Deep Learning and Blockchain-Enabled Healthcare Data Protection for Industrial Cyber-Physical Systems: A Review

Dr. J. Lenin 1 , Dr Sudhakar K[2],

[1] Postdoctoral Research Scholar, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia. lenin.j@alliance.edu.in

[2] Department of AI & DS, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed-to-be University), Bengaluru, Karnataka, India. ksudhakar.cs@gmail.com

---

Abstract: Information-driven medical services and Continuous patient health monitoring are allowed by the combination of cloud technologies, medical devices, the Internet of Medical Things (IoMT), and intelligent analytics in industrial cyber-physical healthcare systems. These networked settings are vulnerable to confidentiality ruins, prohibited access, data breaches, and cyber threats. According to current reviews, integrating blockchain technology with deep learning is a better way to protect healthcare data. While blockchain provides decentralized, tamper-proof, and transparent data management, deep learning permits intelligent intrusion detection, anomaly prediction, and real-time threat identification. In this paper, A review is conducted to examine the works on blockchain-enabled medical data protection, deep learning-based healthcare security, and hybrid architecture for vigorous medical information management in industrial cyber-physical healthcare systems.

Keywords: Deep Learning; Blockchain; Healthcare Security; Cyber-Physical Systems; IoMT.

Introduction

Industrial Cyber-Physical Systems (ICPS) are smart integrated environments that integrate computational intelligence, communication networks, and control mechanisms to monitor, analyze, and enable automated, real-time industrial operations. The quick digital transformation of healthcare has directed to the development of Industrial Cyber-Physical Systems (ICPS), which combines physical medical devices with computational intelligence and networked communication. These methods empower real-time monitoring, automated diagnosis, and remote medical services. Medical data are extremely sensitive and valuable, directing them prime targets for cyberattacks such as ransomware, data breaches, identity theft, and illegal access. Existing centralized security frameworks regularly struggle to guarantee data integrity, confidentiality, traceability, and flexibility in distributed ICPS systems. There exists an increase in vulnerability in areas of security coverage, such as cloud technologies, Internet of Medical Things (IoMT), and edge devices. These devices become more susceptible to internal and external threats and subsequently attacks.

In addition, threat detection, anomaly detection, intrusion detection systems, and predictive risk analysis can be handled precisely by Deep Learning (DL), both in complicated industrial systems and sophisticated healthcare networks. The key feature implemented here is the fact that Deep Learning can continually understand patterns from very high-dimensional data, enabling it to detect in a proactive manner sophisticated cyber-attacks in real-time. The integration of blockchain technologies, which uses cryptographic hashing, consensus protocols, and smart contracts to handle tamper-resistant and transparent data management processes. The decentralized systems of blockchain technology ensure practical implementation of CIA (confidentiality, integrity and authorization). This ensures secure data transfer without having to deal with any centralized systems. These centralized systems can act as a

vulnerability point, which in turn will be highly susceptible to threats and eventually cyber-attacks. The synergy of Deep Learning techniques and blockchain technology there is a promise of secure storage, authenticated and authorized access controls, increased ability to audit records, and integrity of medical data within Industrial Cyber-Physical Systems (ICPS)ecosystems.

This review paper examines the convergence of deep learning and blockchain technologies for the protection of medical data in Industrial Cyber-Physical Systems. It investigates classical and pre-existing frameworks, security frameworks, limitations, and cutting-edge research trends, emphasizing strengths, boundaries, and open research narratives. Through the discovery of recent progress, this review paper aims to reveal a complete comprehension of how exactly intelligent analytics and decentralized protection frameworks can cooperatively enhance data security, robustness, and trust in next-generation healthcare industrial systems. However, the IoMT-enhanced healthcare industry is more likely to be attacked due to the usage of different devices and ecosystems, unreliable communication channels, and centralized data storage protocols [1]. Cyberattacks such as ransomware, illegal data access, and device manipulation create difficult dangers to patient safety and data confidentiality [2].

To address these issues, a system is proposed by combining deep learning-based threat detection techniques with a blockchain-based decentralized data protection architecture. Such hybrid systems enhance medical data privacy and system flexibility [3].

