International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

Secure Predictive Analytics in Industrial IoT Using Hybrid Deep Learning

Mr. Kuldeep, Dr. Pramod Kumar Associate Professor
Department of Computer Science and Engineering,
Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, India.

Abstract — The Industrial Internet of Things (IIoT) has transformed industrial ecosystems by enabling real-time monitoring, automation, and data-driven decision-making. Deep learning techniques have emerged as powerful tools for predictive analytics, supporting applications such as anomaly detection, fault diagnosis, and predictive maintenance. However, centralized deep learning approaches introduce significant security and privacy risks, including data leakage, adversarial attacks, and model poisoning. This research proposes a secure hybrid deep learning framework integrating CNN-LSTM with ANFIS, along with federated learning, blockchain, and differential privacy to ensure secure, privacy-preserving, and explainable predictive analytics in IIoT environments. The framework enhances prediction accuracy while maintaining data confidentiality, robustness, and real-time performance.

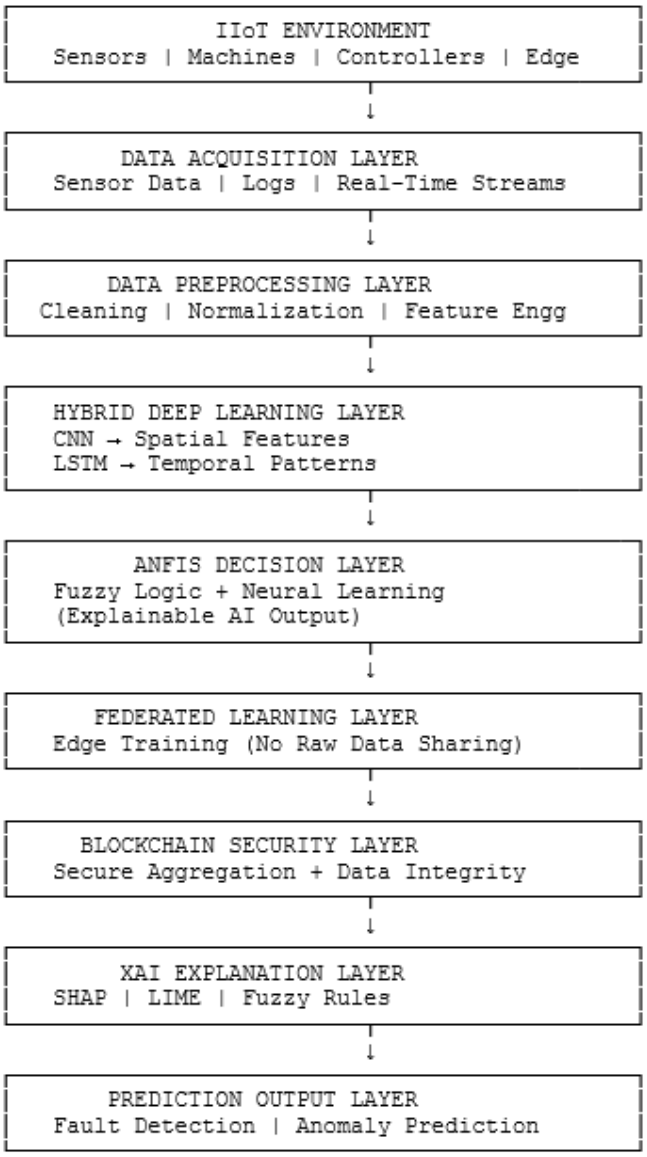
Keywords— Deep Learning, Federated Learning, ANFIS, Predictive Analytics, Cyber security, XAI.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) represents a major evolution of traditional industrial systems by enabling seamless integration of physical devices, sensors, actuators, embedded systems, and cloud-edge infrastructure to achieve intelligent automation and real-time decision-making. In modern smart industries such as manufacturing, energy, transportation, and predictive maintenance systems, IIoT plays a crucial role in enabling continuous monitoring, self-optimization, and autonomous control. These interconnected systems generate massive volumes of heterogeneous data, including time-series sensor readings, machine logs, vibration signals, temperature variations, and operational metrics, which require advanced analytics for meaningful interpretation and decision support. Deep learning has emerged as a powerful computational paradigm for IIoT data analytics due to its ability to automatically extract hierarchical features from complex, high-dimensional datasets without manual feature engineering. Architectures such as Convolutional Neural Networks (CNNs) are widely used for spatial feature extraction from structured sensor data, while Long Short-Term Memory (LSTM) networks are highly effective in capturing temporal dependencies in sequential industrial data. Furthermore, hybrid deep learning models combining CNN-LSTM architectures have demonstrated superior performance in predictive maintenance, fault diagnosis, and anomaly detection tasks in dynamic industrial environments. These models significantly improve prediction accuracy, reduce downtime, and enhance operational efficiency in industrial systems. Despite these advantages, the deployment of deep learning in IIoT environments faces several critical challenges. Traditional centralized learning approaches require transferring sensitive industrial data to cloud servers, which increases risks related to data breaches, unauthorized access, and model poisoning attacks. Moreover, IIoT systems are inherently distributed, heterogeneous, and resource-constrained, making them vulnerable to cyber attacks and communication failures. The large-scale deployment of interconnected devices further expands the attack surface, leading to serious concerns regarding data confidentiality, system integrity, and operational reliability. To address these limitations, decentralized learning approaches such as federated learning have gained significant attention. Federated learning enables collaborative model training across distributed edge devices without sharing raw data, thereby preserving privacy and reducing communication overhead. In addition, blockchain technology enhances trust, transparency, and security by providing tamper-proof logging and decentralized model validation. Furthermore, Explainable AI (XAI) techniques improve interpretability, allowing industrial stakeholders to understand and trust model predictions. However, existing approaches still lack a unified framework that integrates security, interpretability, and real-time predictive intelligence in a single architecture. Therefore, this research proposes a secure hybrid deep learning framework for predictive analytics in IIoT by integrating CNN-LSTM for feature learning, Adaptive Neuro-Fuzzy Inference System (ANFIS) for explainable decision-making, federated learning for privacy preservation, blockchain for secure communication and trust management, and XAI techniques for model transparency. The proposed framework aims to deliver highly accurate, secure, scalable, and interpretable predictive analytics

