



IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

“BLOCKCHAIN ENABLED APPROACH TO SECURE AND SCALABLE PATIENT E-HEALTH DATA: A LITERATURE REVIEW”

Rekha Singh ¹, Ankur Khare ²

¹ Research Scholar, Department of Computer Science and Application, Rabindranath Tagore University, Raipur, India

² Assistant Prof., Department of Computer Science and Application, Rabindranath Tagore University, Raipur, India

rekha.researchwork24@gmail.com, khareankur94@gmail.com`

ABSTRACT

The increasing use of Electronic Health Records (EHRs) and digital healthcare services has created significant challenges related to security, privacy, integrity, interoperability, and data management. Blockchain provides decentralized and tamper-resistant data management, while Artificial Intelligence (AI) supports healthcare data processing and disease prediction. This review analyses 20 recent studies on blockchain and AI applications in healthcare, focusing on EHR security, privacy, interoperability, access control, consent management, federated learning, and secure storage. The review shows that most existing studies address blockchain security and AI-based healthcare analytics separately. Limited research integrates AI-assisted data preprocessing, feature selection, SVM/CNN-based disease classification, encryption, off-chain storage, and blockchain-based indexing within a unified framework. The review therefore identifies these areas as important research gaps and provides a foundation for developing an AI-assisted blockchain framework for secure, intelligent, and privacy-preserving healthcare data management.

Key Words: Blockchain, Artificial Intelligence, EHR, Healthcare Data, Privacy, Security, Disease Classification, SVM, CNN.

I. INTRODUCTION

The rapid adoption of digital healthcare systems has resulted in the generation and exchange of large volumes of EHRs, medical reports, diagnostic information, and patient data. These data are essential for clinical decision-making and healthcare analytics but contain highly sensitive information that requires strong protection. Conventional centralized healthcare systems face challenges such as unauthorized access, data breaches, privacy violations, data manipulation, limited interoperability, and inefficient data sharing.

Blockchain technology has emerged as a promising solution for addressing several of these challenges. Its decentralized architecture, immutability, transparency, cryptographic protection, and smart-contract capabilities can support secure healthcare data sharing and access management. Recent studies have explored blockchain for EHR security, interoperability, patient consent, authentication, access control, cloud storage, and privacy preservation. However, storing large healthcare datasets directly on a blockchain can introduce scalability, storage, and computational limitations. Consequently, several researchers have investigated off-chain storage and blockchain-based indexing or metadata management.

At the same time, AI and machine-learning techniques provide opportunities for intelligent healthcare data analysis and disease prediction. AI can assist in data cleaning, missing-value handling, anomaly detection, feature selection, and disease classification. However, many existing healthcare studies focus primarily on prediction accuracy without

<https://www.ijrtsm.com> © International Journal of Recent Technology Science & Management

sufficiently addressing the security and privacy of the underlying patient data. Similarly, many blockchain-based healthcare studies focus on security without incorporating comprehensive AI-assisted data processing.

The integration of AI and blockchain can therefore provide a promising approach for developing intelligent and secure healthcare systems. AI can process and analyse healthcare data, while blockchain can provide secure indexing, integrity verification, access control, and traceability. Nevertheless, the reviewed literature indicates that an end-to-end framework integrating AI-assisted data preprocessing, feature selection, SVM/CNN-based disease classification, encryption, secure off-chain storage, and blockchain-based indexing remains insufficiently explored.

Therefore, this review examines recent research on blockchain and AI applications in healthcare, identifies major technological developments and limitations, and highlights the research gaps that need to be addressed. The review particularly focuses on the need for an integrated AI-assisted blockchain framework for secure, intelligent, scalable, and privacy-preserving healthcare data management.

