Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 4, Number: 1, Pages: 44 - 49, Year: 2026

Industrial IoT–Edge Computing Security: A Comprehensive Review of Threats, Mitigation Strategies, and Future Directions

Uneeb Raziq Khan, and Irshad Ahmed Sumra

Department of Informatics and System, School of System and Technology, University of Management and Technology, Lahore, 54000, Pakistan

Corresponding author: Uneeb Raziq Khan (Email: uneeb.khitran@gmail.com)

Received: 12/01/2026, Revised: 22/03/2026, Accepted: 15/04/2026

***Abstract*— Recent advancements in Industrial Internet of Things (IIoT) systems introduce two major trends: connecting with edge computing and the connectivity with Cyber-Physical Systems (CPS) that bring in real-time industrial automation, while exposing a much broader threat surface than conventional IT networks. This paper reviews a systematic survey that presents a comprehensive analysis of IIoT architectures, edge computing integration, CPS vulnerabilities, and a complete attack taxonomy spanning the perception, network, processing, and application layers. The review evaluates AI/ML-based intrusion detection systems, federated learning frameworks, blockchain-based audit mechanisms, cryptographic protocols, and Zero Trust Architecture as security countermeasures. Key findings confirm that advanced combinations of machine learning, federated learning, blockchain, and IDS are essential for data protection and real-time attack detection. Critical gaps are identified in standardized benchmarking environments, hardware-level security, and quantum-safe cryptographic migration pathways.**

***Index Terms*—Blockchain, Cybersecurity, Cyber-Physical Systems, Edge Computing, Machine Learning, Intrusion Detection Systems, Zero Trust Architecture.**

I. INTRODUCTION

CPS with the industrial Internet of Things (IIoT) integrates physical and digital objects, driving the manufacturing revolution and emerging as a major research area identified by the National Science Foundation (NSF) [1-3]. CPS seamlessly integrate physical processes with digital control systems [4], enabling industries such as smart manufacturing, energy grids, and healthcare to achieve unprecedented operational efficiency. Data security and privacy in IIoT environments require lightweight cryptographic protocols compatible with resource-constrained devices [5]. Security plays an integral part in CPS-IIoT integration. Industrial devices connected to the Internet are vulnerable to device tampering, DDoS attacks, malware attacks and other cyberattacks which might bring a halt in production, and there are considerable economic and safety implications [6,7]. The convergence of operational technology (OT) and information technology (IT) environments creates unique security challenges, as traditional IT security controls are often incompatible with the real-time and availability requirements of industrial systems. Most existing solutions that aim to secure CPS-IIoT systems rely on a combination of blockchain, ML, and advanced authentication. Blockchain provides traceability, stability, and resilience that are appropriate for IIoT initiatives [8-10]. Machine learning algorithms, particularly deep neural networks and federated learning frameworks, have demonstrated promising results in detecting anomalies and intrusions in real-time without requiring centralized data storage.

The review paper organizes the article around four research questions: (RQ1) What can be defined as IIoT networks and what technologies facilitate their optimal operation? (RQ2) What is the relationship between edge computing and IIoT? (RQ3) What types of CPS exist and how do they integrate with IIoT? (RQ4) What security challenges and solutions exist for CPS-IIoT-edge integration? These research questions form the structural backbone of this review.

The remainder of this paper is organized as follows: Section II reviews related work on IIoT security, edge computing, and limitations of prior surveys; Section III provides an overview of the IIoT layered architecture, industry applications, technology stack, and attack surface across each layer; Section IV examines the role of edge computing in IIoT deployments, Section V discusses the integration of Cyber-Physical Systems with IIoT, covering attack taxonomies and the challenges posed by legacy OT environments; Section VI presents methods for enhancing CPS security using edge computing, encompassing AI/ML and federated learning approaches, IT/OT convergence security, intrusion detection systems, cryptographic protocols, and a comparative analysis of fourteen security frameworks. Section VII presents the discussion and VIII provide the conclusions.

