2025 Volume: 01 Issue: 03 www.ijrpa.com Review Article

International Journal Research Publication Analysis

Page: 98-103

BLOCKCHAIN IN HEALTHCARE: SECURING THE FUTURE OF DIGITAL HEALTH SYSTEMS

***[1]Banupriya S. and [2]Sharmila P.**

[1]Department of Computer Science, Navarasam Arts and Science College for Women, Affiliated to Bharathiar University, Arachalur, Erode - 638101, Tamil Nadu, India.

[2]School of Computing Science, KPR College of Arts Science and Research, Affiliated to Bharathiar University, Arasur, Coimbatore - 641048, Tamil Nadu, India.

Article Received: 11 June 2025
Article Revised: 02 July 2025
Published on: 22 July 2025

***Corresponding Author: Banupriya S.**
Department of Computer Science, Navarasam Arts and Science College for Women, Affiliated to Bharathiar University, Arachalur, Erode - 638101, Tamil Nadu, India. Email Id: priyamca126phd@gmail.com,

ABSTRACT

The healthcare industry is undergoing a digital transformation, but challenges such as data breaches, interoperability issues, and limited patient control over health records continue to hinder its progress. Blockchain technology, originally developed for financial transactions, offers a revolutionary framework for secure, decentralized, and transparent data management. In healthcare, blockchain can address critical concerns such as data security, privacy, access control, and information sharing. This article explores the impact of blockchain on healthcare, focusing on its application in electronic medical record (EMR) systems, data interoperability, research data sharing, and patient empowerment. Through a review of recent research and pilot systems such as MedRec, MediBchain, and privacy-preserving Internet of Things (IoT) networks, the paper highlights how blockchain offers promising solutions to modern healthcare problems while identifying challenges to large-scale adoption.

KEYPOINTS: Blockchain, Healthcare, applications.

1. INTRODUCTION

As healthcare evolves into a data-driven field, the management of sensitive medical data has become a critical concern. Centralized databases used by hospitals and clinics are often vulnerable to data breaches, unauthorized access, and inefficient information exchange between providers. According to the HIPAA Journal, healthcare data breaches in the United States increased by 25% in 2023 alone, affecting over 80 million records.

To address these limitations, blockchain technology has emerged as a transformative solution. Blockchain is a distributed ledger that maintains an immutable record of transactions, verified by consensus mechanisms. Its core features—transparency, security, decentralization, and traceability—are increasingly being explored in healthcare to improve data sharing, ensure privacy, and give patients greater control over their personal information.

2. Key Applications of Blockchain in Healthcare

a. Secure and Immutable Electronic Medical Records

Traditional EMR systems are prone to tampering and unauthorized modifications. Blockchain allows healthcare providers to store EMR metadata or hashes on a distributed ledger, ensuring that once data is recorded, it cannot be altered. Systems like **MedRec** leverage smart contracts to manage patient-provider relationships and access control, allowing patients to maintain a complete history of who accessed their data and why (Azaria et al., 2016).

b. Data Interoperability Across Institutions

Blockchain acts as a universal access layer between disconnected health information systems. It enables **secure, real-time data sharing** without centralized authority. The **Cyran model**, for example, uses containerized microservices and the InterPlanetary File System (IPFS) to allow diverse hospital systems to share patient data seamlessly while maintaining strong encryption and authentication (Cyran, 2017).

c. Patient-Centric Data Ownership and Access Control

Blockchain empowers patients by giving them **full ownership of their health data**. With cryptographic key-pair systems, patients can control access permissions and share data selectively with doctors, insurers, or researchers. The **MediBchain** system implements this model by enabling privacy-preserving, user-managed health record sharing (Al Omar et al., 2017).

d. Support for Research and Public Health

Incentivized blockchain frameworks allow for the **ethical sharing of anonymized health data** with researchers. For instance, MedRec rewards participants with access to valuable datasets in exchange for maintaining the blockchain infrastructure, promoting a **data economy** while protecting privacy.

e. Integration with IoT and Remote Monitoring Devices

Healthcare IoT devices like wearables generate continuous streams of health data. Blockchain solutions tailored for IoT—such as the **Dwivedi framework**—use lightweight consensus mechanisms and cryptographic ring signatures to ensure secure, real-time data logging from low-power devices (Dwivedi et al., 2019). Similarly, **Cai et al.** introduce a sharding-based blockchain with many-objective optimization to address performance bottlenecks in Industrial IoT systems (Cai et al., 2020).

3. Enhancing Cloud Security Using Blockchain-Enabled AES Framework

Cloud computing has revolutionized data storage and processing by offering scalable, on-demand access to shared computing resources. However, with the increasing reliance on cloud services, concerns over data security, privacy, and trust have also escalated. Traditional cryptographic solutions, including the Advanced Encryption Standard (AES), though widely used, have shown limitations in efficiently securing cloud data against evolving cyber threats. Integrating **blockchain technology** with an enhanced AES framework presents a promising solution to these issues, offering a tamper-proof, decentralized approach to data protection.

Blockchain as a Foundation for Trust

Blockchain technology is inherently secure due to its decentralized and immutable nature. It enables distributed ledger systems where all transactions are recorded and verified across multiple nodes, making data manipulation nearly impossible. When integrated into cloud environments, blockchain can serve as a **trust layer**, ensuring data integrity, transparency, and accountability across distributed systems.

The proposed **Secure Framework for Cloud Computing (SFCC)** by Awan et al. (2020) introduces a modified AES algorithm optimized for blockchain-integrated cloud systems. This enhanced AES uses a **double round key mechanism**, increasing the encryption speed from 800 to 1000 blocks per second while maintaining low latency and power consumption. Blockchain supports the framework by verifying encryption key exchanges and managing access control in a secure, decentralized manner.