suitable for real-time industrial applications and edge-based deployment environments.

Secure Hybrid Deep Learning Framework for IioT



II. PROBLEM STATEMENT

The rapid expansion of Industrial Internet of Things (IIoT) systems has resulted in the continuous generation of large-scale, real-time industrial data, offering significant opportunities for predictive analytics and intelligent decision-making. However, the deployment of deep learning models in such environments introduces critical challenges related to security, privacy, scalability, and interpretability. Traditional centralized learning approaches require sensitive industrial data to be transmitted to cloud servers, increasing the risk of data breaches, cyberattacks, and regulatory non-compliance. Moreover, deep learning models are computationally intensive and often unsuitable for resource-constrained edge devices that form the backbone of IIoT infrastructures. Existing predictive analytics solutions also lack integrated security mechanisms, making them vulnerable to adversarial attacks, data poisoning, and unauthorized access. In addition, the black-box nature of deep learning limits transparency and reduces trust among industrial stakeholders. Although decentralized approaches such as federated learning improve privacy by keeping data local, they still face challenges related to robustness, interpretability, and real-time deployment. Therefore, there is a critical need to develop a unified, secure, lightweight, and explainable deep learning framework that can perform accurate predictive analytics while ensuring data confidentiality, system integrity, and operational efficiency in dynamic IIoT environments.