II. RELATED WORK

Incompatible IIoT devices, due to inadequate protocols and differing technologies, are among the major challenges in real-time M2M (Machine-to-Machine) communication in Industry 4.0. In IIoT environments, controlling latency requires addressing heterogeneous device ecosystems and proprietary industrial protocols [7,8,11]. Blockchain and federated learning represent promising frameworks for addressing the combined challenges of data integrity, privacy, and real-time intrusion detection in distributed IIoT deployments [9,10].

To conduct the systematic literature review, Scopus and Google Scholar search engines were utilized to find papers related to the keywords 'IIoT', 'edge computing', 'cyber-physical systems', 'attack', from 2020 to 2024. The number of articles was reduced from an initial pool to 25 high-quality studies after applying inclusion and exclusion criteria that prioritized empirical evaluations and novel security framework proposals.

The difference between the work of Zhukabayeva et al. [1] and six previous surveys is that it covers the entire IIoT architecture, integration with the edge layer, CPS security, and a full attack taxonomy—all in a single work. Prior surveys tend to focus either on IoT security in isolation or on edge computing performance, rarely addressing the compound security scenarios that emerge at the CPS-IIoT-edge intersection.

III. OVERVIEW OF INDUSTRIAL INTERNET OF THINGS

The different layers of an IIoT network include the Perception layer (sensors, actuators, controllers), the Network layer (connectivity and data transportation), the Processing layer (data analysis and decision-making), and the Application layer (end-user services). This layered architecture provides a conceptual framework for analyzing security vulnerabilities at each stratum of the IIoT stack [11].

A. IIoT Industry Applications

The IIoT is being used in various fields and revolutionizes industrial operations through improvements in automation, data analytics and communications. In smart manufacturing, IIoT enables real-time monitoring of production lines using predictive maintenance algorithms and automated quality control systems. Connected sensors reduce unplanned downtime by enabling proactive intervention before equipment failures occur [10].

Smart Grids and Energy Management Systems (EMS) use real-time information to optimize energy distribution and usage [7]. To overcome scalability and privacy challenges, federated learning models are deployed at energy grid edge nodes, enabling collaborative anomaly detection without exposing sensitive operational data. Healthcare, logistics, and transportation similarly leverage IIoT for remote monitoring, asset tracking, and autonomous vehicle coordination [12].

B. IIoT Technology Stack

To function and ensure security of IIoT systems, a number of enabling technologies need to be integrated. Time-aligned industrial automation demands ultra-low-latency and high-bandwidth communications, which 5G and forthcoming 6G networks provide. These connectivity standards support massive device densities and network slicing capabilities, which are essential for diverse industrial application profiles.

IIoT uses cloud infrastructure connected to edge computing to boost computational capacity and storage, and to enable local data processing. Edge computing can reduce average processing latency from 4.03 ms to 3.03 ms compared to purely cloud-based architectures [1]. AI/ML techniques process edge data locally for real-time decision support, while blockchain ensures data immutability and provides tamper-evident audit trails across the distributed IIoT ecosystem (Fig. 1).

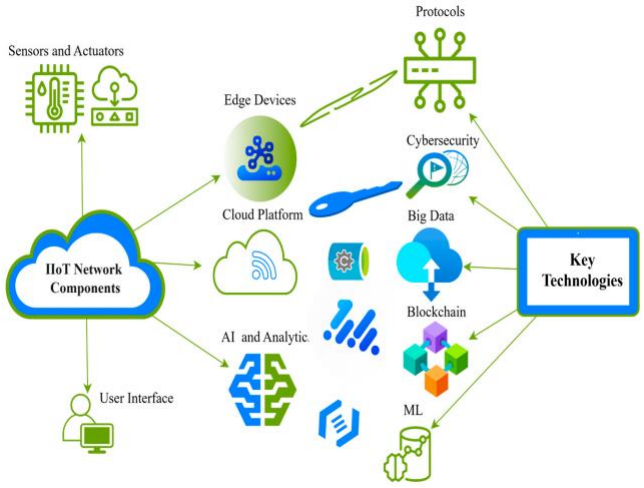

Fig. 1. Interaction of key IIoT components and technologies [1].

