Journal of Information Hiding and Multimedia Signal Processing ©2025 ISSN 2073-4212
Ubiquitous International Volume **16**, Number **3**, September **2025**

AI-Driven Security Solutions for Industrial IoT: Challenges and Future Directions

Thi-Xuan-Huong Nguyen^{1,3}, Thi-Kien Dao^{2,3*}, Trinh-Dong Nguyen^{1,3}, Trong-The Nguyen^{2,3}

^{1}Software Engineering Department,
University of Information Technology, Vietnam
^{2}Multimedia Communications Lab.,
University of Information Technology, Vietnam
^{3}Vietnam National University, Ho Chi Minh City 700000, Vietnam
{huongntx, kiendt, dongnt, thent}@uit.edu.vn

Truong-Giang Ngo^{4}

^{4}Faculty of Computer Science and Engineering,
Thuyloi University, Hanoi, Vietnam, Hainoi, Vietnam
giangnt@tlu.edu.vn

*Corresponding author: Thi-Kien Dao*

Received May 30, 2025, revised July 18, 2025, accepted July 21, 2025.

Abstract. *The Industrial Internet of Things (IIoT) is a cornerstone of Industry 4.0, enabling smart manufacturing, predictive maintenance, and autonomous industrial systems. However, the increasing connectivity of IIoT devices introduces significant cybersecurity risks, including data breaches, Distributed Denial of Service (DDoS) attacks, and malicious intrusions. Traditional security mechanisms often fall short in addressing these dynamic threats, necessitating adaptive and intelligent solutions. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a powerful tool for enhancing IIoT security by enabling real-time threat detection, anomaly identification, and automated response systems. This paper reviews state-of-the-art AI-driven security solutions for IIoT, focusing on their applications across the perception, network, and application layers. We analyze key challenges, including adversarial attacks, model interpretability, data privacy, and computational constraints. Finally, we outline future research directions, such as federated learning for privacy preservation, lightweight AI models for edge deployment, and hybrid AI-blockchain security frameworks.*

Keywords: Industrial IoT (IIoT); Artificial Intelligence (AI); Cybersecurity; Machine Learning (ML); Deep Learning (DL); Threat Detection.

1. Introduction.

The Industrial Internet of Things (IIoT) has emerged as a transformative force in Industry 4.0, enabling smart manufacturing, predictive maintenance, and autonomous industrial processes through interconnected sensors, actuators, and control systems. By integrating advanced data analytics, real-time monitoring, and machine-to-machine (M2M) communication, IIoT enhances operational efficiency, reduces downtime, and optimizes resource utilization [1][2]. However, the exponential growth of connected industrial devices has significantly expanded the attack surface, making IIoT systems prime targets for cyber threats such as Distributed Denial of Service (DDoS) attacks, malware infections, data breaches, and ransom-ware [3]. Traditional cybersecurity mechanisms—including firewalls, intrusion detection systems (IDS), and encryption protocols—are often inadequate for IIoT environments due to their static nature, high computational overhead, and inability to adapt to evolving attack vectors [4]. The heterogeneous and distributed architecture of IIoT, coupled with resource-constrained edge devices, further complicates security enforcement. Moreover, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks, which form the backbone of IIoT, were historically designed for isolated operational technology (OT) environments and lack inherent security features [5][6]. Figure 1 illustrates an overview of commonly used approaches for enhancing security in IIoT environments, encompassing hardware-based, software-based, and network-level protection methods. Examples include Anomaly Detection, Predictive Maintenance and Threat Anticipation, Intrusion Detection and Prevention Systems (IDPS), and Cryptographic and Authentication Enhancements.