II. LITERATURE REVIEW

Li et al. (2024) described TrustHealth, a secure healthcare data-sharing framework that combines blockchain technology with Trusted Execution Environments (TEE). Blockchain and smart contracts are used to provide integrity and traceability of healthcare data, while TEE protects sensitive processing operations from an untrusted environment. The framework uses SQLCipher for encrypted database operations and a TEE-based session-key generation mechanism for authentication and secure key sharing. The system was implemented using Hyperledger Fabric and ARM TrustZone. The reported evaluation achieved processing of approximately 5000 encrypted records per second, demonstrating the feasibility of the framework. The framework primarily concentrates on secure data sharing and trusted execution; it does not integrate AI-based healthcare data processing and disease prediction into the blockchain architecture.

Mandarino et al. (2024) developed a blockchain-based EHR architecture for edge computing to address security, performance, and cost issues associated with healthcare data management. The approach exploits blockchain's immutability and transparency while keeping large healthcare data off-chain. Blockchain is mainly used to validate externally stored information, thereby reducing blockchain storage requirements and associated costs. The architecture aims to improve the accessibility and integrity of EHRs while making the system more suitable for large-scale healthcare environments. Although the work addresses cost and scalability, it does not provide an integrated AI-assisted preprocessing, feature selection, and disease classification mechanism.

Kumari et al. (2024) presented a survey and research manifesto for blockchain-based healthcare systems. The paper reviews existing blockchain applications in healthcare, particularly electronic health records, and examines how decentralization, immutability, transparency, interoperability, and trust can address healthcare data-management problems. It categorizes existing research according to healthcare challenges and blockchain-based solutions and identifies future research directions. Being primarily a survey/research-direction paper, it does not implement an end-to-end healthcare system combining AI-based data processing with blockchain-based secure storage and access management.

Omidian (2024) examined the potential synergy between blockchain and artificial intelligence in healthcare. The paper discusses blockchain applications in healthcare data management, pharmaceutical supply chains, clinical trials, and insurance, while AI is considered for intelligent healthcare analysis and decision-making. The work highlights potential benefits of combining the two technologies for secure and intelligent healthcare services. It also discusses technical, privacy, ethical, regulatory, and interoperability challenges and proposes future research directions. The paper provides a conceptual perspective rather than implementing a complete AI-assisted blockchain framework for healthcare data processing and disease classification.

Mahajan et al. (2024) investigated the integration of Healthcare 4.0, blockchain, cloud computing, and EHR systems. The work focuses on improving the security and management of healthcare records stored in cloud environments. Blockchain is used to strengthen data integrity, security, traceability, and trust, while cloud computing provides scalable storage and accessibility. The study demonstrates how blockchain can complement cloud-based healthcare systems by reducing risks associated with centralized data management. The framework focuses mainly on secure cloud-based EHR management and does not sufficiently integrate AI-driven data cleaning, feature selection, and disease prediction.

Reegu et al. (2023) developed an interoperable blockchain-based EHR framework designed to improve secure

information exchange between healthcare organizations. The study reviews existing EHR and blockchain implementations and identifies interoperability requirements based on standards such as HL7 and HIPAA. The proposed framework aims to provide secure, immutable, privacy-preserving, and user-controlled healthcare data exchange without depending on centralized storage. The study concentrates on interoperability and secure EHR exchange rather than AI-assisted healthcare data processing and intelligent disease classification.

Ali et al. (2023) investigated the combination of blockchain, federated learning, and electronic medical records to support precision medicine. Federated learning enables healthcare organizations to collaboratively train machine-learning models without directly sharing sensitive patient data. Blockchain can provide trust, transparency, integrity, and accountability for interactions among participating healthcare entities. The approach addresses the privacy requirements associated with distributed healthcare AI and precision medicine. Although AI and blockchain are jointly considered, the work is primarily focused on federated learning and precision medicine rather than a complete pipeline covering data cleaning, missing-value handling, feature selection, classification, and secure blockchain indexing.

Zubaydi et al. (2023) provides a systematic literature review of blockchain applications for security and privacy in the Internet of Things. The authors examine blockchain architectures, consensus mechanisms, application domains, security objectives, evaluation environments, and open research problems. The study demonstrates that blockchain can address several IoT security issues by providing decentralized trust, integrity, authentication, and resistance to centralized points of failure. The review is broader than healthcare and IoT and does not provide a specific AI-assisted blockchain architecture for healthcare data management.

