Chapter 2
AI-Powered Intrusion Detection and Response in Industrial IoT: Advancing Cyber Resilience in Smart Manufacturing

Vishal Jain
https://orcid.org/0000-0003-1126-7424
Sharda University, India

Archan Mitra
https://orcid.org/0000-0002-1419-3558
Nitte Institute of Communication, India

Sanchita Paul
https://orcid.org/0009-0006-6437-3991
Neil Patel Digital India, India

ABSTRACT

The rapid adoption of the Industrial Internet of Things (IIoT) has transformed manufacturing through enhanced automation and productivity, but it has also broadened the cybersecurity attack surface. As threats grow more complex, traditional security solutions struggle to detect and mitigate intrusions in real time. This paper proposes an AI-powered intrusion detection and response framework specifically designed for smart manufacturing. Using machine learning and deep learning to analyze network traffic and device behavior, the system identifies anomalies linked to cyber threats. Edge computing and federated learning enable low-latency processing and privacy-preserving collaboration. A real-time adaptive response module dynamically isolates threats and updates defenses. Evaluated on a simulated smart factory testbed, the framework shows notable improvements in detection accuracy, speed, and reliability over conventional IDS approaches, supporting the development of resilient IIoT ecosystems.

DOI: 10.4018/979-8-3373-3241-3.ch002

1. INTRODUCTION

1.1 Background

The convergence of advanced digital technologies such as artificial intelligence (AI), cyber-physical systems (CPS), and the Industrial Internet of Things (IIoT) has given rise to the Fourth Industrial Revolution, commonly known as Industry 4.0 (Khujamatov et al., 2021). This new paradigm has transformed traditional manufacturing environments into smart manufacturing systems characterized by automation, real-time data exchange, and interconnectivity between machines, sensors, and control systems. By enabling predictive maintenance, optimized production flows, and improved decision-making capabilities, Industry 4.0 has significantly increased operational efficiency and productivity across industrial sectors (Zonta et al., 2020; Vijay et al., 2024).

At the core of this transformation lies the Industrial Internet of Things, a network of intelligent, interconnected devices and systems designed to collect, transmit, and analyze data within industrial environments. IIoT facilitates seamless communication between operational technology (OT) and information technology (IT) layers, empowering industries to make data-driven decisions and automate complex processes. However, this growing interconnectivity has also expanded the attack surface of industrial networks, making them increasingly vulnerable to cyber threats (Zhukabayeva et al., 2025).

Unlike conventional IT systems, industrial control systems (ICS) operate in real-time and often control critical infrastructure such as energy grids, transportation systems, and manufacturing plants. A successful cyberattack on such systems can lead to severe consequences, including prolonged downtime, loss of intellectual property, financial damage, environmental hazards, and even threats to human safety (Kayan et al., 2022; Bhamare et al., 2020). High-profile incidents such as the Stuxnet worm, the Triton malware, and ransomware attacks like WannaCry have demonstrated the devastating impact of cyber intrusions on industrial ecosystems (Ryan, 2021).

Traditional cybersecurity solutions, while effective in IT contexts, struggle to meet the unique demands of IIoT environments due to their dynamic nature, heterogeneous devices, and resource-constrained edge devices. This has prompted a growing need for adaptive, intelligent, and real-time cybersecurity frameworks tailored specifically for industrial automation settings (Kayan et al., 2022; Bhamare et al., 2020).

1.2 Problem Statement

Conventional intrusion detection systems (IDS) in industrial networks often rely on static, rule-based, or signature-based techniques that detect known attack patterns. While these approaches are useful for identifying previously encountered threats, they lack the agility to detect zero-day attacks, polymorphic malware, and subtle anomalies that evolve over time. The complexity and dynamic behavior of IIoT environments renders traditional IDS ineffective, resulting in high false positive rates and delayed threat detection. Therefore, there is an urgent need to develop intelligent IDS solutions that can learn from data, adapt to the changing nature of threats, and respond swiftly to minimize operational disruptions.

1.3 Research Aim and Objectives

- To identify and analyze key cybersecurity challenges in IIoT-based smart manufacturing systems.
- To design and develop an AI-powered intrusion detection framework for real-time threat detection.