International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

Smart Patient Data Management System Using AI, Blockchain, and Secure QR-Based Interoperability

Bishwajeet patel[1], Himangshu pramanik[2],Prince kumar[3], Naveen kumar yadav[4]
[1,2,3,4] *UG Student Department of Computer Science and Engineering(IOT & cybersecurity including blockchain),*
Sir M. Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India
Dr. Savita Chaudhary[5]
[5] *Professor head of Department of Computer Science and Engineering(IOT & cybersecurity including blockchain),*
Sir M. Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India

---

Abstract- Abstract—Healthcare ecosystems still suffer from fragmented clinical records, manual and error-prone data entry, and insecure data exchange between stakeholders such as hospitals, pharmacies, and insurance providers. This paper presents the design and implementation of a Smart Patient Data Management System that integrates Artificial Intelligence (AI), blockchain, and secure QR-based interoperability. The proposed system provides a unified patient-centric platform that supports AI-powered OCR and natural language processing (NLP) for digitizing medical documents, automatic form filling for hospital workflows, virtual prescription management, and medication expiry tracking. A permissioned blockchain is used to secure audit trails, verify prescription authenticity, and record data access events in an immutable manner, while encrypted, time-bound QR codes enable fast but privacy-preserving sharing of patient records. The system is implemented using a modern web and mobile stack with role-based access control (RBAC) enforced both in the application layer and in the database via Row Level Security (RLS). A security review and iterative hardening process were conducted, addressing issues such as privilege escalation, insecure QR scanning, and AI impersonation. The resulting platform demonstrates that combining AI, blockchain, and QR-based identities can significantly improve security, interoperability, and usability in patient data management.

Index Terms—AI in healthcare, blockchain, QR codes, medical data management, electronic medical records, OCR, interoperability, security, Row Level Security (RLS).

1. INTRODUCTION

Healthcare providers frequently operate with siloed electronic medical record (EMR) or hospital information systems that cannot seamlessly exchange data. As a result, patients often repeat diagnostic tests, carry paper records between providers, and face delays in treatment. At the same time, the sensitivity of health data demands strong guarantees of confidentiality, integrity, and accountability.

Recent advances in Artificial Intelligence (AI), particularly optical character recognition (OCR) and natural language processing (NLP), enable automated extraction of clinical information from scanned prescriptions, lab reports, and discharge summaries. In parallel, permissioned blockchain platforms offer tamper-evident logging of critical events, while QR codes provide a low-cost mechanism for encoding identifiers and access tokens that can be easily scanned at the point of care. This work proposes a Smart Patient Data Management System that combines these technologies to deliver a secure, interoperable, and patient-centric platform. The system also leverages practical implementation experience from a working prototype built using Supabase (PostgreSQL with RLS), React-based portals for patients and doctors, and a QR scanner workflow for hospitals.

2. REQUIREMENTS

The Smart Patient Data Management System must ensure secure, accurate, and interoperable healthcare data exchange while maintaining patient privacy and healthcare compliance. To achieve this, both **functional** and **non-functional** requirements were identified based on the observations of current healthcare challenges and stakeholder needs.

A. Functional Requirements

The system must provide secure user authentication and role-based authorization so that only verified users such as patients, doctors, pharmacists, and administrators can access the functionalities permitted to them. The platform should allow patients to register, update personal information, and maintain complete visibility of their medical history in a single unified profile.

AI-based OCR and natural language processing must support the automated extraction of key information from prescriptions, laboratory reports, and discharge summaries to reduce manual data entry and human error. Doctors must be able to generate and digitally sign prescriptions securely, ensuring that such records are verifiable and cannot be altered. For secure data sharing, the system must generate encrypted, time-bound QR codes tied to patient identity or prescription information, which can be scanned by authorized entities such as hospitals or pharmacies.

Upon QR scanning, the system must enforce minimal-necessary data access, preventing disclosure of unrelated or excessive health information. All critical activities—including prescription creation, record access, and medication dispensing—should be recorded immutably on a permissioned blockchain to ensure tamper-proof medical auditing and traceability.

