

## **A COMPREHENSIVE ANALYSIS OF BLOCKCHAIN INTEGRATION IN HEALTHCARE SYSTEMS**

Kavitha N,  
Department of Computer Science and Engineering,  
C Byregowda Institute of Technology,  
Kolar, Karnataka, India  
[kavithakn.cse.cbit@gmail.com](mailto:kavithakn.cse.cbit@gmail.com)

Dr.S.N Chandrashekara  
Department of Computer Science and Engineering,  
C Byregowda Institute of Technology,  
Kolar, Karnataka, India  
[kavithakn.cse.cbit@gmail.com](mailto:kavithakn.cse.cbit@gmail.com)

**Abstract:** This literature review synthesizes findings from thirteen peer-reviewed IEEE research papers published between 2019 and 2026, collectively examining the application of blockchain technology across healthcare data management, land records, and other critical domains. The reviewed works converge on a central challenge: the inadequacy of centralized data systems in guaranteeing security, privacy, integrity, and interoperability of sensitive records. Blockchain's inherent properties of decentralization, immutability, and auditability are consistently proposed as countermeasures. The papers span diverse technical approaches including Hyperledger Fabric, Ethereum, IPFS-based hybrid storage, post-quantum cryptographic schemes (XMSS, KYBER, FALCON), federated learning integration, attribute-based encryption (CP-ABE), elliptic curve cryptography (ECC), SHA-256 hashing, multilevel authentication, and smart contract automation. Collectively, the reviewed literature demonstrates high-performance outcomes: signature verification accuracies exceeding 97%, tampering detection rates of 98-100%, prediction accuracies of 94.7% in federated learning frameworks and transaction latencies well below real-time clinical thresholds. Key research gaps include quantum vulnerability in legacy schemes, scalability limitations of on-chain storage, lack of universal interoperability standards, and insufficient real-world deployment validation. Future directions point toward post-quantum security, AI-augmented diagnostics, federated learning with differential privacy, and cross-domain blockchain interoperability

**Keywords:** EHR Security • Blockchain Architectures • Post-Quantum Cryptography • Federated Learning • Smart Contracts

### **I. INTRODUCTION**

Leveraging Blockchain Technology to Secure Electronic Health Information in the Cloud: International Adoption and Future Directions. The worldwide digitization of highly sensitive personal information, such as patient medical records, land ownership documents, pharmaceutical supply chains, and credit card information, authorizes unprecedented efficiency gains and exceptional vulnerabilities. Conventional centralized architectures provide a convenient single point of failure that facilitates single points of intrusion, data theft, and a lack of tamper-evident audit trail. The growing number cyberattacks on healthcare firms made the limitations of legacy centralized systems impossible to ignore in 2023

alone, when over 15 million healthcare records were leaked. Blockchain technology, the distributed ledger that first enabled Bitcoin (Nakamoto, 2008), has become a multi-domain security and data solution provider. Its core qualitative properties, including decentralization, immutability, transparency, and cryptographic integrity, can effectively mitigate the limitations of centralized systems. The healthcare domain is one of the most sensitive sources of personal data in the world and one of the most heavily regulated by privacy law (HIPAA and GDPR). For these reasons, the healthcare domain is one of the most active domains for blockchain research and implementation.

## **II. LITERATURE SURVEY**

The thirteen papers examined in this review represent a cross-section of current research spanning: [1] EHR security using permissioned blockchain networks with attribute-based access control; [2] post-quantum cryptographic enhancements to resist emerging quantum computing threats; [3] federated learning integrated with blockchain for privacy-preserving multi-institutional model training; [4] decentralized storage via IPFS combined with on-chain metadata; [5] hybrid blockchain architectures for land records; and [6] multilevel authentication schemes for wallet-level security. Together, these works constitute a rich technical ecosystem addressing the multidimensional challenge of secure, scalable, and interoperable digital record management.

The rapid adoption of Electronic Health Records (EHRs) has fundamentally transformed patient care by enabling real-time access to medical histories, improving diagnostic accuracy, and facilitating inter-institutional collaboration. The thirteen reviewed papers collectively represent a comprehensive cross-section of blockchain applications in sensitive record management, published across IEEE conferences and journals between 2019 and 2026. Each paper addresses specific technical challenges and proposes distinct architectural solutions. The following subsections survey each paper's contribution organized thematically.

However, these advantages are negated when systems depend on centralized repositories that are prone to ransomware, insider attacks and regulatory non-compliance. Additionally the impending threat posed by quantum computing may render classical cryptographic primitives, RSA, ECC, ECDSA, computationally breakable, leading to the immediate need for post-quantum secure alternatives.

Concurrently, healthcare is not the only domain facing similar challenges. Land records in developing economies are rife with fraud and disputes over documentation. 66% of legal disputes in India alone are about land ownership.

Real estate transaction is slow, intermediary based and susceptible to fraud. It is these similar challenges that make cross-domain applicability of blockchain evident in the reviewed literature. This review paper systematically categorizes and discusses the contributions, approaches, findings, gaps identified as well as future directions suggested in the thirteen research papers selected.

The paper provides a comprehensive understanding of the state of research on blockchain based record management and its future direction towards quantum-resistant, AI-augmented and globally interoperable systems for researchers, practitioners and policymakers.