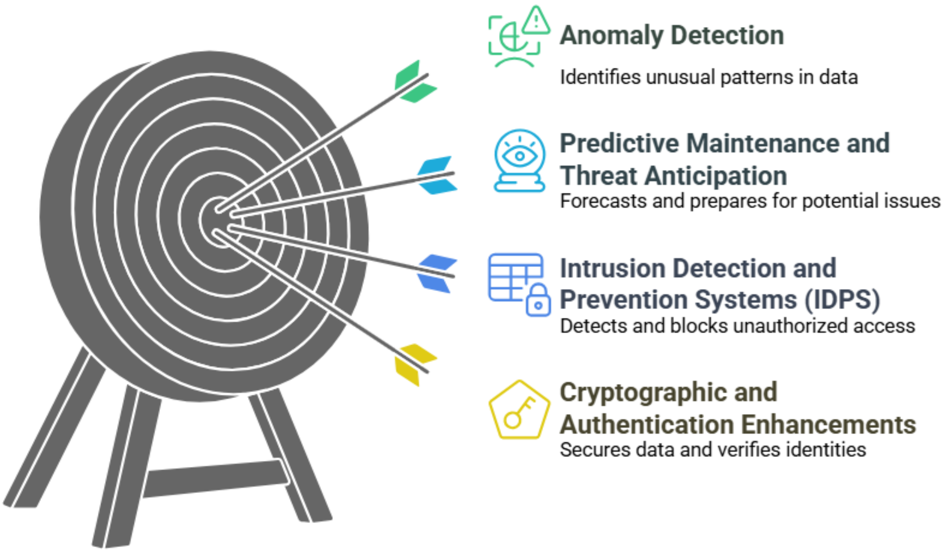

Anomaly Detection
Identifies unusual patterns in data
Predictive Maintenance and Threat Anticipation
Forecasts and prepares for potential issues
Intrusion Detection and Prevention Systems (IDPS)
Detects and blocks unauthorized access
Cryptographic and Authentication Enhancements
Secures data and verifies identities

Figure 1. Common security solution methods for Industrial Internet of Things (IIoT) systems.

To address these challenges, Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has gained prominence as a dynamic and adaptive security solution for IIoT. AI-driven approaches excel in: Anomaly Detection: Identifying deviations from normal behavior in real-time sensor data and network traffic [7]. Predictive Threat Intelligence: Forecasting potential attacks using historical and behavioral data patterns [8]. Automated Incident Response: Mitigating threats autonomously through adaptive security policies [9]. Despite these advantages, AI-based security solutions face significant hurdles, including adversarial attacks that deceive ML models, the "black-box" nature of deep learning systems, and the computational limitations of edge devices [10]. Additionally, the reliance on large datasets for training raises concerns about data privacy and regulatory compliance, particularly in sensitive industrial sectors [11]. The contributions of this paper highlight how AI-driven security solutions offer a promising alternative by leveraging machine learning (ML) and deep learning (DL) to detect anomalies, predict attacks, and autonomously mitigate threats.

- Systematic Categorization: This section classifies AI-based security solutions by the IIoT architectural layer (perception, network, application).
- Critical Challenge Analysis: It emphasizes unresolved issues such as adversarial ML and computational constraints.

- Forward-Looking Insights: Finally, it proposes research directions for developing privacy-preserving, scalable, and resilient IIoT security solutions.

This paper provides a comprehensive review of AI-driven security solutions for IIoT, structured as follows: Section 2 examines AI applications across IIoT layers (perception, network, and application). Section 3 analyzes key challenges, including adversarial robustness, explainability, and scalability. Section 4 outlines future directions, such as federated learning, lightweight AI, and hybrid AI-blockchain frameworks. By synthesizing current research and identifying gaps, this review aims to guide future advancements in securing IIoT ecosystems against increasingly sophisticated cyber threats.

2. **AI-Driven Security Solutions for IIoT.**

This section provides a comprehensive analysis of state-of-the-art AI solutions deployed across these layers. The Industrial IoT ecosystem comprises three fundamental layers - the perception layer (sensors/actuators), network layer (communication infrastructure), and application layer (data processing and user interfaces). Each layer presents unique security vulnerabilities that require tailored AI-based protection mechanisms [12].

2.1. **Perception Layer.**

The perception layer serves as the foundation of the IIoT architecture, comprising sensors, actuators, and embedded devices responsible for data collection and physical interaction with the environment. Due to their exposure and limited computational capabilities, these components are highly vulnerable to attacks such as spoofing, jamming, and unauthorized access. This section explores how AI-based techniques enhance security at this layer through advanced authentication, anomaly detection, and anti-jamming mechanisms. Figure 2 shows a layer structure of Industrial IoT ecosystem.

