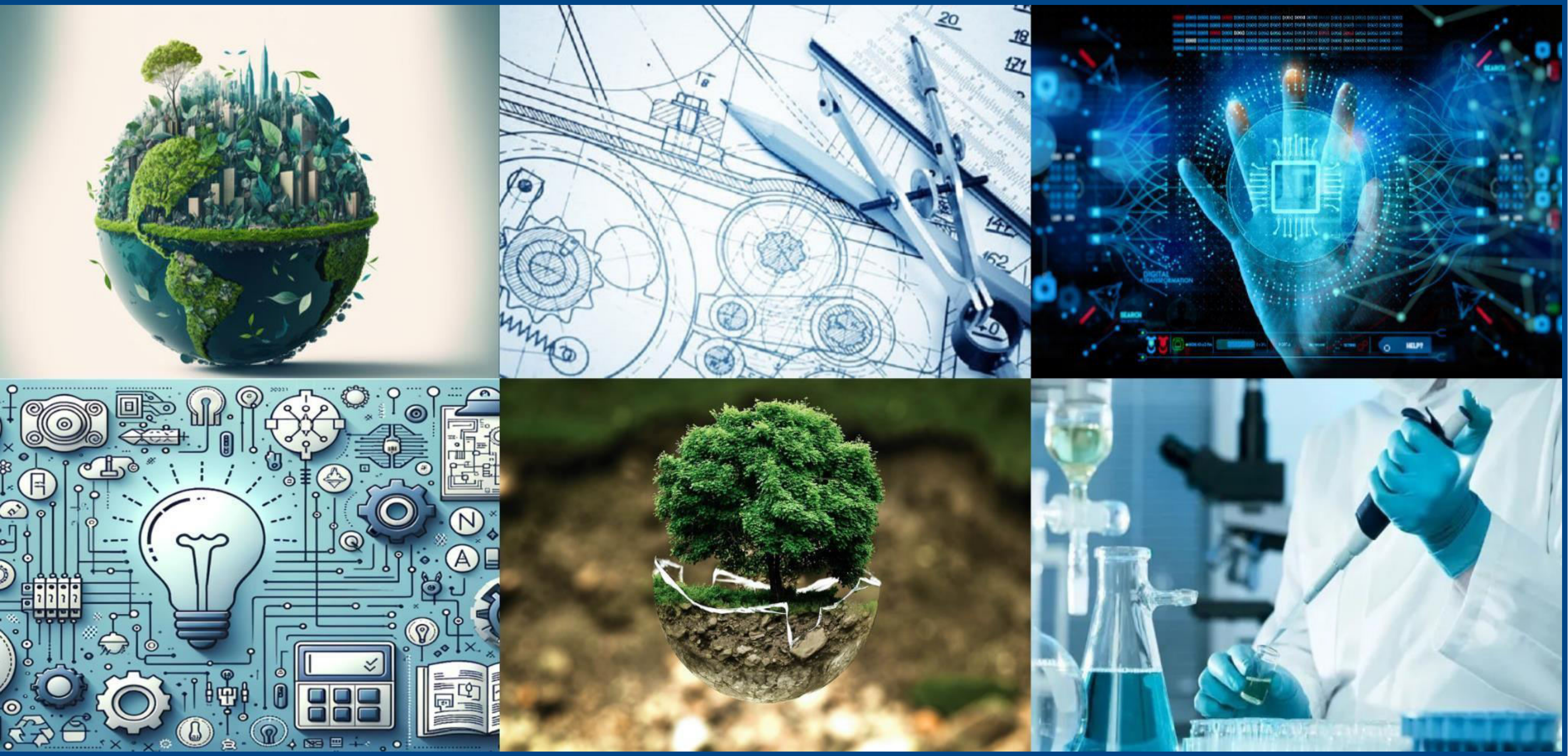
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 7, July 2025

www.ijmrset.com ijmrset@gmail.com +91 6381 907 438 +91 63819 07438

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Development of a Secure Healthcare Management System Utilizing Blockchain Technology for Encrypted Patient Data Transmission

Parkavi K[1], Dhanush Balaji G[2], Sriram A[3], Darshan R[4], Vasanth V[5]

Assistant Professor, Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India[1]

UG Scholars, Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India[2, 3, 4, 5]

ABSTRACT: In the digital healthcare era, ensuring the security of sensitive patient data during transmission and storage is crucial. This project introduces a secure healthcare management system that integrates blockchain technology with AES encryption and SHA-256 hashing to protect medical information. General physicians input patient data—such as diagnoses and prescriptions—which is encrypted using AES and shared securely with departments like Radiology, Surgery, and Pharmacy. Each department accesses data using unique decryption keys controlled by role-based access policies. SHA-256 hashing ensures data integrity by detecting any unauthorized modifications. Blockchain technology underpins the system by maintaining a decentralized, tamper-proof ledger that logs all data access and updates with timestamps, allowing for transparent and auditable operations. This approach enhances security, transparency, and interoperability across healthcare units and external networks. The combined use of encryption, hashing, and blockchain provides a scalable, efficient, and trustworthy framework suitable for modern digital healthcare systems.

