR	Secure IoT-based EHR data sharing.	Device heterogeneity; latency.
[29]	Intelligent healthcare systems	IoT/AI + blockchain for automated secure data flows.	Scalability; regulatory constraints.
[30]	IoT-enabled healthcare	Secure IoT data; improved privacy and interoperability.	Energy limits; latency.
[31]	IoMT frameworks	Decentralized authentication; immutable IoMT exchange.	Device-level security; integration complexity.
[32]	Blockchain-enabled RPM /	Fabric-based secure RPM; off-chain	Scalability; multi-organization setup; device

Ref	Subcategory	Contribution	Limitations / Challenges
	IoMT	imaging support.	heterogeneity.
[33]	Fog-enabled IoMT security	FB-ECC + GBCOA for low-latency secure IoT data.	Fog-node overhead; optimization complexity; large-scale scalability.
[34]	Digital-twin IoT security	ECC + blockchain for authenticated resilient DT ecosystems.	Infrastructure demands; DT update overhead.
[35]	5G edge IoMT privacy	HBZKP for secure, low-latency IoMT in 5G edge environments.	ZKP complexity; edge-node dependence.
[36]	IoT privacy & anonymity	Fabric + Idemix for end-to-end privacy, anonymity, integrity.	High computational cost; heterogeneous device integration.

2.4 AI and Blockchain Convergence

Please use a 9-point Times Roman font, or other Roman font AI–blockchain convergence research highlights how blockchain provides trusted, immutable data pipelines for AI models, while AI enhances fraud detection, anomaly identification, clinical decision support, and operational intelligence [37–42]. Together, these technologies strengthen data reliability, automate decision workflows, and support secure analytics across distributed healthcare ecosystems. Recent contributions introduce advanced architecture that extend this synergy. Dual-layer sharded digital-twin blockchains improve throughput and resilience in distributed environments [43], while secure digital-twin data-sharing frameworks integrate attribute-based encryption and cloud-assisted access control to ensure confidentiality and controlled interoperability [44]. Despite these benefits, persistent challenges include algorithmic opacity, ethical and governance risks, computational overhead, and integration complexity across heterogeneous clinical systems. Table 4 summarizes the main contributions and limitations of AI–blockchain convergence research.

Table 4. AI–Blockchain Convergence

Ref	Subcategory	Contribution	Limitations / Challenges
[37]	AI–Blockchain review	Trusted data governance; AI-supported decision processes.	Ethical and regulatory barriers.
[38]	AI-enhanced blockchain	Secure exchange; improved automated decision workflows.	Privacy concerns; integration complexity.
[39]	Digital health trends	AI + blockchain for workflow automation and data integrity.	Adoption barriers.
[40]	AI cybersecurity risks	Blockchain mitigates AI-driven vulnerabilities; consent governance.	Professional acceptance; regulatory rigidity.
[41]	Blockchain-enabled AI disease classification	Hybrid blockchain–DL model for secure, accurate prediction.	Computational overhead; dataset dependence; integration complexity.
[42]	Blockchain-enabled deep learning	Tri-level SRNN + blockchain for secure, scalable processing.	Computational overhead; dataset dependence; workflow integration.
[43]	DT blockchain sharding	Dual-layer sharded DT blockchain with high throughput.	Complex architecture; edge-infrastructure requirements.
[44]	DT secure data sharing	Blockchain-enabled DT sharing with cloud-assisted ABE.	Added computation; integration complexity.

2.5 Telemedicine and Remote Healthcare Systems

Blockchain-enabled telemedicine systems enhance secure remote consultations, strengthen patient identity management, and support trustworthy cross-institutional data exchange through decentralized architectures that improve auditability, automate consent, and reduce reliance on vulnerable centralized platforms [45, 46]. These systems provide verifiable access control, transparent data-sharing workflows, and resilient communication channels for distributed care delivery. Recent contributions expand this evidence base. Privacy-preserving analytics using zk-SNARKs enable verifiable computation without exposing raw patient data [47], while systematic evaluations of decentralized telemedicine architectures highlight emerging encryption methods, interoperability requirements, and deployment considerations [48]. Despite these advances, persistent challenges include interoperability gaps, regulatory uncertainty, heterogeneous encryption mechanisms, and integration complexity across diverse telemedicine platforms. Table 5 summarizes the core contributions and limitations of blockchain-enabled remote healthcare systems.

Table 5. Telemedicine & Remote Healthcare

Ref	Subcategory	Contribution		Limitations / Challenges
[45]	Block MedCare	Secure remote data exchange; improved privacy and workflow transparency.		Limited real-world deployment.
[46]	BLOCKMEDCARE	Ethereum + AI + IoT for secure EHR and telemedicine.		Privacy concerns; scalability limits.
[47]	Privacy-preserving telemedicine analytics	zk-SNARK-based verifiable analytics without raw-data exposure.		High computation; multi-tenant cloud complexity.
[48]	Telemedicine blockchain review	Overview of decentralized telemedicine architectures and encryption methods.		Limited deployment evidence; heterogeneous platforms.

2.6 Healthcare Insurance and Financial Systems

Blockchain-enabled insurance systems enhance fraud detection, automate claims processing, and improve transactional transparency across healthcare finance through secure, tamper-resistant data exchange and verifiable audit trails [49–52]. These approaches strengthen billing integrity, streamline verification workflows, and support compliant, traceable interactions among insurers, providers, and patients. Recent contributions expand this landscape by examining blockchain's role in financial transparency, tokenized instruments, and privacy-preserving insurance automation [53–55]. These works highlight emerging models for decentralized financial governance, secure claims execution, and cost-hedging mechanisms enabled by tokenization and zero-knowledge proofs. Despite these advances, persistent challenges remain including regulatory constraints, legacy system integration, interoperability gaps, and limited organizational maturity. Table 6 summarizes Group F contributions and limitations.

Table 6. Healthcare Insurance & Financial Systems

Ref	Subcategory	Contribution	Limitations / Challenges
[49]	Insurance data security	Secure data exchange; fraud prevention; automated verification.	Scalability; regulatory integration.
[50]	Physician workflows	Secure workflows, billing, and fraud-reduction mechanisms.	Workflow-integration challenges.
[51]	AI-enhanced insurance security	Blockchain + AI for integrity protection and anomaly detection.	Dataset dependence; legacy integration; potential model bias.
[52]	Insurance market viability	HIPAA-aligned blockchain models linked to market readiness.	Low commercial traction.
[53]	Blockchain-enabled healthcare economics	Transparency improvements; reduced administrative friction; new financial models.	Editorial perspective; limited empirical evidence.
[54]	Blockchain-enabled financial instruments	Tokenized indices/futures for price transparency and cost hedging.	Need standardized data; regulatory uncertainty; interoperability barriers.
[55]	Blockchain-based insurance automation	zk-SNARK-enabled claims with high throughput and privacy.	Network dependence; legacy-integration complexity.

2.7 Adoption Models, Governance, and Policy

Governance-focused research emphasizes that blockchain adoption in healthcare depends on organizational readiness, regulatory alignment, and robust governance structures [56–68]. Common frameworks—including TOE, Fit-Viability, and institutional maturity models—highlight the importance of stakeholder coordination, compliance pathways, and structured decision processes for successful implementation. Recent analyses identify security, infrastructure readiness, and training availability as key enablers for blockchain adoption in emerging-economy healthcare supply chains [69]. Despite growing interest, persistent barriers remain including high implementation costs, skills shortages, regulatory fragmentation, and resistance to organizational change. Table 7 synthesizes the main contributions and limitations of governance and adoption research.

Table 7. Adoption, Governance & Policy

Ref	Subcategory	Contribution	Limitations / Challenges
[56]	Security adoption	Immutable audit trails; decentralized storage; breach protection.	High integration cost.
[57]	Practical adoption	Real-world deployments improving privacy and interoperability.	Regulatory uncertainty.
[58]	Clinical adoption	Enhanced consent, interoperability, and operational efficiency.	Legacy-system constraints.
[59]	2024 trends	Identity management; secure exchange; public-health infrastructure.	Regulatory readiness gaps.
[60]	Adoption barriers	Transparency, privacy, and efficiency improvements.	Scalability; integration issues.
[61]	Web3 healthcare	Decentralized identity; tokenized payments; cross-border exchange.	Legal uncertainty.
[62]	Editorial on DLT	Emerging DLT architectures for secure exchange and workflows.	Standardization gaps.
[63]	IET report	DLT for integrity, privacy, interoperability, and consent.	Administrative inefficiencies.
[64]	Complaint management	Privacy-preserving complaint handling.	Confidentiality concerns; scalability.
[65]	R&D governance	Need for blockchain research programs in medical centers.	Organizational barriers.
[66]	Knowledge governance	Trust, auditability, and evidence-driven decisions.	Regulatory and organizational barriers.
[67]	Pharma innovation governance	Blockchain/DAO for decentralized innovation sourcing.	Legal uncertainty; governance rigidity.
[68]	Adoption model	TOE + Fit-Viability + institutional theory for adoption drivers.	Government coercion reduces adoption.

Ref	Subcategory	Contribution	Limitations / Challenges
[69]	Adoption decision modeling	BWM-based model identifying key enablers (security, infrastructure, training).	Expert-driven results; readiness gaps.

