Chapter 8
Industrial Control Systems (ICS) Security:
AI-Based Threat Detection and Prevention

Ayush Tripathi
https://orcid.org/0009-0007-6869-0588
Sharda University, India

Prashant Upadhyay
https://orcid.org/0000-0002-9257-9181
Sharda University, India

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

ABSTRACT

Industrial Control Systems (ICS) are crucial to modern infrastructure but remain susceptible to sophisticated cyber attacks due to legacy architectures, limited security patches, and increasing connectivity. The chapter presents AI-based solutions for enhancing ICS security through anomaly detection, intrusion prevention, and predictive threat modeling. Machine learning (ML) and deep learning (DL) algorithms, including supervised, unsupervised, and reinforcement learning approaches, are examined for their effectiveness in identifying zero-day attacks, network anomalies, and incident response automation. Artificial intelligence-based threat intelligence, drawing on real-time data from sensors, logs, and network traffic, increases proactive defense against advanced persistent threats (APTs). The chapter also discusses how AI is employed in safeguarding ICS components such as SCADA systems, programmable logic controllers (PLCs), and remote terminal units (RTUs).

INTRODUCTION

Industrial Control Systems (ICS) form the foundation of critical infrastructure, such as power grids, water treatment facilities, manufacturing plants, and transportation networks. They are traditionally designed for operational efficiency and reliability and have a tendency to focus on availability rather

DOI: 10.4018/979-8-3373-3241-3.ch008

than security. With increasing integration of ICS with modern IT networks and the Internet of Things (IoT), they have become the preferred target for cyber attacks. The appearance of sophisticated malware, insider attacks, and state-sponsored attacks uncovered vulnerabilities in legacy ICS designs that require complex security controls to prevent potential disruptions. A recent IEEE study highlights that legacy ICS architectures lack inherent security-by-design principles, making them susceptible to advanced persistent threats (APTs) (Ding et al. 2018). Traditional security controls such as firewalls and intrusion detection are incapable of countering these unique challenges due to the complex real-time behavior of ICS. This requires a transition towards AI-based security models that can anticipate and neutralize threats before they result in serious harm.

Artificial intelligence (AI) has emerged as a powerful tool in the cybersecurity world, offering scalable, adaptive, and intelligent defense against ever-evolving threats. AI techniques such as machine learning (ML) and deep learning (DL) are the best drivers in the ICS security environment as shown in Figure 1., as they enable automation of threat detection, anomaly detection, and predictive analytics. Research published in Springer demonstrates that ML-based anomaly detection systems can achieve over 95% accuracy in identifying ICS-specific attacks by analyzing network traffic patterns (Umer et al. 2022). These techniques enable real-time observation of network traffic, log information, and sensor data, helping organizations detect zero-day vulnerabilities, unauthorized access, and malicious activity. AI models are distinguished from legacy signature-based approaches in that they can learn patterns in data on an ongoing basis, improving their ability to detect sophisticated attacks and minimizing false positives. An MDPI study further validates that AI-driven threat intelligence reduces false positives by 40% compared to traditional methods, while enhancing detection rates for SCADA-specific exploits (Bellamkonda 2020). Further, threat intelligence powered by AI enables proactive identification of vulnerabilities in SCADA, PLC, and RTU, reducing the likelihood of disruption to business.