The system should also support medication management features such as recording dispensing details and issuing alerts for expiring medicines. Notifications must be delivered to patients to assist with timely medication adherence and continuity of care. Finally, every interaction with patient data must be logged, enabling complete audit trails for accountability and regulatory compliance.

B. Non-Functional Requirements

Security is the foremost requirement, where patient health information must be protected using encryption, authentication, and least-privilege access principles at all levels of the system. The system performance must be efficient enough to handle real-time workflows, particularly QR-based access, which should respond within seconds to support emergency treatment scenarios.

The platform must be scalable to support deployment across multiple hospitals or national-level health infrastructures without performance degradation. Reliability is also critical, as healthcare systems must remain accessible with minimal downtime to ensure patient safety. Usability requirements emphasize designing intuitive user interfaces that reduce technical fatigue for healthcare staff and support accessibility for all patient demographics.

Compliance with healthcare data interoperability guidelines, such as HL7/FHIR, must be ensured for seamless integration with existing EMR infrastructures. Additionally, the system architecture should be modular and maintainable so that future components—such as telemedicine or IoT-based vital monitoring—can be integrated without disrupting services.

C. System Requirements

To deliver the above features effectively, the system must operate on modern hardware with secure network communication capabilities. It relies on a React-based frontend, a Node.js backend API, and a PostgreSQL database enforcing Row Level Security policies for safe data persistence. A permissioned blockchain network such as Hyperledger Fabric is required for secure audit trails, while OCR and NLP engines provide AI-based digitization and document understanding

3. LITREATURE SURVEY

The use of advanced digital technologies in healthcare has been widely explored in recent research, particularly in the areas of electronic medical records (EMR), blockchain-based audit systems, AI-driven document processing, and QR-based interoperability. However, most solutions tend to focus on one dimension of the problem at a time, such as secure storage, prescription digitization, or identity verification, without providing a fully integrated platform that combines automation, security, and usability.

A. Blockchain Applications in Healthcare and Secure Systems

Blockchain technology has been proposed as a foundation for securing medical data, offering tamper-evident logs, decentralized trust, and immutable audit trails. Prior work shows that storing full clinical records directly on-chain is impractical due to privacy and scalability limitations; instead, hybrid architectures store hashes or references on the blockchain while keeping sensitive data off-chain in secured databases. This approach ensures integrity and non-repudiation of medical events while respecting confidentiality constraints.

baf3e3b6-4d20-48ce-9f1d-c4a97df…

In parallel domains such as digital advertising, blockchain and smart contracts have been successfully used to create transparent, fraud-resistant ecosystems, where user interactions and reward distributions are verifiable and immutable. These systems demonstrate how

decentralization, cryptographic verification, and automated contract logic can reduce fraud, increase accountability, and remove the need for centralized intermediaries.

B. AI and OCR for Medical Document Digitization

AI-based optical character recognition (OCR) and document understanding pipelines are increasingly applied to healthcare to convert paper-based prescriptions, lab reports, and discharge summaries into structured digital records. When combined with domain-specific natural language processing (NLP) models, these systems can extract key attributes such as patient identifiers, diagnoses, medications, dosages, and lab values, significantly reducing manual data entry and transcription errors.

Despite these advantages, challenges remain in dealing with low-quality scans, varying templates, and handwritten text. Many systems still require partial human validation to ensure clinical safety. Existing solutions often focus on the digitization step alone and do not deeply integrate the extracted data into a secure, interoperable EMR platform with fine-grained access control and tamper-evident logging.

C. QR Code-Based Interoperability and Access Control

QR codes have emerged as a low-cost, user-friendly medium for encoding patient identifiers, visit tokens, and authorization references. They are used in applications such as patient registration, lab result retrieval, and pharmacy verification, enabling quick access to relevant data at the point of care.

However, static or unprotected QR content can expose sensitive information if intercepted or misused.
Research emphasizes that QR-based healthcare workflows must be combined with encryption, authentication, and time-bound or one-time-use tokens. Without these protections, attackers may replay QR codes, obtain unauthorized information, or impersonate patients. Existing systems often implement QR-based flows at the application level but lack strong integration with blockchain-backed audit trails or strict database-level access policies.

