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

Dr. J. Lenin, Postdoctoral Research Scholar, Lincoln University College, Malaysia.
Dr. Sudhakar K, Department of AI & DS, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed-to-be University), Bengaluru, Karnataka, India

Abstract: The fast adoption of Industrial Cyber-Physical Systems (ICPS), Internet of Medical Things (IoMT), cloud computing, and telemedicine technologies has completely changed the way modern healthcare delivery systems work. But at the same time, the growing level of connectivity of medical devices and healthcare infrastructure increases the attack surface of the healthcare sector and makes it more vulnerable to ransomware, data breaches, unauthorized access and insider attacks. Centralized security approaches can hardly protect the system from new emerging cyber threats and maintain data integrity and privacy at the same time. Although Deep Learning algorithms have already shown great potential for intrusion detection and anomaly recognition, they do not provide any guarantees concerning safe data sharing and tampering-proof storage. In turn, although Blockchain provides decentralization, immutability and transparency, it does not have intelligent threat detection capabilities. In order to resolve these issues, this paper suggests using a hybrid framework based on Deep Learning and Blockchain for healthcare Industrial Cyber-Physical Systems. The architecture of the suggested framework incorporates Convolutional Neural Networks (CNN), LSTM neural networks, Autoencoders, Smart Contracts, Distributed Ledgers and access control via Blockchain.
Keywords: Industrial Cyber-Physical Systems, Internet of Medical Things, Healthcare Cybersecurity, Deep Learning, Blockchain, Intrusion Detection, Smart Contracts, Privacy Preservation.

Introduction

There is a process of digitalization in the sphere of healthcare by means of the implementation of Industrial Cyber-Physical Systems, Cloud-based healthcare solutions, and the Internet of Medical Things technologies. The connected medical devices, wearables, EHRs, telemedicine portals, and smart hospitals produce a huge amount of private data, which needs protection during storage, transfer, and processing. Although the implementation of new technologies brings benefits to patients and healthcare institutions, it also creates severe cybersecurity issues. Modern healthcare infrastructures became an attractive target for ransomware attacks, data breaches, and access of unentitled users because of the high cost of medical records on the dark web.

Research Motivation

The rise in deployment of Industrial Cyber Physical Systems in health care institutions has made it mandatory to develop intelligent and distributed security solutions. The proliferation of Internet of Medical Things (IoMT), cloud computing and remote health care applications has resulted in the widening of the health care attack surface. Rule based security systems cannot detect complex cyber-attacks and zero day attacks efficiently. Also, it is essential for health care institutions to have assurances of the confidentiality, integrity, availability, and accountability of the patient data.

Table 1. Existing Security Technologies in Healthcare ICPS

Technology	Advantages	Limitations
Deep Learning	High attack detection accuracy	No data integrity assurance
Blockchain	Immutable and decentralized	Scalability and latency issues
Traditional Security Models	Established controls and standards	Vulnerable to advanced attacks
Centralized Systems	Easier administration	Single point of failure

Proposed Hybrid Framework	Intelligent and secure architecture	Increased implementation complexity

Research Objectives

Mainly, the purpose of this study is to create an architecture for a robust Industrial Cyber-Physical System (ICPS) for healthcare systems by considering intelligence-based threat detection along with decentralization techniques for security. In particular, it focuses on developing a deep learning intrusion detection system, use of Blockchain technology for managing healthcare data securely, and providing resilience against attacks.

Proposed Hybrid Security Architecture

The proposed architecture is built with four primary layers, which include the Data Layer, the Intelligence Layer, the Blockchain Layer, and the Healthcare Service Layer. The Data Layer gathers data from IoMT sensors, wearable devices, medical devices, and electronic health records. The Intelligence Layer conducts intelligent cyber-threat detection through the use of deep learning approaches such as CNN, LSTM, and Autoencoder. The Blockchain layer provides features for secure data storage, access control, auditing and smart contract execution.