KEYWORDS: Blockchain, Healthcare Management System, AES Encryption, Patient Data Security, SHA-256 Hashing, Encrypted Prescription, Data Confidentiality, Secure Data Transmission, Access Control, Medical Record Protection, Smart Contracts, Decentralized System, Data Integrity, Health Informatics, Privacy Preservation

I. INTRODUCTION

In today's digital healthcare landscape, securely handling and transmitting sensitive patient data is critical, particularly as information flows between departments like Surgery, Radiology, Laboratory, and Pharmacy. This proposed healthcare management system addresses these challenges by using Advanced Encryption Standard (AES) to encrypt prescriptions generated by general physicians, ensuring secure communication across units. Each department receives a unique, securely distributed decryption key, with Role-Based Access Control (RBAC) limiting data access strictly to what is necessary for each role—protecting privacy through the principle of least privilege. To maintain data integrity, all records stored in the centralized database are hashed using SHA-256, ensuring any unauthorized modifications are immediately detectable. The system also integrates blockchain technology to provide a decentralized, tamper-proof ledger that logs all access and modifications with timestamps, enabling transparent auditing and enhancing trust among healthcare providers and patients. This combined use of AES encryption, SHA-256 hashing, and blockchain, along with robust access controls, creates a secure, scalable, and interoperable digital infrastructure. It not only minimizes the risks of data breaches and misuse but also improves interdepartmental coordination and patient care outcomes, making it a practical and future-ready solution for hospitals, clinics, and telemedicine platforms.

II. LITERATURE REVIEW

Thanaruk Theeramunkong and Somchart Fugkeaw [1] proposed a secure and verifiable Boolean keyword searchable encryption scheme for Cloud Data Warehouses (CDW). Their method combines Partial Homomorphic Encryption (PHE), B+ Trees, inverted indexes, and bitmapping to support privacy-preserving searches over encrypted data. Blockchain and smart contracts are integrated to automate authentication and search verification, eliminating the need for third-party involvement.

Tutut Herawan and Abul Beg [2] introduced MaxD K-Means, an improved clustering algorithm that automatically determines the number of clusters and initial centroids without user input. This approach addresses the sensitivity of traditional K-Means to initial conditions and reduces iterations by up to 78%, as demonstrated in experiments with synthetic datasets.

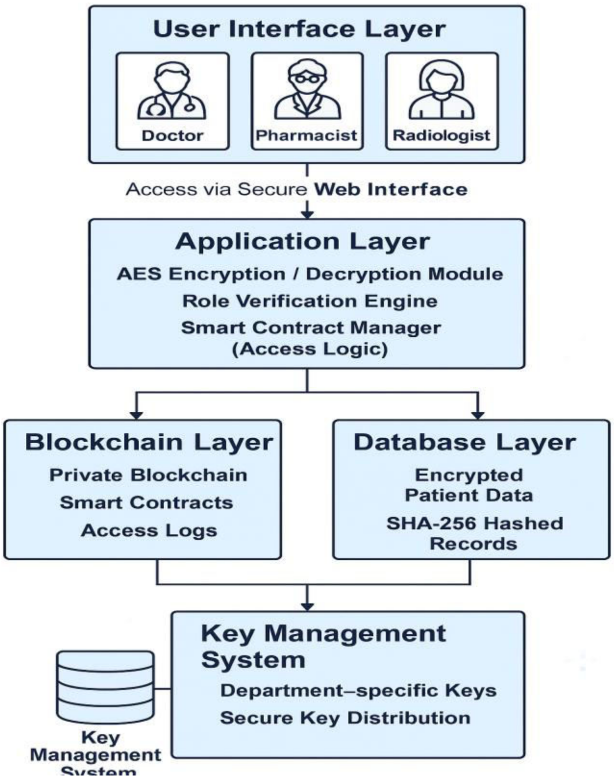
Rongxing Lu, Ximeng Liu, and Jianfeng Ma [3] developed a privacy-preserving patient-centric clinical decision support system (PPCD) using Naive Bayesian classification. The system securely processes cloud-stored patient data using an additive homomorphic proxy aggregation scheme, enabling accurate disease risk prediction while protecting individual privacy. It also introduces a secure top-k disease retrieval protocol for enhanced user interaction.

