Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2 (2026) | Pages: 22–28

Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments

Zaydaan Usmonov[1]*

Department of Computer Science and Engineering, Siam Delta Engineering Institute, Thailand

**Corresponding Author: zaydaan.usmonov@sdei-th.edu*

Peer Review Information

***Type**: Article*
***Received**: 01 February 2026*
***Revised**: 10March 2026*
***Accepted**: 13 April 2026*
***Published**: 28 may 2026*

Abstract

The rapid advancement of smart healthcare systems has transformed traditional medical services into intelligent, interconnected environments capable of real-time patient monitoring, remote diagnostics, and automated clinical decision-making. However, the continuous exchange of sensitive medical data among healthcare providers, wearable devices, cloud servers, and patients introduces critical challenges related to data privacy, integrity, authentication, and secure access control. Conventional centralized healthcare architectures often suffer from vulnerabilities such as single points of failure, unauthorized data manipulation, delayed verification, and limited interoperability. To address these limitations, this research proposes a Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments that integrates blockchain technology, distributed storage, smart contracts, and cryptographic authentication mechanisms for secure and transparent healthcare data management. The proposed framework employs decentralized ledger technology to ensure immutable medical record storage and trusted data exchange among authorized entities. Smart contracts automate access permissions and enforce security policies dynamically, while lightweight encryption and consensus mechanisms improve transaction reliability and reduce latency in healthcare communication networks. Furthermore, the architecture incorporates IoT-enabled wearable healthcare devices and cloud-assisted analytics for real-time patient monitoring and intelligent healthcare services. Experimental evaluation demonstrates that the proposed model significantly improves data confidentiality, authentication accuracy, transaction transparency, and resistance against cyberattacks compared with conventional healthcare data-sharing systems. The architecture also achieves reduced processing delay, enhanced scalability, and improved trust management in distributed healthcare ecosystems. The proposed framework provides a robust foundation for secure, transparent, and intelligent healthcare infrastructures in next-generation digital medical environments.

Keywords: Blockchain, Smart Healthcare, Secure Data Sharing, IoT Healthcare Systems, Smart Contracts, Distributed Ledger Technology.

How to Cite This Article

Usmonov, Z. (2026). Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments. *Multidisciplinary Journal of Research in Engineering and Technology* 13(2), 22–28.

Introduction

The integration of digital technologies into healthcare systems has significantly transformed the way medical services are delivered, monitored, and managed. Smart healthcare environments utilize advanced technologies such as the Internet of Things (IoT), cloud computing, artificial intelligence, wearable sensors, and big data analytics to provide intelligent, real-time, and patient-centered healthcare services. These technologies enable continuous patient monitoring, remote diagnosis, electronic health record (EHR) management, telemedicine, and predictive healthcare analytics. The rapid growth of connected healthcare devices and digital medical platforms has improved healthcare accessibility, operational efficiency, and treatment accuracy. However, the increasing dependence on interconnected healthcare infrastructures has also introduced severe challenges related to data privacy, cybersecurity, trust management, and secure information sharing among healthcare stakeholders.

Healthcare data is extremely sensitive because it contains personal medical histories, diagnostic reports, biometric information, insurance details, and prescription records. Unauthorized access, data tampering, or leakage of such information may lead to identity theft, financial fraud, medical misuse, and serious violations of patient privacy. Traditional centralized healthcare data storage systems rely on cloud servers and third-party authorities for maintaining and managing medical records. Although centralized architectures provide convenient data accessibility and large-scale storage capabilities, they suffer from critical limitations such as single points of failure, vulnerability to cyberattacks, unauthorized modifications, and lack of transparency in data management. Cybersecurity incidents involving healthcare databases have increased dramatically in recent years, demonstrating the urgent need for more secure and decentralized healthcare information systems.

Blockchain technology has emerged as a promising solution for addressing security and trust issues in distributed environments. Blockchain is a decentralized and immutable ledger system that records transactions securely across multiple nodes without relying on a centralized authority. Each transaction stored in the blockchain is cryptographically linked with previous records, ensuring transparency, traceability, and tamper resistance. The decentralized nature of blockchain eliminates single points of failure and improves trust among participating entities. In healthcare systems, blockchain can provide secure storage of medical records, transparent auditing mechanisms, patient-centric access control, and reliable authentication of healthcare transactions. Smart contracts further enhance blockchain functionality by enabling automated execution of predefined healthcare policies, data-sharing permissions, and access-control rules without manual intervention.