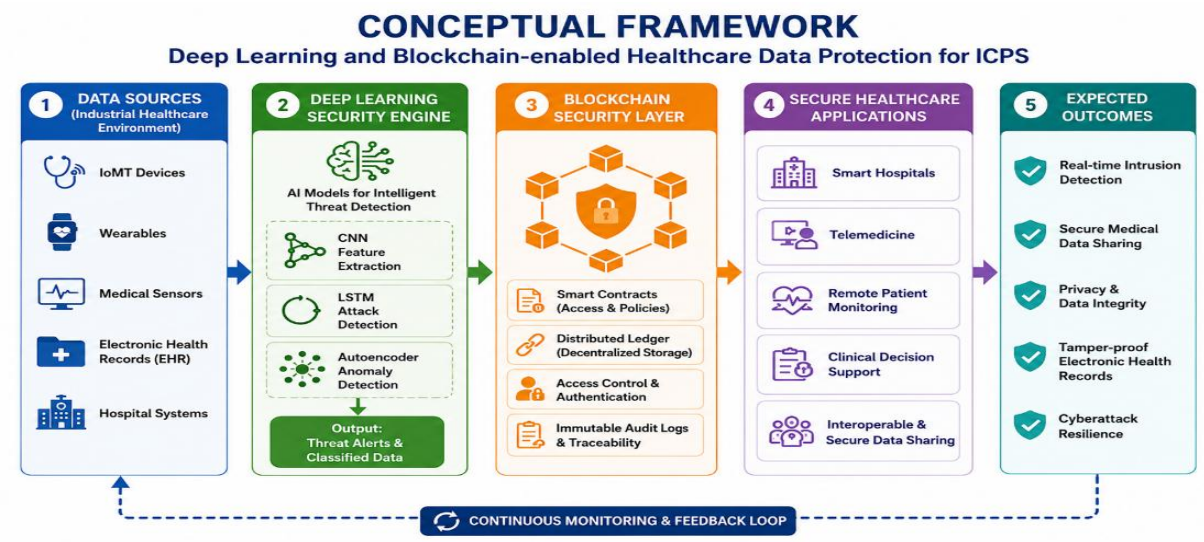

Table 2. Proposed Framework Components

Technology	Advantages	Limitations
Deep Learning	High attack detection accuracy	No data integrity assurance
Blockchain	Immutable and decentralized	Scalability and latency issues
Traditional Security Models	Established controls and standards	Vulnerable to advanced attacks
Centralized Systems	Easier administration	Single point of failure
Proposed Hybrid Framework	Intelligent and secure architecture	Increased implementation complexity

Deep Learning Security Model

The Deep Learning part of the framework integrates various learning approaches in order to enhance the performance of cybersecurity. CNNs are used in order to conduct feature extraction and classification of attack patterns. LSTM networks learn temporal dependencies in addition to attack

sequences in the healthcare data traffic. Unsupervised learning is conducted through the use of autoencoders, which detect anomalies and identify zero-day attacks by learning normal behavioral patterns.

Table 3. Deep Learning Modules

Model	Function	Expected Benefit
CNN	Feature extraction	Fast attack classification
LSTM	Sequential analysis	Detection of evolving attacks
Autoencoder	Anomaly detection	Zero-day attack identification

Blockchain-Based Security Framework

Blockchain technology is used in the proposed framework to provide a secure and transparent system for the management of healthcare information. Access control policies, patient consents, and security measures are automated using smart contracts. Healthcare transactions are stored securely and permanently using distributed ledgers that serve as an immutable audit trail. Blockchain provides confidentiality through restricted access, integrity through immutability, and availability through decentralization.

Table 4. Blockchain Security Contributions

Security Objective	Blockchain Contribution
Confidentiality	Controlled access mechanisms
Integrity	Immutable healthcare records
Availability	Distributed architecture
Accountability	Complete audit trails

Dataset Selection and Methodology

Implementation stage applies benchmarking cyber security datasets such as NSL-KDD, CICIDS2017, CICIoT2023, and healthcare IoMT datasets. The data preprocessing procedure will include data cleaning, feature selection, normalization, and balancing of classes. Afterward, the deep learning algorithms are trained on the preprocessed data and then integrated with the blockchain module for securing data management. Finally, the evaluation of the suggested framework will be carried out using different performance parameters.