III. SYSTEM ARCHITECTURE

The proposed healthcare management system is designed with a multi-layered architecture to ensure secure, efficient, and decentralized handling of sensitive patient information. The system consists of the following key components:

1. User Interface Layer

Developed using HTML, CSS, JavaScript, and Bootstrap, this layer provides role-based access for users such as doctors, pharmacists, and administrators. It supports patient registration, prescription generation, and medical record updates while restricting unauthorized access.



2. Application Layer

Implemented with Java and Spring Boot, this layer manages core logic including AES-based encryption/decryption, role verification, API handling, and smart contract execution to ensure secure operations.

3. Blockchain Layer

A private blockchain (e.g., Ethereum or Hyperledger) logs all data transactions, stores hashed pointers, and manages smart contracts for transparent access control and audit trails.

4. Database Layer
Encrypted patient records are stored in a secure RDBMS (e.g., PostgreSQL), while SHA-256 hashing ensures data integrity. Blockchain holds metadata and activity logs.

5. Key Management System
Each department has its own decryption key, securely managed and distributed via a KMS with strict access controls and key rotation policies. This layered architecture integrates encryption, hashing, and blockchain to safeguard patient data from breaches and unauthorized access.

IV. METHODOLOGIES

The development of the secure healthcare management system follows a structured approach:
1. Requirement Analysis and System Design: This phase identifies key data types (e.g., prescriptions, records), security needs, and compliance with regulations like HIPAA. A modular, scalable architecture is designed using Ethereum blockchain for its smart contract capabilities and decentralized data integrity.

2. Blockchain Integration: Smart contracts written in Solidity manage access control, encryption, and data transactions. A private blockchain ensures immutable storage, while AES encryption secures data before storage, protecting against unauthorized access.

3. System Development: The frontend, built with HTML, CSS, JavaScript, and ReactJS, provides user-friendly interfaces. The backend, developed using Spring Boot, handles authentication and blockchain interactions. PostgreSQL supports auxiliary data storage.

4. Data Encryption & Access Control: Data is encrypted at rest and in transit using AES and SSL/TLS. A public-private key scheme manages access, and all actions are logged via smart contracts to maintain traceability.

5. Testing & Validation: Unit, integration, and penetration testing ensure system functionality and security. Compliance checks verify adherence to healthcare standards like HIPAA.

6. Deployment & Maintenance: The system is deployed with secure blockchain nodes and integrated into hospital infrastructure. Continuous monitoring and updates maintain system reliability and security.

V. IMPLEMENTATION

The Secure Healthcare Management System ensures secure data transmission and storage through encryption and blockchain integration. It is built with a focus on user interface, backend processing, database management, and encryption.

1. **Frontend Design:** Developed using HTML, CSS, JavaScript, and Bootstrap, the frontend offers a responsive UI for healthcare professionals and patients. Key features include user authentication, patient data display, and an interactive dashboard for managing records.

2. **Backend Design:** The backend, built with Java and Spring Boot, handles user authentication, business logic, and database operations. It uses RESTful APIs for CRUD operations and Spring Security for role-based access control. Patient data is securely stored in PostgreSQL.

3. **Database Integration:** A relational database (PostgreSQL) stores patient data, medical histories, and appointment records. CRUD operations are performed through Spring Data JPA.

4. **Blockchain Integration:** Blockchain (Hyperledger or Ethereum) ensures data integrity by storing patient consent and validation records. Smart contracts automate data access management.

5. **Encryption Workflow:** AES encryption secures data at rest, while SSL/TLS ensures secure data transmission. JWT tokens handle secure user authentication and API access, with sensitive data encrypted before storage.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This implementation ensures secure, scalable, and efficient management of patient data in a healthcare setting.

VI. RESULT & ANALYSIS

The Secure Healthcare Management System demonstrated enhanced security, integrity, and access control, outperforming traditional systems.

1. Security Performance Evaluation

The system ensured:

- **Confidentiality:** AES encryption protected data at rest.
- **Data Integrity:** Blockchain maintained immutability and traceability of patient records.
- **Access Control:** Role-based access prevented unauthorized data access.
- **Secure Transmission:** SSL/TLS encryption safeguarded data during transmission.

2. Comparison with Traditional Systems

The following table highlights the comparison between the proposed system and traditional healthcare management systems:

Feature	Traditional Systems	Proposed System (Blockchain-based)
Data Storage	Centralized	Decentralized (Blockchain + Database)
Security Mechanism	Basic encryption (if any)	AES encryption + Blockchain hash
Data Integrity	Easily alterable	Tamper-proof due to blockchain
Audit Trail	Manual or limited	Automatic and transparent
User Access Control	Password-based	Role-based with token-based auth (JWT)
Trust Level	Requires third-party trust	Trustless (data validated by blockchain)
Data Recovery after Breach	Difficult	Blockchain retains historical records

The proposed system showed **enhanced transparency**, **data traceability**, and **zero data loss** compared to traditional approaches.