C. Attack Layers and Intrusion Methods

The vulnerabilities in each layer are mapped in [1] and are distinct. Physical/Perception layer attacks target IoT wireless infrastructure, video systems, or sensor data manipulation, impacting data integrity. Network layer threats include MITM attacks, eavesdropping, and protocol-based exploits. ML-based classifiers, such as CNN-LSTM, achieve 98.4% accuracy for detecting network-layer intrusions in IIoT environments [12]. Application layer attacks encompass ransomware, false data injection, and unauthorized API access [1,8].

The greater connectedness of the world—thanks in part to 5G and the advent of 6G—will boost IIoT capabilities and create new threat vectors. Side-channel attacks pose a security and data management challenge, necessitating cryptographic techniques such as ECC and post-quantum schemes to protect edge nodes against physically co-located adversaries [13].

IV. ROLE OF EDGE COMPUTING IN IIoT

The idea behind edge computing is to shift data processing towards the data's origin, minimizing delay or latency time and bandwidth required for IIoT applications needing quick responses [7,13]. Edge computing reduces dependency on centralized cloud infrastructure, enabling autonomous local decision-making critical for safety-sensitive industrial processes.

Real-time anomaly detection is an important security capability enabled by edge deployment. Edge computing and Federated Learning (FL) combined provide better capabilities in detecting anomalies while ensuring data privacy without centralized storage [13,12]. 1D-CNN architectures have achieved an F1 score of 98.4% for network intrusion detection when deployed on edge nodes, demonstrating the viability of computationally efficient deep learning models in resource-constrained environments.

Security frameworks implemented at the fog level include Zero Trust Architecture (ZTA), where no implicit security trust is assumed; Blockchain-based audit logs with tamper-evident records; and Digital Twins for real-time virtualisation and reconstruction of physical assets [14]. These complementary approaches create a defense-in-depth posture appropriate to the heterogeneous threat landscape of IIoT-edge deployments.

A. Applications and Performance in Edge Computing

Edge computing plays a key role in IIoT deployments. Advantages include real-time data processing, enhanced cybersecurity, and AI-based anomaly detection. DNN achieves 94.67% accuracy in traffic classification tasks when deployed at the edge, and an ensemble classifier combining Extra Tree (E-Tree), DNN, and Random Forest (RF) delivers high-precision intrusion detection with reduced false-positive rates [12].

Technologies including cloud computing, blockchain, SDN, and Federated Learning reduce latency and improve cyber efficiency of industrial systems substantially. Advanced systems at the edge with built-in cybersecurity and decentralized intelligence represent the next generation of IIoT infrastructure that is both performant and resilient [1].

V. INTEGRATION OF CYBER-PHYSICAL SYSTEMS WITH IIOT

CPS tightly integrate computational control with physical processes. PLCs, SCADA systems, Distributed Control Systems (DCS), and industrial robots are all examples of CPS in IIoT applications. They interface with IIoT connectivity to improve operational performance while simultaneously introducing security exposures that are absent in traditionally isolated OT environments [14].

Network segmentation and access control reduce the effect of DoS attacks that try to destabilize systems by disruption of communications. When combined with AI-based anomaly detection at the edge, these network-level controls provide layered protection against both volumetric and targeted attacks on industrial control systems.

The quantifiable operational impact of CPS implementation in IIoT environments is illustrated through a simulation of cybersecurity and industrial performance metrics over the period 2020–2024 [1]. Following IEC 62443 security standards, organizations implementing structured CPS-IIoT security programmes report measurable improvements in mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to cyber incidents [11].

Legacy devices and firmware, multiple vendor ecosystems, lack of patch windows, and the need to maintain safety integrity levels that may not align with security controls all contribute to security challenges in CPS environments. These operational constraints require security solutions that are lightweight, non-disruptive, and compatible with the long lifecycle requirements of industrial assets.

