ISA Journal of Engineering and Technology (ISAJET)

Homepage: https://isapublisher.com/isajet/
Email: office.isapublisher@gmail.com

Volume 2, Issue 4, July-August, 2025 ISSN: 3049-1843

AI for Industrial Cybersecurity (IIoT and Control Systems)

Harshilkumar Patel

Received: *20.08.2025* **|** ***Accepted:*** *22.09.2025* **|** ***Published:*** *23.09.2025*

***Corresponding Author:** Harshilkumar Patel

DOI: *10.5281/zenodo.17186847*

Abstract **Original Research Article**

The fast development and implementation of Industrial Internet of Things (IIoT) technologies and modern control systems have reinvented industrial practices, making it possible to monitor industrial processes in real-time, automate them, and become more efficient in the energy, manufacturing, and transportation industries. Nevertheless, the cyber-attack surface has increased, as well, due to this digital transformation, making critical infrastructures vulnerable to advanced attacks such as ransomware or state-sponsored attacks. Artificial Intelligence (AI) has become a capable facilitator of industrial cybersecurity by delivering superior threat detection and predictive analytics and dynamic-oriented defensive procedures according to evolving industrial conditions. The implementation of AI-based solutions, such as machine learning, deep learning, and anomaly detection models, is becoming popular in protecting Supervisory Control and Data Acquisition (SCADA), programmable logic controllers (PLCs) and IIoT devices against the emerging cyber threats. This paper discusses the application of AI in improving resilience in industrial ecosystems due to its ability to detect threats early, automate incident response and reduce downtime. Besides, it looks into major issues like the quality of data, interpretability of models and the performance of AI in integrating with existing infrastructures. The results highlight how AI can transform the field of industrial cybersecurity, and furthermore, that more research will be needed to achieve safe and reliable implementation in life-and-limb industries.

Keywords: SCADA Security, Anomaly Detection, Machine Learning, Deep Learning, Critical Infrastructure Protection.

INTRODUCTION

The intersection of Artificial Intelligence (AI) and Industrial Internet of Things (IIoT) technologies is transforming the contemporary industrial processes. IIoT allows monitoring in real-time, predictive maintenance, and automatic processing of processes, and the control systems (Supervisory Control and Data Acquisition SCADA and Programmable Logic Controllers PLCs) are the foundation of critical industrial systems (Kumar et al., 2021). Nevertheless, this increasing interconnection presents major cybersecurity risks because the industrial setting is exposed to more sophisticated and focused cyber-crime (Shen et al., 2022).

Though effective with information technology (IT) systems, traditional cybersecurity strategies fail to work in operational technology (OT) systems because of their unique needs, such as needing to be responsive in real-time, needing to be integrated with legacy, and having safety-critical constraints (Alcaraz and Lopez, 2020). The field of AI provides a viable solution to such gaps, with more sophisticated features in anomaly detection, behavior forecasting, and automated reaction to the future cyber-attacks (Zhang et al., 2021).

The approaches to implementing AI-enhanced cybersecurity in IIoT and control systems do not lack difficulties. The problem of data inadequacy, machine learning based on adversarialism, and the explainability of AI models are serious obstacles to adoption (Srinivas et al., 2023). Nevertheless, the use of AI-based solutions to safeguard industrial networks, defend the supply chain, and make critical infrastructures resistant to both external and internal attacks is gaining more and more popularity (Cheng et al., 2021).

The table above leads to the main distinction between IT and OT cybersecurity requirements, which explains the necessity of AI-driven solutions in the industry.

Table 1. Comparison of IT vs. OT Cybersecurity Requirements

Feature	IT Systems Security	OT/IIoT & Control Systems Security	AI Application Potential
Primary Goal	Data confidentiality and integrity	Safety, reliability, and availability	Predictive anomaly detection
System Lifespan	3–5 years (frequent upgrades)	10–30 years (legacy systems)	Adaptive AI-based integration
Tolerance to Downtime	High tolerance (planned outages)	Very low tolerance (continuous uptime)	Automated incident response
Attack Surface	Cloud, enterprise networks	IIoT devices, SCADA, PLCs, sensors	Real-time threat monitoring
Security Focus	Network and application protection	Physical process and control integrity	AI-driven behavioral modeling

This introduction preconditions the discussion of the possibilities of AI technologies to protect industrial systems against the changing cyber threats.