2.8 Bibliometric and Systematic Reviews

Bibliometric and systematic reviews provide consolidated evidence that blockchain research in healthcare has expanded across domains including EHR security, supply-chain traceability, telemedicine, IoT, insurance, and pandemic response [70–79]. These reviews consistently highlight blockchain's contributions to secure data exchange, provenance tracking, interoperability, and decentralized identity. Recent large-scale analyses further strengthen this foundation. Bibliometric and LDA-based studies identify persistent thematic challenges and research clusters [80]; systematic reviews examine how generative AI and blockchain jointly enhance security, interoperability, and predictive analytics [81]; cross-domain analyses map adoption barriers and evolutionary trends across healthcare sectors [82]; tertiary reviews develop validated decision-making flowcharts for blockchain suitability [83]; and value-chain assessments evaluate blockchain's contributions to patient outcomes and organizational efficiency [84]. Global bibliometric mappings reveal expanding collaboration networks and thematic clusters [85], while domain-specific reviews cover EHRs, pharmaceuticals, smart healthcare, digital twins, and intelligent systems [86–90]. Additional contributions examine technical barriers, architectural trends, decentralized EHR ecosystems, and privacy-preserving blockchain techniques [91–94]. Across these reviews, recurring challenges remain central: scalability constraints, privacy and confidentiality risks, interoperability gaps, governance and regulatory alignment issues, and high energy consumption. Emerging trends include AI–blockchain convergence, digital-twin ecosystems, decentralized identity, federated learning, and the increasing dominance of Hyperledger Fabric in enterprise-grade healthcare deployments. Table 8 summarizes Group H contributions and limitations.

Table 8. Bibliometric & Systematic Reviews

Ref	Subcategory	Contribution	Limitations / Challenges
[70]	SLR on secure sharing	Reviews blockchain for secure data sharing; integrity and transparency.	Weak access-control models.
[71]	Blockchain + digital tech SLR	AI/IoT integration for secure digital ecosystems.	Scalability; interoperability.
[72]	DLT in healthcare SLR	Secure exchange; interoperability; supply-chain applications.	Regulatory-alignment issues.
[73]	Overview of blockchain in healthcare	Summarizes blockchain use cases across healthcare domains.	Scalability; regulatory challenges.
[74]	SLR of 42 studies	Security, privacy, interoperability, efficiency improvements.	Scalability; compliance gaps.
[75]	Survey of blockchain	Architectural models, consensus, interoperability, security issues.	Scalability; privacy concerns.
[76]	Survey of real-world deployments	Reviews 15 deployments showing gains in security and interoperability.	Limited scalability evidence; uneven adoption; legacy integration barriers.
[77]	Bibliometric review	Maps eight blockchain domains in PHC.	Need for policy/ethical frameworks.
[78]	Bibliometric & ML trend analysis	Analyzes 1,885 PHC articles; highlights blockchain in pandemic response.	Policy readiness; literature-only scope; evolving post-COVID trends.
[79]	Genomics SLR	Genomic privacy and interoperability via blockchain.	Scalability; regulatory compliance.
[80]	Bibliometric challenge analysis	Identifies six persistent adoption barriers using LDA.	Literature-only scope; evolving thematic clusters.
[81]	AI–Blockchain systematic review	Shows how generative AI + blockchain enhance security and analytics.	Scalability; energy use; interoperability; ethical risks.
[82]	Cross-domain systematic review	Synthesizes adoption across EHRs, supply chains, trials, telemedicine.	Regulatory, scalability, and integration challenges.
[83]	Tertiary review & decision flowchart	Provides a validated flowchart for blockchain suitability.	Based on existing reviews; limited real-world validation.
[84]	Blockchain value-chain review	Shows blockchain's patient and business value contributions.	Conceptual focus; limited empirical measurement.
[85]	Global bibliometric mapping	Identifies thematic clusters and global collaboration trends.	Bibliometric scope only; no technical evaluation.
[86]	EHR blockchain review	Reviews EHR prototypes showing security and interoperability gains.	Limited deployment; governance and compliance conflicts.
[87]	Pharmaceutical blockchain SLR	Traceability and counterfeit-prevention applications.	Scalability; interoperability; regulatory harmonization.
[88]	Smart healthcare review	Blockchain for EHR security, federated learning, IoT monitoring.	Throughput limits; energy use; GDPR conflicts.
[89]	Blockchain + digital-twin review	DT security, integrity, traceability, real-time interaction.	Scalability; privacy gaps; lack of clinical-grade deployment.
[90]	Integrated intelligent healthcare review	Blockchain + AI + IoT + big data for secure, interoperable systems.	Device integration; scalability; privacy management.

Ref	Subcategory	Contribution	Limitations / Challenges
[91]	HIS integration barriers	Reviews interoperability, standardization, scalability issues.	Added complexity; energy demands.
[92]	Secure e-health data review	Blockchain frameworks for secure e-health data.	Compliance; energy efficiency; cross-platform interoperability.
[93]	EHR blockchain survey	Surveys decentralized EHR systems and privacy models.	Privacy leakage; HL7/FHIR gaps; regulatory barriers.
[94]	Privacy-preserving blockchain review	Analyzes privacy techniques and risks in blockchain healthcare.	Pseudo-linkability; leakage risks; complex privacy management.

3. SYSTEM DESIGN AND ARCHITECTURE

The proposed remote healthcare system adopts a full-stack architecture integrating a permissioned blockchain network with modern web technologies, ensuring secure, auditable, and distributed access to medical records. The system was designed to ensure seamless interaction between the user interfaces, the backend server, and the underlying blockchain infrastructure. The selected technology stack was chosen based on factors such as performance, scalability, security, and ease of integration. The design objectives include:

- **Secure Remote Access**— ensure that doctors, patients, and administrators can access medical records securely from distributed locations.
- **Role-Based Access Control**— enforce strict permissions based on user roles.
- **Data Integrity and Immutability**— guarantee that medical records cannot be tampered with.
- **Transparent Auditability**— provide immutable logs of all data interactions.
- **Logical Deletion**— allow records to be marked inactive without violating blockchain immutability.
- **Modular and Scalable Architecture**— support future expansion and integration with external systems.

3.1 Technology Stack Overview

The system relies on the following core components:

- **Blockchain Layer** – Hyperledger Fabric provides decentralized consensus, identity-based access control, and immutable storage of medical records.
- **Smart Contract Layer** – Go Chaincode implements patient management, diagnosis logging, and validation logic.
- **Backend Layer** – Node.js & Express exposes RESTful APIs, manages identities via the Fabric SDK, and enforces JWT-based authentication.
- **Frontend Layer** – ReactJS was selected for its modularity, component reusability, and ability to support responsive role-based interfaces (Doctor Panel, Patient Viewer, Admin Panel) with secure Axios-based communication.
- **Containerization** – Docker & Docker Compose guarantees reproducible deployment of peers, orderers, CAs, backend, and Blockchain Explorer.
- **Monitoring** – Hyperledger Blockchain Explorer provides visibility into blocks, transactions, channels, and chaincode.
- **Supporting Tools**— JWT, bcrypt, Axios, dotenv, Fabric SDK, React Router, PostgreSQL.

As illustrated in Fig. 2, the technology stack orchestrates the interaction between the frontend, backend, and blockchain layers, ensuring cohesive and secure system operation.

3.2 Hyperledger Fabric Configuration

Hyperledger Fabric (v2.5+) forms the foundation of the blockchain network. Rationale for Hyperledger Fabric include permissioned access control, modular and pluggable architecture, channel-based confidentiality, smart contract isolation, and enterprise-grade integration. The network consists of:

- **Two Organizations (Org1 and Org2)**—were used to simulate multi-institution healthcare collaboration, enabling cross-organizational endorsement and trust.
- **One Orderer Node**—implements Raft consensus for transaction ordering.
- **Certificate Authorities**— issue digital certificates for users and peers.
- **Channel (mychannel)**—enables secure communication between organizations.
- **Membership Service Providers (MSPs)**—define identity and access policies.

The integration of these components, as shown in Fig. 3, guarantees that every transaction is transparent, verifiable, and resistant to tampering, which is fundamental for maintaining trust in our healthcare system.

3.3 Smart Contract Design

The chaincode defines the core business logic for managing patient data. It performs operations such as adding patient records, querying data, and updating diagnoses. Running in isolated Docker containers, the chaincode reinforces the security and integrity of the operations by enforcing pre-defined rules on every transaction. Key components include:

- **Data Models**— Patient records - follow a JSON structure including id, name, age, blood type, diagnosis, last updated, and active. Diagnosis - Doctor ID, description, date. Metadata - logical deletion flags.
- **Core Functions**— AddPatient, QueryPatient, AddDiagnosis, GetAllPatients, DeletePatient (logical deletion), PatientExists, ValidatePatient. Logical deletion marks records as inactive while preserving historical integrity, ensuring compliance with blockchain immutability.
- **Security Input—** validation, timestamping, and logical deletion ensure ledger integrity and prevent unauthorized manipulation. It guarantees required fields are present, prevents duplicate patient IDs, and restricts diagnosis logging to authorized doctors.