4. Key Features of the Blockchain-Enabled Framework

A. Data Integrity and Provenance: Immutable ledgers track every data interaction, ensuring accountability and the ability to trace unauthorized access.

B. **Secure Key Management**: The integration of blockchain in the key exchange process prevents man-in-the-middle attacks by validating encryption keys in a distributed network.
C. **Enhanced Performance with AES Modifications**: By deploying a double round key structure, the framework achieves faster encryption and decryption without compromising security.
D. **Energy and Network Efficiency**: The proposed model reduces energy consumption by 14.43%, network usage by 11.53%, and processing delay by 15.67%, as demonstrated in CloudSim and iFogSim simulations.
E. **Decentralized Trust Management**: Blockchain's consensus algorithms eliminate the need for centralized authorities, reducing single points of failure and enhancing system resilience.

5. Blockchain's Role in Secure Cloud Ecosystems

Incorporating blockchain into the cloud infrastructure enables **fine-grained access control**, smart contracts for automated security enforcement, and a distributed trust model. This integration helps overcome the traditional challenges of centralized cloud systems, such as data breaches, unauthorized access, and lack of transparency. Trusted gateways within the framework verify IP addresses and allow data decryption only for authenticated users, adding an extra layer of blockchain-backed security.

6. CONCLUSION

The fusion of blockchain and an enhanced AES algorithm establishes a powerful foundation for secure, efficient, and transparent cloud computing. The SFCC model demonstrates that blockchain can significantly elevate cloud security by decentralizing control, validating encryption processes, and ensuring data immutability. This approach is well-suited for organizations seeking robust, scalable, and trustworthy data protection in cloud environments.

However, blockchain's full-scale implementation in healthcare is still in its early stages. Technical challenges like scalability, latency, regulatory compliance, and integration with legacy systems must be resolved. Nonetheless, with ongoing research and pilot implementations demonstrating tangible benefits, blockchain holds substantial promise as the backbone of next-generation healthcare infrastructure.

REFERENCES

1. Awan, I. A., Shiraz, M., Hashmi, M. U., et al. (2020). *Secure Framework Enhancing AES Algorithm in Cloud Computing*. *Security and Communication Networks*, 2020. https://doi.org/10.1155/2020/8863345
2. Abikoye, O. C., Haruna, A. D., Abubakar, A., et al. (2019). *Modified Advanced Encryption Standard Algorithm for Information Security*. *Symmetry*, 11(12), 1484.
3. Tsai, K.-L., Huang, Y.-L., Leu, F.-Y., et al. (2018). *AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments*. *IEEE Access*, 6, 45325–45334.
4. Saha, R., Geetha, G., Kumar, G., & Kim, T.-H. (2018). *RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys*. *Security and Communication Networks*, 2018.
5. Elgendy, I. A., Zhang, W.-Z., Liu, C.-y., & Hsu, C.-H. (2018). *An Efficient and Secured Framework for Mobile Cloud Computing*. *IEEE Transactions on Cloud Computing*.
6. Silki, J., & Abhilasha, V. (2018). *An Improved Security Framework for Cloud Environment Using ECC Algorithm*. *IJRASET*, 6(1).
7. Oussama, A., & Abdelha, Z. (2019). *A Security Framework for Cloud Data Storage (CDS) Based on Agent*. *Applied Computational Intelligence and Mathematical Methods*, Springer.
8. Subramanian, K., & John, F. L. (2018). *Secure Unstructured Data Sharing in Multi-Cloud Storage Using Hybrid Crypto-System*. *International Journal of Advanced and Applied Sciences*, 5(1), 15–23.
9. Surya, V., Ranichandra, S., & Ranjani, R. (2018). *Secure Cloud Storage Using AES Encryption*. *IJIIRCCE*, 6(6).
10. Sison, A. M., Edjie, M., & Medina, R. P. (2019). *Modified AES Cipher Round and Key Schedule*. *IJEEI*, 7(1).
11. Arab, A., Rostami, M. J., & Ghavami, B. (2019). *An Image Encryption Method Based on Chaos System and AES Algorithm*. *The Journal of Supercomputing*, 75(10), 6663–6682.
12. Salama, D., & Elminaam, A. (2018). *Hybrid Cryptography Algorithms for Cloud Security*. *IJEIE*, 8(1), 40–42.
13. Bui, D.-H., Puschini, D., Bacles-Min, S., et al. (2016). *Low-Power AES Architecture for IoT Applications*. In *ICICDT*, IEEE.
14. Jain, J. R., & Abu, A. (2016). *Data Logging Framework to Enhance Cloud Security*. *SoutheastCon 2016*, IEEE.
15. Singh, J. (2018). *Client Side AES Encryption in Cloud Computing*. *IJIRMPS*, 6(5).

16. Marwan, M., Kartit, A., & Ouahmane, H. (2018). *Secure Medical Image Storage in Cloud*. *Journal of Electronic Commerce in Organizations*, 16(1), 1–16.
17. Meng, F., Lin, R., Wang, Z., et al. (2018). *Multi-Connection Encryption Algorithm for Secure Channels*. *EAI Endorsed Transactions on Security and Safety*, 5(15).
18. Rani, N. S., Juliet, A. N. M., & Renuka Devi, K. (2019). *Comparison of Image and Text AES Encryption*. *IJSTR*, 8(7).
19. Omotosho, O. I. (2019). *A Review on Cloud Computing Security*. *IJCSMC*, 8(9), 245–257.
20. Nair, A., & Anand, S. S. (2019). *My Load Balancer Technique for Cloud Performance*. *IJRTE*, 8(1).
21. Aazam, M., & Huh, E.-N. (2014). *Fog Computing and Smart Gateway for Cloud of Things*. *Future Internet of Things and Cloud*, IEEE.