9. Kiania et al. (2023) conducted a systematic literature review of blockchain-based privacy and security approaches for electronic healthcare systems. The review examined 51 papers published from 2018 to December 2022, considering blockchain types, research approaches, evaluation metrics, and tools. The study identifies blockchain as a promising mechanism for improving EHR security, privacy, decentralization, and resistance to centralized attacks. It also discusses open challenges and future research directions. The study provides a broad review but does not develop an integrated framework combining AI-based processing, intelligent classification, and blockchain-based secure healthcare management.

Pampattiwar and Chavan (2023) examines the major security and privacy challenges associated with electronic health records, including data loss, unauthorized access, data sharing, interoperability, data management, and retrieval. It discusses centralized and cloud-based EHR approaches and explains how blockchain can support decentralized data management, secure transactions, access control, and traceability. The chapter also highlights challenges such as scalability, interoperability, cost, confidentiality, and privacy. The chapter provides a conceptual security analysis rather than implementing an integrated AI-blockchain healthcare framework.

Chandini and Basarkod (2023) developed a patient-centric blockchain EHR system with pre-transaction signature verification and smart contracts. The approach aims to strengthen the security of healthcare transactions by verifying signatures before transactions are recorded. Smart contracts automate transaction processing and help establish secure communication between healthcare stakeholders. The framework addresses the challenge of protecting EHR data during transmission and decentralized management. The work focuses on authentication, signatures, and transaction security, but does not incorporate AI-based healthcare data analysis or disease classification.

Murala et al. (2023) investigated blockchain for securing cloud-based electronic health records. The approach uses blockchain hashes to provide tamper evidence and combines encryption with distributed ledger mechanisms to support confidentiality, integrity, authentication, availability, and access control. The work addresses security problems arising when sensitive EHR data are stored or transferred through cloud service providers. The study primarily addresses cloud security and blockchain protection, without an integrated AI layer for healthcare data preprocessing and disease prediction.

Díaz and Kaschel (2023) developed a scalable EHR management system using a dual-channel blockchain architecture based on Hyperledger Fabric. The approach separates blockchain communication into channels to improve privacy and scalability while managing healthcare records. The system addresses the security and privacy risks associated with electronic medical records and seeks to make blockchain-based EHR management more scalable. The focus is on blockchain architecture, scalability, and privacy, rather than AI-assisted data processing and medical prediction.

Taherdoost (2023) reviewed the applications, challenges, and future perspectives of blockchain for healthcare privacy and security. The study discusses blockchain applications in healthcare data management, secure information exchange, authentication, access control, and privacy protection. It also examines limitations including scalability,

interoperability, computational requirements, regulatory compliance, and privacy concerns. The paper is primarily a conceptual/review contribution and does not present an integrated AI-based healthcare processing and blockchain management architecture.

Mhamdi et al. (2022) introduced SEMRAchain, a blockchain-based secure electronic medical record system. The framework combines blockchain, smart contracts, and Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). These mechanisms provide decentralized, fine-grained, and dynamic access control for EMR sharing. The system also uses a multi-agent architecture and evaluates security, availability, privacy, integrity, and transaction costs. SEMRAchain provides strong access-control mechanisms but does not integrate AI-assisted preprocessing or disease classification.

Hu et al. (2025) implemented MedBlockTree, a blockchain-based data structure designed to improve the scalability of patient-centric EMR sharing. The approach uses a block tree with multiple branches, a chameleon hash mechanism, and an EnhancedPro consensus algorithm. Multiple branches can process new blocks within a consensus round, addressing blockchain throughput limitations for healthcare applications. Simulation experiments evaluate branch count, worker count, collision rate, and network latency and report substantial throughput improvements over a conventional blockchain-based EMR architecture. The work focuses strongly on blockchain scalability and transaction throughput, rather than AI-based healthcare analytics.