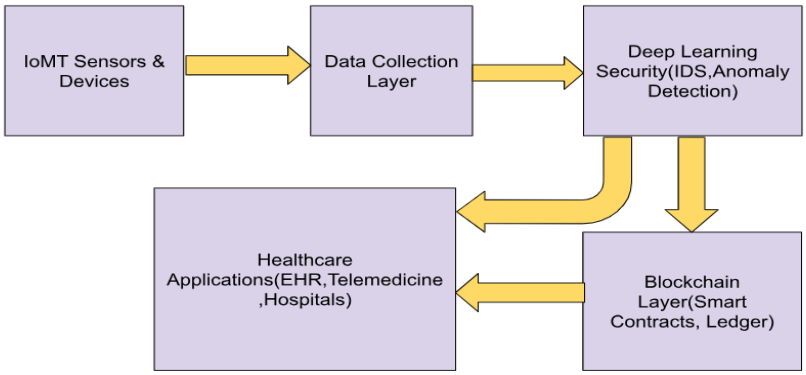

Fig. 1 : Architecture for secure healthcare data management

The Fig. 1 proves the architecture for secure healthcare data management in Industrial Cyber-Physical Systems (ICPS) using Deep Learning and Blockchain technologies. It depicts that the data is produced from IoMT sensors, and medical devices are initially gathered through a data collection layer. The collected medical data are then examined by a Deep Learning-based security module, which accomplishes intrusion detection and anomaly detection to find cyber threats in the current situation. After the protection assessment, the data are protected and recorded in the Blockchain layer, where smart contracts and distributed ledgers confirm data integrity, transparency, and tamper resistance. Lastly, the secured and assessed data are sent to healthcare domains such as Electronic Health Records (EHR), telemedicine platforms, and hospital management systems, confirming protected, consistent, and reliable medical services.

Literature Survey

In [11], the author developed a system BDAFL-DNN a blockchain-based architecture that joins the Deep Neural Networks (DNNs) and Federated Learning (FL) to help the real-time data to be used securely, with

integrity through the cloud. Paper [12] demonstrates that the proposed system, which is a blockchain-integrated framework combined with the latest encryption standards, is examined based on the performance parameters of access control and data security. The proposed method is a very efficient, robust, and powerful solution for reliable, secure, and effective medical data across various domains. The author of [13] proposed an architecture called PBDL, which combines Deep Learning (DL) concepts with Permissioned Blockchain smart contracts. The system works in two phases where the first phase uses blockchain to register, authenticate, and examine the entities using smart protocols. The second phase combines the Stacked Sparse Variational Autoencoder (SSVAE) with the Self-Attention-based Bidirectional Long Short-Term Memory (SA-BiLSTM) to transform the medical data securely. If there is any attack, this proposed system will detect by examining the network traffic. The chapter in [14] presents a sustainable and intelligent health monitoring framework developed for the initial detection of myocardial infarction using federated Internet of Medical Things (IoMT). Heterogeneous data is collected, and a multimodel fusion strategy is used to integrate the various types of data streams. This method gives enhanced prediction performance when compared to the existing approaches. This algorithm proves that the system provides a secure, scalable, reliable, and sustainable solution for detecting cardiac attacks earlier.

Security Mechanisms in Cyber-Physical Healthcare System

Security mechanisms in Cyber-Physical Healthcare Systems (CPHS) are developed to secure delicate healthcare data, interconnected devices, and serious healthcare infrastructure from cyber threats while confirming patient safety and system consistency. The main security mechanisms are:

A. Authentication and Access Control

This mechanism is the fundamental mechanism that processes the verification of user identity. Some of the common authentication methods involve Multi-factor authentication (MFA) where security check takes place in two stages, Role-based access control (RBAC), where the rules are framed and accessed, and an Attribute-based access control mechanism guarantees that only the known users or devices can access the healthcare systems. Access control determines what the authenticated user is allowed to do.

B. Blockchain-Based Security

This mechanism is a decentralized privacy approach that utilizes blockchain technology to secure data trust, confirm transparency, and avoid illegal updation of records. Blockchain-based security depends on a distributed ledger model where data is stored in blocks that are cryptographically linked together. In Healthcare services, Blockchain can privately store patient data, achieve permission, track medical data access, and confirm reliable data sharing between hospitals, laboratories, and insurance providers.

C. Privacy-preserving techniques

Privacy-preserving methods are techniques employed to secure delicate information while still permitting data to be assessed, shared, or managed. Privacy-preserving methods confirm that individual or private data (such as patient data) is not visible, even when used for analytics, machine learning, or data sharing. In healthcare and cyber-physical systems, a huge volume of patient data is gathered. These methods support preserving privacy, secrecy, and controlling compliance while allowing research and intelligent decision-making.

Security Challenges in Cyber-Physical Healthcare Systems

A. IoMT Vulnerabilities

IoMT devices frequently suffer from weak authentication protocols, limited processing abilities, and inadequate encryption, allowing them vulnerable to cyberattacks [1].

B. Data Privacy Risks

Centralized medical databases are susceptible to breaches, illegal access, and data manipulation, leading to difficult secrecy concerns [4].

C. Cyber Threats in Healthcare ICPS

Most important cyber threats contain Distributed Denial-of-Service attacks, malware injection, insider threats, and data tampering [2].

Deep Learning for Healthcare Security

A. Intrusion Detection Systems

Deep learning techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders have established huge amount of accuracy in detecting cyber threats in healthcare networks [6].

B. Anomaly Detection

Deep learning methods examine network traffic patterns and detect abnormal activities, permitting primary identification of cyberattacks [7].

C. Advantages

Deep learning offers:

- Continuous day-to-day threat detection, Adaptive learning ability and High classification accuracy.

Yet, issues contain computational complications and susceptibility to adversarial attacks [7].

Blockchain for Healthcare Data Protection

A. Decentralized Data Management: Blockchain uses a distributed ledger that assures private and tamper-proof storage of medical records [3].

B. Secure Data Sharing: Blockchain permits the protected exchange of electronic medical records across healthcare institutions while preserving transparency and data integrity [4].