## **2.1 Attribute-Based EHR Security on Permissioned Blockchain**

Sankar et al. (2025) propose a multi-attribute-based access control system for Chronic Kidney Disease (CKD) EHRs deployed on Hyperledger Fabric. The system employs Elliptic Curve Cryptography (ECC) for generating tamper-resistant digital signatures, SHA-256 for data hashing, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enforce fine-grained access policies based on user role, department, and institutional location. The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism provides rapid, energy-efficient agreement across nodes. A hybrid storage architecture stores encrypted EHR data off-chain (via IPFS or encrypted cloud) while recording hashed metadata and access logs on-chain. Evaluation on a real-world CKD EHR dataset from Abu Dhabi demonstrates signature verification accuracy of 99.2% for nephrologists and 97.2% mean across all roles, 100% access grant rate for full attribute matches, over 98% tampering detection across ten attack scenarios, and over 99% reduction in on-chain data through hybrid storage. The framework provides a scalable, auditable, and future-proof solution for critical healthcare environments.

## **2.2. Blockchain Technology: Properties and Cross-Domain Applications**

Joshi et al. (2024) provide a comprehensive review of blockchain's foundational properties and emerging applications. The paper examines decentralization, immutability, transparency, security, consensus mechanisms (Proof-of-Work and Proof-of-Stake), and scalability solutions including the Lightning Network and Ethereum 2.0. Application domains surveyed include finance and DeFi, supply chain management, healthcare EHR management, voting systems, and identity management. Future applications discussed include decentralized social media platforms, carbon footprint tracking, blockchain-based land registries, democratic decision-making, community-based natural resource management, and personalized drug discovery. The review highlights that scalability, regulatory uncertainty, interoperability, and energy efficiency remain unresolved challenges requiring multi-stakeholder collaboration and technical innovation.

## **2.3 Post-Quantum Blockchain with Autonomous AI for Healthcare Information Exchange**

He et al. (2025, IEEE JBHI) address the quantum computing threat to conventional cryptographic mechanisms by proposing a healthcare data-sharing framework that integrates the Extended Merkle Signature Scheme (XMSS) with consortium blockchain (Hyperledger Fabric) and IPFS. XMSS, based on hash functions rather than number-theoretic assumptions, provides forward security and post-quantum resistance (PQ-EU-CMA compliance). The framework additionally incorporates an autonomous AI model to assist physicians in generating diagnostic reports from patient EMR data. Security analysis in the random oracle model demonstrates resilience against data tampering, impersonation, replay attacks, man-in-the-middle attacks, and quantum attacks. Performance evaluation shows approximately 49% reduction in total computational overhead and 36% reduction in blockchain storage compared to competing schemes, achieved by storing only EMR hashes on-chain. The proposed scheme demonstrates better scalability and lower latency as the number of EMRs increases.

## **2.4 Blockchain-Enabled Secure Federated Learning for EMR Management**

Yatini et al. (2025) propose a Secure Federated Learning (FL) framework integrated with a permissioned blockchain (Hyperledger Fabric with Raft consensus) for privacy-preserving, multi-institutional EMR management. Enhancing Interoperability of Healthcare Systems: A Blockchain-based Federated Learning Approach.

Across simulated virtual hospitals, the system runs local model training using a decentralized setup powered by blockchain technology. Update checks stay secure, nodes prove who they are through trusted validation, while permissions limit entry points. Encryption that allows calculations on coded data, along with careful addition of random noise to hide individual details - roughly at a level near two - and layering protections between data pairs adds extra safeguards confidentiality.

Achieving 94.7% prediction accuracy on MIMIC-III, the FL+BC method shows an F1 score reaching 93.6%. While tested in intensive care settings, performance remains strong across patient records. Notably high results appear despite data complexity. With consistent outcomes, the approach handles diverse clinical inputs well. Around ninety-four percent accuracy marks a reliable edge. Even under variable conditions, scores stay close to peak levels

A score of 0.971 on AUROC - beating the standard FL setup along with the centralised version. Halfway through each cycle, delay hits about 210 milliseconds. Eighteen percent less data moves through than standard federated learning setups. That gap shows up clearly when systems exchange updates.

When anomaly detection steps in, the attack success rate for injecting a backdoor drops sharply - falling from 62% down to just 18%. Detection acts like a shield, blocking hidden threats before they take hold. Instead of slipping through easily, malicious attempts get flagged early. This shift shows how visibility into odd behavior changes outcomes. Without such checks, more breaches slip past unnoticed. The drop reflects real progress in spotting what does not belong differential privacy. Every change to the model shows up clearly on the blockchain, locked in place so it cannot be altered, yet still keeps its ability to predict accurately performance.

## **2.5 Hybrid Blockchain-based Land Records Management**

Kadam et al. (2020) propose a hybrid blockchain architecture combining public and private blockchain properties for land records management in large, densely populated countries. Ownership details sit across many computers at once. Records of who bought what appear here too. This setup links every change to its moment in time. No single entity controls the flow of updates. Each participant holds an identical copy. Changes need agreement before sticking. Past entries stay untouched forever after entry. State-approved nodes ensure changes cannot happen once recorded, resist meddling, yet spread safely across locations. Broken things, like when storms or earthquakes hit. Citizens view data through a web app. Government counterparts update it. Access differs by role validation authority.

With Proof-of-Stake, the private network checks each transaction. Verification happens as nodes agree behind closed doors. A stake-based method confirms validity across the system. Agreement forms when participants back correct records. Security grows as validators commit resources silently. Ownership shifts happen through code written in Solidity, where rules live inside smart contracts; access stays limited by personal keys. A web of connections forms through an Ethereum-powered version of Geth. Each node links up without central control. Communication flows directly between participants. This setup runs on open-source code built for decentralization. Trust comes from shared rules, not intermediaries.