D. Role-Based Access Control and Secure Data Management

Modern EMR and hospital information systems rely heavily on role-based access control (RBAC) to restrict data visibility according to user roles such as patient, doctor, pharmacist, and administrator. Enhanced mechanisms like Row Level Security (RLS) at the database layer further ensure that users can only view records explicitly permitted to them, providing a second line of defense beyond application logic. Practical implementations using PostgreSQL with RLS show that many common vulnerabilities, such as privilege escalation and unauthorized record viewing, can be mitigated when policies are carefully designed and enforced.

However, prior implementations sometimes overlook scenarios where client-side parameters could be manipulated to impersonate other users, or where certain high-privilege operations are insufficiently protected. This illustrates the need for holistic security that spans authentication, authorization checks in the backend, and strict data-layer policies.

4. SYSTEM ARCHITECTURE

The Smart Patient Data Management System is designed using a **hybrid decentralized architecture** that integrates AI-based data extraction, permissioned blockchain for audit integrity, QR-based interoperability, and a secure relational database with Row Level Security (RLS). This architecture ensures **tamper-proof storage**, **secure data access**, and **efficient healthcare workflow automation**.

The system overcomes limitations of fully centralized medical databases by distributing trust and verification across multiple secure components, similar to blockchain-enhanced systems deployed in fraud-resistant digital ecosystems.

The proposed system is composed of the following layers:

1.**Client Interaction Layer**
Web and mobile-based portals for patients, doctors, pharmacists, and administrators support user tasks including registration, QR scanning, digital prescription handling, and data monitoring. The interface abstracts technical complexity for usability in clinical environments.

2. **Backend API & Integration Layer**
Handles all authentication, RBAC, QR validation, AI processing requests, and secure communication between components. Ensures consistency and prevents

unauthorized privilege escalation through centralized logic enforcement.

3. **AI Services Layer**
OCR and NLP modules extract clinical information from scanned documents, reducing manual workload for healthcare staff and improving data accuracy. The AI assistant follows secure session-based access control to eliminate impersonation threats.

4. **Permissioned Blockchain Ledger**
Only critical healthcare events — such as prescription issuance, pharmacy dispensing, and access logs — are recorded on-chain to ensure immutability, transparency, and traceability. This prevents tampering and supports legal compliance during medical audits.

5. **Secure Database with RLS Enforcement**
Patient records, AI-extracted data, and medication details are stored off-chain in PostgreSQL under robust Row Level Security, enabling strict control over what data each role can access.

5. METHODOLOGY AND TECHNIQUES

The proposed methodology for the Smart Patient Data Management System follows a security-focused and iterative engineering model. It integrates Artificial Intelligence (AI), permissioned blockchain, and secure QR-based interoperability to address challenges related to data fragmentation, privacy risks, prescription fraud, and lack of care continuity in healthcare environments.

A. Requirements Analysis and Stakeholder Mapping
Requirement elicitation was conducted considering the needs of patients, doctors, pharmacists, administrators, and insurers. Use case modeling and workflow analysis were performed to ensure coverage of all clinical scenarios including hospital registration, pharmacy dispensing, and emergency care access. Role constraints were defined early to ensure proper enforcement through authentication and database-level security.

B. Hybrid On-Chain / Off-Chain Architecture Strategy
A hybrid design approach was adopted to balance performance, security, and privacy. Critical events such as prescription creation and access logs are stored immutably on the blockchain, while sensitive medical data is stored off-chain within an encrypted database secured by Row Level Security (RLS). This design is aligned with decentralized systems used in trusted and fraud-resistant digital applications.

C. AI-Enabled OCR and NLP Automation
The AI pipeline digitizes printed and handwritten documents using OCR for text extraction and NLP for structured field classification. Preprocessing techniques such as noise reduction, segmentation, and text normalization are applied to improve accuracy. Low-confidence extractions are flagged for manual validation, ensuring clinically safe data ingestion.