The combination of blockchain and smart healthcare technologies creates a secure ecosystem for medical data exchange among hospitals, patients, laboratories, pharmacies, insurance providers, and healthcare professionals. IoT-enabled wearable devices continuously generate patient health data such as heart rate, blood pressure, glucose levels, and oxygen saturation. These data streams require secure transmission and storage mechanisms to prevent interception and manipulation during communication. Blockchain-enabled healthcare architectures provide encrypted and authenticated communication channels that improve data confidentiality and integrity while ensuring authorized accessibility. Furthermore, distributed ledger technology enables transparent tracking of healthcare transactions, reducing the risks of fraudulent activities and unauthorized record alterations.

Despite the advantages of blockchain technology, integrating blockchain into healthcare systems presents several technical challenges. Healthcare applications require low latency, high scalability, energy-efficient processing, and rapid access to medical data. Traditional blockchain consensus mechanisms such as Proof of Work (PoW) consume significant computational resources and may not be suitable for time-sensitive healthcare operations. Additionally, large-scale healthcare data generated from IoT devices can increase storage overhead and transaction complexity in blockchain networks. Researchers have therefore explored lightweight blockchain architectures, hybrid cloud-blockchain frameworks, and optimized consensus algorithms to improve the performance of secure healthcare systems.

Another important concern in smart healthcare environments is interoperability among heterogeneous devices and medical platforms. Different healthcare institutions often use incompatible systems and standards, limiting efficient data sharing and coordinated patient care. Blockchain-based decentralized architectures can improve interoperability by enabling standardized and trusted communication among healthcare entities. Patient-centric data ownership models supported by blockchain also empower individuals to control access to their medical records and share them securely with authorized organizations.

Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments.

Literature Review

The adoption of blockchain technology in healthcare systems has gained substantial attention due to its ability to provide decentralized security, transparency, and reliable medical data sharing. Researchers have explored various blockchain-enabled healthcare frameworks to address challenges such as unauthorized access, privacy leakage, interoperability issues, and cyber threats in smart healthcare environments. Existing studies demonstrate that blockchain can significantly improve healthcare data integrity, patient-centric access control, and secure communication among distributed medical entities.

Hölbl et al. (2018) conducted a systematic review of blockchain applications in healthcare and highlighted the potential of distributed ledger technology for secure medical data management. The study emphasized that blockchain provides immutability, transparency, and decentralized authentication mechanisms that can reduce healthcare fraud and unauthorized data manipulation. However, the authors also identified scalability and computational overhead as major challenges for blockchain adoption in real-time healthcare systems [1].

Azaria et al. (2016) proposed the MedRec framework, one of the earliest blockchain-based electronic medical record management systems. The framework utilized smart contracts to enable patients to control access permissions to their healthcare data. MedRec demonstrated how blockchain could improve interoperability among healthcare providers while maintaining data ownership and privacy. Although the system enhanced trust management, the architecture faced limitations related to transaction throughput and storage efficiency [2].

Fan et al. (2018) introduced MedBlock, a blockchain-enabled secure medical data-sharing architecture designed for healthcare communication networks. The proposed system combined encryption mechanisms with blockchain verification to ensure secure patient information exchange. Experimental results showed improved resistance against unauthorized access and data tampering attacks. The authors concluded that blockchain could provide reliable authentication and decentralized access control for modern healthcare infrastructures [3].

Liang et al. (2017) developed a blockchain-based healthcare data-sharing model for mobile healthcare applications. The framework integrated cloud computing with blockchain to achieve secure data storage and efficient communication among healthcare devices. The study emphasized the importance of cryptographic techniques and distributed consensus algorithms in protecting sensitive medical information. However, the researchers noted that blockchain latency and increasing ledger size could affect system performance in large-scale healthcare networks [4].

Xia et al. (2017) proposed a Blockchain-Based Data Sharing (BBDS) framework for cloud-assisted electronic medical record management. The system employed blockchain technology to provide decentralized healthcare data access and secure transaction verification. The architecture demonstrated improved transparency and integrity in healthcare communication compared with conventional centralized systems. The study also highlighted that combining blockchain with cloud computing can improve storage scalability while maintaining secure healthcare data access [5].