Romel et al. (2025) developed a patient-centric EHR architecture that separates data storage from access control. Encrypted FHIR resources are stored off-chain, while the blockchain stores cryptographic commitments and patient-signed, time-limited permissions. The architecture supports authorization, auditing, confidentiality, integrity, and patient control. The reported implementation also evaluates transaction cost and access latency, demonstrating the feasibility of separating storage from blockchain-based authorization. The framework emphasizes patient-controlled authorization and secure storage, but does not integrate AI-based data preprocessing, feature selection, and disease classification.

Addobea et al. (2026) implemented a certificateless hybrid signcryption scheme for secure decentralized healthcare data management. The method combines ECC, Tag-based Key Encapsulation Mechanism (Tag-KEM), and Data Encapsulation Mechanism (DEM) with decentralized off-chain storage. Blockchain is used primarily for integrity verification while large medical datasets are stored off-chain. The authors report a 40.01%–97.71% reduction in computational cost compared with the evaluated existing approaches. The method provides advanced cryptographic protection and efficient decentralized storage, but it does not address AI-assisted healthcare data processing and disease prediction.

Chenthara et al. (2020) introduced Healthchain, a blockchain-based framework for preserving the privacy of electronic health records. The work investigates the use of blockchain to improve privacy, security, integrity, and controlled sharing of healthcare records. The framework seeks to reduce weaknesses associated with conventional centralized EHR architectures and provide patients and healthcare stakeholders with a more trustworthy mechanism for managing medical records. Healthchain focuses mainly on privacy-preserving EHR management and does not incorporate advanced AI-based healthcare analytics or disease classification.

Frempong et al. (2024) developed a blockchain-enabled consent-management framework for healthcare. The framework uses distributed ledger technology and smart contracts to record, enforce, and monitor patient consent. It aims to provide transparent and tamper-resistant consent management while supporting privacy preferences, regulatory compliance, interoperability, and patient control. The paper particularly discusses compliance with frameworks such as GDPR and HIPAA. The work focuses on consent and regulatory compliance, rather than AI-based healthcare data processing, disease prediction, or integrated healthcare analytics.

The reviewed studies demonstrate that blockchain has been extensively investigated for EHR security, privacy, interoperability, access control, consent management, scalability, and decentralized storage. Several recent works also investigate the combination of blockchain with AI, federated learning, and trusted execution environments. However, the literature shows a relative lack of end-to-end integration of AI-assisted healthcare data processing with blockchain-based secure management. In particular, many existing studies treat data security and healthcare analytics as separate components.

Table 1 describes several prior works related to healthcare, AI/ML and blockchain.

Table 1: Comparative Analysis

Authors	Main Focus	Blockchain	AI/ML	EHR/EMR	Main Limitation/Gap
Li et al. (2024)	TEE + secure eHealth	✓	—	✓	No integrated disease analytics
Mandarino et al. (2024)	Edge-based EHR	✓	—	✓	Limited AI processing
Kumari et al. (2024)	Research survey/directions	✓	—	✓	No implemented integrated framework
Omidian (2024)	Blockchain + AI	✓	✓	✓	Mainly conceptual
Mahajan et al. (2024)	Healthcare 4.0 + cloud EHR	✓	—	✓	No AI classification pipeline
Reegu et al. (2023)	Interoperable EHR	✓	—	✓	Focus on interoperability
Ali et al. (2023)	Federated learning + precision medicine	✓	✓	✓	Focus on FL rather than complete preprocessing
Zubaydi et al. (2023)	Blockchain + IoT security	✓	—	—	Not healthcare-specific
Kiania et al. (2023)	Blockchain EHR SLR	✓	—	✓	Review rather than implementation
Pampattiwar & Chavan (2023)	EHR security/privacy	✓	—	✓	Conceptual security focus
Chandini & Basarkod (2023)	Signatures + smart contracts	✓	—	✓	No AI analytics
Murala et al. (2023)	Cloud EHR security	✓	—	✓	No intelligent classification
Díaz & Kaschel (2023)	Hyperledger scalability	✓	—	✓	No AI processing
Taherdoost (2023)	Blockchain privacy/security	✓	—	✓	Review/conceptual focus
Mhamdi et al. (2022)	RBAC + ABAC + EMR	✓	—	✓	No AI analytics
Hu et al. (2025)	Block-tree scalability	✓	—	✓	Blockchain-centric
Romel et al. (2025)	Patient-centric access control	✓	—	✓	No disease prediction
Addobea et al. (2026)	Hybrid signcryption	✓	—	✓	Cryptography-centric
Chenthara et al. (2020)	Privacy-preserving EHR	✓	—	✓	No AI processing
Frempong et al. (2024)	Consent management	✓	—	✓	Consent-centric