VI. METHODS FOR ENHANCING CPS SECURITY USING EDGE COMPUTING

A. AI Methods: Machine Learning and Federated Learning

By integrating blockchain and edge computing, issues of data privacy, intrusion detection, and resource limitation in CPS-IIoT can be addressed. The AILBSM leverages blockchain technology combined with the optimized Sprinter Convolutional Siamese Network (SCSN) for high-accuracy intrusion detection while maintaining data privacy across distributed IIoT nodes [14]. The SecureIIoT framework employs federated learning empowered approaches to secure IIoT against data breaches [15-18]. Blockchain-orchestrated FL further enhances security by providing cryptographically verified model aggregation and tamper-evident audit trails [16].

B. IT/OT Convergence Security

The combination of IT/OT security and edge computing provides a strong foundation for tackling specific IIoT challenges. Edge manufacturing networks can be secured against threats using standards such as IEC 62443-3-3 and can be scaled to full production environments while maintaining interoperability across heterogeneous vendor ecosystems [18]. Unified monitoring platforms that bridge IT and OT security operations centers enable holistic visibility into threat activity spanning both domains.

C. Intrusion Detection Systems

Intrusion Detection Systems (IDS) are crucial security tools for IIoT and edge computing environments. A combination of Extra Trees (E-Tree), Deep Neural Networks (DNN), and Random Forest (RF) has proven effective for intrusion detection via an ensemble approach, achieving high recall for rare attack categories [19,13]. These hybrid classifiers exploit the complementary strengths of different algorithm families while maintaining low false positive rates suitable for production deployment.

D. Cryptographic Approaches

The SPTM-EC framework uses a modified ElGamal encryption and digital signature technology for the exchange, storage, and computation of data in an edge IIoT environment, outperforming state-of-the-art schemes in computational efficiency [20]. ECC-based authentication protocols provide equivalent security to RSA with significantly smaller key sizes, making them practical for resource-constrained IIoT edge devices [5,21].