Running tests on setups as large as twenty nodes reveals how long it takes, on average, to process one transaction. That number holds steady across trials. Stays fixed at 12.7 seconds, even when more nodes are added - shows it scales well. Yet timing doesn't shift, no matter the setup size. That steady pace hints at solid performance under growth. Even with extra parts joining in, the clock reads the same. It holds its ground, second after second, node after node.

Beyond just theory, the study highlights how hybrid blockchain outperforms traditional paper methods. Forgery risks weigh heavily against paper systems. Instead of relying on physical records, a digital layer adds verification strength. The writers point to tampering issues as a core weakness in handwritten logs. Digital trails make changes harder without detection. Where paper fails under manipulation attempts, the mixed model holds up better. Security gaps shrink when both technologies work together. Not every solution fits all cases - but here, blending old and new shows clear gains yet one main issue remains: centralizing data increases risk during cyber threats.

## **2.6 EMRChain**

Decentralized Medical Records Using Ethereum and IPFS present a hybrid blockchain based decentralized application named EMRChain for electronic medical records. Running operations through Ethereum combined with IPFS. Medical records encrypted with AES 256 stored on IPFS via encrypted Content ID. Stored inside the chain, (CID) stays protected so access remains blocked even when CIDs get intercepted. Ownership of data sits entirely with patients under a setup built around role-defined permissions.

Some files stay stored securely while letting certain people reach them too - like physicians, they might add new details or pull up existing ones about individuals. Once a patient says yes, medical files may be shared. Hospitals have the ability to sign people up. Those running things make sure it happens for adding participants to the network. Smart contracts handle every access rule. Every transaction gets stamped forever in a tamper-proof record. Kept up to date by the software without manual input.

Running on Solidity, the setup uses Truffle for testing. Ganache steps in to simulate the network locally. MetaMask joins to handle wallet interactions smoothly. React.js shapes how users engage with the interface.

Security evaluation shows that EMRChain meets all the essential security requirements: confidentiality (AES-256 + RBAC access control), integrity (SHA-256 hash), availability (decentralized storage in IPFS), non-repudiation (public and private keys of ECDSA with timestamping) and scalability (decentralized distributed storage in IPFS). The comparative analysis shows that EMRChain is the

only system among the ones reviewed which offers confidentiality and all other security properties.

## **2.7 Blockchain-Based Healthcare Outcome Improvement: A Decentralized Patient Care Model**

Nekkalapudi et al. (2024) present a comprehensive review of blockchain applications in healthcare management and propose a system model addressing data siloing, privacy, interoperability, and administrative inefficiency. The proposed architecture incorporates a blockchain network for immutable EHR storage, smart contracts for automated consent management and data sharing, an interoperability layer for integration with existing healthcare information systems, AES and public/private key cryptography for data protection, and an immutable audit trail for regulatory compliance. The paper examines multiple blockchain platforms (Ethereum, Hyperledger) and discusses integration with emerging technologies including AI, IoT, and federated learning. The review acknowledges that blockchain adoption in healthcare remains in early stages, with scalability, high computational costs, and regulatory barriers as primary impediments. HIPAA and GDPR compliance are identified as non-negotiable requirements for any production deployment.

## **2.8 Quantum-Resistant Blockchain Using KYBER and FALCON Protocols**

Divya et al. (2026) address the quantum computing threat to Wireless Body Area Networks (WBANs) and healthcare data transmission by proposing a quantum-resistant blockchain system employing KYBER for key exchange, FALCON for digital authentication, and a code-based Key Encapsulation Mechanism (KEM) as an additional security layer. Patient medical records encryption and secure access via blockchain using smart contracts.

The KEM based approach proposed in this paper has lower computational overhead and faster key exchange compared to the current RSA and ECDSA based systems. The blockchain transaction time is consistent because of the use of lightweight cryptographic operations. This makes this system suitable for use in real-time health care applications. The system is validated using a web application where patients can interact with doctors, book appointments and get the prescription.

This system is a scalable future-proof solution to protect sensitive health information against quantum attacks especially for resource constrained IoTs in WBAN environments.

## **2.9 Decentralized EHR Using Ethereum and IPFS with ZKP and Emergency Access**

Harshavardhan et al. (2025) propose a novel Ethereum-based decentralized EHR system advancing on prior frameworks (MedRec, Patientory, MedChain) by introducing three key innovations: [1] a time-bound emergency access protocol reducing critical care response time by 20%; [2] an AI-driven module for digitizing paper records; and [3] Zero-Knowledge Proofs (ZKPs) for privacy-preserving data verification. The system employs IPFS for scalable off-chain storage, AES-256 encryption for all EHR files, SHA-256 hashing for integrity verification, and smart contracts for dynamic consent management and data

sharing agreements. The architecture complies with FHIR/HL7 standards and GDPR, with MetaMask providing patient-centric identity management. The granular access control model exposes only contextually relevant information, minimizing overexposure risk. Smart contracts also enable automated payments for third-party data use (research, insurance), enforcing trustless data governance without administrative overhead.

## **2.10 Decentralized Cloud-Based EHR Security with Dual Encryption**

Senthilselvi et al. (2025) propose a cloud-based EHR management system combining ECDSA digital signatures and SHA-256 hashing for dual-layer cryptographic protection. Starting off, ECDSA makes digital marks which protect information from being faked or changed. These signs ensure trust by showing data stayed exactly as intended. What happens is each signature ties uniquely to both message and sender. Without matching keys, altering even one part breaks the proof completely. So verification catches mismatches every single time. A string altered in any way shows up clearly through SHA-256's consistent output size. Changes become obvious at a glance.

With blockchain, data lives across many places at once, making it nearly impossible to alter. A break somewhere does not crash the whole system because everything runs on shared strength instead of one central hub. This setup avoids collapse from a lone weak spot by spreading trust everywhere problem.