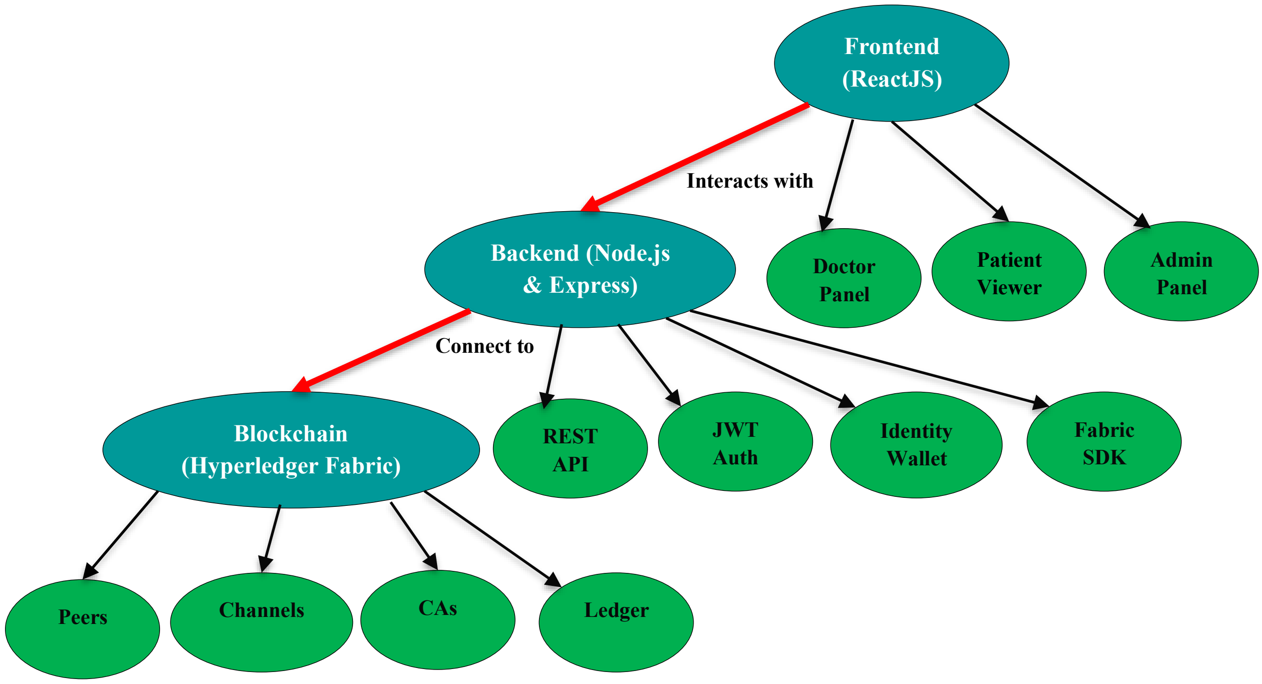

Fig. 2. Technology Stack Overview

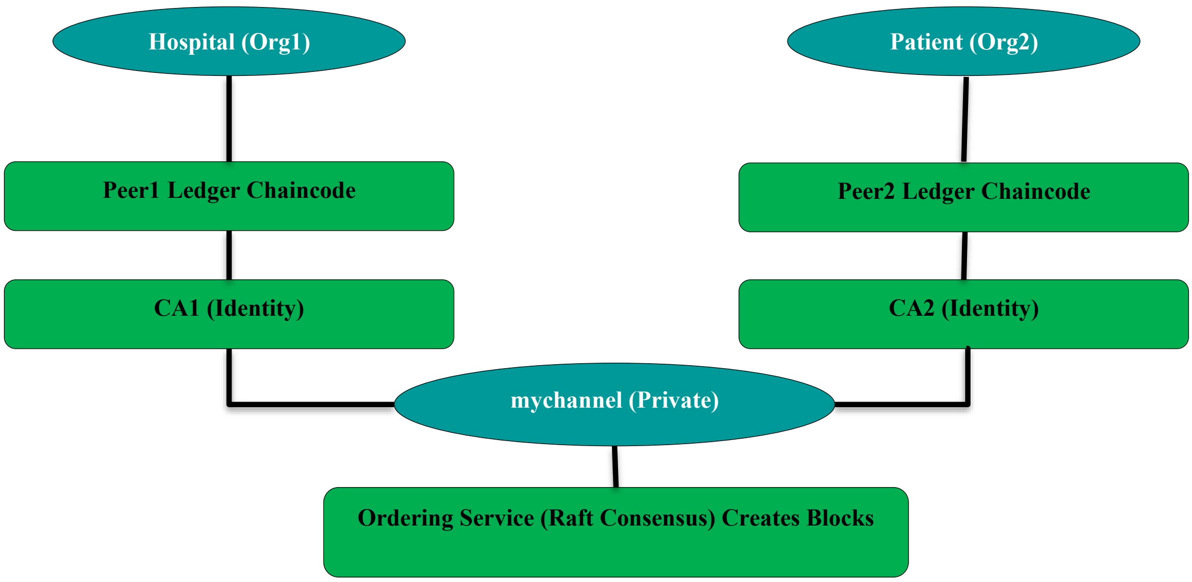

Fig. 3. Blockchain Network Architecture

3.4 Backend and Frontend Integration

- **Backend API (Node.js & Express)**— the backend acts as the middleware between the frontend and the blockchain network. It handles RESTful API routing, identity and wallet management, JWT authentication, bcrypt password hashing, Fabric SDK transaction submission and evaluation. JWT was selected due to its stateless nature, enabling scalable authentication across distributed healthcare clients.
- **Frontend Architecture (ReactJS)**— the frontend provides intuitive interfaces tailored to user roles, enabling seamless interaction with the blockchain network. The ReactJS provides a modular, responsive interface with Role-specific panels (Doctor, Patient, Admin), Component-based UI (forms, cards, navigation), React Router for navigation, and Axios for secure API calls with JWT tokens. Fig. 4 illustrates the logical structure of the Frontend Architecture.

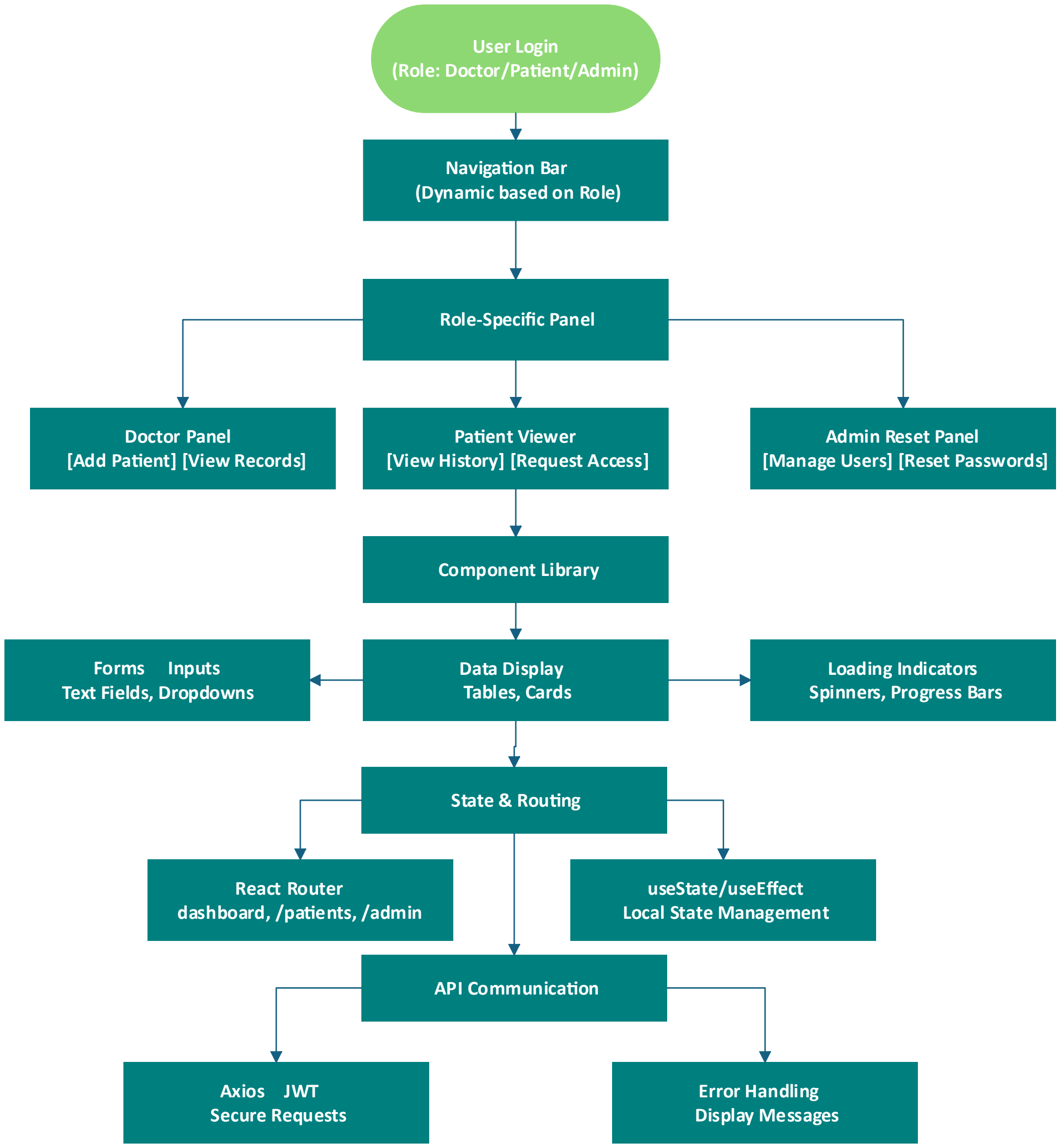

Fig. 4. Frontend Architecture

3.5 Data Flow and Transaction Lifecycle

Fig. 5 illustrates the communication flow between the system's major components. The React-based frontend interacts with the Node.js and Express backend through secure HTTP/HTTPS requests authenticated using JWT tokens. The backend, in turn, communicates with the Hyperledger Fabric network via Fabric SDK calls, enabling seamless integration between user interfaces and blockchain operations. This flow guarantees secure data exchange and consistent transaction handling across all layers of the proposed architecture.