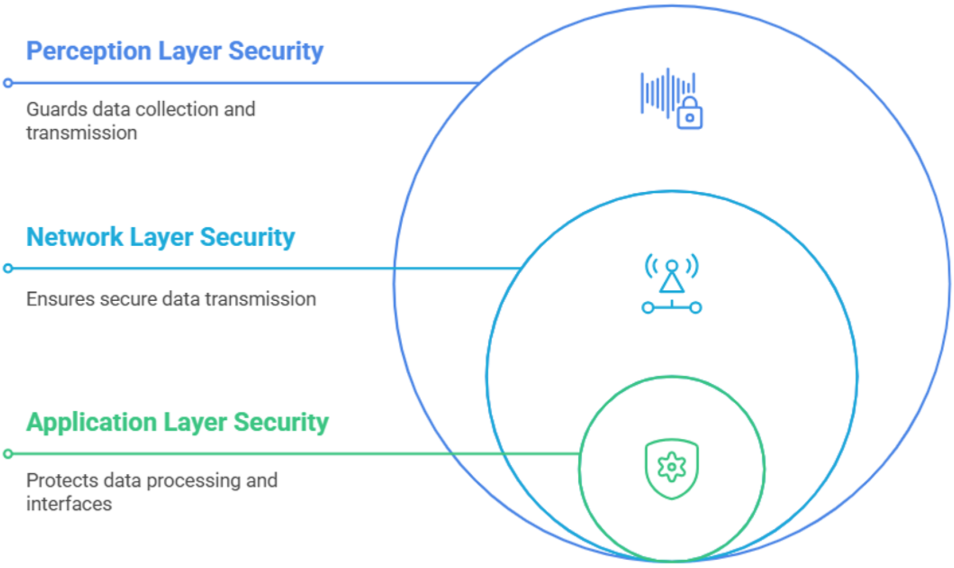
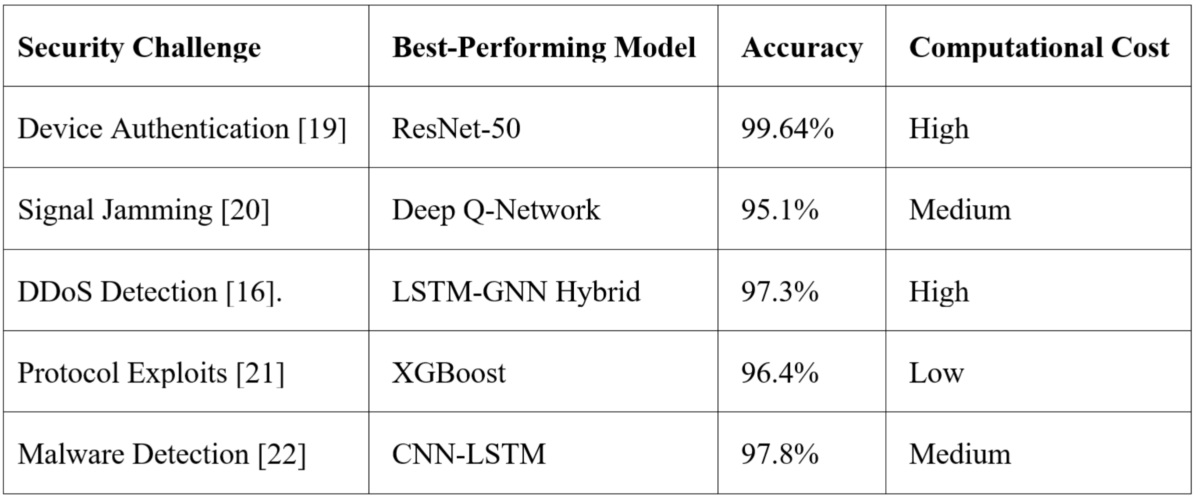

Perception Layer Security
Guards data collection and transmission
Network Layer Security
Ensures secure data transmission
Application Layer Security
Protects data processing and interfaces

FIGURE 2. Several layers of Industrial IoT ecosystem.

The Industrial Internet of Things (IIoT) ecosystem presents unique security challenges across its three architectural layers, each requiring specialized AI-driven protection mechanisms [12]. At the perception layer, where sensors and actuators operate, AI has proven particularly effective in device authentication and anti-jamming applications. Residual

Table 1. A comparison of AI models across IIoT security domains



Security Challenge	Best-Performing Model	Accuracy	Computational Cost
Device Authentication [19]	ResNet-50	99.64%	High
Signal Jamming [20]	Deep Q-Network	95.1%	Medium
DDoS Detection [16].	LSTM-GNN Hybrid	97.3%	High
Protocol Exploits [21]	XGBoost	96.4%	Low
Malware Detection [22]	CNN-LSTM	97.8%	Medium

Neural Networks (ResNet) achieve remarkable 99.64% accuracy in physical layer authentication by analyzing unique channel state information fingerprints, while ensemble learning methods demonstrate superior performance in detecting spoofed devices [13]. For wireless signal jamming, deep reinforcement learning agents autonomously develop optimal frequency-hopping patterns, and random forest classifiers effectively identify jamming attacks through signal-to-noise ratio analysis. These solutions address critical vulnerabilities in the physical infrastructure of IIoT systems [14].