Testing with made-up medical records reveals how ECDSA along with SHA-256 performs Encryption plus hash operations finish in just 115 milliseconds - faster than RSA's 185 and ahead of AES at 150. When records hit 1MB, blockchain checks take about 50 milliseconds. Bigger files, say 10MB, bump that up to 90ms - still quick. Speed holds steady even as data grows. No major lag appears at higher volumes records. Even if someone tries to repeat old messages, it holds firm. When strangers sneak between connections, it notices right away. Altered information gets rejected without delay.

A new method using two layers of encoding actually runs faster while keeping data safer. Not only does it guard information more effectively, but it also cuts down processing delays. Security improves without slowing things down. Instead of trading speed for protection, both get better at once. Less time computing, yet harder to break - results show a clear step forward That makes it workable within cloud-driven health systems.

## **2.11 Multilevel Authentication for Blockchain-Based EHR Systems**

Radhakrishnan et al. (2019) identify five categories of blockchain attacks — network attacks, user wallet attacks, smart contract attacks, transaction verification mechanism attacks, and mining pool attacks — and propose a Multi-Level Authentication (MLA) scheme targeting user wallet-based vulnerabilities. A single person signs up through what's called the User Management Layer. This part handles who gets access plus how they log in later. Built right under it sits control for permissions and profiles. The next level deals with data, keeping records safe while allowing updates. One step deeper runs the analysis tools that process everything quietly. Last comes integration with outside systems so

information flows where needed Validation QR Code Generation EHR Creation and Access via OTP Login Key Management Block Generation EHR Storage Layer Distributed Blockchain Across Providers HER Permissions handled through roles that define who sees what. Sharing depends on assigned access levels. Control flows from user position in system hierarchy.

A phone number links to a SIM card when setting up access. That link needs a personal code alongside it. A temporary passcode comes next, changing every minute. Each piece fits together like puzzle parts at the right moment password generated by Google Authenticator through QR code scanning.

Using more than one verification step stops fake websites from stealing login details. It also blocks attempts that rely on guessing common passwords. Even if someone tries to access funds without physical control, they fail. Attempts to trick users into revealing keys do not work either.

Before anything goes on the blockchain, getting the patient's go-ahead on their EHR data stops duplicate entries from slipping through. Using Flutter makes the setup possible, while patient records sit in JSON files to move faster through tasks.

## **2.12 SecureChain: Dual-Domain Blockchain for Healthcare and Real Estate Sharma et al.**

Sharma et al. (2025) present SecureChain, a dual-purpose blockchain platform addressing security challenges in both healthcare data management and real estate transactions. For healthcare, medical reports are encrypted with AES-256, stored in IPFS, and linked on-chain via cryptographic hashes; smart contracts enforce patient-controlled access permissions. For real estate, smart contracts automate ownership verification and transfer, recording permanent, tamper-proof ownership history on blockchain. The system uses Proof-of-Authority (PoA) consensus for energy efficiency and transaction finality. Security evaluation confirms SHA-256 data integrity, AES-256 confidentiality, digital signature authentication, and complete audit trails. Performance evaluation demonstrates: medical report retrieval time reduced from 8.5 to 3.2 seconds; real estate transaction time reduced from 15-20 days to under 24 hours; and near-elimination of fraudulent transactions. The platform is designed for compliance with HL7 FHIR healthcare interoperability standards and includes GDPR-compatible patient consent mechanisms.

## **2.13 ReChain: Secured Blockchain-Based Digital Medical Health Record Management**

Nautiyal et al. (2023) propose ReChain, a blockchain-based medical health record management system addressing the fragmentation, inaccessibility, and vulnerability of traditional centralized EHR systems. The system is built on the Ethereum Goerli testnet, uses IPFS (via Web3.storage) for decentralized file storage, and implements hierarchical access control: Admin (can authorize/unauthorize doctors), Doctor (can add patients, create and read records), and Patient (can read own records and upload files). Smart contracts are written in Solidity and organized into modular contracts for Patients, Doctors, Records, and Access Control, plus a MedicalInfoAddGet contract for unified frontend interaction. The system uses Web3.js as the blockchain-frontend bridge and MetaMask for wallet authentication. Comparative analysis against ten prior systems demonstrates that ReChain uniquely provides all eleven evaluated features simultaneously: data store, data fetch, authentication, access control,

record access, IPFS storage, smart contracts, hierarchical level access, scalability, data validation, and the ability to increase access level dynamically.

### **III GAP ANALYSIS**

Despite the significant advances documented across the thirteen reviewed papers, a critical examination reveals persistent and cross-cutting research gaps that limit the practical deployment and broad adoption of blockchain-based record management systems. These gaps span technical, regulatory, operational, and adoption dimensions.

#### **3.1 Quantum Vulnerability in Legacy Cryptographic Schemes**

The majority of reviewed systems still rely on classical cryptographic primitives — RSA, ECDSA, ECC — which are mathematically vulnerable to Shor's algorithm running on sufficiently advanced quantum computers. While He et al. (XMSS) and Divya et al. (KYBER + FALCON + KEM) directly address this gap, most other reviewed frameworks (Sankar, Rajasekharan, Senthilselvi, Radhakrishnan, Nautiyal) continue to employ ECC and SHA-256 without consideration of quantum-era vulnerabilities. As quantum computing hardware advances toward cryptographically relevant capabilities, systems secured only by classical algorithms face existential long-term security risks, particularly given that healthcare records must remain confidential for decades. A systematic migration path from classical to post-quantum cryptographic standards is absent from most reviewed works.

