Chapter 20
Machine Learning and Federated Learning in Industrial Cybersecurity

Rampelli Manojkumar
https://orcid.org/0000-0002-8141-0321
BVRIT HYDERABAD College of Engineering for Women, India

Sanivarapu Prasanth Vaidya
BVRIT HYDERABAD College of Engineering for Women, India

Prasanta Kumar Jena
https://orcid.org/0000-0002-5626-6241
BVRIT HYDERABAD College of Engineering for Women, India

Sarabu Ashok
https://orcid.org/0000-0002-5138-5524
BVRIT HYDERABAD College of Engineering for Women, India

Sandeep Dasari
Woxsen University, India

ABSTRACT

The integration of Artificial Intelligence and Machine Learning into industrial cybersecurity addresses the limitations of traditional methods against evolving cyber threats. This chapter explores supervised, unsupervised, and reinforcement learning techniques for threat detection, anomaly detection, and adaptive response mechanisms. It emphasizes Federated Learning (FL) as a privacy-preserving approach in the Industrial Internet of Things, enabling collaborative model training without data exposure. Ethical and legal challenges, including bias, accountability, and regulatory compliance, are analyzed to ensure responsible AI deployment. Case studies in automotive, energy, and industrial control systems demonstrate FL's effectiveness in predictive maintenance. Future trends such as Quantum AI and Explainable AI are discussed for enhancing cryptographic security and transparency. The chapter concludes with managerial implications for adopting AI-driven solutions, emphasizing privacy, and cross-industry collaboration to safeguard critical infrastructure in Industry 5.0.

DOI: 10.4018/979-8-3373-3241-3.ch020

INTRODUCTION

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into industrial cybersecurity represents a paradigm shift in how industries protect their critical infrastructure from evolving cyber threats. As industries increasingly adopt automation, digitization, and the Internet of Things (IoT), the attack surface for cybercriminals has expanded significantly. Industrial systems, such as power grids, manufacturing facilities, and oil refineries, are now more interconnected than ever, making them vulnerable to sophisticated cyberattacks that can lead to catastrophic failures. Traditional cybersecurity approaches, which rely on rule-based systems and signature-based detection methods, are no longer sufficient to counter these advanced threats. In contrast, AI-driven cybersecurity solutions offer proactive, adaptive, and real-time defence mechanisms that can predict, detect, and respond to cyber threats with unprecedented accuracy and speed.

This chapter explores the transformative role of AI and ML in industrial cybersecurity, highlighting the limitations of traditional approaches and the advantages of AI-driven solutions. It delves into the various ML techniques—supervised, unsupervised, and reinforcement learning (RL)—and their applications in threat detection, anomaly detection, and adaptive cybersecurity. Furthermore, the chapter examines the ethical and legal challenges associated with AI in cybersecurity, including issues of accountability, bias, data privacy, and regulatory compliance. The discussion also extends to emerging technologies such as Federated Learning (FL), which enables privacy-preserving AI models in the Industrial Internet of Things (IIoT), and the integration of Quantum AI and Explainable AI (XAI) in cybersecurity frameworks.

Contributions of the Chapter

This chapter makes several key contributions to the field of industrial cybersecurity:

1. Comparative Analysis of Traditional and AI-Driven Approaches: The chapter provides a detailed comparison between traditional rule-based cybersecurity methods and AI-driven approaches, highlighting the advantages of AI in terms of accuracy, speed, scalability, and effectiveness against zero-day attacks.
2. Comprehensive Exploration of ML Techniques: The chapter offers an in-depth exploration of supervised, unsupervised, and RL techniques, demonstrating their applications in threat detection, anomaly detection, and adaptive cybersecurity. It also discusses the strengths and limitations of each approach, providing insights into their suitability for different industrial contexts.
3. Ethical and Legal Considerations: The chapter addresses the ethical and legal challenges associated with AI in cybersecurity, including issues of bias, data privacy, accountability, and regulatory compliance. It emphasizes the need for transparent and fair AI systems and discusses the evolving regulatory landscape governing AI in cybersecurity.
4. Introduction to Federated Learning: The chapter introduces FL as a privacy-preserving approach to cybersecurity in IIoT, highlighting its benefits in terms of data privacy, regulatory compliance, and resilience against cyberattacks. Real-world case studies demonstrate the practical applications of FL in industrial cybersecurity.