2.2. **Network Layer.** The network layer facilitates the transmission of data between IIoT devices and backend systems via various communication protocols. It is a critical point of vulnerability, frequently targeted by attackers aiming to intercept, disrupt, or manipulate data flow. In this network layer, AI solutions focus on protecting data transmission and communication protocols. Long Short-Term Memory (LSTM) networks [15] have shown exceptional capability in predicting Distributed Denial of Service (DDoS) attack patterns, with some implementations achieving 94.2% accuracy in preemptive detection [16]. Graph Neural Networks (GNNs) provide another powerful approach by analyzing network topology to identify compromised devices. For routing protocol vulnerabilities, self-organizing maps and attention-based GNNs offer effective detection of attacks targeting industrial communication standards [17]. These network-layer solutions are particularly valuable as they can operate within the stringent latency requirements of industrial environments while maintaining high detection accuracy.

2.3. **Application Layer.** The application layer benefits from AI's ability to analyze complex data patterns and user interactions. XGBoost classifiers have demonstrated 96.4% accuracy in detecting exploits targeting industrial protocols like MQTT, while deep reinforcement learning algorithms effectively mitigate congestion attacks in CoAP implementations. For malware detection, hybrid CNN-LSTM architectures analyze API call sequences with 97.8% precision, providing robust protection for industrial control systems [18]. These application-layer solutions are increasingly incorporating few-shot learning techniques to address the challenge of limited training data for novel attack vectors.

Table 1 presents a comparative analysis of various artificial intelligence (AI) approaches, highlighting their key characteristics, strengths, limitations, and typical application areas. The selection of appropriate AI techniques involves crucial trade-offs between detection accuracy, computational requirements, and implementation complexity. While deep learning models achieve superior performance for complex threats like DDoS attacks, simpler ensemble methods often provide adequate protection against protocol-level exploits with significantly lower resource demands.

The selection of appropriate AI techniques involves careful consideration of multiple factors, including detection accuracy, computational requirements, and implementation complexity. While deep learning models excel at detecting sophisticated multi-stage attacks, simpler ensemble methods often provide adequate protection against common protocol-level exploits with significantly lower resource demands. Emerging approaches such as neuromorphic computing and digital twin technology promise to further enhance AI's effectiveness in IIoT security while addressing current limitations in energy efficiency and real-time performance. This evolving landscape of AI solutions offers a robust toolkit for securing industrial systems against an increasingly sophisticated threat environment.

3. **Challenges in AI-Based IIoT Security.** Although AI-driven security has made progress, it still encounters several challenges, including adversarial attacks, difficulties in model interpretability, concerns about data privacy, and limited computational resources. Since IIoT devices typically have low processing capacity, lightweight AI models such as TinyML are essential for deployment at the edge. The promising capabilities of AI in securing Industrial IoT systems, several critical challenges must be addressed for effective real-world deployment. One of the most pressing concerns is adversarial robustness, where AI models remain vulnerable to carefully crafted attacks that can manipulate input data to bypass detection systems. Recent studies show that even state-of-the-art deep learning models can be fooled with high success rates, particularly in physical-world attack scenarios where subtle perturbations to sensor data can go undetected. The inherent black-box nature of many AI algorithms presents another significant barrier, especially in industrial environments where explainability and trust are paramount. Many industrial operators remain skeptical of security alerts generated by opaque deep learning systems, and regulatory requirements increasingly demand transparent decision-making processes. While techniques like SHAP and LIME have improved interpretability, they often prove inadequate for complex time-series industrial data, leaving a crucial gap in model trustworthiness [23]. Practical implementation faces substantial hurdles due to the resource constraints of typical IIoT edge devices. The computational and memory requirements of modern AI models frequently exceed the capabilities of industrial sensors and controllers, forcing difficult trade-offs between security effectiveness and system performance. Energy consumption represents a particularly acute challenge, as continuous AI inference can dramatically reduce battery life in wireless industrial sensors [24]. Data quality and availability issues further complicate AI deployment in IIoT security. The lack of comprehensive, labeled datasets for industrial attack scenarios makes model training challenging, while the rapid evolution of attack techniques leads to concept drift that can quickly render trained models obsolete. Privacy concerns add another layer of complexity, as industrial data often contains sensitive operational information that cannot be freely shared for model training.