#### **3.2 On-Chain Scalability and Storage Overhead**

Blockchain networks inherently impose strict limitations on the volume of data that can be stored on-chain economically and efficiently. While hybrid on-chain/off-chain architectures using IPFS have emerged as the dominant mitigation strategy, this approach introduces new dependencies on the availability and integrity of off-chain storage providers. Transaction fees on public blockchains (Ethereum) can be prohibitive for high-frequency medical data operations, and Radhakrishnan et al. explicitly identify storage as a future challenge. The reviewed systems are predominantly evaluated in controlled simulation environments with small datasets; none demonstrate performance at the scale of a national healthcare system processing millions of daily transactions across thousands of institutions. Furthermore, as blockchain size grows over time, node storage requirements increase, potentially leading to centralization pressure where only resource-rich organizations can operate full nodes.

#### **3.3 Interoperability Across Heterogeneous Systems**

Interoperability remains a significant unsolved challenge. Most reviewed systems operate in isolation, tested on single blockchain platforms (Ethereum or Hyperledger Fabric) without cross-chain compatibility. Real-world healthcare ecosystems involve disparate EHR systems, hospital information management platforms, insurance databases, and government registries — each with distinct data models, APIs, and governance structures. While Harshavardhan et al. specifically design FHIR/HL7-compliant APIs, and Sharma et al. reference HL7 FHIR compliance as a design goal, none of the reviewed papers demonstrate actual integration with live legacy healthcare IT infrastructure or cross-institutional blockchain interoperability in production environments. The absence

of universal blockchain interoperability standards creates fragmented ecosystems that undermine the fundamental promise of seamless data sharing.

### **3.4 Limited Real-World Deployment and Validation**

With the exception of Sankar et al., who use a real-world anonymized CKD dataset from Abu Dhabi, the majority of reviewed systems are evaluated in simulation environments, local blockchain testnets (Goerli, Ganache), or with synthetic/fabricated datasets. Yatini et al. explicitly acknowledge that their federated learning framework uses simulated hospital networks rather than live institutional infrastructure, noting that real deployments will encounter unpredictable network latency, device heterogeneity, and governance complexities. The absence of pilot programs, clinical trials, or phased rollouts in actual healthcare facilities means that critical real-world performance parameters — system reliability under heavy transactional load, clinician usability, regulatory audit outcomes, and patient trust — remain empirically unvalidated.

### **3.5 Regulatory Compliance and Legal Recognition**

Healthcare data governance is subject to complex, jurisdiction-specific regulatory frameworks including HIPAA (United States), GDPR (European Union), the Personal Data Protection Bill (India), and equivalent national regulations. While several reviewed papers reference HIPAA and GDPR compliance as design goals, none provide formal legal analysis, regulatory audit results, or certification against specific compliance frameworks. The legal status of blockchain-recorded evidence, smart contract enforceability, and the right to erasure (a GDPR requirement potentially incompatible with blockchain immutability) are unresolved tensions that none of the reviewed papers adequately address. For land records, Kadam et al. acknowledge that the system must adhere to existing land registry regulations, but the specific legal pathway for recognizing blockchain records as legally binding ownership evidence is not established.

### **3.6 Smart Contract Security Vulnerabilities**

Smart contracts, once deployed on blockchain networks, are generally immutable and cannot be easily patched. Yet they represent a significant attack surface: Radhakrishnan et al. identify smart contract attacks (exploiting source code and virtual machine vulnerabilities) as a distinct category of blockchain vulnerability. The proposed healthcare system uses a four layer design including user management for registration Validation QR Code Generation EHR Creation and Viewing Login via OTP-Based MLA Key Generation. Block Generation EHR Storage Layer Distributed Blockchain across Providers Permissions handled through roles that define who sees what. Sharing set by user type, each level unlocks different areas. Control comes from assigned positions in the system. Some views appear only when your role allows it.

A working phone number sits at the core of access. Access follows only after that detail is confirmed. A secret word must line up correctly too. Timing matters because a temporary code changes often, created on the spot to match moments

Start things off with a quick scan of the QR code through Google Authenticator. This way gets you moving without extra steps or confusion along the path.

One way the system stays secure? It uses multi-step login checks. These stop fake websites from stealing access. Guessing passwords won't work either. Even basic trial-and-error attacks fail completely. Cold attempts with stolen data get blocked too. Some wallets get hacked. Others stay online where thieves can reach them.

Before anything goes into the blockchain, the patient checks it. That check stops anyone using the same data twice. Once approved, the record moves forward securely. No second uses slip through when permission comes first. Approval acts like a gate - only one path stays open type attacks.

This system runs smoothly when built with Flutter, while EHR information takes shape as JSON files. Efficiency comes through that pairing, each part playing its role without extra weight. The way things flow depends on how neatly those pieces fit together. SecureChain: Dual-Domain Blockchain for Healthcare and Real Estate Sharma et al.

If patients lose their private keys, they might never get back into their own health files. Staff training requirements, workflow integration complexity, and change management challenges in clinical settings are unaddressed.

#### **IV. FUTURE RESEARCH DIRECTIONS**

The gaps identified in the literature survey collectively define a rich research agenda for the next generation of blockchain-based record management systems. The following directions represent the most critical and impactful areas for future investigation.