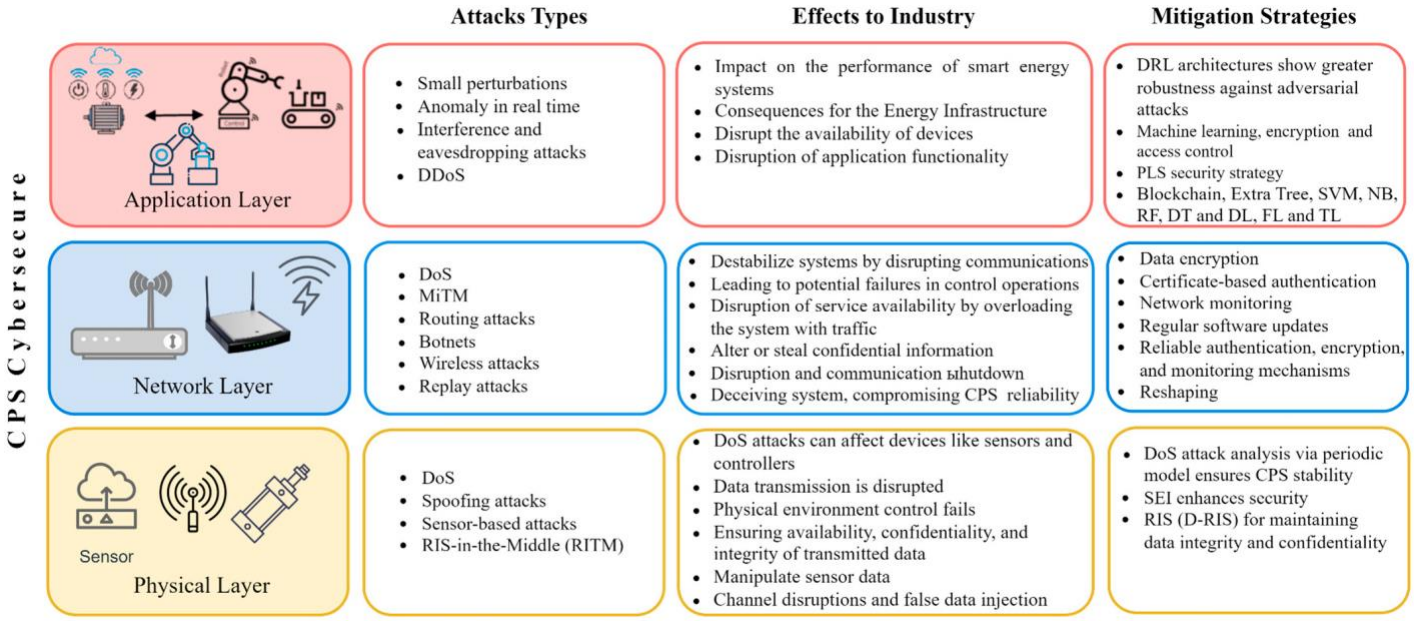

Fig. 2: Security methods in CPS of IIoT with edge computing integration [1].

E. Edge Computing Security Framework

The IoT-Defender framework uses a modified genetic algorithm (MGA) associated with an LSTM network for cyberattack detection. This reduces the number of features to be selected and optimizes model parameters, improving detection performance while reducing computational overhead at the edge node [1,20]. The ViT4Mal lightweight vision transformer further demonstrates the feasibility of deploying sophisticated detection models on constrained edge devices [20].

F. Comparative Analysis of Security Approaches

Fourteen studies have been organized in a tabular format comparing against six capability dimensions: ML/DL/FL, blockchain, IDS, IT/OT integration, cryptography/encryption, and CPS-IIoT-edge computing coverage. Blockchain-based certificateless signature schemes are also included in the comparison [9,10]. This comparative framework reveals that no single approach addresses all dimensions comprehensively, motivating the design of integrated multi-layer security architectures (see Fig. 2).

Omer et al. [12] advance ML/DL/FL in IDS for IIoT towards high accuracy including FL for anomaly detection. The authors of [13] contribute an edge-based FL approach for anomaly detection. The SecureIIoT environment by [15] addresses ML/DL/FL security. The blockchain-orchestrated FL approach by [16] addresses privacy-preserved cyberattack detection, while collectively these works highlight the breadth of AI-based security research in the IIoT-edge domain.

The review also finds that the majority of existing studies focus on a single or limited combination of security dimensions, without addressing compound scenarios. Limited real-world validation represents another critical gap—most proposed frameworks are evaluated on benchmark datasets rather than deployed industrial environments, limiting generalizability of reported performance metrics.

VII. VII. DISCUSSION AND CONCLUSIONS

A. Discussion

Globally, cyber-attacks are increasing with a significant number of cases reported in 2023–2024 [2]. According to the ENISA 2024 Threat Landscape, ransomware, DDoS, malware, data threats, information manipulation, and supply chain attacks are among the top threat categories affecting critical infrastructure operators [2,1]. IIoT environments are disproportionately affected due to the combination of high-value targets and historically weak security postures inherited from pre-connectivity OT deployments.

AI-based detection techniques show high accuracy for all types of CPS attacks: Kalman Filter for DoS Detection, FL+GRU+RF for Intrusion Detection with 99% success rate, and CNN/SVM/RF Ensemble for CPS attack classification [12]. These results demonstrate the maturity of AI-based detection for known attack categories, while highlighting the ongoing challenge of zero-day threat detection.

According to [16], three types of key research gaps exist. First, existing research often focuses on the cyber dimension while overlooking the physical aspects of CPS, leaving hardcoded vulnerabilities at the device and hardware level that purely software-based defenses cannot address. Second, most studies assume availability of labelled training data, which is scarce in industrial settings. Third, the integration of blockchain and federated learning requires further exploration in compound multi-layer security scenarios [22,16].