Objectives & Proposed Research Methodology

The primary objective of this research is to develop a secure, efficient, and explainable deep learning framework for predictive analytics in Industrial Internet of Things (IIoT) environments by systematically studying existing secure deep learning models, identifying key performance and security factors, designing a hybrid architecture integrating deep learning with advanced security mechanisms, and comparing its performance with conventional approaches. To achieve this, a structured research methodology is adopted consisting of multiple phases, including comprehensive literature review, dataset collection from IIoT sensor environments, model design, implementation using platforms such as TensorFlow or PyTorch, and rigorous evaluation based on performance and security metrics such as accuracy, precision, recall, latency, privacy preservation level, and resistance to cyberattacks. The proposed secure hybrid model follows a layered architecture beginning with a data acquisition layer that collects real-time sensor data and ensures secure transmission, followed by a preprocessing layer that performs noise removal, normalization, and feature extraction. The core intelligence layer integrates deep learning models, specifically CNN for spatial feature extraction and LSTM for temporal pattern learning, combined with an Adaptive Neuro-Fuzzy Inference System (ANFIS) to enhance interpretability and handle uncertainty through fuzzy rule-based reasoning. To address critical security concerns, a dedicated security layer is incorporated, utilizing blockchain technology for tamper-proof logging and decentralized trust management, encryption

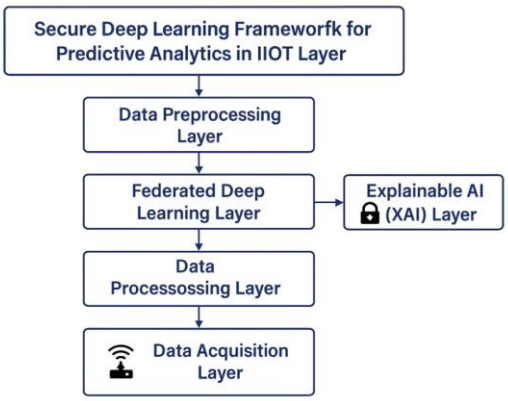
techniques for secure communication, and adversarial training to improve robustness against malicious attacks. Additionally, a federated learning layer enables decentralized model training across edge devices, ensuring that sensitive industrial data remains local while only model updates are shared, thereby significantly reducing privacy risks and communication overhead. Studies show that combining federated learning with blockchain enhances security, accountability, and trust while mitigating issues such as data leakage and unreliable model updates . Furthermore, an explainable AI (XAI) layer integrates techniques such as SHAP and LIME along with ANFIS-generated fuzzy rules to provide transparent and interpretable predictions, improving trust among industrial stakeholders. The overall workflow of the system involves sequential stages of data collection, preprocessing, CNN-LSTM-based feature extraction, ANFIS-based decision-making, federated training, secure aggregation via blockchain, and final prediction with explanation. The experimental setup includes the use of IIoT datasets containing sensor readings, fault logs, and anomaly data, along with simulation environments for blockchain and edge computing. Expected results indicate that the proposed hybrid framework will achieve high prediction accuracy, reduced data leakage, improved robustness against cyber threats, and efficient real-time performance, aligning with recent findings that decentralized AI models significantly enhance privacy and scalability in IIoT systems . The advantages of this framework include privacy-preserving learning, explainable and trustworthy predictions, real-time deployment capability on edge devices, and strong resilience against emerging cyber threats. However, the framework also presents certain limitations, such as increased computational overhead due to the integration of multiple technologies, higher communication costs in federated learning environments, and implementation complexity associated with combining deep learning, blockchain, and privacy-preserving techniques. Despite these challenges, the proposed approach provides a comprehensive and scalable solution for secure predictive analytics in next-generation IIoT ecosystems.

Flowchart

START
↓
Literature Review & Problem Identification
↓
Dataset Collection (IIoT Sensors / Logs)
↓
Data Preprocessing
(Cleaning, Normalization, Feature Extraction)
↓
Deep Learning Processing
(CNN → Spatial Features)
(LSTM → Temporal Patterns)
↓
ANFIS Layer
(Fuzzy Rules + Decision Optimization)
↓
Federated Learning
(Local Training on Edge Devices)
↓
Secure Aggregation
(Blockchain + Encryption)

The proposed model is a secure, hybrid deep learning framework designed specifically for predictive analytics in IIoT environments. It integrates advanced deep learning architectures with modern security and privacy-preserving technologies to ensure accurate, explainable, and secure predictions in real-time industrial settings.