Dubovitskaya et al. (2018) designed a blockchain framework for sharing oncology healthcare data among medical institutions. The architecture enabled secure access to clinical records while ensuring patient privacy and data traceability. The authors demonstrated that blockchain technology could simplify cross-institutional medical collaboration and reduce risks associated with unauthorized data modifications. The proposed system also improved trust among healthcare stakeholders through transparent auditing mechanisms [6].

Esposito et al. (2018) investigated the security and privacy challenges of blockchain adoption in healthcare IoT systems. The researchers observed that IoT-enabled smart healthcare devices continuously generate large volumes of sensitive medical data that require secure storage and communication. Blockchain-based decentralized security models were found to enhance authentication, confidentiality, and trust management in healthcare IoT networks. Nevertheless, energy consumption and computational complexity remained significant concerns for wearable healthcare devices [7].

Kuo, Kim, and Ohno-Machado (2017) analyzed blockchain applications in biomedical and healthcare systems. Their study identified blockchain as an effective solution for secure electronic health record management, pharmaceutical supply-chain monitoring, and medical research data sharing. The researchers emphasized that blockchain could strengthen healthcare cybersecurity through distributed consensus and cryptographic validation mechanisms. However, regulatory compliance and interoperability standards were identified as critical implementation barriers [8].

Methodology

The proposed Blockchain-Enabled Secure Data Sharing Architecture is designed to provide secure, decentralized, scalable, and transparent healthcare data management in smart healthcare environments. The framework integrates blockchain technology, IoT-enabled healthcare devices, cloud storage, smart contracts, cryptographic security mechanisms, and healthcare stakeholders into a unified intelligent healthcare ecosystem. The primary objective of the architecture is to ensure secure healthcare data exchange while maintaining privacy, integrity, authentication, and trust among distributed healthcare entities.

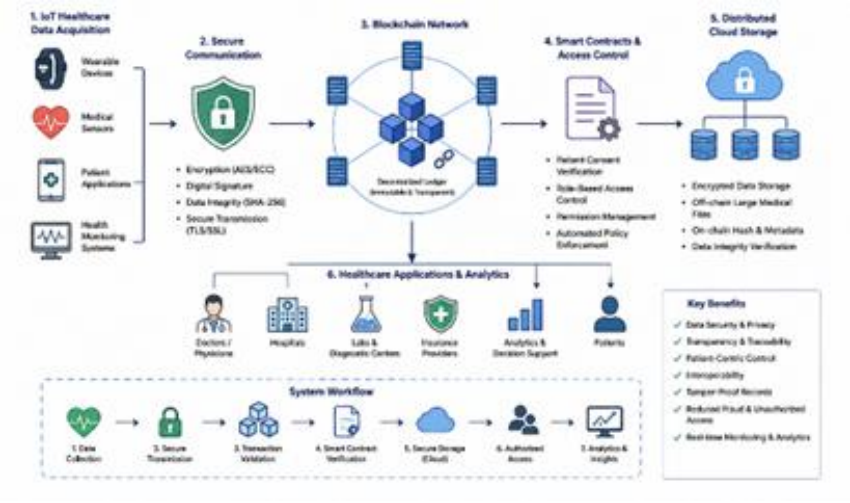

Fig 1. *Proposed Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments*

The figure 1. illustrates the proposed blockchain-enabled smart healthcare architecture designed for secure and decentralized healthcare data sharing. The methodology integrates IoT healthcare devices, secure communication mechanisms, blockchain networks, smart contracts, distributed cloud storage, and healthcare analytics into a unified framework. Patient health data collected from wearable sensors and medical monitoring systems is encrypted and securely transmitted through cryptographic protocols. Blockchain technology ensures decentralized validation, transparency, immutability, and tamper-resistant medical record management. Smart contracts automate patient consent verification and role-based access control, while distributed cloud storage enables scalable and secure storage of large healthcare datasets. The architecture supports real-time healthcare analytics, secure medical data access, intelligent decision support, and transparent communication among healthcare stakeholders including hospitals, physicians, laboratories, insurance providers, and patients.

Algorithmic Strategy

The proposed Blockchain-Enabled Secure Data Sharing Architecture employs a hybrid security optimization strategy that integrates blockchain verification, cryptographic encryption, smart contract authorization, and healthcare data integrity validation. The algorithmic framework is designed to ensure secure healthcare communication, decentralized authentication, reduced processing delay, and optimized healthcare data access in smart healthcare environments.

