Chapter 24
Cyber Security in Industrial Automation Using AI

Kathirvel Ayyaswamy
https://orcid.org/0000-0002-5347-9110
Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, India

N. Gobalakrishnan
https://orcid.org/0000-0003-3820-6744
Saveetha Engineering College, Chennai, India

Naren Kathirvel
Anand Institute of Higher Technology, India

ABSTRACT

As industries adopt digital technologies like the Internet of Things (IoT) and Industrial Control Systems (ICS), the vulnerability of these systems to cyberattacks has increased, making traditional cybersecurity measures insufficient. AI enhances industrial cybersecurity by leveraging machine learning algorithms for anomaly detection, enabling predictive analytics to forecast potential vulnerabilities, and automating incident responses for faster mitigation of threats. Additionally, AI improves malware detection through behavioral analysis, complementing signature-based approaches, and streamlining routine security tasks. The predictive capabilities of AI enable organizations to proactively address risks, ensuring that critical infrastructure remains secure. As a result, AI significantly bolsters the security posture of industrial systems, providing adaptive and scalable solutions to the challenges posed by modern cyber threats.

1. INTRODUCTION

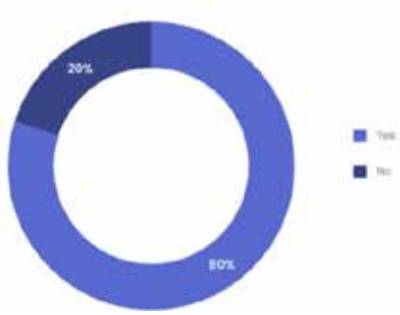
We are currently witnessing the shift of AI in industrial cybersecurity from being a mere curiosity to an essential component. The rapid integration of Operational Technology (OT) and Information Technology (IT) has significantly transformed industrial settings, making them more digital and interconnected. While this digital transformation fosters innovation and boosts efficiency, it also opens up new and broader attack surfaces. In response to these challenges, AI has become an invaluable tool for

DOI: 10.4018/979-8-3373-3241-3.ch024

cybersecurity professionals, providing advanced capabilities in threat detection, risk management, and automated responses.

However, the adoption of AI is not without its challenges. It introduces its own set of risks that must be carefully managed. Leaders must thoroughly evaluate how AI fits into their cybersecurity strategy, ensuring it strengthens rather than complicates their security posture. A recent industry-wide survey revealed some surprising findings many organizations still underestimate the cyber risks they face (Wang et al. 2022). Figure 1 shows the benefits of AI cybersecurity. This highlights that while AI offers substantial potential, its integration must be approached with caution, ensuring it effectively addresses the ever-evolving threat landscape.

Figure 1. Potential benefits of AI in cybersecurity



For those looking to explore or expand their use of AI in industrial cybersecurity, I strongly recommend downloading the free Decision Point Report. This resource offers an in-depth strategic analysis of the current AI landscape and provides teams with the insights needed to make well-informed decisions.

1.1 The Role of AI in Industrial Cybersecurity: Where Opportunity and Complexity Converge

AI has rapidly emerged as a game-changer in the cybersecurity field, particularly in industrial environments where OT and IT converge. Figure 2 depicts industrial cybersecurity. With its ability to process large volumes of data in real-time and learn from patterns, AI can offer unmatched insights into potential threats that might go unnoticed by human teams.