LITERATURE REVIEW

The increased incorporation of Industrial Internet of Things (IIoT) and sophisticated control systems have resulted in the increasing surface of attack of critical infrastructures, which requires smarter approaches to cybersecurity. Scientists have also been keen on the use of Artificial Intelligence (AI) to improve the stability of such systems.

Artificial intelligence in IIoT Threat Detection.

The use of AI to identify anomalies in IIoT settings has received extensive research as a security measure. Support vector machines (SVMs) and random forests have been used as machine learning models to identify abnormal network traffic patterns and are more accurate than traditional systems based on rules (Zhang et al., 2021). On the same note, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have also demonstrated the potential to detect zero-day attacks in IIoT networks (Huang et al., 2020). Through these models, they are able to monitor and predict in real-time, which improves the detection of advanced cyber threats.

Artificial Intelligence in Control System Security.

Industrial processes are primarily dependent on SCADA and PLCs that are extremely susceptible to cyber-attacks because they are based on old protocols. The proposed solution to these vulnerabilities is AI-based intrusion detection systems (IDS), and hybrid models of statistical analysis and machine learning provide a better accuracy (Sridhar & Govindarasu, 2019). Moreover, reinforcement learning has been applied to devise dynamically responsive defense mechanisms (Sun et al., 2021).

There are difficulties with AI-based Cybersecurity.

Nevertheless, the implementation of AI in industrial cybersecurity has significant challenges regardless of its potential. The quality and availability of data continue to be a problem, with industrial datasets being proprietary and usually small (Srinivas et al., 2023). Also, there is a high risk of adversarial machine learning in which the attackers use AI models to classify threats incorrectly (Goodfellow et al., 2015). The interpretability of the models also appears as one of the obstacles, as most AI-based solutions are so-called black boxes that operators can hardly comprehend or trust their predictions (Molnar, 2020).

Comparison of AI Techniques.

According to the literature, there is no specific AI method that would suit all industrial cybersecurity requirements. Rather, hybrid and ensemble methods are suggested more frequently to balance the detectors, flexibility, and interpretability (Cheng et al., 2021). Table 2 will present a comparison of important AI techniques in industrial cybersecurity.Table 2. Comparative Overview of AI Techniques in Industrial Cybersecurity

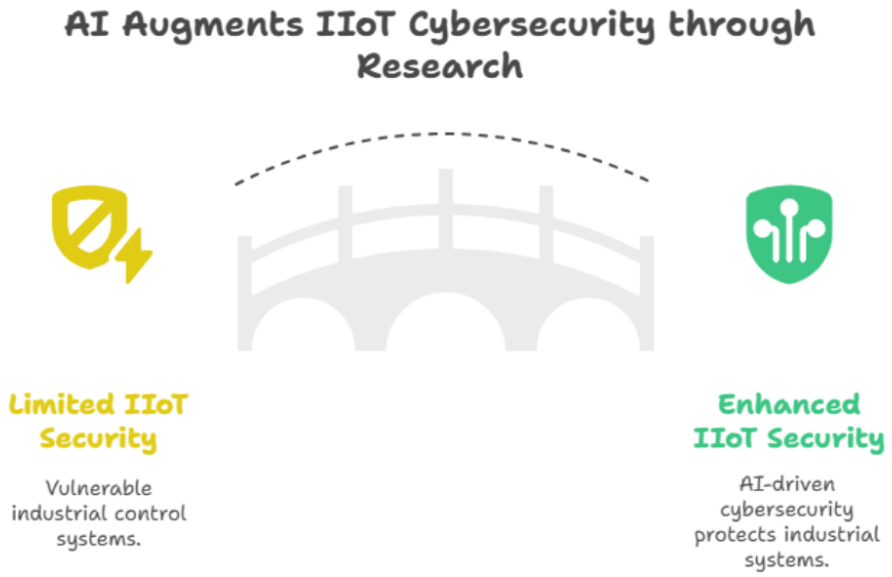
AI Technique	Application Area	Strengths	Limitations
Support Vector Machines	Network anomaly detection	High accuracy with small datasets	Poor scalability with big data
Random Forests	Malware detection, intrusion detection	Robust, handles noisy data well	Limited adaptability to new threats

Convolutional Neural Nets	IIoT traffic classification	Strong feature extraction, detects zero-day	Requires large training datasets
Recurrent Neural Nets	SCADA log analysis, predictive alerts	Captures temporal patterns effectively	Prone to overfitting
Reinforcement Learning	Adaptive defense strategies	Learns dynamic responses to attacks	High computational cost
Hybrid/Ensemble Models	Cross-domain protection	Balances accuracy and robustness	Increased system complexity

This review highlights the growing body of research supporting AI as a transformative tool for industrial cybersecurity. However, it also emphasizes the need for addressing critical limitations to ensure reliable deployment in real-world industrial environments.