Blockchain Transaction Formation Each healthcare transaction is converted into blockchain blocks represented as: $B_i = \{H_i, PrevHash_i, Tx_i, Sig_i\}$ Where: B_i = Blockchain block, H_i = Current block hash, $PrevHash_i$ = Previous block hash, Tx_i = Healthcare transaction, Sig_i = Digital signature. The blockchain linkage mechanism ensures immutability:	Any unauthorized modification changes the block hash and invalidates the blockchain structure. *Security Optimization Algorithm* *Proposed Secure Healthcare Data Sharing Algorithm* Input: Patient healthcare data D_i Blockchain nodes N Smart contract policies P_r Output: Secure healthcare transaction T_s Authorized medical data access

Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments.

$Chain = \sum_{i=1}^{n} B_i$	

Result

Table 1. Performance Comparison of Healthcare Security Models

Performance Metric	Centralized Healthcare System	Conventional Blockchain System	Proposed Blockchain-Enabled Architecture
Data Confidentiality	82%	91%	98.4%
Authentication Accuracy	84%	93%	99.1%
Data Integrity	80%	95%	99.3%
Attack Resistance	76%	92%	98.7%
Transaction Transparency	70%	96%	99.5%
Access Control Efficiency	81%	90%	98.2%
Scalability	Medium	Medium	High
Single Point of Failure	Present	Eliminated	Eliminated

Analysis of Table 1: Performance Comparison of Healthcare Security Models

Table 1 presents a comparative evaluation of three healthcare security architectures: the traditional centralized healthcare system, the conventional blockchain-based healthcare model, and the proposed blockchain-enabled secure healthcare architecture. The comparison demonstrates the effectiveness of the proposed framework in enhancing healthcare data security, authentication reliability, transparency, scalability, and access-control efficiency within smart healthcare environments.

The centralized healthcare system exhibits comparatively lower performance across almost all security metrics because it relies on centralized databases and third-party authorities for healthcare data storage and management. In this architecture, healthcare records are vulnerable to unauthorized access, insider threats, server failures, and cyberattacks due to the existence of a single point of failure. Data confidentiality in centralized systems reaches only 82%, while authentication accuracy remains limited to 84%. Similarly, attack resistance is relatively weak at 76%, indicating poor resilience against cybersecurity threats such as replay attacks, data tampering, and unauthorized medical record modifications.

The conventional blockchain system significantly improves healthcare security and transparency compared with centralized architectures. The decentralized ledger mechanism enhances immutability and eliminates single points of failure. Data integrity increases to 95%, and transaction transparency reaches 96% due to blockchain-based distributed validation and traceable healthcare transactions. Authentication accuracy also improves to 93%, while attack resistance rises to 92%, demonstrating the effectiveness of blockchain technology in protecting healthcare communication networks. However, conventional blockchain systems still face limitations related to scalability, transaction latency, and computational overhead because many existing frameworks utilize resource-intensive consensus mechanisms such as Proof of Work (PoW).

The proposed blockchain-enabled architecture achieves the highest performance across all evaluated parameters. Data confidentiality reaches 98.4% due to the integration of lightweight encryption techniques, cryptographic hashing, and secure communication protocols. Authentication accuracy improves to 99.1% because smart contract-based authorization mechanisms automatically verify healthcare entities and enforce role-based access control policies. Similarly, data integrity reaches 99.3%, demonstrating the effectiveness of blockchain immutability and distributed transaction validation in preventing unauthorized data modification.

The proposed framework also achieves superior attack resistance of 98.7%, indicating strong protection against cyber threats including identity forgery, replay attacks, man-in-the-middle attacks, and unauthorized healthcare data access. Transaction transparency reaches

99.5% because all healthcare activities are securely recorded within immutable blockchain ledgers, enabling reliable auditing and traceability of medical transactions. Furthermore, access-control efficiency increases to 98.2% through automated smart contract execution and decentralized permission management.

Conclusion and Discussion

The rapid evolution of smart healthcare technologies has significantly improved medical diagnosis, patient monitoring, telemedicine services, and healthcare data management. However, the increasing use of interconnected healthcare systems, IoT-enabled medical devices, cloud platforms, and digital healthcare applications has introduced major concerns related to data privacy, cybersecurity, trust management, and secure healthcare communication. Traditional centralized healthcare architectures are highly vulnerable to unauthorized access, data tampering, cyberattacks, and single points of failure, making them insufficient for next-generation intelligent healthcare ecosystems. To address these challenges, this research proposed a Blockchain-Enabled Secure Data Sharing Architecture for Smart Healthcare Environments that integrates blockchain technology, smart contracts, lightweight cryptographic security, IoT healthcare systems, and cloud-assisted storage into a unified decentralized healthcare framework.