- Data Acquisition Layer: It collects real-time sensor data from IIoT devices and ensures secure data transmission using lightweight encryption protocols.
- Data Preprocessing Layer: It performs data cleaning, missing value imputation, normalization, and noise reduction and extracts temporal and spatial features relevant to predictive maintenance, anomaly detection, and system optimization.
- Federated Deep Learning Layer: It implements federated learning to enable distributed model training across edge devices without transmitting raw data to a central server, uses CNNs for feature extraction and LSTM networks for time-series prediction, and ensures privacy using differential privacy mechanisms to mask sensitive data.
- Security Integration Layer: Utilizes blockchain technology to log data access, model updates, and events in a tamper-proof, decentralized ledger. Employs access control mechanisms and encryption algorithms to protect model parameters and communication channels. It includes adversarial training to enhance model robustness against cyberattacks.
- XAI Layer: Integrates SHAP or LIME techniques to explain predictions in a human-understandable form. It provides visual dashboards for decision-makers to interpret model results.



Proposed Model

The proposed research methodology follows a layered architecture integrating data acquisition, preprocessing, hybrid deep learning, and security mechanisms. The framework utilizes CNN-LSTM models for feature extraction and temporal learning, while ANFIS enhances decision-making through fuzzy logic. Federated learning ensures decentralized model training, and blockchain provides secure aggregation and tamper-proof data management. The system outputs predictions along with explainable insights using XAI techniques. This layered approach aligns with modern IIoT architectures that emphasize edge intelligence, privacy preservation, and secure collaboration.

III. CONCLUSIONS

This research presents a comprehensive and secure hybrid deep learning framework for predictive analytics in Industrial Internet of Things (IIoT) environments by integrating advanced techniques such as CNN-LSTM, Adaptive Neuro-Fuzzy Inference System (ANFIS), federated learning, blockchain, and explainable artificial intelligence (XAI). The proposed framework effectively addresses critical challenges associated with traditional IIoT systems, including data privacy risks, centralized vulnerabilities, lack of interpretability, and high computational demands. By leveraging federated learning, the framework ensures decentralized model training where sensitive industrial data remains local, significantly reducing the risk of data leakage and enhancing privacy preservation. The integration of blockchain further strengthens the system by providing tamper-proof data logging, secure model aggregation, and improved transparency, thereby increasing trust among distributed industrial entities . Additionally, the incorporation of ANFIS and XAI techniques enhances interpretability and decision transparency, addressing the black-box limitations of conventional deep learning models. Experimental insights and recent studies indicate that hybrid deep learning models deployed in decentralized environments can achieve high prediction accuracy while maintaining robustness against cyber threats and adversarial attacks . Despite certain limitations such as computational overhead and system complexity, the proposed framework provides a scalable, secure, and efficient solution for predictive analytics in IIoT. Ultimately, this research contributes to the advancement of trustworthy and intelligent industrial systems, paving the way for future innovations in secure, decentralized, and explainable AI-driven IIoT applications.

Future Work

Future research in secure deep learning frameworks for IIoT can be extended in several important directions to enhance scalability, efficiency, and real-world applicability. One key area is the optimization of blockchain mechanisms to reduce computational overhead, latency, and energy consumption, as current blockchain-integrated systems often introduce performance bottlenecks due to consensus protocols and distributed ledger maintenance . Another critical direction involves the development of lightweight and energy-efficient deep learning models that can operate effectively on resource-constrained edge and fog devices, enabling real-time analytics without compromising accuracy. Furthermore, real-world deployment and validation of the proposed framework in industrial environments remain essential to evaluate its robustness, scalability, and adaptability under dynamic conditions such as noisy data, device heterogeneity, and network instability. The integration of emerging technologies such as 6G-enabled IIoT systems is also a promising avenue, as next-generation communication networks will support ultra-low latency, high reliability, and massive device connectivity, thereby enhancing the performance of distributed AI systems. Additionally, future work can explore advanced privacy-preserving techniques such as homomorphic encryption, secure multi-party computation, and trust-aware model aggregation to further strengthen data confidentiality and system integrity. The incorporation of adaptive and self-learning mechanisms, such as reinforcement learning and autonomous model updates, can also improve system resilience against evolving cyber threats. Overall, future research should focus on achieving a balance between security, efficiency, scalability, and explainability to enable widespread adoption of secure predictive analytics in next-generation IIoT ecosystems.