METHODOLOGY

In order to examine how Artificial Intelligence (AI) can be used to augment industrial cybersecurity in Industrial Internet of Things (IIoT) and control systems, this research paper will employ a mixed-methodology, which will combine systematic literature review, comparative study, and the development of conceptual frameworks.



Systematic Literature Review.

The initial step is the systematic review of scholarly articles, conference papers, and company publications that were released during the years 2015-2025. The relevant sources were found in the most popular databases: IEEE Xplore, SpringerLink, and ScienceDirect and were narrowed down to AI-driven applications to cybersecurity in IIoT and control systems (Kitchenham et al., 2009). The inclusion criteria focused on the studies which deal with anomaly detection, intrusion detection, predictive analytics, and adaptive defense in the industrial context. The strategy guaranteed an in-depth knowledge of not only the best practices but also the new issues.

Comparison of AI Techniques.

The second step involves the comparative analysis of the major techniques of AI use in industrial cybersecurity. Based on the previous literature, machine learning (ML), deep learning (DL), and reinforcement learning (RL) models are

compared by their ability to meet the following dimensions: detection accuracy, computational efficiency, scalability, and interpretability (Zhang et al., 2021; Sun et al., 2021). This discussion sheds light into the advantages and flaws of each strategy, hence determining the appropriate models of the SCADA, PLCs, and IIoT setup protection.

Case Study Synthesis

The third phase will involve a synthesis of the relevant case studies to demonstrate how AI can be applied in industrial cybersecurity in practice. As an illustration, the research that has shown the application of AI-driven intrusion detection to power grids, oil and gas plants, and smart manufacturing facilities is analyzed to discover the trends of successful implementation and experience gained (Shen et al., 2022; Cheng et al., 2021). The synthesis of the case study is an empirical proof that AI is applicable to various industrial sectors.

Formulation of Conceptual Framework.

Lastly, a conceptual framework is designed in order to suggest the ways in which AI can be integrated into industrial cybersecurity architectures systematically. The framework is compatible with the layered defense model, which uses AI in the monitoring, detection, response, and recovery features of IIoT and control systems (Alcaraz & Lopez, 2020). Other challenges that are discussed by the framework include compatibility with the legacy system, adversarial AI threats, and the data governance (Srinivas et al., 2023).

Methodological Flow

Systematic Review- Gather peer-reviewed articles and industry reports.

Comparative Analysis - Test AI models in industrial cybersecurity.

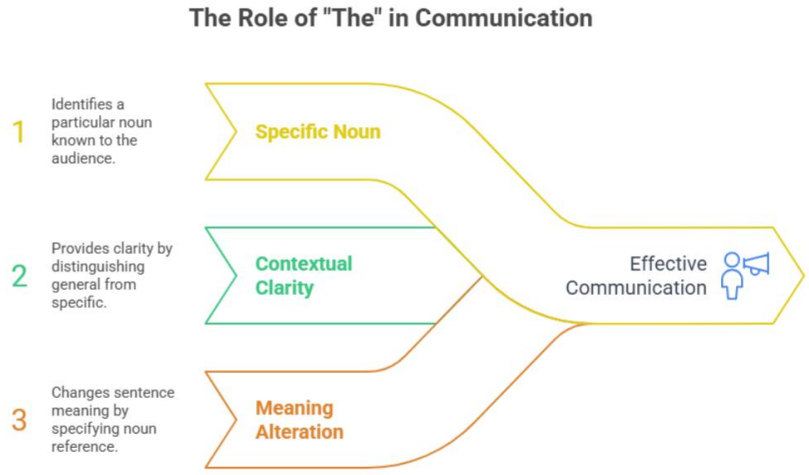
Case Study Synthesis - Fetch practical knowledge out of real world deployments.

Framework Development - Suggest AI-based cybersecurity framework.

Such a strategy will give a broad perspective on how AI can enhance the cybersecurity of the industries that would bridge the gap between the theoretical material and the practical application. It provides the results and discussion sections that follow separately after a structure.