##### **4.1 Post-Quantum Cryptographic Migration**

Future systems must prioritize a systematic migration from classical cryptographic schemes to NIST-standardized post-quantum algorithms. XMSS (as demonstrated by He et al.), CRYSTALS-KYBER for key encapsulation, and CRYSTALS-Dilithium or FALCON for digital signatures represent the most promising candidates. Research is needed on:

- (a) hybrid classical-post-quantum transition protocols that maintain backward compatibility with existing systems
- (b) performance optimization of post-quantum algorithms for resource-constrained IoT devices and Wireless Body Area Networks
- (c) formal security proofs of post-quantum blockchain systems in quantum random oracle models; and
- (d) cross-chain post-quantum interoperability standards. The urgency of this transition is amplified by —harvest now, decrypt later! threats, where adversaries collect encrypted health data today intending to decrypt it once quantum computers become capable.

## 4.2 AI-Augmented Blockchain Healthcare Systems

The integration of autonomous AI models with blockchain-secured healthcare systems represents a transformative research direction. Future work should explore:

- (a) AI-driven anomaly detection for real-time identification of suspicious blockchain transactions or access patterns;
- (b) federated learning with blockchain-verified model provenance to enable multi-institutional AI training without centralized data aggregation;
- (c) explainable AI frameworks integrated with immutable blockchain audit trails so that AI-generated diagnoses can be legally traced and verified;
- (d) natural language processing for automated digitization of paper medical records into FHIR-compliant structured formats;
- (e) predictive analytics for population health management using blockchain-secured longitudinal patient data. The AI models must themselves be cryptographically signed and verifiable to prevent adversarial model substitution.

## 4.3 Cross-Chain Interoperability and Standardization

Achieving genuine interoperability across heterogeneous blockchain networks, legacy healthcare IT systems, and cross-national regulatory frameworks requires concerted standards development. Future research should focus on:

- (a) atomic cross-chain swaps and relay protocols enabling data sharing across Hyperledger Fabric, Ethereum, and other platforms without centralized bridges;
- (b) universal healthcare blockchain APIs built on FHIR R4/R5 standards enabling plug-and-play integration with existing EHR systems (Epic, Cerner, Meditech);
- (c) decentralized identity standards (W3C DID, Verifiable Credentials) enabling portable patient identities across healthcare systems and national borders;
- (d) regulatory harmonization frameworks defining minimum technical standards for blockchain-based health data exchange across jurisdictions
- (e) cross-domain blockchain integration enabling seamless data flow between healthcare, insurance, pharmacy, and public health surveillance systems.

## 4.4 Scalable Layer-2 and Sharding Solutions

Achieving the transaction throughput required for national-scale healthcare deployments demands architectural innovations beyond current Layer-1 blockchain capabilities. Promising directions include:

- (a) Layer-2 payment channels and rollup technologies (Optimistic Rollups, zk-Rollups) reducing on-chain transaction load while preserving security guarantees;
- (b) sharding mechanisms distributing blockchain state across parallel chains, applicable to regional or specialty-based healthcare consortia
- (c) zero-knowledge proof systems (zk-SNARKs, zk-STARKs) enabling privacy-preserving computation on blockchain without revealing sensitive health data
- (d) dynamic block size adjustment algorithms responding to transaction volume fluctuations in healthcare environments
- (e) efficient garbage collection and archival mechanisms for managing the long-term growth of healthcare blockchain networks.

#### **4.5 IoMT Integration and Real-Time Patient Monitoring**

The Internet of Medical Things (IoMT) — encompassing wearable biosensors, implantable devices, smart hospital equipment, and ambient monitoring systems — generates continuous streams of patient data requiring secure, real-time processing. Future research should investigate:

- (a) lightweight blockchain protocols optimized for resource-constrained IoMT devices with limited processing power and battery life
- (b) edge computing architectures enabling local data pre-processing and aggregation before blockchain inscription, reducing latency and bandwidth consumption;
- (c) dynamic EHR updating mechanisms allowing real-time patient data from IoMT devices to be cryptographically signed, verified, and immutably recorded
- (d) fog computing layers providing intermediate storage and processing between IoMT devices and blockchain networks
- (e) emergency detection systems that automatically trigger time-bound emergency access protocols when IoMT data indicates critical patient conditions, as explored conceptually by Harshavardhan et al.

#### **4.6 Privacy-Preserving Analytics and Zero-Knowledge Proofs**

Healthcare research and public health management require access to population-level data patterns, yet individual privacy must be rigorously protected. Future directions include:

- (a) zero-knowledge proof systems enabling verification of medical facts (vaccination status, disease-free certification) without revealing underlying health records
- (b) secure multi-party computation protocols allowing multiple healthcare institutions to jointly compute aggregate statistics without sharing individual patient records
- (c) differentially private query mechanisms for public health surveillance that provide formal privacy guarantees against re-identification attacks
- (d) homomorphic encryption enabling computation on encrypted healthcare data without decryption, though practical performance remains a challenge requiring algorithmic optimization
- (e) privacy-preserving federated learning with formal convergence guarantees and fairness constraints across heterogeneous patient populations.

#### **4.7 Biometric and Multi-Factor Authentication Enhancement**

Strengthening identity verification without increasing user burden represents an important design challenge. Future research should explore:

- (a) biometric authentication (fingerprint, iris, facial recognition) integrated with blockchain identity management, offering non-repudiable user verification without password vulnerabilities;
- (b) continuous authentication mechanisms that verify user identity throughout a session based on behavioral biometrics (typing patterns, mouse movements) rather than only at login
- (c) decentralized key recovery mechanisms (social secret sharing, threshold cryptography) enabling patients to recover lost private keys without relying on centralized recovery authorities

- (d) hardware security modules (HSMs) and secure enclaves (Intel SGX, ARM TrustZone) for protecting cryptographic keys in clinical environments
- (e) smart card integration for seamless authentication in hospital settings where quick record access is critical during patient care.