Figure 3 illustrates the challenges in applying AI-driven security solutions for IIoT systems—much like the tip of the iceberg. Despite significant advancements, several issues persist, including vulnerability to adversarial attacks, limited model interpretability, data privacy concerns, and computational constraints on edge devices. Addressing these challenges requires robust defense mechanisms, explainable AI techniques, privacy-preserving approaches such as federated learning, and lightweight models suitable for resource-constrained environments. Finally, system integration challenges emerge when

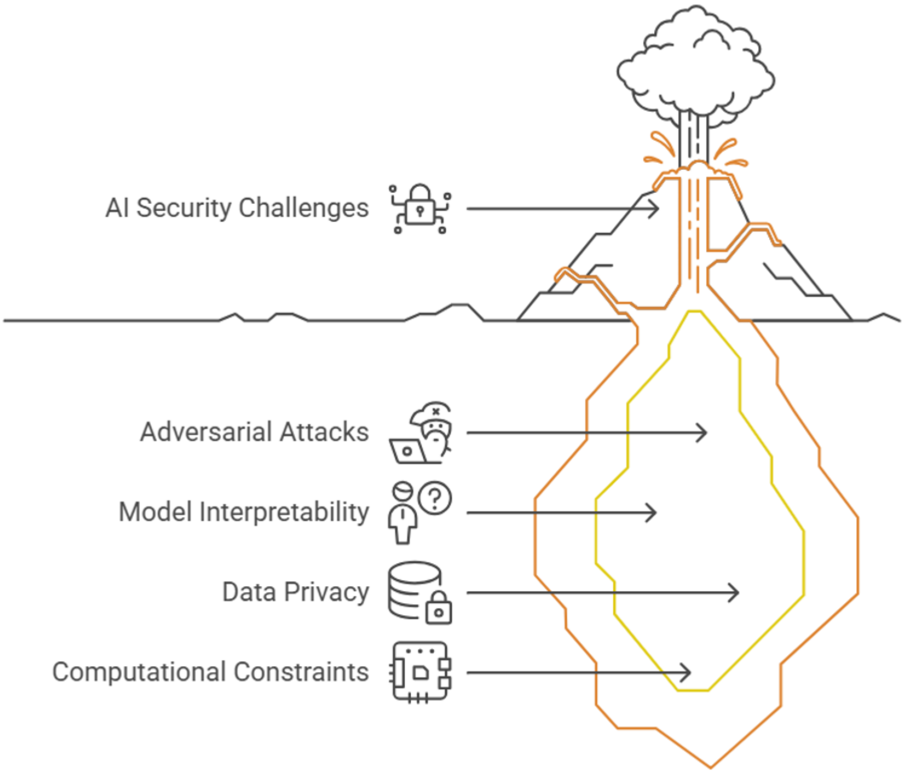


Figure 3. Challenges in AI-driven security for IIoT systems.

Table 2. Summary of Key Challenges and Mitigation Approaches

Challenge	**Current Status**	**Promising Solutions**	**Adoption Barrier**
Adversarial Attacks [27]	High risk	Ensemble defenses, formal verification	Computational cost
Explainability [28]	Limited	Hybrid models, attention mechanisms	Performance tradeoffs
Resource Limits [13	Severe	TinyML, neuromorphic computing	Development expertise
Data Quality [29]	Inadequate	Synthetic data, transfer learning	Domain knowledge
Privacy [10]	Critical	Federated learning, SMPC	Regulatory uncertainty
Integration [15]	Complex	Edge-cloud co-design	Legacy infrastructure

attempting to incorporate AI security solutions into existing industrial infrastructure [25]. Legacy equipment and proprietary protocols frequently lack the interfaces needed for seamless AI integration, while performance requirements for real-time industrial control systems may conflict with the computational demands of security algorithms [26]. These challenges collectively highlight the need for continued research and innovation to make AI-based IIoT security both effective and practical for industrial deployment.

Table 2 summarizes some key challenges and mitigation approaches. These challenges highlight the need for continued research and standardization efforts. While no single solution addresses all limitations, a combination of algorithmic advances, hardware innovations, and architectural improvements is gradually overcoming these barriers. The next section explores emerging approaches that may provide breakthroughs in these areas.

4. **Future Research Directions.** The rapid evolution of IIoT systems demands continuous advancement in AI-based security solutions. Several promising research directions are emerging to address current limitations and anticipate future threats. Neuromorphic computing architectures represent a particularly exciting frontier, with spiking neural networks demonstrating potential for ultra-low-power anomaly detection while maintaining high accuracy. These biologically-inspired systems could enable real-time security processing directly on energy-constrained edge devices, overcoming one of the most significant barriers to widespread AI deployment in industrial settings [30]. Figure 3 illustrates advancements in AI security within the IIoT. Future directions include federated learning for privacy preservation, which enables decentralized data processing without compromising individual privacy; hybrid AI-blockchain security frameworks, enhancing data integrity and trust among devices; lightweight AI for edge computing, facilitating real-time decision-making without overloading device resources; and self-learning adaptive systems, which autonomously evolve to counter new threats, making IIoT networks more resilient. These innovations pave the way for robust and secure industrial applications.