3. Case Studies / Test Scenarios

To evaluate the system under real-world conditions, several test scenarios were created:

Case Study 1: Unauthorized Access Attempt

- **Scenario:** An unauthorized user tries to access patient data.
- **Result:** Access was denied, and the attempt was logged. AES encryption and JWT protected the data.

Case Study 2: Doctor Updates Patient Records

- **Scenario:** A doctor updates a prescription.
- **Result:** The update was successful, recorded on the blockchain, and fully traceable.

Case Study 3: Data Tampering Test

- **Scenario:** Attempt to alter patient data in the backend.
- **Result:** The blockchain record showed a discrepancy, highlighting the data integrity breach.

Conclusion of Analysis

The system successfully protected healthcare data with robust security measures, making it far more reliable than traditional systems.

VII. DISCUSSION

The secure healthcare management system enhances data security, integrity, and accessibility in healthcare. By integrating blockchain technology and encryption, it ensures tamper-proof and confidential patient data. The system also offers a user-friendly interface for easy interaction.

1. Strengths:
High Security: AES encryption and SSL/TLS protect patient data.
Data Integrity: Blockchain guarantees tamper-proof records.
Access Control: Role-based access with JWT tokens ensures authorized data access.
Scalability: Spring Boot supports modular and scalable development.
User Interface: Responsive frontend with HTML, CSS, JavaScript, and Bootstrap.

2. Limitations:
Blockchain Overhead: Adds complexity and performance overhead.
Data Storage Issues: Large files require off-chain storage.
Limited Interoperability: Difficult integration with existing systems.
Learning Curve: Time needed for understanding blockchain-based systems.

3. Challenges During Development
Blockchain Integration: Ensuring data consistency and performance.
Secure API Communication: Setting up secure data transmission via HTTPS.
Authentication: Implementing JWT tokens and secure session management.
Encryption Balance: Integrating AES without compromising system performance.
Frontend-Backend Communication: Resolving CORS and API issues.

4. Future Improvements
Smart Contracts: Automate data access, billing, and insurance claims.
AI Integration: Use AI for decision support and health risk predictions.
Interoperability: Add HL7/FHIR compatibility for system integration.
Mobile App: Develop a mobile version for better accessibility.
Audit Logging: Improve logging with real-time alerts for security breaches.
Decentralized Storage: Explore IPFS for securely storing large files linked to blockchain.

VIII. CONCLUSION

Summary of Contributions
This project combines blockchain technology with encryption to create a secure healthcare data management system. Key contributions include:

- Blockchain Integration: Ensures tamper-proof medical records through an immutable blockchain ledger.
- End-to-End Encryption: Protects patient data both at rest and during transmission.
- User-Centric Design: Provides an intuitive and responsive interface for both healthcare professionals and patients.
- Role-Based Access Control: Restricts data access to authorized individuals only, reducing internal misuse.
- Comprehensive Testing: Validated security, performance, and reliability through real-world test scenarios.

Potential for Real-World Deployment
The system is well-suited for real-world use, offering:

- Healthcare Institutions: Secure management of patient records and treatment history.
- Telemedicine Platforms: A secure backbone for remote consultations.
- Compliance: Aligns with HIPAA and GDPR, ensuring regulatory adherence.
- Scalability & Interoperability: Can integrate with existing EHR systems using HL7/FHIR standards.
- Trust & Transparency: Blockchain ensures traceability and data integrity, building trust among users.

In conclusion, the system provides a strong foundation for the future of secure digital healthcare infrastructure.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
2. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. S. B. Zanjal and G. R. Teli, "Medical Records Management Using Blockchain Technology," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 1135–1139, 2019.
4. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain With Novel Privacy Risk Control," Journal of Medical Systems, vol. 40, no. 10, Oct. 2016.
5. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–3, 2016.
6. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, 2016.
7. L. Fan et al., "A Blockchain-Based Privacy-Preserving Scheme for Large-Scale Health Data," IEEE Access, vol. 8, pp. 101073–101086, 2020.
8. S. P. R. K. Chaurasia, "Blockchain for Healthcare Data Security: State of the Art and Future Trends," International Journal of Medical Informatics, vol. 166, pp. 104876, 2023.
9. N. Kumar, V. N. S. S. R. S. S. Reddy, and R. S. Chouhan, "Recent Advances in Blockchain-Based Healthcare Systems and Data Privacy," Future Generation Computer Systems, vol. 130, pp. 307–325, 2023.
10. D. O. Adeyemo and A. A. Alaba, "Blockchain-Based Approaches for Secure Health Data Management," Journal of Healthcare Engineering, vol. 2023, Article ID 7261990, 2023.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com