Chapter 4
Smart Intrusion Detection and Prevention for IIoT Using AI

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, Ghaziabad, India

ABSTRACT

With the growth in industrial automation, Industrial IoT (IIoT) systems become more vulnerable to cyber attacks, and intelligent Intrusion Detection and Prevention Systems (IDPS) are needed. This chapter delves into the ways in which AI improves IDPS by detecting and preventing security threats in real time. It discusses machine learning and deep learning models employed in network anomaly detection, such as decision trees, support vector machines, and neural networks. Main points of discussion are signature-based and anomaly-based detection, challenges in datasets, as well as in-field deployment. The chapter also outlines how IDPS powered by AI can adjust to emerging threats, minimize false positives, and integrate into prevailing cybersecurity architectures. Real-world applications of AI-fueled IDPS are illustrated through case studies, providing an insight into their effectiveness in securing IIoT infrastructures.

INTRODUCTION

As Industry 4.0 develops at breakneck speed and Industrial Internet of Things (IIoT) devices become widely used, industrial automation has become an integral part of contemporary manufacturing, energy, transport, and healthcare industries. IIoT allows end-to-end connectivity between actuators, sensors, and industrial control systems (ICS), enabling real-time information exchange and process optimization.

DOI: 10.4018/979-8-3373-3241-3.ch004

But as IIoT systems increase in size and complexity, they also make attractive targets for cyber attacks. Conventional security solutions, including firewalls and antivirus programs, cannot effectively resist sophisticated cyberattacks, and intelligent Intrusion Detection and Prevention Systems (IDPS) must be used. Artificial Intelligence (AI), specifically machine learning (ML) and deep learning (DL), has become an effective means to improve IDPS for IIoT applications. AI-based IDPS is able to examine enormous amounts of network traffic information, detect anomalies, identify known and unknown threats, and act proactively in real time. AI-based solutions differ from traditional signature-based detection where attacks have predefined patterns. AI-based solutions learn from information, become immune to new attacks as threats evolve, and their accuracy improves with time. Recent studies have demonstrated the effectiveness of AI-driven IDPS in detecting zero-day attacks and evolving threats, making them indispensable for securing IIoT ecosystems (ICTAACS et al. 2021). IIoT networks are very dynamic and usually deployed in distributed and resource-scarce environments. These systems are coupled with traditional industrial protocols and hence are exposed to cyberattacks that target unpatched vulnerabilities. IIoT systems also produce huge amounts of heterogeneous data, which renders manual security monitoring impossible. The growing number and complexity of cyberattacks require security mechanisms that can offer proactive defense instead of reactive measures. AI-based IDPS overcomes such limitations by learning from network behavior continually, identifying anomalies, and anticipating potential threats before they can actually harm the system.

The dependency on conventional IDPS, especially signature-based detection, is a major limitation in IIoT security. Signature-based systems excel at detecting known threats but cannot detect zero-day attacks and new intrusion patterns. Attackers often change malware signatures and use encryption methods to evade conventional security systems. AI-based anomaly detection models, on the other hand, examine network traffic, device behavior, and communication patterns to detect anomalies that can signal cyber threats. These models utilize supervised, unsupervised, and reinforcement learning methods to classify and neutralize attacks in real-time. A recent study highlights the superiority of unsupervised learning techniques in identifying novel attack patterns in IIoT networks, which traditional methods often miss (Choi et al. 2024). Another security challenge for IIoT is the excessive rate of false positives and false negatives associated with traditional IDPS solutions. False positives result when innocent activity is erroneously classified as malicious, resulting in pointless disruptions. False negatives result when true cyber threats are missed and the system is left vulnerable to attacks. AI-based IDPS mitigates such risks through its constant update of detection algorithms, using methods like autoencoders, Generative Adversarial Networks (GANs), and deep reinforcement learning to improve accuracy. Research has shown that GANs can significantly reduce false positives by generating synthetic data to train more robust detection models (Park et al. 2022). Through minimizing false alarms, AI-based systems optimize operational effectiveness and help security teams concentrate on true threats. Implementing AI-based IDPS in IIoT demands strong infrastructure to support massive-scale real-time data processing. Most industrial environments function in edge computing environments, where data is processed locally on IoT devices instead of being sent to centralized cloud servers. AI-driven IDPS solutions need to be edge computing optimized for low-latency detection and quick response to threats. Federated learning is proving to be an exciting solution in this area, enabling distributed devices to jointly train models without revealing raw data, thus strengthening privacy and security. A recent study on federated learning in IIoT security demonstrates its potential to enhance privacy while maintaining high detection accuracy (Chen et al. 2023).