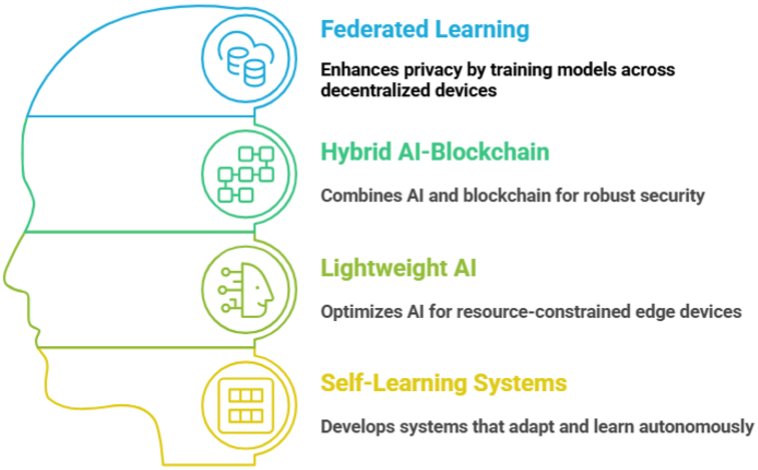

Federated Learning
Enhances privacy by training models across decentralized devices
Hybrid AI-Blockchain
Combines AI and blockchain for robust security
Lightweight AI
Optimizes AI for resource-constrained edge devices
Self-Learning Systems
Develops systems that adapt and learn autonomously

Figure 4. Key advancing AI Security in IIoT.

Explainable AI (XAI) techniques are gaining importance as industrial operators require transparent and interpretable security decisions. Emerging approaches combine causal reasoning with deep learning to create hybrid models that maintain detection performance while providing actionable insights into threat patterns. Digital twin technology further enhances this capability by enabling virtual testing and validation of security measures against simulated attacks before deployment in physical systems. These developments are particularly crucial for meeting stringent industrial compliance requirements and building operator trust in AI-driven security solutions.

The growing threat of quantum computing has spurred research into quantum-resistant security frameworks. Lattice-based cryptography and quantum key distribution systems are showing promise for protecting IIoT communications against future attacks, though

Table 3. Roadmap for AI-Driven IIoT Security Research

Timeframe	Focus Area	Key Milestones	Expected Impact
2024-2026	Edge-AI Optimization	<1MB detection models	50% wider deployment
2025-2027	Physics-Informed AI	Certified safe learning	10× fewer false positives
2026-2028	Quantum Protection	Practical QKD networks	Future-proof encryption
2027-2030	Self-Evolving Systems	Autonomous patching	90% faster response
2028+	Sustainable Security	Zero-power AI	Unlimited device lifespan

significant challenges remain in implementation efficiency. Concurrently, research into quantum machine learning suggests potential breakthroughs in processing speed for complex threat detection tasks, with early experiments demonstrating orders-of-magnitude improvements in pattern recognition capabilities.

Self-evolving security systems represent another critical research direction, addressing the challenge of rapidly adapting to novel attack vectors. Meta-learning architectures and continuous learning frameworks are being developed to enable security systems to incrementally update their knowledge without catastrophic forgetting of previous threats. These adaptive systems may incorporate automated feature engineering and dynamic model selection to maintain effectiveness as both IIoT infrastructure and attack methods evolve [31].

Human-AI collaboration interfaces are emerging as a vital component of future industrial security ecosystems. Mixed-reality visualization systems and cognitive load-optimized alert mechanisms are being developed to enhance security operators' situational awareness and decision-making capabilities [32-34]. These human-centric approaches complement technical security measures by improving incident response times and reducing operator fatigue during extended monitoring periods.

Sustainable security paradigms are gaining attention as environmental considerations become increasingly important. Research into energy-harvesting security systems and bio-inspired algorithms aims to reduce the environmental footprint of IIoT protection measures while maintaining robust security postures. Lifecycle management approaches, including self-healing systems and responsible AI retirement frameworks, are being developed to ensure long-term viability of security solutions throughout industrial equipment lifecycles. These diverse research directions collectively represent a comprehensive approach to addressing both current challenges and anticipated future requirements in IIoT security.