The existing literature confirms that blockchain can strengthen the security, privacy, integrity, interoperability, access control, and traceability of healthcare data. Recent studies have further explored blockchain integration with trusted execution environments, edge computing, federated learning, artificial intelligence, and decentralized storage. However, most existing approaches concentrate on a particular aspect of healthcare management, such as secure storage, interoperability, access control, consent management, cryptographic protection, or blockchain scalability. Even studies combining blockchain and AI generally emphasize federated learning or conceptual integration rather than a complete healthcare data-processing pipeline. Therefore, there remains a research opportunity to develop an integrated AI-assisted blockchain framework that performs healthcare data preprocessing, feature selection, SVM/CNN-based disease classification, encrypted off-chain storage, blockchain-based indexing and metadata management, and comprehensive security and performance evaluation.

III. CRITICAL RESEARCH GAPS

The review of existing studies on blockchain, artificial intelligence, and EHRs indicates that considerable research has been conducted to improve healthcare data security, privacy, interoperability, access control, and decentralized storage. However, several important research gaps remain.

1. Lack of an End-to-End Integrated Framework

Most existing studies address individual aspects of healthcare management, such as blockchain-based storage, privacy, authentication, interoperability, consent management, or access control. There is limited work that integrates AI-assisted data processing, disease classification, secure storage, and blockchain management into a single end-to-end framework.

2. Limited AI-Assisted Healthcare Data Processing

Existing blockchain-based healthcare systems generally assume that healthcare data are already clean and suitable for analysis. Limited attention has been given to systematic AI-assisted preprocessing, including: Data cleaning, Missing-value handling, Duplicate detection, Data normalization, Categorical encoding and Anomaly/inconsistency detection. Thus, the quality of healthcare data before analysis and blockchain storage remains insufficiently addressed.

3. Insufficient Integration of Feature Selection and Disease Classification

Several studies use AI or machine learning for healthcare applications, while others focus exclusively on blockchain security. However, there is limited integration of feature selection with disease classification within a blockchain-enabled healthcare architecture. An effective framework should identify the most relevant healthcare attributes before classification to reduce dimensionality, computational cost, and redundant information.

4. Limited Use of SVM and CNN within Blockchain-Based Healthcare Frameworks

Although machine-learning and deep-learning techniques have been investigated for healthcare prediction, their integration with blockchain-based EHR systems remains limited. In particular, there is a need for an integrated classification layer using Support Vector Machine (SVM) and Convolutional Neural Network (CNN) for disease classification and prediction.

5. Separation of AI Analytics and Blockchain Security

A major limitation in existing research is the separation between intelligent healthcare analytics and secure healthcare data management. AI-based studies primarily concentrate on prediction, whereas blockchain-based studies concentrate on security and privacy. A unified architecture that connects these two functions is comparatively less explored.

6. Limited Secure Off-Chain Storage and Blockchain Indexing

Storing complete medical records directly on a blockchain can create scalability, storage, and computational challenges. Although some studies use off-chain storage, there is limited investigation of an integrated mechanism in which (a) Sensitive healthcare records are encrypted and stored off-chain, (b) Blockchain stores hashes and essential metadata, (c) Data integrity can be verified through blockchain (d) Access to detailed records is controlled securely.