The transaction lifecycle guarantees end-to-end security and traceability across all architectural layers, progressing through the following phases:

1. **User Interaction**— the process begins when a user (doctor, patient, or admin) interacts with the frontend (e.g., add a patient record).
2. **API Request**— the frontend sends an HTTP POST request to the backend API endpoint (e.g., /addPatient), including the JWT token in the header for authentication.
3. **Backend Processing**— the backend validates the request (verifies JWT token and role permissions) and processes the data. It then constructs a transaction proposal and sends it to the blockchain network via the Hyperledger Fabric SDK.
4. **Blockchain Transaction**— the transaction is endorsed by the required peers, ordered into a block, and committed to the ledger. This process guarantees that the transaction is securely recorded and immutable.
5. **Response Handling**— Once the transaction is successfully committed, the backend sends a confirmation response back to the frontend, which updates the user interface accordingly.
6. **Blockchain Explorer** — updates the transaction history.

3.6 Summary

The proposed architecture employs multiple security mechanisms to ensure data integrity and privacy. These include certificate-based identities managed by Certificate Authorities (CAs) and Membership Service Providers (MSPs), JWT-based authentication, TLS-secured communication, bcrypt password hashing, and role-based middleware for controlled access.

Logical deletion further reinforces ledger immutability. These architectural guarantees form the foundation for the implementation and testing procedures described in Section 4.

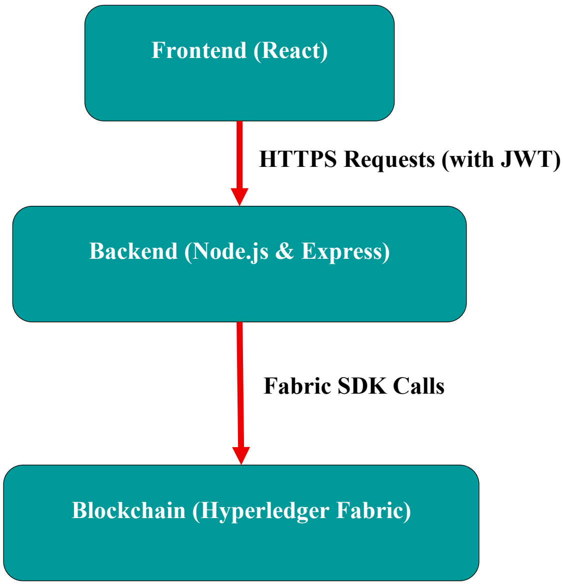

Fig. 5. Communication flow diagram

4. IMPLEMENTATION AND TESTING

4.1 Environment Setup

The system was deployed in a multi-tier environment integrating containerized blockchain components, a Node.js backend, and ReactJS frontends, ensuring reproducibility, isolation, and consistent behavior across development and testing stages.

- **Development Environment**— the setup utilized Hyperledger Fabric v2.5+, Go 1.20 for chaincode, Node.js 18+ with Express, ReactJS 18+, Docker and Docker Compose. Hyperledger Explorer was included for network monitoring. The network was deployed locally for testing and demonstration, with environment variables securely stored in a *.env* file to prevent hardcoded secrets.
- **Hyperledger Fabric Network Preparation**— Fabric CA generated cryptographic identities for peers, orderers, and administrators. Configuration files—*configtx.yaml* and *crypto-config.yaml*—defined organizational structures, channel parameters, and certificate generation policies.
- **Containerization**— Docker Compose orchestrated services for CAs, peers, orderer, backend API, and Blockchain Explorer. Persistent volumes were configured to preserve ledger data and certificates across container restarts, ensuring durability and seamless recovery.

4.2 Blockchain Deployment

The deployment process followed a structured workflow based on the Hyperledger Fabric test network, which was customized to meet healthcare-specific requirements such as identity management, access control, and secure channel configuration.

- **Network Initialization**— the Fabric samples repository was cloned and customized to serve as the foundation for the deployment. Core configuration files were updated to define the organizational MSPs, establish the application channel (*mychannel*), and align environment variables with project-specific endpoints and paths.
- **Network Launch and Verification**— Docker Compose orchestrated the startup of Certificate Authorities, peer nodes, the ordering service, and auxiliary components such as the backend API and Blockchain Explorer. Network health and inter-component communication were verified through container logs and Explorer dashboards.
- **Chaincode Deployment**— the custom Go-based chaincode was installed, approved, and committed to *mychannel* using automated Fabric CLI scripts. This ensured consistent chaincode lifecycle management and synchronization across all participating peers.

4.3 Backend API Implementation

The backend, implemented using Node.js and Express, serves as the secure intermediary between the ReactJS frontend and the Hyperledger Fabric network. Its asynchronous architecture supports scalable transaction handling, while middleware enforces strict authentication and role-based access control.

- **API Routing and Middleware**— RESTful endpoints support authentication, patient registration, diagnosis logging, and record retrieval. Middleware enforces JWT-based session validation and role-based access control to ensure that only authorized users can invoke sensitive operations.
- **Blockchain SDK Integration**— the backend uses the Hyperledger Fabric SDK to evaluate and submit transactions. Each request is validated, transformed into a chaincode invocation, endorsed by peers, and committed to the ledger before a structured response is returned to the client.
- **Security and Identity Management**— File-based wallets store cryptographic identities required for signing blockchain transactions. JWT tokens secure user sessions, while structured error handling provides clear feedback for invalid inputs, unauthorized access, or failed blockchain interactions. Fig. 6 illustrates an invalid login attempt, demonstrating backend-level authentication and validation.

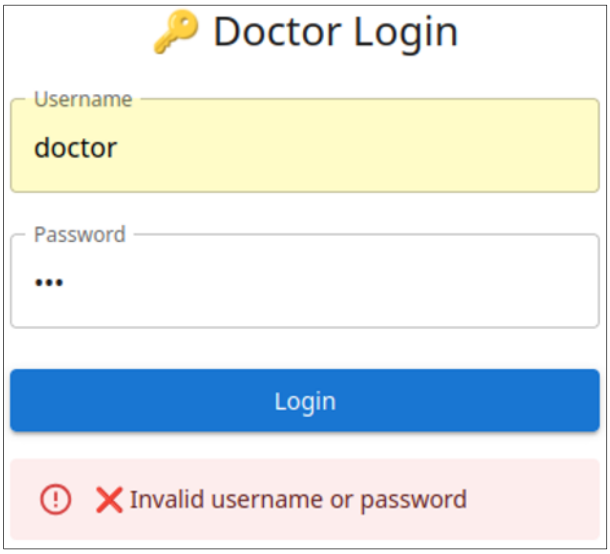

Fig. 6. Backend login validation

4.4 Frontend Deployment

ReactJS was selected for its modular component architecture and ability to deliver responsive, role-specific interfaces for doctors, patients, and administrators.

- **Component Structure**— the frontend was organized into functional modules—Doctor Panel, Patient Viewer, and Admin Panel—each encapsulating its respective workflows and UI elements.
- **State Management and Routing**— React Router managed navigation across role-based views, while React

Hooks (useState, useEffect) handled component state and lifecycle events to maintain smooth interaction.

- **Secure API Communication—** Axios was used for backend communication, transmitting requests with JWT tokens in the Authorization header. Error interceptors provided structured feedback and improved user experience during failed or unauthorized operations.
- **Deployment—** React builds were optimized and served through static hosting or integrated with the backend server. Fig. 7, 8, and 9 present the Doctor, Patient, and Admin interfaces, respectively.