#### **4.8 Regulatory Compliance by Design and Legal Validation**

Achieving regulatory acceptance requires moving beyond compliance-as-afterthought to Privacy by Design and Security by Design principles embedded in blockchain system architectures from inception. Future research directions include:

- (a) formal verification of smart contract logic against regulatory requirements using model checking tools;
- (b) privacy impact assessment frameworks specifically designed for blockchain-based healthcare systems;
- (c) legal analysis of blockchain record admissibility in national court systems for healthcare liability, property disputes, and insurance claims;
- (d) GDPR-compatible selective deletion mechanisms using chameleon hash functions or redactable blockchain approaches that preserve the integrity of the broader chain while enabling compliant erasure of individual data
- (e) automated compliance monitoring using blockchain-recorded audit trails that generate regulatory reports without manual intervention.

### **V . CONCLUSION**

Thirteen examined studies together show blockchain works well for protecting private digital information. Healthcare stands out as the area where it matters most - data there is highly delicate, rules are tough to follow. Other areas benefit too: property logs, product tracking networks, personal identification setups. Tests confirm solid performance - tampering gets caught almost every time, signatures match correctly beyond ninety-nine percent, shared machine learning runs efficiently, delays in processing stay within reasonable limits. Systems combine public ledgers with external storage like IPFS, scale without breaking, guard entry using methods such as CP-ABE and role-based permissions. Yet lab wins do not always transfer smoothly into live environments. Quantum computing risks linger unresolved. Widespread testing remains limited. Laws differ across regions, creating hurdles. Systems struggle to connect across platforms. What comes next involves stitching in defenses against future quantum attacks, smart tools that trace their own origins, learning models preserving privacy, medical device monitoring updated constantly, cryptographic proofs hiding raw data entirely. Progress depends on experts from different fields working closely. Shifts now favor patients holding power over records, moving away from single controlling hubs toward distributed trust. Moving small tests into broad usage stays the biggest barrier left to cross.

### **REFERENCES**

- [1]. A, Jayasudha, and D, Pugazhenth, "Classification of Textures using Patch Based Energy Features of Selected Wavelet Coefficients", Journal of Applied Sciences, Vol. 14, No. 7, 2014, pp. 709-713.
- [2]. Sankar R. et al., "A Secured Signature Verification Scheme with Multiple Attribute based Electronic Health Record Maintenance Scheme using Blockchain Technology," 2025 International Conference on Recent

- Innovation in Science Engineering and Technology (ICRISET), IEEE, DOI: 10.1109/ICRISET64803.2025.11252247.
- [3]. Joshi M. et al., "Block Chain Technology & Its Scope in Various Fields: A Comprehensive Review," 2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI), IEEE, DOI: 10.1109/ICSCAI61790.2024.10866600.
- [4]. He L. et al., "A Post-Quantum Blockchain and Autonomous AI-Enabled Scheme for Secure Healthcare Information Exchange," IEEE Journal of Biomedical and Health Informatics, Vol. 29, No. 9, September 2025, DOI: 10.1109/JBHI.2025.3579722.
- [5]. Yatini B. I. et al., "Blockchain-Enabled Secure Federated Learning for Electronic Medical Records: A Scalable and Privacy-Preserving Framework," 2025 8th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), IEEE, DOI: 10.1109/ISRITI68345.2025.11393406.
- [6]. Kadam R. et al., "Land Records System Using Hybrid Blockchain," 2020 International Conference on Convergence to Digital World – Quo Vadis (ICCDW), IEEE, DOI: 10.1109/ICCDW45521.2020.9318693.
- [7]. Rajasekharan A. and Koshy R., "EMRChain: Electronic Medical Records Management System using Blockchain," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), IEEE, DOI: 10.1109/ICBDS61829.2024.10837244.
- [8]. Nekkalapudi S. et al., "Blockchain-Based Healthcare Outcome Improvement: A Decentralized Method of Patient Care," 2024 First International Conference on Data, Computation and Communication (ICDCC), IEEE, DOI: 10.1109/ICDCC62744.2024.10961792.
- [9]. Divya G. et al., "Secure Healthcare Data Transmission through Quantum-Resistant Blockchain Employing Kyber and Falcon Protocols," 2026 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL), IEEE, DOI: 10.1109/ICSADL67539.2026.11452079.
- [10]. Harshavardhan H. et al., "Decentralized Electronic Health Records using Ethereum and IPFS: A Blockchain-Based Secure Access Framework," 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), IEEE, DOI: 10.1109/ICBDS67396.2025.11377969.
- [11]. Senthilselvi A. et al., "A Decentralized Cloud-Based Approach to Enhancing EHR Security with Blockchain and Dual Encryption," 2025 International Conference on Knowledge Engineering and Communication Systems (ICKECS), IEEE, DOI: 10.1109/ICKECS65700.2025.11035741.
- [12]. Radhakrishnan B. L. et al., "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), IEEE.
- [13]. Sharma V. et al., "SecureChain: A Blockchain-Based Framework for Secure Medical Records Management and Real Estate Transactions," 2025 IEEE 6th Global Conference for Advancement in Technology (GCAT), IEEE, DOI: 10.1109/GCAT66372.2025.11368435.
- [14]. Nautiyal N. et al., "Rechain: A Secured Blockchain-Based Digital Medical Health Record Management System," 2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT), IEEE, DOI: 10.1109/ICITIIT57246.2023.100.
- [15]. V. R, P. R. Kumar, D. Das, G. H, W. Hanbin and E. A, "Machine Learning-Driven Predictive Maintenance for Wind Turbines," 2026 International Conference on Electric Power and Renewable Energy (EPREC), Durg, India, 2026, pp. 1-6, doi: 10.1109/EPREC66546.2026.11412064.