Other structural gaps identified by [1] include: the absence of standardized benchmarking environments for evaluating IIoT system security; a lack of security interoperability standards allowing security tools from different vendors to work together; and insufficient attention to energy and computational constraints of ultra-low-power edge nodes that cannot support heavyweight cryptographic operations [1,23-25].

VIII. Conclusions

This survey delivers a comprehensive, systematic review advancing understanding of IIoT-edge security. Advanced technologies including ML, FL, blockchain, and IDS are essential for data protection and real-time attack detection. The establishment of robust security frameworks that address both cyber and physical dimensions is paramount to the continued expansion of IIoT deployments in critical industrial sectors as provided in Table I.

Future research priorities identified by the authors include: energy-efficient cryptographic protocols for ultra-constrained IIoT devices; privacy-preserving FL with formal differential privacy guarantees; quantum-safe cryptographic migration pathways for long-lifecycle industrial assets; and standardized, open-source IIoT security benchmarking environments that reflect real-world heterogeneity. The integration of Digital Twin technology with security monitoring represents a particularly promising direction for proactive threat detection and incident response in complex CPS-IIoT ecosystems.

TABLE 1. Structured Summary of IIoT-Edge Computing Cybersecurity Approaches

Layer	Attack / Threat	Defence Method	Technology / Tool	Ref.
Network	DoS / DDoS	Anomaly-based IDS	ML / DL at edge	[8,12]
Network	MITM / Eavesdrop.	Lightweight crypto	ElGamal, ECC, dig. sigs	[5,21]
Physical	Sensor spoofing	SDN + ML auth.	SVM, Decision Tree, CNN-LSTM	[1]
Physical	Supply chain	Firmware verification	Blockchain audit logs	[2]
Processing	Ransomware / Malware	Behavioural detection	ViT4Mal, DL-based IDS	[2,20]
Processing	False data injection	Statistical anomaly det.	Blockchain-FL	[16]
Application	Unauth. access	Zero Trust Architecture	Per-session auth.	[25]
Application	API exploitation	Input validation + IDS	Ensemble (E-Tree, DNN, RF)	[19]
CPS / ICS	Replay attacks	Timestamp + nonce valid.	SPTM-EC, crypto nonces	[5]
CPS / ICS	APT (e.g. Stuxnet)	Threat intel + ZTA	Digital twins + ensemble ML	[24]
Edge / Fog	Node compromise	Blockchain + FL IDS	Fed-Trust / BoEI	[22,16]
Cross-layer	IT/OT convergence	Unified monitoring	IEC 62443, IT/OT edge sec.	[23,18]

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, U.R.K. and I.A.S.; methodology, U.R.K.; validation, U.R.K. and I.A.S.; writing—original draft preparation, U.R.K.; writing—review and editing, U.R.K. and I.A.S.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions," Sensors, vol. 25, p. 213, 2025.

[2] ENISA, "ENISA Threat Landscape 2024," European Union Agency for Cybersecurity, 2024. [Online]. Available: https://industrialcyber.co/reports/enisa-threat-landscape-2024

[3] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A Survey on Cyber-Physical Systems Security," IEEE Internet Things J., vol. 10, pp. 21670–21686, 2023.

[4] S. J. Oks et al., "Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization, and Outlook," Inf. Syst. Front., vol. 26, pp. 1731–1772, 2022.

[5] A. S. M. S. Hosen, P. K. Sharma, I.-H. Ra, and G. H. Cho, "SPTM-EC: A Security and Privacy-Preserving Task Management in Edge Computing for IIoT," IEEE Trans. Ind. Inform., vol. 18, pp. 6330–6339, 2022.

[6] A. Sánchez-Zumba and D. Avila-Pesantez, "Cybersecurity for Industrial IoT: Threats, Vulnerabilities, and Solutions: A Brief Review," in Proc. 8th Int. Congress on Information and Communication Technology (ICICT 2023), London, UK, Feb. 2023, vol. 693.

[7] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya, "Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions," in Fog/Edge Computing for Security, Privacy, and Applications, vol. 83. Cham: Springer, 2021.