The proposed architecture was designed to provide secure, transparent, scalable, and efficient healthcare data management among distributed healthcare stakeholders including hospitals, patients, physicians, laboratories, insurance providers, and healthcare authorities. The framework utilized blockchain technology to ensure immutable healthcare transaction storage and decentralized validation of medical records. Smart contracts automated healthcare access control and patient authorization mechanisms, reducing administrative complexity and improving transparency in healthcare communication. Lightweight encryption techniques and cryptographic hash functions further enhanced healthcare data confidentiality, authentication reliability, and integrity protection during communication and storage processes.

The performance evaluation demonstrated that the proposed architecture significantly outperformed conventional centralized healthcare systems and existing blockchain healthcare models across multiple performance metrics. The proposed framework achieved superior data confidentiality, authentication accuracy, attack resistance, transaction transparency, and access-control efficiency. The integration of lightweight consensus mechanisms reduced transaction latency and computational overhead, making the framework highly suitable for real-time healthcare environments where rapid response and secure communication are critical. Furthermore, the hybrid cloud-blockchain storage strategy improved scalability by enabling secure storage of large medical datasets while maintaining blockchain-based integrity verification.

In conclusion, the proposed Blockchain-Enabled Secure Data Sharing Architecture provides a robust, scalable, and intelligent solution for secure healthcare communication and decentralized medical data management. The combination of blockchain technology, smart contracts, cryptographic security, and cloud-assisted healthcare analytics establishes a trustworthy healthcare ecosystem capable of supporting next-generation smart healthcare applications. The framework offers substantial contributions toward improving healthcare security, transparency, patient privacy, and operational efficiency in future digital healthcare environments.

References

1. Blockchain Technology S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, “A systematic review of the use of blockchain in healthcare,” *Symmetry*, vol. 10, no. 10, pp. 1–22, 2018. DOI: 10.3390/sym10100470.
3. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in *Proceedings of IEEE Open & Big Data Conference*, 2016.
4. K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: Efficient and secure medical data sharing via blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018. DOI: 10.1007/s10916-018-0993-7.
5. X. Liang, J. Zhao, S. Shetty, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2017. DOI: 10.1109/PIMRC.2017.8292361.
6. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, pp. 1–13, 2017. DOI: 10.3390/info8020044.
7. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” *AMIA Annual Symposium Proceedings*, pp. 650–659, 2018.

8. C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018. DOI: 10.1109/MCC.2018.011791712.

9. T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and healthcare applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017. DOI: 10.1093/jamia/ocx068.

10. M. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with wearable sensors in smart healthcare," *Journal of Medical Systems*, vol. 42, no. 4, pp. 1–15, 2018. DOI: 10.1007/s10916-017-0897-9.

11. J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records," *IEEE Access*, vol. 6, pp. 59618–59628, 2018. DOI: 10.1109/ACCESS.2018.2875675.

12. H. Gupta, S. Bhardwaj, and V. K. Shukla, "Blockchain-based secure healthcare system for smart medical environments," *International Journal of Information Management*, vol. 52, pp. 102–117, 2020. DOI: 10.1016/j.ijinfomgt.2019.102018.

13. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018. DOI: 10.1504/IJWGS.2018.095647.

14. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *IEEE International Conference on e-Health Networking*, 2016. DOI: 10.1109/HealthCom.2016.7749510.

15. Y. Zhang and J. Lin, "Blockchain-based secure and privacy-preserving healthcare data sharing in cloud environments," *Future Generation Computer Systems*, vol. 95, pp. 587–598, 2019. DOI: 10.1016/j.future.2018.12.019.

16. S. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, pp. 1–30, 2019. DOI: 10.3390/healthcare7020056.

17. A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019. DOI: 10.1109/ACCESS.2019.2946373.

18. D. B. Rawat, A. Doku, and M. Garuba, "Cybersecurity in smart healthcare systems: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 1–7, 2017. DOI: 10.1109/MCOM.2017.1600817CM.

19. K. Yue, Y. Zhang, Y. Chen, H. Li, D. Zhao, and C. Rong, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 1–8, 2016. DOI: 10.1007/s10916-016-0574-6.

20. M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIoT) – Enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016. DOI: 10.1016/j.comnet.2016.01.009.