These research directions collectively address the fundamental tension between security effectiveness and practical deployability in industrial environments [35]. Successful advancement along these trajectories will require unprecedented collaboration between AI researchers, industrial engineers, cybersecurity experts, and policymakers. The ultimate goal remains the development of IIoT security systems that are simultaneously more robust, more efficient, and more trustworthy than current solutions - enabling the full realization of Industry 4.0's potential without compromising safety or reliability.

5. Conclusion.

AI-driven security solutions have demonstrated significant potential in safeguarding Industrial IoT systems, achieving high detection accuracy for threats like DDoS attacks, device spoofing, and protocol exploits. However, challenges such as adversarial vulnerabilities, computational constraints, and model interpretability hinder widespread adoption. Future advancements must focus on neuromorphic edge-AI for real-time processing, physics-informed models for explainability, and self-evolving systems that adapt to emerging threats. Quantum-resistant cryptography and human-AI collaboration frameworks will further enhance resilience. As IIoT expands, a balanced approach—combining robust AI defenses with energy efficiency, regulatory compliance, and workforce upskilling—will be critical. The next decade presents a pivotal opportunity to build secure, scalable IIoT ecosystems, ensuring Industry 4.0's success without compromising safety. Collaborative efforts across research, industry, and policy will be essential to overcome current limitations and realize AI's full potential in industrial cybersecurity.

Acknowledgment. This study was partially supported by the Vietnam National University, Ho Chi Minh City (VNU-HCM) under the VNUHCM-University of Information Technology's Scientific Research Support Fund.

REFERENCES

[1] D. Evans, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything, *CISCO white paper*, no. April, pp. 1–11, 2011, doi: 10.1109/IEEESTD.2007.373646.

[2] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics*IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2019, doi: 10.1109/JIOT.2018.2869847.

[3] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A review of security and privacy concerns in the internet of things (IoT), *Journal of Sensors*, vol. 2022, 2022.

[4] A. Prasanth and S. Jayachitra, "A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications, *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1905–1920, 2020, doi: 10.1007/s12083-020-00945-y.

[5] A. Khan, A. Ahmad, M. Ahmed, J. Sessa, and M. Anisetti, "Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends, *Complex & Intelligent Systems*, vol. 8, no. 5, pp. 3919–3941, 2022.

[6] A. Salam and A. Salam, "Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends, *Internet of things for sustainable community development: wireless communications, sensing, and systems*, pp. 299–327, 2020.

[7] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework, *Expert Systems with Applications*, vol. 133, pp. 97–108, 2019.

[8] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things, *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636-1675, 2018.

[9] U. A. Kumar S R, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks, *Journal of Sensors*, vol. 2015, no. 203814, 2015.

[10] Y. Qiao, T. K. Dao, J. S. Pan, S. C. Chu, and T. T. Nguyen, "Diversity teams in soccer league competition algorithm for wireless sensor network deployment problem, *Symmetry*, vol. 12, no. 3, p. 445, Mar. 2020, doi: 10.3390/sym12030445.

[11] M. N. Omidvar, X. Li, and X. Yao, "A review of population-based metaheuristics for large-scale black-box global optimization—Part I, *IEEE Transactions on Evolutionary Computation*, vol. 26, no. 5, pp. 802-822, 2021.

[12] D. Wu and N. Ansari, "A trust-evaluation-enhanced blockchain-secured industrial IoT system, *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5510–5517, 2020.

[13] F. He, T. Liu, and D. Tao, "Why resnet works? residuals generalize, *IEEE transactions on neural networks and learning systems*, vol. 31, no. 12, pp. 5349–5362, 2020.

[14] Y. Hu, H. Tang, and G. Pan, "Spiking deep residual networks, *IEEE Transactions on Neural Networks and Learning Systems,* vol. 34, no. 8, pp. 5200–5205, 2021.

[15] S. Zhang, X. Su, X. Jiang, M. Chen, and T.-Y. Wu, “A Traffic Prediction Method of Bicycle-sharing based on Long and Short term Memory Network., *J. Netw. Intell.,* vol. 4, no. 2, pp. 17–29, 2019.

[16] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, “Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework, *Journal of Network and Computer Applications,* vol. 67, pp. 147–165, 2016.

[17] J. Zhou et al., “Graph neural networks: A review of methods and applications, *AI open,* vol. 1, pp. 57–81, 2020.

[18] M. Alhussein, K. Aurangzeb, and S. I. Haider, “Hybrid CNN-LSTM model for short-term individual household load forecasting, *Ieee Access,* vol. 8, pp. 180544–180557, 2020.