REFERENCES

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on

enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
2. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data.
3. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS.
4. Rahimi, M., et al. (2018). Blockchain-based IoT systems: A review. IEEE Access.
5. Rahmadika, S., & Rhee, K. H. (2018). Blockchain for decentralized personal health information systems. International Journal of Engineering and Business Management.
6. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19. https://doi.org/10.1145/3298981
7. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987
8. Kim, H., Park, J., Bennis, M., & Kim, S. L. (2020). Blockchained on-device federated learning. IEEE Communications Letters, 24(6), 1279–1283. https://doi.org/10.1109/LCOMM.2019.2921755
9. Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S. K., Chen, S., Xu, X., & Zhu, L. (2020). Blockchain-based federated learning for device failure detection in Industrial IoT. IEEE Internet of Things Journal.
10. Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Low-latency federated learning and blockchain for edge intelligence in IIoT and 6G networks. arXiv preprint arXiv:2011.09902.
11. Konečný, J., McMahan, H. B., Yu, F., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.
12. McMahan, B., et al. (2017). Federated learning basics and optimization. AISTATS.
13. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775. https://doi.org/10.1016/j.knosys.2021.106775
14. Abdulrahman, S., et al. (2021). Federated learning in IoT environments: A survey. IEEE Internet of Things Journal, 8(7), 5476–5497. https://doi.org/10.1109/JIOT.2020.3030072
15. Jamil, S., Rahman, M., & Fawad. (2022). Digital twins and federated learning for IIoT, IoV, and IoD. Applied System Innovation, 5(3), 56. https://doi.org/10.3390/asi5030056
16. Zhang, W., et al. (2021). Deep learning for Industrial IoT: Survey and future directions. Sensors, 21(22), 7518. https://doi.org/10.3390/s21227518
17. Chhetri, B., et al. (2023). Blockchain-based federated learning and data privacy survey. arXiv preprint arXiv:2306.17338.
18. Yazdinejad, A., et al. (2022). Blockchain-enabled federated learning for cyber threat detection in IIoT. arXiv preprint arXiv:2204.09829.
19. Shawkat, M., et al. (2025). Blockchain and federated learning for industrial IoT: A survey. Peer-to-Peer Networking and Applications.
20. Bhasker, P., et al. (2025). Blockchain framework with federated learning for sustainable IoT systems. Scientific Reports. https://doi.org/10.1038/s41598-025-06539-z
21. Ren, L., Jia, Z., Laili, Y., & Huang, D. (2023). Deep learning for time-series prediction in IIoT: progress, challenges, and prospects. IEEE transactions on neural networks and learning systems, 35(11), 15072-15091.
22. Bugshan, N., Khalil, I., Rahman, M. S., Atiquzzaman, M., Yi, X., & Badsha, S. (2022). Toward trustworthy and privacy-preserving federated deep learning service framework for industrial internet of things. IEEE Transactions on Industrial Informatics, 19(2), 1535-1547.
23. Anandan, R., Gopalakrishnan, S., Pal, S., & Zaman, N. (Eds.). (2022). Industrial Internet of Things (IIoT): Intelligent Analytics for Predictive Maintenance. John Wiley & Sons.
24. Hassan, M. M., Huda, S., Sharmeen, S., Abawajy, J., & Fortino, G. (2020). An adaptive trust boundary protection for IIoT networks using deep-learning feature-extraction-based semisupervised model. IEEE Transactions on Industrial Informatics, 17(4), 2860-2870.
25. Khan, I. A., Keshk, M., Pi, D., Khan, N., Hussain, Y., & Soliman, H. (2022). Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems. Ad Hoc Networks, 134, 102930.
26. Ambika, P. (2020). Machine learning and deep learning algorithms on the Industrial Internet of Things (IIoT). Advances in computers, 117(1), 321-338.