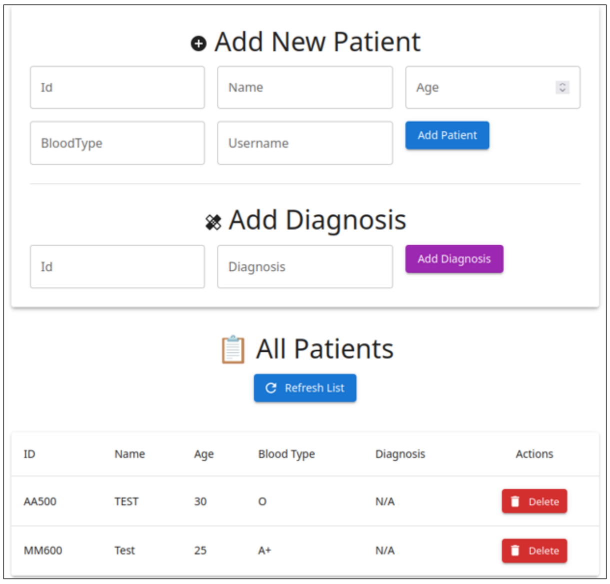

Figure 7. Doctor panel interface

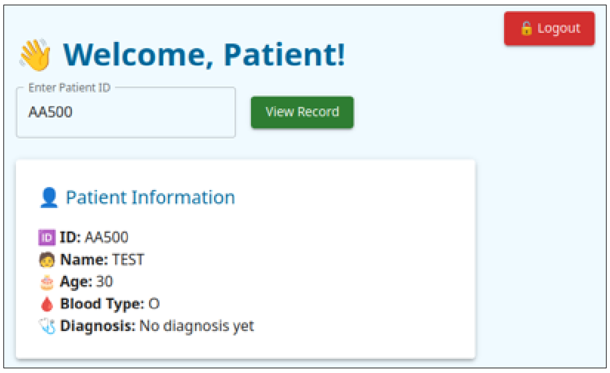

Figure 8. Patient viewer interface

4.5 Testing and Troubleshooting

Integration testing validated end-to-end functionality across all layers, confirming reliable transaction flow from user interaction to ledger commitment.

- **Testing Approach—** the system was evaluated through end-to-end tests, component-level checks, and stress simulations. These tests verified full transaction execution—from frontend submission to blockchain recording—covering API interactions, JWT authentication, and Fabric SDK operations.
- **Functional Testing—** core functions such as patient registration, diagnosis logging, logical deletion, role-based access control, data retrieval, and chaincode validation logic were tested under minimal load. All features operated as expected across the integrated environment.
- **Troubleshooting—** key issues involved container connectivity, JWT authentication failures, and chaincode deployment errors. Configuration audits, enhanced logging, and iterative debugging resolved most problems and improved system stability.
- **Deployment Challenges—** challenges included coordinating multiple Docker services, maintaining configuration consistency, and conducting scalability tests. These were addressed through structured container orchestration, centralized environment management, and iterative performance tuning.

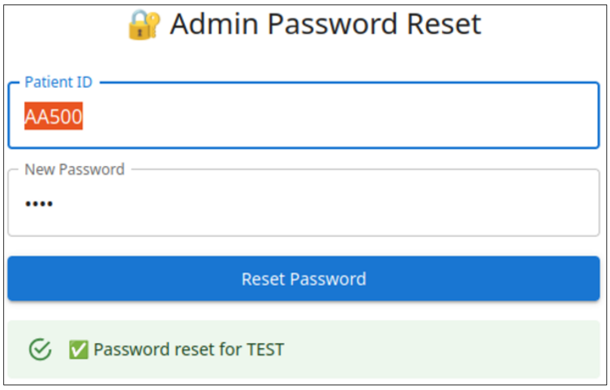

Figure 9. Admin panel interface

4.6 Technical Challenges

Integrating heterogeneous components introduced significant architectural complexity, particularly in coordinating Fabric network configuration, container orchestration, and cross-component communication.

- **Key Challenges—** component interoperability, configuration complexity, container orchestration, and blockchain-related latency were the primary issues. Minor misconfigurations frequently caused network instability or chaincode deployment failures.
- **Mitigation Strategies—** iterative testing, enhanced logging, Docker dependency management, and a modular API design improved stability and reduced integration overhead.

4.7 Solutions and Mitigations

A series of targeted solutions were implemented to enhance reliability, security, and performance across all layers of architecture.

- **Interoperability Solutions—** modular API design and extensive logging improved communication between frontend, backend, and blockchain components.
- **Configuration Management—** centralized *.env* handling and clearly documented configuration files reduced deployment inconsistencies and configuration-related failures.
- **Security Enhancements—** JWT-based authentication, MSP-driven identity management, and logical deletion ensured secure access control, data integrity, and compliance.
- **Security Testing—** authentication was validated through JWT enforcement; authorization was ensured via role-based permissions; data integrity was maintained through ledger immutability; auditability was confirmed using Blockchain Explorer.
- **Performance Optimization—** stress testing and peer configuration tuning improved throughput and reduced latency.
- **Performance Evaluation—** under minimal load, the system achieved 1–2 seconds transaction latency, 30–

40 TPS throughput in local deployment, and moderate CPU/memory utilization.

Comprehensive stress testing remains part of future work to further validate scalability under realistic healthcare workloads.

5. RESULTS AND EVALUATION

5.1 System Deployment Results

The deployment of the Hyperledger Fabric network, backend API, and ReactJS frontend confirmed that the proposed architecture is fully operational and capable of supporting secure remote healthcare workflows. All core functionalities—including patient registration, diagnosis updates, identity validation, and secure data retrieval—executed successfully. All Fabric components (peers, orderer, Certificate Authorities, and chaincode containers) launched without errors. Deployment logs confirmed successful initialization of all containers, including peer0.org1, peer0.org2, orderer.example.com, and the backend API, demonstrating correct orchestration of the multi-container environment and stable inter-service communication.

5.2 Blockchain Network Performance

- **Transaction Execution—** end-to-end testing demonstrated deterministic chaincode execution across organizations, with immediate ledger updates following block commitment. The Raft consensus mechanism contributed to low-latency block formation and predictable transaction ordering.
- **Fault Tolerance and Error Handling—** network failure simulations—such as stopping peer containers—produced predictable and traceable error logs. Backend output messages such as *Failed to connect before the deadline on Endorser… no discovery results* validated the robustness of Fabric SDK error reporting and the backend's ability to detect and respond to disruptions.

5.3 Performance and Transaction Analysis

This subsection presents preliminary performance estimates for the Hyperledger Fabric network based on minimal-load observations and benchmark comparisons. Although full stress testing is planned for future iterations, the current deployment provides a realistic baseline for system behavior under light usage. Estimated throughput ranges between 30–40 TPS, average transaction latency remains around 1–2 seconds, and resource utilization shows moderate CPU usage (50–60%) with stable memory consumption in the Docker environment. These values align with reported performance for similar Fabric-based healthcare implementations and confirm that the system maintains stable execution, predictable block formation, and efficient resource handling. Fig. 10–12 illustrate system stability, patient-addition response time, and blockchain transaction processing, providing visual insight into baseline operational performance.

5.4 Backend Evaluation

- **Functional Validation**—the backend API demonstrated stable performance across all endpoints. Execution logs confirmed correct routing, JWT authentication, and Fabric SDK integration. The message *API Server running at http://localhost:3050* indicated continuous backend availability even during stress scenarios.
- **Security Enforcement—** incorrect login attempts were rejected as designed, with clear error messages enhancing both usability and security. The backend returned the appropriate error message *Invalid username or password*. Role-based access control further prevented unauthorized operations, ensuring compliance with healthcare privacy requirements.

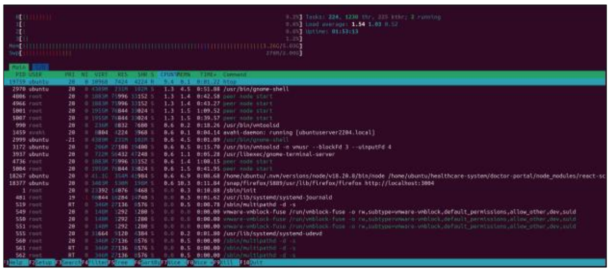

Fig. 10. Stability and system resource consumption

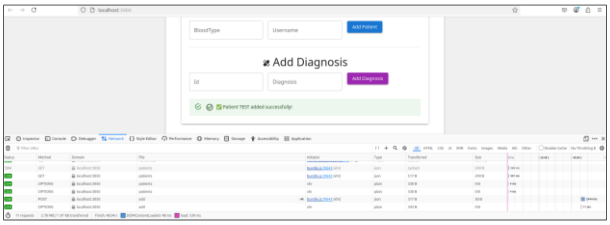

Fig. 11. Average response time to add a patient

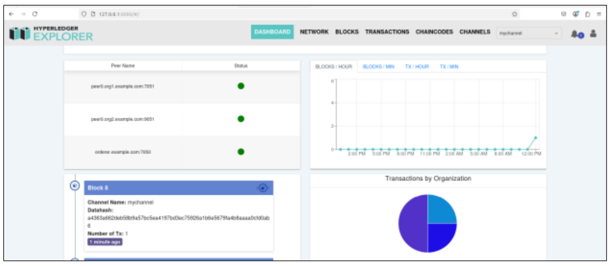

Fig. 12. Blockchain network response to add a transaction

5.5 Frontend Usability and Interaction

- **User Interface Responsiveness—** the ReactJS frontend delivered a smooth user experience across all panels. React Hooks ensured responsive state updates, while React Router maintained consistent navigation across Doctor, Patient, and Admin interfaces.
- **Secure Communication—** Axios requests successfully transmitted JWT tokens to protected endpoints. When the blockchain network was intentionally disrupted, the frontend displayed clear error messages, confirming robust exception handling and secure communication flows. As shown in Fig. 13, the frontend displayed clear error messages during simulated login failures, demonstrating robust exception handling and secure communication flows. Fig. 14 presents a successful patient login, resulting in the generation and storage of a valid authentication token for the patient interface.