[8] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," Sensors, vol. 21, p. 3654, 2021.

[9] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A Blockchain-Based Machine Learning Framework for Edge Services in IIoT," IEEE Trans. Ind. Inform., vol. 18, pp. 1918–1929, 2021.

[10] D. Jiang, Z. Wang, Y. Wang, L. Tan, J. Wang, and P. Zhang, "A Blockchain-Reinforced Federated Intrusion Detection Architecture for IIoT," IEEE Internet Things J., vol. 11, pp. 26793–26805, 2024.

[11] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," IEEE Trans. Ind. Inform., vol. 18, pp. 7059–7067, 2022.

[12] F. Omer, L. Awad, H. Rafea, A. Abdulrahman, A. Jasim, and O. Ata, "Enhancing IIoT Security with Machine Learning and Deep Learning for Intrusion Detection," Malays. J. Comput. Sci., vol. 37, pp. 107–123, 2024.

[13] S. V. Haldikar, O. F. M. A. Kader, and R. K. Yekollu, “Edge Computing and Federated Learning for Real-Time Anomaly Detection in Industrial Internet of Things (IIoT),” in Proc. 2024 Int. Conf. on Inventive Computation Technologies (ICICT), IEEE, 2024.

[14] A. A. Ahmed, “The Role of Blockchain Technology in Enhancing Cybersecurity,” Int. J. Sci. Res. Eng. Manag., vol. 8, pp. 1–5, 2024.

[15] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J.-H. Park, “SecureIIoT Environment: Federated Learning Empowered Approach for Securing IIoT From Data Breach,” IEEE Trans. Ind. Inform., vol. 18, pp. 6406–6414, 2022.

[16] M. Abdel-Basset, N. Moustafa, and H. Hawash, “Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach,” IEEE Trans. Ind. Inform., vol. 18, pp. 7920–7934, 2022.

[17] N. Sahli, M. Benmohamed, and E. B. Bourennane, “Security for Industrial Automation and Control Systems,” in Proc. CPI’13, 2013, pp. 40–46.

[18] M. Bhole, W. Kastner, and T. Sauter, “IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities,” in Proc. IEEE 29th Int. Conf. on Emerging Technologies and Factory Automation (ETFA), Padova, Italy, Sep. 2024.

[19] A. Abdulaziz, I. Ullah, T. A. Ahanger, and M. Atiquzzaman, “Ensemble Technique of Intrusion Detection for IoT-Edge Platform,” Sci. Rep., vol. 14, p. 11703, 2024.

[20] A. Ravi, V. Chaturvedi, and M. Shafique, “ViT4Mal: Lightweight Vision Transformer for Malware Detection on Edge Devices,” ACM Trans. Embed. Comput. Syst., vol. 22, p. 117, 2023.

[21] S. Hirendra and S. Sengar, “An ECC Based Secure Authentication Protocol for M2M Communication in Industrial IoT Edge Device,” Int. J. Sci. Technol. Eng., vol. 12, pp. 30–40, 2024.

[22] S. Ali, Q. Li, and A. Yousafzai, “Blockchain and Federated Learning-Based Intrusion Detection Approaches for Edge-Enabled Industrial IoT Networks: A Survey,” Ad Hoc Netw., vol. 152, p. 103320, 2024.

[23] T. Kampa, C. K. Müller, and D. Großmann, “Interlocking IT/OT Security for Edge Cloud-Enabled Manufacturing,” Ad Hoc Netw., vol. 154, p. 103384, 2024.

[24] G. Bhoi, R. K. Sahu, E. Oram, and N. Z. Jhanjhi, “Risk Assessment and Security of Industrial Internet of Things Network Using Advanced Machine Learning,” in Machine Learning for Cyber Physical System: Advances and Challenges. Cham: Springer Nature, 2024.

[25] H. Yu, J. Zhou, and M. Ma, “Anonymous Batch Message Authentication Aided by Edge Servers in Industrial Internet of Things,” in Proc. 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, May 29–31, 2024.