[19] T.-Y. Wu et al., “Security Analysis of Rhee et al.’s Public Encryption with Keyword Search Schemes: A Review, *Journal of Network Intelligence,* vol. 3, no. 1, pp. 16–25, 2018.

[20] D. Fudenberg and J. Tirole, “A” signal-jamming” theory of predation, *The RAND Journal of Economics,* pp. 366–376, 1986.

[21] R. P. Jover and V. Marojevic, “Security and protocol exploit analysis of the 5G specifications, *IEEE Access,* vol. 7, pp. 24956–24963, 2019.

[22] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, “A survey on malware detection using data mining techniques, *ACM Computing Surveys (CSUR),* vol. 50, no. 3, pp. 1–40, 2017.

[23] T.-T. Nguyen, T.-K. Dao, T.-G. Ngo, and T.-D. Nguyen, “Node WSN localisation based on adaptive crossover-mutation differential evolution, *International Journal of Sensor Networks,* vol. 44, no. 1, pp. 1–22, Jan. 2024, doi: 10.1504/IJSNET.2024.136339.

[24] T. T. Nguyen, J. S. Pan, and T. K. Dao, “An Improved Flower Pollination Algorithm for Optimizing Layouts of Nodes in Wireless Sensor Network, *IEEE Access,* vol. 7, pp. 75985–75998, 2019, doi: 10.1109/ACCESS.2019.2921721.

[25] T.-K. Dao, T.-X.-H. Nguyen, N.-T. Vu, and T.-T. Nguyen, “An Enhanced Harmony Search Algorithm for Cascade Reservoirs Planning *Advances in Intelligent Information Hiding and Multimedia Signal Processing,* 2022, pp. 207–217.

[26] T.-G. Ngo, T.-T. Nguyen, Q.-T. Ngo, D.-D. Nguyen, and S.-C. Chu, “Similarity shape based on skeleton graph matching, *Journal of Information Hiding and Multimedia Signal Processing,* vol. 7, no. 6, 2016.

[27] C.-J. Weng et al., ”Enhanced Secret Hiding Mechanism Based on Genetic Algorithm”,*Smart Innovation, Systems and Technologies* vol. 156. 2020.

[28] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, “Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey, *IEEE Transactions on Network and Service Management,* vol. 19, no. 2, pp. 1159–1175, 2021.

[29] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, “Wireless sensor network security: A recent review based on state-of-the-art works, *International Journal of Engineering Business Management*, vol. 15, p. 18479790231157220, Feb. 2023, doi: 10.1177/18479790231157220.

[30] T.-T. Nguyen, T.-K. Dao, T.-T.-T. Nguyen, and T.-D. Nguyen, “An Optimal Microgrid Operations Planning Using Improved Archimedes Optimization Algorithm, *IEEE Access*, vol. 10, pp. 67940–67957, 2022, doi: 10.1109/ACCESS.2022.3185737.

[31] T.-T. Nguyen, T.-D. Nguyen, S.-C. Chu, and T.-K. Dao, “An Improved Ants Colony Optimization for Mobile Robot Path Planning, *Advances in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies* 2022, pp. 239–249.

[32] T. T. Nguyen, J. S. Pan, and T. K. Dao, “An Improved Flower Pollination Algorithm for Optimizing Layouts of Nodes in Wireless Sensor Network,” *IEEE Access,* vol. 7, pp. 75985–75998, 2019, doi: 10.1109/ACCESS.2019.2921721. K. S. Nguyen, X. T. Tran, and T. H. Mai, ”Reversible Data Hiding based on dual images adapt to the secret message,” *Journal of Information Hiding and Multimedia Signal Processing,* vol. 14, no. 1, pp. 20-30, March 2023.

[33] M. A. Belhamra, and E. M. Souidi, “An Information Hiding Scheme for Live P2P Streaming Based on the R2 Protocol,” *Journal of Information Hiding and Multimedia Signal Processing,”* vol. 12, no. 2, pp. 102-115, June 2021.

[34] J.-S Pan, M. Zhu and S.-C. Chu, “Robust digital watermarking with parallel compact sparrow search algorithm applied for QR code”, *Journal of Information Hiding and Multimedia Signal Processing,* vol. 13, vo. 2, pp. 124-144, June 2022.

[35] T. K. Dao, T.T. Nguyen, T.X.H. Nguyen, T. D. Nguyen, ”Recent Information Hiding Techniques in Digital Systems: A Review”, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 15, no.1, pp. 10-20, 2024.