5.6 System Reliability

- **End-to-End Workflow Validation—** repeated test cycles validated the complete workflow, from authentication to ledger commitment, confirming reliable real-time data retrieval and secure identity verification, which are essential for healthcare compliance and continuity of service. This confirms that the integration between ReactJS, Node.js, and Hyperledger Fabric is stable and production-ready.
- **Interoperability—** the modular architecture enabled seamless communication between heterogeneous components. Docker Compose ensured consistent orchestration, while Fabric's MSP and CA services maintained strong identity management across the network.

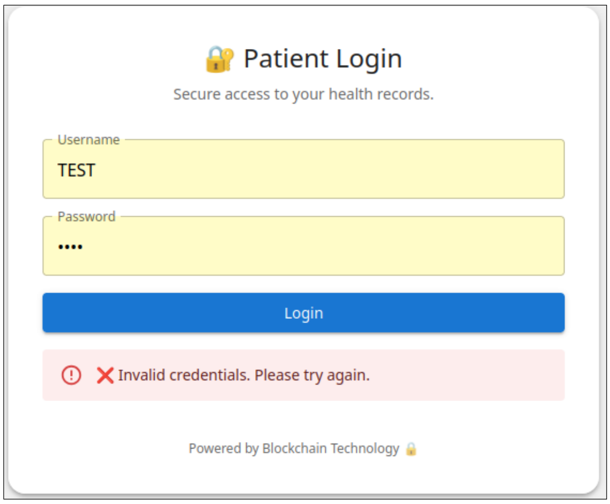

Fig. 13. Patient login interface – invalid credentials

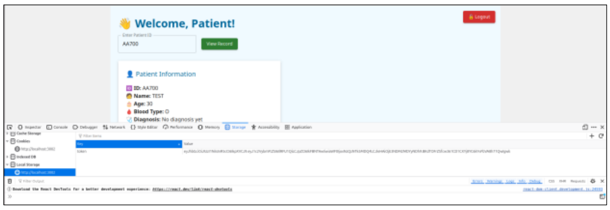

Fig. 14. Patient interface – successful login and token generation

5.7 Discussion

The results demonstrate that Hyperledger Fabric effectively addresses privacy, integrity, and auditability challenges in remote healthcare systems. Its permissioned architecture guarantees that only authenticated users can access sensitive medical data, while chaincode enforces strict business logic and immutability. Failure-condition behavior highlights the importance of robust error handling and network monitoring. Although misconfigurations or container failures can disrupt service availability, the integration of Blockchain Explorer and detailed backend logs provides real-time visibility and rapid troubleshooting. From a usability perspective, the ReactJS frontend proved intuitive and responsive, enabling healthcare professionals and patients to interact with blockchain-secured data without requiring technical expertise. The results collectively demonstrate that Hyperledger Fabric effectively addresses the privacy, integrity, and auditability requirements of remote healthcare systems. The architecture balances decentralization with privacy, offering a practical solution for environments requiring strict data governance.

5.8 Key Contributions

Key findings include:

- **Full Hyperledger Fabric Deployment**— successful initialization of a complete permissioned blockchain network, including peer nodes, the ordering service, and Certificate Authorities.
- **Deterministic Chaincode Execution**— reliable and immutable patient-record management achieved through consistent chaincode invocation across organizations.
- **Robust Backend Security**— strong authentication mechanisms and role-based access control ensuring that only authorized users can perform sensitive operations.
- **Usable and Secure—** a user-friendly ReactJS interface with secure communication flows supported by JWT-protected API interactions.
- **Effective Fault Detection**— comprehensive error detection and logging during network failure simulations, demonstrating resilience and operational transparency.

These contributions collectively demonstrate the feasibility of deploying a secure, blockchain-enabled remote healthcare system capable of supporting real-world clinical workflows.

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

This work presented a secure remote healthcare system built on Hyperledger Fabric, addressing critical privacy, integrity, and auditability challenges in digital medical data management. The permissioned blockchain architecture guarantees that only authenticated and authorized participants—doctors, patients, and administrators—can access or modify sensitive healthcare records. Implementation and testing demonstrated reliable performance under normal and stressed conditions. The blockchain network maintained consistent endorsement and ordering behavior, while the backend enforced strict authentication and role-based access control. The ReactJS frontend provided intuitive interfaces that abstracted blockchain complexity from end users. Network failure simulations further validated the robustness of error handling and logging mechanisms. Overall, the results confirm that Hyperledger Fabric is a viable foundation for secure remote healthcare applications. Its permissioned model, strong identity management, and immutable ledger provide the guarantees required for environments where confidentiality, traceability, and compliance are paramount. While the current deployment was evaluated under minimal load and local network conditions, the results indicate that blockchain technology—combined with modern web frameworks—can significantly enhance the security and reliability of remote healthcare services.

6.2 Future Work

Future work will focus on extending privacy and scalability through mechanisms such as private data collections and zero-knowledge proofs, enabling more granular confidentiality controls. Integrating HL7/FHIR standards will enhance interoperability with existing electronic health record systems, while advanced analytics and monitoring tools can provide deeper insights into performance and security events. Additional opportunities include mobile-optimized interfaces for broader accessibility and AI-driven decision support modules for diagnosis assistance and anomaly detection—implemented with careful attention to auditability and regulatory compliance.

7. ACKNOWLEDGMENTS

This research was supported by the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University.

8. REFERENCES

[1] Sharma, S.K. and Parwej, F. 2025. Design and implementation of a blockchain-based secure data sharing framework to enhance the healthcare system. *Blockchains*. 3, 10.

[2] Adeniyi, J.K., Ajagbe, S.A., Adeniyi, A.E., Adeyanju, K.I., Afolorunso, A.A., Adigun, M.O. and Ogene, I. 2025. A blockchain-based smart healthcare system for data protection. *iScience*. 28 (4), 112109.

[3] Ullah, A., Ullah, Z., Rizvi, S.S., Gul, L. and Kwon, S.J. 2025. Toward blockchain-based electronic health record management with fine-grained attribute-based encryption

and decentralized storage mechanisms. *Scientific Reports*. 15, 34542.

[4] Eegu, F.A. Abas, H., Gulzar, Y., Xin, Q., Alwan, A.A., Jabbari, A., Sonkamble, R.G.; and Dziyauddin, R.A. 2023. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*. 15, 6337.

[5] Chen, Z., Xu, W., Wang, B. and Yu, H. 2021. A blockchain-based preserving and sharing system for medical data privacy. *Future Generation Computer Systems*. 124, 338–350.

[6] Palkar, S.S., Mehra, R. and Hadimani, L. 2026. A blockchain-based self-sovereign identity in adaptive access control framework and differential privacy for real-time privacy-preserving EHR management. *OPSEARCH*.

[7] Masood, I. Daud, A., Wang, Y., Masood, M. and Khan, M.A. 2024. A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*. 83, 60443–60467.

[8] Bautista, J.R., Harrell, D.T., Hanson, L., de Oliveira, E., Abdul Moheeth, M., Meyer, E.T. and Khurshid, A. 2023. MediLinker: A blockchain-based decentralized health information management platform for patient-centric healthcare. *Frontiers in Big Data*. 6, 1146023.

[9] Rathod, S.G., Patel, P.O., Bhirud, V.S., Dodwadkar, V.P. and Kokadwar, S.D. 2026. Design and development of a blockchain-based system to protect medical records. *Blockchain Healthcare Today*. 9, 381.

[10] Chafik, K., Hanine, M., Ouaguid, A. and Alshuhri, S. 2026. Blockchain technology to enhance clinical data management in healthcare: A systematic literature review. *Blockchain Healthcare Today*. 9, 471.

[11] Khan, M.H. and Muntaha, S.T. 2024. Blockchain-based secure data sharing framework for healthcare industry: A case study of U.S. healthcare. *International Journal of Computer Applications*. 186(40), 34–37.

[12] Ali, M., Kumar, R., Tunio, M.Z. and Lakhan, A. 2026. DBH Chain: A decentralized blockchain-enabled healthcare framework for end-to-end delay optimization. *Scientific Reports*. 16, 7496.

[13] Ali, F. and Asmatullah. 2025. Leveraging blockchain for secure and transparent healthcare data management: Enhancing patient privacy and interoperability in medical systems. *Sarhad Journal of Management Sciences*. 11, 53–66.

[14] Pawar, V. and Sachdeva, S. 2023. ParallelChain: A scalable healthcare framework with low energy consumption using blockchain. *International Transactions in Operational Research*. 31, 3621–3649.

[15] Punia, A., Gulia, P., Gill, N.S., Kaushik, D., Alduaiji, N., Shukla, P.K. and Pandey, A. 2025. An access control system for cloud-based healthcare systems driven by blockchain. *Journal of Cloud Computing*. 14, 78.

[16] Jarariya, R.K., Saritha, S.K. and Jain, S. 2026. Efficient health information exchange automation system based on blockchain and IPFS. *Blockchain Healthcare Today*. 8, 423.

