Chapter 9
AI-Powered Intrusion Detection and Prevention System (IDPS) for Industrial IoT

Emmanuel Innocent Umoh
https://orcid.org/0009-0007-7918-8294
Sharda University, India

Hussaini Bishara
https://orcid.org/0009-0004-8734-2413
Sharda University, India

Amrita
https://orcid.org/0000-0001-6922-3403
Sharda University, India

ABSTRACT

The accelerated evolution of Industrial Internet of Things (IIoT) 5.0 brings human-centric automation, hyperconnectivity, and Artificial Intelligence (AI) based real-time data analytics. The growth presents cybersecurity challenges with an increased attack surface and advanced threats. Legacy Intrusion Detection and Prevention System (IDPS) are not scalable and lack the agility to deal with these threats. This chapter discusses AI-based IDPS through machine learning, deep learning, and FL to enable real-time threat detection. This chapter also mentions the importance of Explainable AI, blockchain, and edge AI in improving security. The future directions are quantum computing and light AI models, and this provides a roadmap to secure IIoT 5.0 against future cyber-attacks.

1. INTRODUCTION

Industrial Internet of Things (IIoT) revolutionized contemporary industries with high-end automation, data-driven decision making, and seamless integration of cyber physical systems. Through interconnection of industrial devices, sensors, and control systems via smart networks, IIoT improves efficiency, productivity, and scalability in the manufacturing, energy, healthcare, and logistics industries. The shift

DOI: 10.4018/979-8-3373-3241-3.ch009

from IIoT 4.0 to IIoT 5.0 is a massive technological upgrade, moving from machine-centric automation to a more human-centric and intelligent industrial ecosystem. IIoT 5.0 combines Artificial Intelligence (AI), 6G connectivity, edge computing, and blockchain to create a hyperconnected and self-optimizing industrial ecosystem. The wave of industrial innovation of the future focuses on improving real-time decision making, improving human machine collaboration, and promoting greater interoperability between industrial systems (Sowmya Anita, 2023; Dasari et al., 2024).

However, ever, the increasing complexity and interconnectedness of IIoT 5.0 pose new cybersecurity risks to the security and reliability of industrial networks. Conventional security models, such as traditional Intrusion Detection and Prevention System (IDPS), struggle to counter the dynamic and sophisticated nature of cyber-attacks in IIoT networks. Security vulnerabilities such as Distributed Denial-of-Service (DDoS) attacks, malware intrusion, zero-day exploits, and insider attacks are increasingly becoming popular with the massive attack surfaces offered by hyperconnected industrial networks. The convergence with smart industrial control systems, cloud infrastructure, and edge computing also contributes to security risks due to cyberattacks targeting more than one entry point and the spread of these in distributed IIoT systems (Radoglou Grammatikis, 2023; Usmani, Happonen, Watada, 2023).

One of the main drawbacks of conventional IDPS is that they are rule-based and signature-based threat detection technology, which are ineffective against adaptive cyberattacks. Conventional systems generate high False Positive (FP) and False Negative (FN), leading to inefficiencies in real-time threat detection and prevention. Further, the static nature of conventional IDPS makes them not suitable for IIoT 5.0 adaptive cybersecurity, where security threats change in real-time and need dynamic countermeasures. The non-scalability of conventional security models also makes them not suitable to be implemented in large scale IIoT systems, which require real-time, autonomous, and intelligent threat detection processes (Kumar et al., 2024). In view of these concerns, AI-based IDPS emerges as a necessary solution for improving security in IIoT 5.0. Unlike conventional security solutions, AI-based IDPS use Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) to automatically detect, analyze, and respond to cyber threats. Next-generation security systems in these AI-based IDPS learn from new patterns of attacks in real-time, thus adapting and maturing over time without human intervention. AI-based IDPS also employ mechanisms of Anomaly Detection (AD) to identify deviations from normal traffic, thus zero-day attacks and APTs can be identified early. Further, the use of Federated Learning (FL) in AI-based security systems provides decentralized and cooperative threat intelligence, thus improving the resilience of IIoT security systems without leaking data privacy (Radoglou Grammatikis, 2023).

Besides, AI-driven IDPS are synchronized with the character of IIoT 5.0 in the way that it coexists with blockchain, edge computing, and upcoming communication networks like 6G. Edge AI enhances security with the capability of sensing and reacting to threats in real-time at the edge of the network, cutting down response time and reducing the exposure of centralized security systems. Blockchain technology is also supportive of IIoT security with data integrity, tamper-proof security logs, and open authentication processes. As IIoT 5.0 evolves, the responsibility of AI-driven security systems will become even more imperative in safeguarding industrial ecosystems from oncoming cyber-threats with operational efficiency and resiliency (Dasari et al., 2024).

This chapter delves into the history of IIoT from its inception to the sophisticated capabilities of IIoT 5.0, highlighting the cybersecurity issues in the wake of hyperconnectivity and edge intelligence. This chapter also addresses the shortcomings of conventional IDPS to counter these security issues and presents AI-enabled IDPS as a new paradigm for IIoT security. Through the use of AI-driven automation, adaptive learning, and real-time AD, AI-enabled IDPS provide a strong, scalable, and self-enhancing security