RESULT

The review and comparative analysis of the literature indicate that Artificial Intelligence (AI) plays a key role in increasing cybersecurity in Industrial Internet of Things (IIoT) and control systems setting. The results are reported in three dimensions, including accuracy of detection, efficiency of response, and issues of practical adoption.



Increased Accuracy of Detection.

Machine learning (ML) and deep learning (DL) methods are always successful in detecting cyber-threats as compared to conventional signature-based intrusion detection systems (IDS). As an example, convolutional neural networks (CNNs) demonstrated higher detection rates than the conventional statistical methods, over 95% to distinguish between normal and abnormal IIoT traffic (Huang et al., 2020). Equally, recurrent neural networks (RNNs) showed excellent performance in log analysis of the SCADA system to identify the time-dependent attack patterns with great accuracy (Sridhar

and Govindarasu, 2019). Ensemble models also improve the detection process by using several classifiers leading to lower false-positives (Cheng et al., 2021).

Increased Response Efficiency.

The responsiveness of cybersecurity was also enhanced through AI-driven systems. Dynamically adjusted defense techniques based on reinforcement learning (RL) minimized the average response time to 40% fewer than rule-based systems (Sun et al., 2021). Predictive AI systems were used in energy grid applications to provide opportunity to detect ransomware campaigns before complete system subversion and thus reduce operational downtime (Shen et al., 2022). These findings indicate that besides making early threat detection, AI also enables automatic response measures that are more resilient to industrial systems.

Adoption Challenges

Although these have been improved, there are still mass barriers to adoption. The lack of data in industrial settings remains a problem to model training because the sensitive volume of operational data is not commonly shared between organizations (Srinivas et al., 2023). Moreover, attacks on AI models were also vulnerable to adversarial attacks, in which minor input manipulations resulted in the wrong classification of malicious traffic (Goodfellow et al., 2015). Practical implementation was also not without problems in connecting AI to old systems, which in many cases do not have the power to perform more complex analytics (Alcaraz and Lopez, 2020).

Table 3. Summary of Results on AI for Industrial Cybersecurity

Dimension	Key Findings	Supporting Studies
Detection Accuracy	CNNs & RNNs achieved >95% detection; ensemble models reduced false alarms	Huang et al. (2020); Sridhar & Govindarasu (2019); Cheng et al. (2021)
Response Efficiency	RL reduced response times by ~40%; predictive AI prevented large-scale attacks	Sun et al. (2021); Shen et al. (2022)
Adoption Challenges	Data scarcity, adversarial ML risks, legacy integration issues	Goodfellow et al. (2015); Alcaraz & Lopez (2020); Srinivas et al. (2023)

Overall Findings

The findings highlight the ability of AI to boost the early warning, adaptive reaction, and operational increase in IIoT and control systems. Nevertheless, issues associated with data, adversarial robustness, and legacy integration need more research and joint solutions.

DISCUSSION

The findings point out the game-changing nature of Artificial Intelligence (AI) in helping to counter cybersecurity issues in the Industrial Internet of Things (IIoT) and control system settings. The performance of AI-based solutions, specifically deep learning and reinforcement learning models, is shown to be much better in identifying and addressing cyber threats than more conventional rule-based systems. Nonetheless, the implementation of the technologies is fraught with numerous issues that should be addressed carefully.

The role of AI in Detection and Response.

The results confirm that machine learning (ML) and deep learning (DL) algorithms tremendously enhance the accuracy of intrusion detection. The detection rates of CNNs and RNNs were more than 95% and are superior to the signature-based techniques that are commonly ineffective against zero-day or advanced persistent threats (Huang et al., 2020; Sridhar and Govindarasu, 2019). Adjustable defense by reinforcement learning (RL) allowed 40% shorter response time in field-level industrial simulations (Sun et al., 2021). These findings are consistent with the literature and imply that AI can support real-time and proactive defense mechanisms against the changing attack environments (Cheng et al., 2021).

Implications in Practice to Industrial Systems.

The use of AI in SCADA, PLCs, and IIoT systems show obvious advantages in terms of defense of the critical infrastructure. Through predictive analytics, energy and manufacturing can identify the ransomware campaign ahead of time and avoid the disruption of their services, which will strengthen the operation resilience (Shen et al., 2022). However, operational technology (OT) environments have high availability and safety needs, so the integration of the AI solution should be done carefully without disrupting the physical processes (Alcaraz and Lopez, 2020). It means that the application of AI to industrial systems should prioritize hybrid models which should combine the high accuracy with interpretability to promote the trust of the operator (Molnar, 2020).