Table 5. Selected Datasets

Dataset	Purpose
NSL-KDD	Network intrusion detection
CICIDS2017	Cyberattack classification
CICIoT2023	IoT threat detection
Healthcare IoMT Dataset	Domain-specific validation

Evaluation Metrics

The suggested model will be evaluated according to the following performance parameters: accuracy, precision, recall, F1 score, and detection rate. Whereas the parameter of accuracy will provide information about the general predictive power of the model, the precision parameter will show the ability of the model to reduce false positives.

Table 6. Performance Metrics

Metric	Purpose
Accuracy	Overall performance

Precision	False positive reduction
Recall	Threat detection capability
F1 Score	Balanced performance
Detection Rate	Security effectiveness

Expected Outcomes

As a result of this approach, the following achievements will be realized: intrusion detection; tampering and security of medical data; enhanced levels of stakeholder trust; improved privacy of patients; and greater resistance to cyber-attacks. Through this fusion of Deep Learning and Blockchain, an intelligent and secure ecosystem for development of next-generation Industrial Cyber-Physical Systems in the healthcare sector can be developed.

Future Work and Conclusion

A Hybrid Deep Learning and Blockchain Security Framework for Industrial Cyber-Physical Systems in the context of Healthcare is discussed in this work. The proposed framework utilizes intelligent threat detection capabilities, as well as decentralization, to resolve significant problems of privacy, security, and trust associated with the healthcare infrastructure. Future works will involve the realization of the framework, conducting experiments, and increasing the computational efficiency of the proposed system. These results will serve as a basis for Conference 3 and Conference 4 in this paper.

References

1. Ferrag, Mohamed Amine, Leandros Maglaras, Ahmed Ahmim, and Helge Janicke. "Deep Learning Approaches for Cyber Security Intrusion Detection Systems: A Survey." *Journal of Information Security and Applications*, vol. 50, 2020, article 102419. https://doi.org/10.1016/j.jisa.2019.102419
2. N. Nezhadsistani, N. S. Moayedian and B. Stiller, "Blockchain-Enabled Federated Learning in Healthcare: Survey and State-of-the-Art," in IEEE Access, vol. 13, pp. 119922-119945, 2025, doi: 10.1109/ACCESS.2025.3587345.
3. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326
4. Kumar, Rakesh, Rajesh Kumar, and Sachin Kumar. "Deep Learning-Based Intrusion Detection System for IoT Using Convolutional Neural Networks." *Journal of Information Security and Applications*, vol. 58, 2021, article 102870. https://doi.org/10.1016/j.jisa.2021.102870
5. Verkerken, Miel & D'Hooge, Laurens & Wauters, Tim & Volckaert, Bruno & De Turck, Filip. (2021). Towards Model Generalization for Intrusion Detection: Unsupervised Machine Learning Techniques. Journal of Network and Systems Management. 30. 10.1007/s10922-021-09615-7.
6. Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K., & Kotecha, K. (2022). Explainable Artificial Intelligence for Intrusion Detection System. Electronics, 11(19), 3079. https://doi.org/10.3390/electronics11193079
7. Langer SG. Cyber-Security Issues in Healthcare Information Technology. J Digit Imaging. 2017 Feb;30(1):117-125. doi: 10.1007/s10278-016-9913-x. PMID: 27730416; PMCID: PMC5267602.
8. Sharma, Aashima & Kaur, Sanmeet & Singh, Maninder. (2023). A secure blockchain framework for the internet of medical things. Transactions on Emerging Telecommunications Technologies. 35. 10.1002/ett.4917.
9. Sakhawat, Abdur & Abbas, Sagheer & Khan, Muhammad & Ghazal, Taher & Adnan, Khan & Mosavi, Amir. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Computers in Biology and Medicine. 150. 106019. 10.1016/j.compbiomed.2022.106019.
10. Kiruthikadevi, K. & Sivaraj, R. & Vijayakumar, M.. (2024). A Blockchain and Hybrid Deep Learning for Secure and Efficient Healthcare Data Transmission and Management. Tehnicki vjesnik - Technical Gazette. 31. 10.17559/TV-20240304001373.