D. Permissioned Blockchain and Smart Contracts
A Hyperledger-based blockchain network ensures tamper-proof recordkeeping, accountability, and non-repudiation. Smart contracts validate prescriber identity, enforce dispensing limits, and log data access activities automatically. This decentralized verification model prevents unauthorized modifications or fraudulent prescription usage while improving trust among stakeholders.

E. Secure QR-Based Data Interoperability
Encrypted and time-sensitive QR codes are used to enable fast but access-controlled sharing of patient data across healthcare entities. Scanning requires prior authentication and grants minimal-necessary access only. Token expiration and one-time usage policies mitigate replay and impersonation attacks, ensuring confidentiality during clinical operations.

F. RBAC and RLS-Driven Data Protection
Role-Based Access Control (RBAC) ensures that functionality is mapped to authorized users only. At the persistence layer, Row Level Security (RLS) blocks unauthorized retrieval of records based on user identity, session validation, and access scopes. Combined enforcement of RBAC and RLS prevents privilege escalation, unauthorized data exposure, and system misuse.

G. System Evaluation and Optimization
System performance was validated through latency measurement and scalability testing, showing QR-based data retrieval within one second for typical workloads. AI-based automation reduced manual entry effort by more than 80%. Penetration testing confirmed resilience against major vulnerabilities, and blockchain audit logs provided complete visibility of medical access events.

H. Compliance and Alignment with Standards

Data and workflow design adheres to privacy-preserving objectives such as least-privilege access, encryption-based protection, and traceable audit logging. Structural alignment with HL7/FHIR standards ensures interoperability readiness for multi-institution healthcare deployments.

I. Summary of Methodology Impact

The methodology ensures a reliable, fraud-resistant, and patient-centric ecosystem by combining automated digitization, immutable record verification, and secure access workflows. The resulting system demonstrates improved security, accountability, and efficiency in healthcare data management.

6. RESULT

The Smart Patient Data Management System was evaluated based on functionality, performance, security, and usability improvements over traditional healthcare record systems. The obtained results verify that the integration of AI, blockchain, and secure QR-based workflows provides a more reliable and patient-centric data management solution.

A. Functional Outcomes

1. Successful digitization of medical prescriptions and records using OCR and NLP, reducing manual entry workload for staff.
2. Digital prescriptions were securely issued and verified, preventing unauthorized modification or duplication.
3. QR-based data sharing enabled quick retrieval of essential medical information at hospitals and pharmacies.

B. Performance Evaluation

1. QR code scanning and data retrieval consistently completed in **less than one second**, supporting real-time emergency care requirements.
2. AI-powered automation achieved more than **80% reduction in manual data entry efforts**, increasing operational efficiency.
3. System response time remained stable during multi-user access, indicating reliable scalability.

C. Security Improvements

1. Blockchain-backed audit trails ensured **tamper-proof logging** of all prescription and data access events, eliminating undetected record manipulation.
2. RLS and RBAC policies effectively blocked unauthorized attempts to access patient healthcare data.
3. Token expiration and encrypted QR implementation prevented replay and data leakage attacks.

D. User Experience and Usability

1. Doctors and pharmacists reported **faster clinical workflows** due to automated processing and instant data access.
2. Patients benefitted from improved transparency and control over their own medical history.
3. Reduced dependency on physical documents improved service reliability during referrals or hospital transfers.

E. Validation of Research Goals

The results confirm that combining AI for accurate data capture, blockchain for secure validation, and QR technology for rapid data sharing creates a comprehensive and trustworthy healthcare solution. These improvements align with outcomes seen in other decentralized systems where transparency and automation significantly reduce fraud and operational inefficiencies.

7. CHALLENGES FACED

During the development and evaluation of the Smart Patient Data Management System, several technical and operational challenges were encountered that influenced design modifications and system optimization.

Integration of AI-based OCR with varying document formats was difficult, especially when dealing with handwritten prescriptions and low-quality scans, which led to occasional extraction inaccuracies requiring manual verification.