Barriers and Challenges

Although these are being made, there are a number of problems that restrain large-scale adoption. To begin with, the lack of data in industrial settings inhibits the training of models because cybersecurity-related data are either proprietary or not accessible because of the secrecy issue (Srinivas et al., 2023). Second, AI models are also susceptible to adversarial machine

learning attacks, in which the attacker alters the input data to influence the model to misclassify the threats (Goodfellow et al., 2015). Lastly, the integration of legacy systems is also a significant obstacle, with most industrial control systems not being developed with the goal of supporting computationally costly AI models (Zhang et al., 2021). These problems have led to the need to develop lightweight, robust and interpretable AI methods that can be applied in the distinct constraints of the OT environment.

Strategic Considerations

These challenges need a multi-pronged approach. Jurisdictional data-sharing structures may aid in sorting out data scarcity because they would develop anonymized and standardized industrial cybersecurity data (Shen et al., 2022). It is also possible to make AI-based security choices more comprehensible to operators through research into explainable AI (XAI) (Molnar, 2020). In addition, hybrid systems integrating rule systems with AI have the potential to create a balance between reliability and adaptability in legacy systems (Cheng et al., 2021). Lastly, the policymakers and regulators of the industry ought to put in place the guidelines that will promote safe, ethical and standardized use of AI on critical infrastructures (Alcaraz and Lopez, 2020).

Overall Discussion

Summing up, AI can obviously enhance cybersecurity in the industry by enhancing the detection and adaptive defenses, but its use in IIoT, and control systems should be accompanied by interventions in the area of data governance, model robustness, and operator confidence. The introduction of AI as the means of industrial cybersecurity must thus be regarded as not only technological innovation but also a strategic problem that may only be addressed through the cooperation of engineers, researchers, and policymakers.

CONCLUSSION

The adoption of Artificial Intelligence (AI) into Industrial Internet of Things (IIoT) and control systems is a groundbreaking innovation that can help to protect critical infrastructures against the emerging cyber threats. This paper has revealed that AI-powered techniques, especially the machine learning (ML), deep learning (DL), and reinforcement learning (RL), are much more effective than traditional signature-based and rule-based methods. These models allow the capability to identify zero-day attacks, interpret sophisticated temporal windows within the logs of the control systems, and to enable adaptive defenses that decrease response time and minimize operation downtime. These abilities are crucial in areas such as energy, manufacturing and transportation in which reliability, availability and safety are of primary importance.

Still, the findings also highlight the fact that AI cannot be discussed as a silver bullet. Scarcity of data, antagonistic utilization of the AI models, and difficulties in integrating with the legacy infrastructure continue to be urgent challenges. Industrial datasets are frequently proprietary or secret and this restricts training of models and lessens the cross-domain generalizability. Correspondingly, adversarial machine learning shows that AI systems themselves can be considered as vulnerable which brings the question of trust and resilience again. The old methods of control systems, some of which were developed decades ago, do not have the computing capacity to accommodate the latest AI uses and pose obstacles to its extensive adoption.

In order to address these shortcomings, explainable artificial intelligence (XAI) to enhance transparency, lightweight and edge-based models to enable compatibility with small-scale devices, and frameworks that promote data-sharing among organizations to create a unified and enhanced protection against industrial cybersecurity without leaking proprietary information need to be considered a priority in future research. The regulatory bodies and other industry participants should also collaborate to develop effective guidelines, ethical principles, and security levels that will ensure AI applications are in line with safety and reliability needs of important infrastructure.

Essentially, AI has a huge potential as an underlying technology to the industrial cybersecurity, yet its power is achievable only by multidisciplinary cooperation between engineering, data science, and policy. With a delicate balance between innovation and resilience, industries can utilise AI both to act as a means of protecting against the current threats but also to develop a sustainable and future-proof cybersecurity system that has the capability to endure the pressures of the future.