7. Limited Comprehensive Privacy and Security Evaluation

Many existing studies discuss security theoretically or evaluate only selected security properties. A more comprehensive framework should evaluate confidentiality, integrity, authentication, access control, privacy, and resistance to unauthorized modification, along with conventional system-performance measures.

8. Scalability and Computational Efficiency Challenges

Blockchain-based healthcare systems can suffer from transaction-processing overhead, storage requirements, latency, and computational costs. Although some studies investigate edge computing, Hyperledger Fabric, or scalable blockchain structures, there is still a need to jointly evaluate AI processing time, blockchain processing time, storage efficiency, and overall system scalability.

9. Limited Evaluation of the Complete Processing Pipeline

Existing research often evaluates individual components rather than the complete workflow. There is a need for systematic evaluation from raw healthcare data to final disease prediction and secure blockchain storage using metrics such as: Accuracy, Precision, Recall, F1-score, Processing time, Storage efficiency and Security and privacy measures.

The review of existing literature reveals that blockchain-based healthcare research has primarily focused on EHR security, privacy preservation, interoperability, authentication, access control, consent management, decentralized storage, and scalability. In parallel, AI-based healthcare studies have mainly concentrated on data analysis and disease prediction. However, these two research directions are often addressed independently, with limited integration of

intelligent healthcare data processing and blockchain-based secure management within a unified framework. Existing approaches also provide limited attention to systematic AI-assisted preprocessing involving data cleaning, missing-value handling, duplicate detection, normalization, categorical encoding, and anomaly/inconsistency detection. Furthermore, the integration of feature selection with SVM/CNN-based disease classification and subsequent encrypted off-chain storage with blockchain-based indexing and metadata management remains insufficiently explored. Comprehensive evaluation combining classification performance, processing efficiency, storage efficiency, security, privacy, and data integrity is also limited. Therefore, there is a need for an integrated AI-assisted blockchain framework capable of transforming heterogeneous healthcare data into reliable and analysable information, performing intelligent disease classification, and securely managing the resulting healthcare data through encryption, off-chain storage, and blockchain-based indexing while maintaining privacy, integrity, and efficient system performance.

IV. CONCLUSION AND FUTURE WORK

This review analysed recent research on blockchain and AI for healthcare data management. Existing studies demonstrate that blockchain can improve security, privacy, integrity, interoperability, access control, and traceability, while AI can support data analysis and disease prediction. However, most existing approaches focus on either blockchain-based security or AI-based healthcare analytics rather than integrating both. The major gaps identified include limited AI-assisted data preprocessing, feature selection, SVM/CNN-based disease classification, encrypted off-chain storage, blockchain indexing, and comprehensive security and performance evaluation. Therefore, future research should focus on an integrated framework combining AI-assisted data processing, intelligent disease classification, encryption, secure off-chain storage, and blockchain-based metadata management to achieve secure, efficient, and privacy-preserving healthcare data management.