C. Smart Contracts for Access Control: Smart contracts ensure an automated authorization procedure (for more security and privacy), allowing controlled access to patient data [.5].

Integration Of Deep Learning and Blockchain

A. Hybrid Security Framework: Deep learning for threat detection, while blockchain for secure data transfer, storage and access control, enhancing medical system resilience [6].

B. Federated Learning and Blockchain: Federated learning integrated with blockchain permits combined model training without sharing delicate patient data, improving secret preservation [10].

C. Security Enhancement in ICPS: Hybrid architecture enhances trust, consistency, and transparency in healthcare cyber-physical systems [8].

Applications In Healthcare Cyber-Physical Systems

Combined deep learning and blockchain architecture helps:

- Smart hospital security
- Remote patient monitoring
- Telemedicine data protection
- Secure electronic health record management
- Emergency healthcare data sharing [9].

Research Challenges

- Blockchain networks attain performance restrictions when handling a huge amount of medical datasets [3].
- IoMT devices lack adequate computational power to provide complicated deep learning techniques [1].
- Guaranteeing confidentiality while allowing data sharing remains a main issue [10].
- Healthcare systems frequently use heterogeneous protocols and standards, complex integration [4].

Conclusion

The implementation of Deep Learning ensures knowledgeable cyber threat detection, while blockchain ensures decentralized and tamper-proof data management process. These address the expandability issues, privacy and protection, and interoperability issues, which will be of primary importance for any large-scale execution. Deep learning enhances knowledgeable cyber threat detection proactively. On the other hand, blockchain enhances decentralization with the implementation of a tamper-proof data management process. Issues such as expandability limitations, cyber protection and privacy, interoperability issues, which are the main concerns for any large-scale implementations and execution.

Future Research Directions

Current research should emphasis on:

- Lightweight blockchain frameworks
- Privacy-preserving deep learning techniques
- Edge-based healthcare security
- Explainable AI for cybersecurity
- Federated learning integration [10].

References

[1] Y. Sun, F. P.-W. Lo, and B. Lo, “Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey,” *IEEE Access*, vol. 7, pp. 183339-183355, 2019.
[2] S. Patel, K. Mehta, and R. Kumar, “Cyber-physical security challenges in smart healthcare systems,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5678-5689, 2023.
[3] A. Haleem, M. Javaid, and R. P. Singh, “Blockchain technology applications in healthcare: An overview,” *J. Industrial Information Integration*, vol. 23, 2021.
[4] S. Shamshad et al., “A secure blockchain-based e-health records storage and sharing system,” *J. Information Security and Applications*, vol. 52, 2020.
[5] Y. Ghadi et al., “The role of blockchain to secure Internet of Medical Things,” *Scientific Reports*, vol. 14, 2024.
[6] S. Chidambaranathan et al., “Deep learning enabled blockchain-based electronic healthcare data attack detection,” *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6858-6868, 2020.
[7] B. B. Gupta et al., “Deep learning-based intelligent attack detection,” *IEEE Transactions on Sustainable Computing*, 2021.
[8] P. Tagde et al., “Blockchain and artificial intelligence technology in e-health,” *Journal of Healthcare Engineering*, 2021.
[9] L. Lodha et al., “Blockchain-based secured IoMT system for healthcare monitoring,” *Measurement: Sensors*, vol. 28, 2023.

[10] V. Stephanie, I. Khalil, and M. Atiquzzaman, “Privacy-preserving federated learning in healthcare with blockchain,” *IEEE Access*, 2023.
[11] Mazin Abed Mohammed, Mohd Khanapi Abd Ghani, Israa Badr Al-Mashhadani, Sajida Memon, Abdullah Lakhan, Haydar Abdulameer Marhoon, and Marwan Ali Albahar, “Blockchain-Integrated Edge-Cloud-Enabled Healthcare Data Analytics Based on Distributed Federated Learning and Deep Neural Networks”, Mesopotomian Journal of Cybersecurity, Vol. 5 No. 3, 2025. DOI: https://doi.org/10.58496//MJCS/2025/060.
[12] Jundale Poonam Abasaheb, Sujata V. Mallapur, “Blockchain-Integrated Secure Healthcare Information Sharing via Advanced Blowfish Encryption Standard With Optimal Key Generation”, Emerging Telecommunications Technologies, Vol. 36, 3, 2025.
[13] Randhir Kumar, Prabhat Kumar, Rakesh Tripathi, Govind P Gupta, A K M Najmul Islam, Mohammad Shorfuzzaman, “Permissioned Blockchain and Deep-Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems”, IEEE Transactions on Industrial Informatics, Vol. 18, 11, 2022, 8065-8073, **DOI:** 10.1109/TII.2022.3161631.
[14] Abhishek Shrivastava, Santosh Kumar, Nenavath Srinivas Naik, “Sustainable health monitoring with multimodal fusion: a federated IoMT framework for early myocardial infarction detection”, Book: Smart City Computational Paradigms, ScienceDirect, pp.213-236, 2026. DOI:10.1016/B978-0-44-327726-9.00019-8.