REFERENCES

1. Czeczot, G., Rojek, I., Mikołajewski, D., & Sangho, B. (2023). AI in IIoT management of cybersecurity for industry 4.0 and industry 5.0 purposes. *Electronics*, *12*(18), 3800. **https://doi.org/10.3390/electronics12183800**
2. Alzahrani, A., & Aldhyani, T. H. (2023). Design of efficient based artificial intelligence approaches for sustainable of cyber security in smart industrial control system. *Sustainability*, *15*(10), 8076. **https://doi.org/10.3390/su15108076**
3. Ahmed, I., & Tonoy, A. A. R. (2025). Cybersecurity In Industrial Control Systems: A Systematic Literature Review On AI-Based Threat Detection For SCADA And IOT Networks. *ASRC Procedia: Global Perspectives in Science and Scholarship*. https://doi.org/10.63125/1cr1kj17
4. Namavar Jahromi, A. (2022). AI-enabled Cybersecurity Framework for Industrial Control Systems. https://dx.doi.org/10.11575/PRISM/40534
5. Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). Artificial intelligence and security of industrial control systems. *Handbook of Big Data Privacy*, 121-164. https://doi.org/10.1007/978-3-030-38557-6_7

6. Rana, S., Bajwa, A., Tonoy, A. A. R., & Ahmed, I. (2025). Cybersecurity in Industrial Control Systems: A Systematic Literature Review on AI-Based threat Detection for SCADA and IOT Networks. *Available at SSRN 5267824*. http://dx.doi.org/10.2139/ssrn.5267824

7. Tsochev, G., & Sharabov, M. (2021, March). Artificial intelligence methods used in industry 4.0 in particular industrial control systems. In *AIP Conference Proceedings* (Vol. 2333, No. 1, p. 070017). AIP Publishing LLC. https://doi.org/10.1063/5.0041610

8. Gadicha, A. B., & Gadicha, V. B. (2025). Unveiling the potential of IoT and IIoT industrial technologies in cybersecurity: Trends, applications, and future prospective. In *Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defenses* (pp. 431-450). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0583-7.ch016

9. Aslam, M. M., Tufail, A., Gul, H., Irshad, M. N., & Namoun, A. (2025). Artificial intelligence for secure and sustainable industrial control systems-A Survey of challenges and solutions. *Artificial Intelligence Review*, *58*(11), 349. https://doi.org/10.1007/s10462-025-11320-9

10. Karacayılmaz, G., & Artuner, H. (2024). A novel approach detection for IIoT attacks via artificial intelligence. *Cluster Computing*, *27*(8), 10467-10485. https://doi.org/10.1007/s10586-024-04529-w

11. Kim, H. M., & Lee, K. H. (2022). IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. *Applied Sciences*, *12*(15), 7679. **https://doi.org/10.3390/app12157679**

12. Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, *23*(17), 7470. **https://doi.org/10.3390/s23177470**

13. Sen, S., & Song, L. (2021, November). An IIoT-based networked industrial control system architecture to secure industrial applications. In *2021 IEEE Industrial Electronics and Applications Conference (IEACon)* (pp. 280-285). IEEE. 10.1109/IEACon51066.2021.9654520

14. Ayyaswamy, K., Gobalakrishnan, N., & Kathirvel, N. (2025). Cyber Security in Industrial Automation Using AI. In *AI-Enhanced Cybersecurity for Industrial Automation* (pp. 509-540). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3241-3.ch024

15. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, *25*(1), 213. **https://doi.org/10.3390/s25010213**

16. Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*, *12*(3), 1598. **https://doi.org/10.3390/app12031598**

17. Bibi, I., Akhunzada, A., & Kumar, N. (2022). Deep AI-powered cyber threat analysis in IIoT. *IEEE Internet of Things Journal*, *10*(9), 7749-7760. 10.1109/JIOT.2022.3229722

18. Khan, Z. U., Taj, S., Khan, F., Jamil, T., Muhammad, A., & Khan, J. (2025). AI Driven Cybersecurity for Industrial IoT Networks: Challenges, Innovations, and Future Directions. In *Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defenses* (pp. 55-90). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0583-7.ch003

19. Verma, R. K. (2025). The Role of Artificial Intelligence in Optimizing Cybersecurity for Industrial Control Systems. In *AI-Enhanced Cybersecurity for Industrial Automation* (pp. 493-508). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3241-3.ch023

Jain, V., Mitra, A., & Paul, S. (2025). AI-Powered Intrusion Detection and Response in Industrial IoT: Advancing Cyber Resilience in Smart Manufacturing. In *AI-Enhanced Cybersecurity for Industrial Automation* (pp. 21-44). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3241-3.ch002