REFERENCES

- [1] Li, J., Luo, X., & Lei, H. (2024). TrustHealth: Enhancing eHealth security with blockchain and trusted execution environments. *Electronics*, 13(12), 2425. <https://doi.org/10.3390/electronics13122425>
- [2] Mandarino, V., Pappalardo, G., & Tramontana, E. (2024). A blockchain-based electronic health record (EHR) system for edge computing enhancing security and cost efficiency. *Computers*, 13(6), 132. <https://doi.org/10.3390/computers13060132>
- [3] Kumari, D., Sharma, S., Chawla, M., & Panda, S. (2024). A manifesto for healthcare based blockchain: Research directions for the future generation. *Journal of the Institution of Engineers (India): Series B*, 105(5), 1–22. <https://doi.org/10.1007/s40031-024-01074-3>
- [4] Omidian, H. (2024). Synergizing blockchain and artificial intelligence to enhance healthcare. *Drug Discovery Today*, 29(9), 104111. <https://doi.org/10.1016/j.drudis.2024.104111>
- [5] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., Alkhayyat, A., & Alhayani, B. (2023). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, 13(3), 2329–2342. <https://doi.org/10.1007/s13204-021-02164-0>
- [6] Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, 15(8), 6337. <https://doi.org/10.3390/su15086337>
- [7] Ali, A., Al-Rimy, B. A. S., Tin, T. T. T., Altamimi, S. N., Qasem, S. N., & Saeed, F. (2023). Empowering precision medicine: Unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. *Sensors*, 23(17), 7476. <https://doi.org/10.3390/s23177476>
- [8] Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review. *Sensors*, 23(2), 788. <https://doi.org/10.3390/s23020788>
- [9] Kiania, K., Jameii, S. M., & Rahmani, A. M. (2023). Blockchain-based privacy and security preserving in electronic health: A systematic review. *Multimedia Tools and Applications*, 82(18), 28493–28519. <https://doi.org/10.1007/s11042-023-14488-w>
- [10] Pampattiwar, K., & Chavan, P. (2023). Security and privacy facets of electronic health record. In *Unleashing*

- the potentials of blockchain technology for healthcare industries (pp. 59–75). Elsevier. <https://doi.org/10.1016/B978-0-323-99481-1.00006-7>
- [11] Chandini, A. G., & Basarkod, P. I. (2023). Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *Journal of Ambient Intelligence and Humanized Computing*, 14(4), 1–15.
- [12] Murala, D. K., Panda, S. K., & Sahoo, S. K. (2023). Securing electronic health record system in cloud environment using blockchain technology. In S. K. Panda, A. R. Sathya, & S. Das (Eds.), *Recent advances in blockchain technology: Real-world applications* (pp. 89–116). Springer. https://doi.org/10.1007/978-3-031-22835-3_4
- [13] Díaz, A., & Kaschel, H. (2023). Scalable electronic health record management system using a dual-channel blockchain Hyperledger Fabric. *Systems*, 11(7), 346. <https://doi.org/10.3390/systems11070346>
- [14] Taherdoost, H. (2023). Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives. *Sci*, 5(4), 41. <https://doi.org/10.3390/sci5040041>
- [15] Mhamdi, H., Ayadi, M., Ksibi, A., Al-Rasheed, A., Soufiene, B. O., & Hedi, S. (2022). SEMRAchain: A secure electronic medical record based on blockchain technology. *Electronics*, 11(21), 3617. <https://doi.org/10.3390/electronics11213617>
- [16] Hu, X., Sahni, J., Simpson, C. R., Samian, N., & Seah, W. K. G. (2025). Efficient patient-centric EMR sharing block tree. In *2025 25th International Conference on Software Quality, Reliability, and Security Companion (QRS-C)* (pp. 137–146). IEEE. <https://doi.org/10.1109/QRS-C65679.2025.00027>
- [17] Romel, T. H., Paul, K. K., Ruhan, T. I., Mim, M. R., & Hoque, A. S. M. L. (2025). A patient-centric blockchain framework for secure electronic health record management: Decoupling data storage from access control. *arXiv*. <https://arxiv.org/abs/2511.17464>
- [18] Addobea, A. A., Obiri, I. A., Siameh, T., Zhang, M., & Khan, I. (2026). A blockchain-enabled hybrid signcryption scheme for decentralized data management. *Peer-to-Peer Networking and Applications*, 19(2), Article 61. <https://doi.org/10.1007/s12083-026-02207-9>
- [19] Chentthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, 15(12), e0243043. <https://doi.org/10.1371/journal.pone.0243043>
- [20] Frempong, D., Benson, C. E., Oyasiji, O., & Okesiji, A. (2024). Blockchain-enabled consent management in healthcare: A framework for enforcing privacy preferences and regulatory compliance. *International Journal of Multidisciplinary Research and Growth Evaluation*, 5(3), 1059–1068. <https://doi.org/10.54660/IJMRGE.2024.5.3.1059-1068>