- [16]. A. Tiwari, J. D. Kumar, W. Syed and G. H, "Efficient FPGA-Based CNN Accelerator for Real-Time Traffic Sign Classification on PYNQ-Z2," 2026 IEEE International Conference on AI Engineering and Innovations (AIEI), NIT Jamshedpur, India, 2026, pp. 1-4, doi: 10.1109/AIEI69164.2026.11496958.
- [17]. G. Ramkumar, M. Alluwaici, T. Vijetha, G. H, A. Venkatraman and R. M, "A Reliable System Performance Through NeuToMa with Spiking Neural Network Transformation in Network on Chip (NoC) Communication," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 215-219, doi: 10.1109/IC3ET64989.2026.11467379.
- [18]. Girish H., Srinivas S., Kavya M., ...Kabbur S. "Swift Autonomous Fire Suppression Robot", 16th International Conference on Advances in Computing Control and Telecommunication Technologies Act 2025
- [19]. Girish H., Soujanya S., "A Comprehensive Cadence-based Design Flow for RISC-V UART SOC IN SCL 180NM", 16th International Conference on Advances in Computing Control and Telecommunication Technologies Act 2025
- [20]. Girish H., Rakesh S., Prasanna Raj C.P., Singh A.S., Yathisha L, "Deep Learning for Diabetic Retinopathy: Automated Detection and Classification from Retinal Images", 16th International Conference on Advances in Computing Control and Telecommunication Technologies Act 2025
- [21]. Girish H., Shyam Sundar V., Priyanka C., Renuka Hebballi R.S, "RISC V Steel Processor Implementation for Communication between Two Chips using AXI Lite", 16th International Conference on Advances in Computing Control and Telecommunication Technologies Act 2025
- [22]. M. H N, G. H and N. K N, "Simulation and Verification of SPI Master and Slave Communication," 2025 6th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2025, pp. 1531-1534, doi: 10.1109/ICOSEC67334.2025.11459684. <https://ieeexplore.ieee.org/document/11459684>
- [23]. S. S. V, P. C and G. H, "Design and Analysis of a D-Band LC Bandpass Filter and Low-Noise Amplifier for 6G Front-End Applications," 2026 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2026, pp. 1-6, doi: 10.1109/IATMSI68868.2026.11466038. <https://ieeexplore.ieee.org/document/11466038>
- [24]. "A Comprehensive Cadence-based Design Flow for RISC-V UART SOC IN SCL 180NM" , Girish H, Soujanya, Grenze International Journal of Engineering and Technology, 2025
- [25]. "Swift Autonomous Fire Suppression Robot" Girish H et. Al., Grenze International Journal of Engineering and Technology, 2025
- [26]. "Deep Learning for Diabetic Retinopathy: Automated Detection and Classification from Retinal Images" , Girish H, Cyril Prasanna Raj P , Grenze International Journal of Engineering and Technology, 2025
- [27]. "RISC V Steel Processor Implementation for Communication between Two Chips using AXI Lite" Shyam Sundar V, Dr Girish H, Priyanka C, Renuka S Hebballi Grenze International Journal of Engineering and Technology, 2025
- [28]. Sujatha.S, Mahendra BM, & Dr. Girish H. (2024). Smart Irrigation System for Optimal Water Conservation. Revista Electronica De Veterinaria, 25(1), 2613 - 2619. <https://doi.org/10.69980/redvet.v25i1.1311>
- [29]. Mamatha K R, Thejaswini S, Rashmi N, & Dr. Girish H. (2024). Laser Fencing Surveillance System With Email Alert. Educational

- Administration: Theory and Practice, 30(2), 1539–1544.  
<https://doi.org/10.53555/kuey.v30i2.7919>
- [30]. Thejaswini S, Mamatha K R, Rashmi N, & Dr. Girish H. (2024). Performance Evaluation of AI Models in Early Heart Disease Diagnosis. *Educational Administration: Theory and Practice*, 30(2), 1531–1538. <https://doi.org/10.53555/kuey.v30i2.7918>
- [31]. Sushma K Sattigeri, Seema Srinivas, Shridhar Kabbur, Girish H, “Revolutionizing Urban Waste Management: An AI-Powered Autonomous Solution for Smart Cities”, *Tuijin Jishu/Journal of Propulsion Technology* ISSN: 1001-4055, Vol. 45 No. 02 (2024)
- [32]. Girish H, Vajjala Sai Sree Hari, Ponde Lakshmi Narasimha, P N Shreya, Dadigala Bhargavi, "THE DESIGN AND VERIFICATION OF A 32-BIT RISC V PROCESSOR USING VEDIC MATHEMATICS", *International Journal of Creative Research Thoughts (IJCRT)*, ISSN:2320-2882, Volume.12, Issue 5, pp.1130-1135, May 2024, Available at :<http://www.ijcrt.org/papers/IJCRTAB02172.pdf>
- [33]. IoT based home automation using Blynk cloud, J. Chetan Naik, B. S. Deeksha, H. Girish, Gurusharan Kashetty, T. G. Shivapanchakshari, Manohar Sai Polakam, *Journal: AIP Conference Proceedings, AIP Conf. Proc. 2965, 020006 (2024)*, <https://doi.org/10.1063/5.0215427>, Published: July 2024
- [34]. IoT based fire alarm system using Blynk app, T. Bhargava, H. Kishor Kumar, Pramod Mahalingappa Godi, H. Girish, J. Chetan Naik, *Journal: AIP Conference Proceedings, AIP Conf. Proc. 2965, 020007 (2024)*, <https://doi.org/10.1063/5.0212325>, Published: July 2024