[17] Thakur, A., Ranga, V. and Agarwal, R. 2026. ABHealChain: Enhancing privacy and security in healthcare data sharing through Hyperledger Fabric and attribute-based access control. *Concurrency and Computation: Practice and Experience*. 38.

[18] Giao, J., Ferreira, F.L., Sarraipa, J. and Jardim Gonçalves, R. 2026. Enhancing health data integrity using distributed ledger technology. *Journal of Cloud Computing*. 15, 34.

[19] Abbasi, A., Humeidi, M.N. and Wang, Q. 2026. Nexa: Enabling secure, scalable, and decentralized management of electronic health records using threshold cryptography and public blockchains. *IEEE Access*. 14, 50791–50810.

[20] Guse, R., Hu, S., Thiebes, S., Erler, C., Caridia, C., Stork, W., Gersch, M. and Sunyaev, A. 2026. Patient perceptions of blockchain-based health information exchange: User-centered design study. *Journal of Medical Internet Research*. 28, e78849.

[21] Aziz, A., Suman, S., Sohail, S.S. and Madsen, D.Ø. 2025. Leveraging blockchain for combatting drug counterfeiting in the pharmaceutical sector. *Cogent Business & Management*. 12(1), 2551811.

[22] Islam, M.A., Chuity, S.M., Sultan, T., Baul, S., Ahamed, J. and Mobin, M.I. 2024. Blockchain technology is revolutionizing the pharmaceutical industry's drug supply chain management. *Proceedings of the 3rd International Conference on Computing Advancements (ICCA 2024)*, Dhaka, Bangladesh, 17–18 October 2024. ACM, New York, NY, USA, 1–8.

[23] IBM, KPMG, Merck and Walmart. 2020. FDA DSCSA Blockchain Interoperability Pilot Project Report. *U.S. Food and Drug Administration*. Available online: https://www.fda.gov/media/169883/download

[24] MediLedger Consortium. 2021. *MediLedger DSCSA Pilot Project Report*. Available online: https://www.fda.gov/media/168283/download

[25] Gomasta, S.S., Dhali, A., Tahlil, T., Anwar, M.M. and Ali, A.B.M.S. 2023. PharmaChain: Blockchain-based drug supply chain provenance verification system. *Heliyon*. 9, e17957.

[26] Euro American Worldwide Logistics. 2025. *Pharmaceutical Serialization and Track and Trace: Ensuring Compliance in 2025*. Published March 31. Available online: https://www.eawlogistics.com/pharmaceutical-serialization-and-track-and-trace-ensuring-compliance-in-2025/

[27] Razavian, S.B., Görçün, Ö.F., Tirkolaee, E.B., Simić, V., Ali, S.S. and Görçün, O.F. 2025. Blockchain-enabled healthcare supply chain management: Identification and analysis of barriers and solutions based on improved zero-sum hesitant fuzzy game theory. *Engineering Applications of Artificial Intelligence*. 154, 110991.

[28] Mallick, S.R., Sobhanayak, S. and Lenkar, R.K. 2025. Secure and trusted data sharing in smart healthcare using blockchain and IoT integration. *Discover Internet of Things*. 5, 90.

[29] Houssein, E.H., Reda, M., Wazery, Y. and Younan, M. 2026. Fundamentals and applications of blockchain: Impact on intelligent healthcare systems. *Discover Internet of Things*. 6, 21.

[30] Asha, N.S. and Rafi, M. 2025. Blockchain and IoT integration in healthcare: A holistic review of applications, barriers, and emerging directions. *International Journal of Scientific Research in Engineering and Development*. 8, 4, 1556–1563.

[31] Malik, A. and Parihar, V. 2026. A survey of blockchain-enabled IoT frameworks for smart healthcare systems. *Discover Computing*. 29, 305.

[32] Sharma, A., Kaushal, R.K., Chitkara, N.K. and Boonchieng, E. 2026. Blockchain-enabled electronic health record model for managing patients' vital data and medical reports. *Blockchain Healthcare Today*. 9, 455.

[33] Awasthi, C., Awasthi, S.P. and Mishra, P.K. 2024. Secure and reliable fog-enabled architecture using blockchain with functional biased elliptic curve cryptography algorithm for healthcare services. *Blockchain Healthcare Today*. 7, 347.

[34] Sharma, V., Kumar, A. and Sharma, K. 2024. Digital twin: Securing IoT networks using integrated ECC with blockchain for healthcare ecosystem. *Knowledge and Information Systems*. 67, 2395–2426.

[35] Maheshwari, V. and Prasanna, M. 2025. Privacy-preserving authentication for 5G healthcare with HBZKP: Hierarchical blockchain-based zero-knowledge proof for secure edge devices. *Ain Shams Engineering Journal*. 16, 103463.

[36] Nasr Esfahani, M., Shahgholi Ghahfarokhi, B. and Etemadi Borujeni, S. 2026. Ensuring end-to-end privacy in IoT-based healthcare systems through Hyperledger Fabric and Identity Mixer. *PLOS ONE*. 21, e0343233.

[37] Liu, J. and Hu, X. 2026. Blockchain meets AI in healthcare: A review of convergent technologies for digital health transformation. *Frontiers in Blockchain*. 9, 1766092.

[38] Zhang, Y., Mohsin, S.M., Mujlid, H., Sadiq, M., Akber, S.M.A., Aslam, S. and Liang, J. 2026. AI-driven blockchain technology in smart healthcare systems: Opportunities, challenges and future implications. *Computer Science Review*. 60, 100909.

[39] Dershem, M., Riley, J.III, Venkataraman, M., Nasr, J. and Hussain, A.S. 2026. Healthcare predictions: AI, blockchain, and the rise of decentralized innovation. *Blockchain Healthcare Today*. 8, 3.

[40] Di Palma, G., Scendoni, R., Ferorelli, D., De Benedictis, A., Tambone, V. and De Micco, F. 2025. AI-induced cybersecurity risks in healthcare: A narrative review of blockchain-based solutions within a clinical risk management framework. *Risk Management and Healthcare Policy*. 18, 3479–3497.

[41] Mohamed, H.G., Alrowais, F., Al Wesabi, F.N., Al Duhayyim, M., Hilal, A.M. and Motwakel, A. 2025. Blockchain-enabled deep learning model with modified Coati optimization for sustainable healthcare disease detection and classification. *Scientific Reports*. 15, 21058.

[42] Alajlan, A.M. and Almasri, M.M. 2026. Tri-level attention-boosted sliced recurrent neural network for secure and scalable blockchain-based healthcare data management. *Neural Computing and Applications*. 38.

[43] Zhao, T., Feng, S., Pan, D. and Wang, Q. 2026. Adaptive resource optimization for blockchain sharding in medical digital twin edge networks: A healthcare data security framework. *IEEE Journal of Biomedical and Health Informatics*. PP.

[44] Tang, Y., Wang, K., Niyato, D., Li, J., Dobre, O.A. and Duong, T.Q. 2025. Secure data sharing and prediction with digital twin and blockchain in healthcare. *IEEE Communications Magazine*. 63, 8, 170–178.

[45] Simonoski, O. and Bogatinoska, D.C. 2024. BLOCK MEDCARE: Advancing healthcare through blockchain integration. *International Journal of Cybernetics and Informatics*. 13, 5.

[46] Simonoski, O. and Bogatinoska, D.C. 2024. BLOCKMEDCARE: Advancing healthcare through blockchain integration with AI and IoT. *International Journal of Network Security & Applications*. 16, 6, 55–72.

[47] Bharath Babu, S. and Jothi, K.R. 2024. A secure framework for privacy-preserving analytics in healthcare records using zero-knowledge proofs and blockchain in multi-tenant cloud environments. *IEEE Access*. 13, 8439–8460.

[48] Ehteshami, A. and Sattari, M. 2026. Applying blockchain in telemedicine: A systematic review. *International Journal of Preventive Medicine*. 17, 4.

[49] Chen, Y., Zhao, C. and Gao, Y. 2025. Blockchain applications in health insurance: A review of applications, challenges, and prospects. *Frontiers in Blockchain*. 8, 1699290.

[50] Sermo. 2025. *Applying Blockchain in Healthcare: Examples and Use Cases for Physicians*. Sermo Resources, published 16 October 2025. Available online: https://www.sermo.com/resources/blockchain-in-healthcare/

[51] Shwetha, S. 2023. The integration of blockchain and artificial intelligence in securing healthcare insurance data. *International Journal of Computer Science and Information Technology Research*. 4, 1, 63–70.

[52] Musunuri, R.L., Brooks, K.S., Patel, S.A., Majgunkar, T.J., Patel, K. and O'Neill, E. 2025. Predictors of commercial success in blockchain healthcare insurance: A mixed-methods analysis. *Blockchain Healthcare Today*. 8, 401.

[53] Wright, R.M. 2025. The evolution of healthcare economics: Blockchain integration amidst Medicare reform. *Blockchain Healthcare Today*. 8, 383.

[54] Goldberg, R., Pitts, P.J. and Hinkel, J. 2024. Healthcare futures: Opportunities, challenges and risks in a blockchain-driven environment. *Blockchain in Healthcare Today*. 7, 345.