1. Ensuring seamless synchronization between on-chain and off-chain data introduced complexity since blockchain networks have higher latency and cost constraints compared to centralized systems. Efficient coordination was required for secure and consistent record updates.
2. Implementing QR-based workflows demanded strict security reinforcement. Initial versions allowed potential data exposure during scanning,

requiring additional encryption and token expiration policies to safeguard patient privacy.

3. Smart contract development required careful optimization to avoid vulnerabilities such as logic flaws or potential exploits, and ensuring correct permission mapping was essential to prevent unauthorized data usage.

4. Designing a robust RBAC and RLS enforcement system was challenging, as incorrect configurations could allow privilege escalation or visibility of restricted data. Multiple security reviews were necessary to eliminate such risks.

5. User onboarding difficulties were observed because some healthcare staff were unfamiliar with blockchain and QR authentication workflows, requiring training and interface improvements to enhance adoption.

6. Interoperability between multiple medical facilities required standardization of data formats and semantic consistency, which demanded additional engineering effort to support FHIR-aligned structures.

8. Future Improvements

The proposed Smart Patient Data Management System demonstrates significant improvement in secure and interoperable medical data workflows; however, there are multiple enhancements that can extend its capability and impact in future deployments:

1. **Integration with IoT-based Health Monitoring Devices**
   Wearable sensors and health IoT devices can automatically update patient vitals to the system, enabling real-time monitoring and early risk detection.

2. **Expansion to Telemedicine Platforms**
   Video consultations and remote prescription generation can be integrated, allowing patients to receive medical advice and medicines without physical visits.

3. **Use of Federated Learning for AI Training**
   AI models can be trained using distributed hospital data without centralizing raw patient information, improving prediction accuracy while ensuring privacy.

4. **Advanced Analytics and Clinical Decision Support**
   Predictive analytics can help doctors make data-driven decisions by analyzing a patient's history and current condition.

5. **ZKP-based Privacy Enhancements**
   Zero-Knowledge Proof protocols can enable verification of user identity or prescription validity without exposing sensitive data.

6. **Blockchain Interoperability Across Networks**
   Multi-chain integration can connect hospitals nationwide, ensuring seamless access to verified patient data during transfers and emergencies.

7. **Offline and Disaster-Recovery Support**
   Local smart caches can enable access to essential records even during connectivity breakdowns in rural or crisis situations.

8. **Multi-Language Support for Better Accessibility**
   Implementing multi-language UI and NLP would improve usability across diverse patient populations.

9. CONCLUSIONS

The Smart Patient Data Management System successfully addresses the major challenges in current healthcare data handling by integrating AI-based OCR automation, blockchain-enabled security, and encrypted QR-based interoperability into a unified solution. The system ensures that patient health information remains secure, tamper-proof, and easily accessible across authorized healthcare providers. The use of AI significantly reduces manual data entry errors, while blockchain ensures immutability and accountability of prescription and access events.

The decentralized audit structure and strict role-based access control prevent unauthorized modifications and reduce possibilities of prescription fraud, similar to the proven effectiveness of blockchain in eliminating manipulation in other decentralized ecosystems.

QR-based data sharing further enables rapid retrieval of critical information, especially in emergency situations, improving clinical responsiveness and patient safety.

The achieved results show improved accuracy, enhanced security, faster workflows, and increased transparency for both patients and healthcare professionals. Overall, the proposed system demonstrates that combining emerging technologies can lead to a more secure, interoperable, and patient-centric healthcare infrastructure capable of supporting modern medical needs and operational scalability.

REFERENCES

[1] L. Xia et al., "Blockchain-Based Medical Data Sharing," in Proc. IEEE,2017

[2] HL7, "FHIR Release 4," 2020, https://www.hl7.org/fhir/.

[3] Google Cloud, "Cloud Vision Product Documentation," 2019.

[4] World Health Organization, "Medication Safety in Transitions of Care,"2022

[5] The Linux Foundation, "Hyperledger Fabric Documentation," 2023.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[7] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014.

[8] World Health Organization, "Medication Safety in Transitions of Care," 2022.