Chapter 16
AI-Driven Cybersecurity in Industrial Automation:
Navigating Ethical and Legal Complexities

Himanshu Tyagi
https://orcid.org/0009-0001-8435-9832
Quantum University, India

Pawan Kumar Goel
https://orcid.org/0000-0003-3601-102X
Raj Kumar Goel Institute of Technology, Ghaziabad, India

Parul Tyagi
https://orcid.org/0009-0001-6710-3608
Quantum University, India

Himani Tyagi
https://orcid.org/0000-0002-5005-9954
Quantum University, India

ABSTRACT

The convergence of artificial intelligence (AI) and industrial automation is reshaping the cybersecurity landscape. As smart factories, intelligent control systems, and interconnected infrastructures become widespread, AI offers powerful tools for detecting, preventing, and responding to cyber threats in real time. However, this advancement also introduces challenges such as algorithmic bias, opaque decision-making, legal complexities, and emerging attack vectors. This work explores AI's dual role in enhancing and complicating cybersecurity within industrial settings. It examines the expanding digital attack surface driven by IoT integration, SCADA system vulnerabilities, and autonomous technologies. Using real-world examples, it highlights both the strengths and limitations of AI in threat mitigation, emphasizing the urgent need for transparency, human oversight, and ethical alignment in deploying AI-driven security solutions.

DOI: 10.4018/979-8-3373-3241-3.ch016

1. INTRODUCTION

1.1. Overview of Industrial Automation

Industrial automation presents a significant and an important advancement in manufacturing and production systems. This positive transition has been from the manual control and oversight to the smooth and uninterrupted combination of advanced technologies, including robotics, programmable logic controllers (PLCs), and real-time data monitoring. These enlightened systems are tailored to boost the productivity levels, bolster safety, minimize human error, and minimize the operational efficiency.

From self-propelling assembly lines to reagent processing plants, industrial automation has become the key principle of indispensable infrastructure. As the complexity of these environments has, there is an urgent need for improved coordination among machines, sensors, and control systems. This control and coordination is worked out through communication protocols such as SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems).

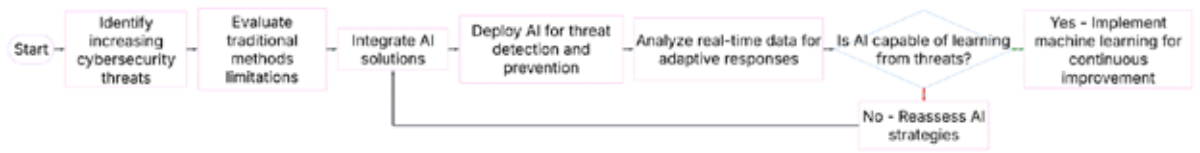
With the growing demand of concomitant systems—predominantly due to the materialization of the Industrial Internet of Things (IIoT)—the landscape for cyber threats has expanded in a considerate amount. This evolution gives new challenges for security and compliance within industrial settings (Bakhshi, 2020).

1.2. Rise of AI in Cybersecurity

The linked combination of Artificial Intelligence (AI) into the field of cybersecurity which the aim of industrial automation has seen a positive shift in how organizations safeguard their systems. Traditional cybersecurity methods, as static rule-based firewalls and signature-based detection, have problem to keep them on track with the speed, scale, and futuristic threats—mainly in dynamic industrial environments.

AI technologies, such as machine learning (ML), deep learning, and natural language processing (NLP), have come to the fore as redoubtable tools for detecting deviations, predicting attacks, automating response actions, and identifying zero-day dangers. In the dominion of industrial automation, where uptime and precision have key important role, AI can convey real-time threat intelligence and adjustive defense mechanisms that unroll alongside emerging attack vectors (Cavoukian, 2009).

Figure 1. Evolution of AI in cybersecurity



However, the assimilation of AI into cybersecurity systems also initiates its own set of risks. These risks can be thought as data bias, model drift, adversarial manipulation, and a lack of explainability. These risks tell about the need of AI-driven security solutions not only from a tech viewpoint but also through the spectacles of governance, ethics, and compliance (Cavoukian, 2009).