[55] Sanober, A. and Anwar, S. 2026. Zero-knowledge-proof-enabled blockchain smart contracts for efficient health insurance systems. *Concurrency and Computation: Practice and Experience*. 38.

[56] Paubox. 2025. *Securing Healthcare Data with Blockchain in 2025*. Paubox Blog, published 8 September 2025. Available online: https://www.paubox.com/blog/securing-healthcare-data-with-blockchain-in-2025

[57] Acropolium. 2025. *Blockchain Technology in Healthcare:*

Real-World Benefits and Solutions. Published 3 February 2025. Available online: https://acropolium.com/blog/blockchain-technology-in-healthcare-real-world-benefits-solutions/

[58] Innowise. 2025. *Blockchain in Healthcare: Guide to Uses, Benefits and Examples*. Published 24 January 2025. Available online: https://innowise.com/blog/blockchain-in-healthcare/

[59] Halamka, J.D. et al. 2024. Blockchain technology predictions 2024: Transformations in healthcare, patient identity, and public health. *PMC*. Available online: https://pmc.ncbi.nlm.nih.gov/articles/PMC10770800/

[60] Selvamuthu, C., Salwin, M., Akshitha, D., Jain, S.D., Kavya, V., Kumar, O.M. and Karwa, V. 2025. Transforming healthcare with blockchain: A study on its applications, benefits and barriers. *Journal of Pioneering Medical Sciences*. 14, 6, 169–179.

[61] TheStreet Crypto. 2025. How Web3 is transforming global healthcare and medical tourism. Published 25 October 2025. Available online: https://www.thestreet.com/crypto/newsroom/web3-global-healthcare-medical-tourism

[62] Kuo, T.-T. and Zhang, P. 2023. Editorial: Blockchain and distributed ledger technology–enabled architectures for improving healthcare. *Frontiers in Blockchain*. 6, 1275474.

[63] Institution of Engineering and Technology (IET). 2024. *Blockchain in Healthcare: How Distributed Ledger Technology Could Help Mitigate Some of the Sector's Biggest Challenges*. IET Insight Report. Available online: Blockchain in Healthcare

[64] Alkhateeb, Y.M. 2021. Blockchain implications in the management of patient complaints in healthcare. *Journal of Information Security*. 12, 212–223.

[65] Usman, M., Kallhoff, V. and Khurshid, A. 2021. The case for establishing a blockchain research and development program at an academic medical center. *Blockchain Healthcare Today*. 4, 161.

[66] Abdulmuhsin, A.A., Dbesan, A.H., Rehman, S.U., Alnoor, A. and Alkhwaldi, A.F. 2026. Redefining knowledge generation driven blockchain for healthcare use: Insights from medical institutions. *Health Services Management Research*. 39, 1, 37–54.

[67] Fantaccini, S., Grassi, L. and Howell, S. 2026. Innovating pharma: Bridging traditional acquisition and emerging technologies. *Blockchain Healthcare Today*. 9, 435.

[68] Bazel, M.A., Mohammed, F., Ahmad, M., Baarimah, A.O. and Al Maskari, T. 2025. Blockchain technology adoption in healthcare: An integrated model. *Scientific Reports*. 15, 14111.

[69] Quayson, M., Avornu, E.K. and Bediako, A.K. 2024. Modeling the enablers of blockchain technology implementation for information management in healthcare supply chains. *Modern Supply Chain Research and Applications*. 6, 101–121.

[70] Tariq, U.U., Sabrina, F., Rashid, M.M., Gordon, S., Lin, Y., Wang, Z. and Azad, S. 2025. Blockchain-based secured data sharing in healthcare: A systematic literature review. *IEEE Access*. 13, 45415–45435.

[71] Fatoum, H., Hanna, S., Halamka, J.D., Sicker, D.C., Spangenberg, P. and Hashmi, S.K. 2021. Blockchain integration with digital technology and the future of healthcare ecosystems: Systematic review. *Journal of Medical Internet Research*. 23, 11, e19846.

[72] Esmaeilnezhadtanha, F., Spalazzi, L., Del Bene, L. and Wautelet, Y. 2025. A systematic literature review on distributed ledger technologies in healthcare: Applications, challenges, and future directions. *Information and Software Technology*. 188, 107894.

[73] Haleem, A., Javaid, M., Singh, R.P., Suman, R. and Rab, S. 2021. Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*. 2, 130–139.

[74] Tandon, A., Dhir, A., Islam, A.K.M.N. and Mäntymäki, M. 2020. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*. 122, 103290.

[75] Ja, A., Isravel, D.P., Sagayam, K.M., Bhushan, B., Sei, Y. and Eunice, J. 2023. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*. 215, 103633.

[76] Daley, S. 2025. *Blockchain in Healthcare: 15 Real-World Examples*. Built In. Available online: https://builtin.com/blockchain/blockchain-healthcare-applications-companies

[77] Damar, M., Aydin, O. and Erenay, F.S. 2025. Blockchain applications in core healthcare services: Patient data, research, and institutional processes. *Blockchain Healthcare Today*. 8, 408.

[78] Damar, M., Pinto, A.D., Erenay, F.S. and Aydin, O. 2025. Impact of COVID-19 on primary healthcare research: Trends and suggestions for better services approaches via blockchain-based applications. *Blockchain Healthcare Today*. 8, 400.

[79] Arya, A. and Malik, A. 2026. A systematic study on blockchain technology for genomic data management in healthcare: Approaches, challenges, and research opportunities. *Medical & Biological Engineering & Computing*. 64, 305–320.

[80] Mehraeen, M. and Mahmoudi, L. 2024. Tracing the blockchain challenges in healthcare: A topic modeling and bibliometric analysis. *Blockchain Healthcare Today*. 7, 335.

[81] Mazhar, T., Khan, S., Shahzad, T., Khan, M.A., Saeed, M.M., Awotunde, J.B. and Hamam, H. 2025. Generative AI, IoT, and blockchain in healthcare: Application, issues, and solutions. *Discover Internet of Things*. 5, 5.

[82] Gupta, S., Mehra, P., Nandy, B., Mohammed, R.P., Pradhan, P.K., Duseja, S., Sharma, N. and Pujari, P.R. 2025. Blockchain in health care, evolutionary or revolutionary – An evidence-based review. *Journal of Pharmacy and Bioallied Sciences*. 17, Suppl. 1, S63–S65.

[83] Li, K., Sai, A.R. and Urovi, V. 2024. Do you need a blockchain in healthcare data sharing? A tertiary review. *Explorations in Digital Health Technology*. 2, 101–123.

[84] Kröckel, P., Wickramasinghe, N., van de Logt, J., Andargoli, A., Ulapane, N. and Bodendorf, F. 2025.

Blockchain in healthcare: Bridging the business value and patient benefit. *IET Blockchain*. 5, e70000.

[85] Zhang, B., Xu, J., Yang, K., Yu, L., Zheng, Q., Qin, Y., Xie, Y. and Sun, J. 2026. Transforming healthcare: A bibliometric review of global blockchain integration and future trends. *Medicine*. 105, 24, e49199.

[86] Chandak, A., Chandak, P. and Soni, N. 2026. Blockchain applications in electronic health records: A systematic review of qualitative and quantitative evidence. *BMC Medical Informatics and Decision Making*. 26, 1.

[87] Faiyazuddin, M., Moharir, K., Gholap, A.D., Christodoss, P.R., Choonara, Y.E., Mnqiwu, K., Sundaram, G. and Tahir, M. 2026. A comprehensive review of the revolutionary potential of blockchain in safe, secure, and sustainable pharmaceutical operations. *Pharmaceutical Research*. 43, 4, 961–1007.

[88] Abbas, S.R., Abbas, Z., Rehman, M.U. and Lee, S.W. 2026. Blockchain for smart healthcare: A systematic review of security, interoperability, and AI–IoT integration. *Digital Health*. 12.

[89] You, Y., Liu, M., Chen, H. and Chen, L. 2026. Application of blockchain-based digital twin technology in healthcare: A scoping review. *Computer Methods and Programs in Biomedicine*. 276, 109231.

[90] Houssein, E.H., Reda, M., Wazery, Y. and Younan, M. 2026. Fundamentals and applications of blockchain impact on intelligent healthcare systems. *Discover Internet of Things*. 6, 21.

[91] Costa, D., Coelho, P.J., Zdravevski, E., Albuquerque, C., Pires, I.M. and Gouveia, A.J. 2026. Overcoming technical barriers in healthcare with blockchain: A systematic review. *Informatics in Medicine Unlocked*. 61, 101741.

[92] Khan, A.A., Bagasah, A.M., Alsafyani, M., Alsufyani, H., Alhazmi, A. and Ullah, S. 2026. Blockchain for e-healthcare: A review on secure data management frameworks and future challenges. *Journal of Big Data*. 13, 20.

[93] Chentouf, F.Z., El Alami Hassoun, M. and Bouchkaren, S. 2026. Electronic health record systems based on blockchain: A comprehensive survey. *Applied Sciences*. 16, 3768.

[94] Sabiri, K., Sousa, F. and Rocha, T. 2025. A systematic review of privacy-preserving blockchain applications in healthcare. *Multimedia Tools and Applications*. 84, 32, 39925–39980.