RADemics

Machine Learning-Based Cybersecurity and Threat Detection Systems for Smart Engineering Networks

Saliha Bathool, Thejo Lakshmi Gudipalli
RV University Bangalore, Koneru
Lakshmaiah Education Foundation

Machine Learning-Based Cybersecurity and Threat Detection Systems for Smart Engineering Networks

[1]Saliha Bathool, Assistant Professor, School of Computer Science and Engineering, RV University Bangalore, Karnataka, India. salihabathool15@gmail.com

[2]Thejo Lakshmi Gudipalli, Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh, India. tejolakshmi.gudipalli@gmail.com

Abstract

Rapid digital transformation within smart engineering networks, driven by Industrial Internet of Things (IIoT) and cyber-physical integration, has introduced unprecedented connectivity alongside an expanded and highly dynamic attack surface. Conventional security mechanisms struggle to address sophisticated, multi-stage, and coordinated cyber-physical threats that exploit heterogeneity, scale, and real-time operational dependencies. This chapter presents a comprehensive examination of machine learning-based cybersecurity frameworks designed for intelligent threat detection in such environments. Emphasis is placed on advanced learning paradigms, including hybrid and ensemble models, which enhance detection accuracy and robustness by leveraging diverse data representations and decision strategies. Critical aspects such as intrusion detection system design, performance evaluation metrics, and the role of benchmark datasets in model validation are systematically analyzed to establish a strong methodological foundation. Key challenges involving data imbalance, limited availability of realistic datasets, adversarial vulnerabilities, and computational constraints in edge-centric deployments are critically discussed. The chapter also highlights emerging directions, including explainable artificial intelligence, federated learning, and adaptive security architectures, which collectively contribute to the development of resilient and scalable cybersecurity solutions. The presented insights aim to bridge the gap between theoretical advancements and real-world implementation, offering a structured pathway toward securing next-generation smart engineering infrastructures against evolving cyber threats.

Keywords: Machine Learning, Cybersecurity, Intrusion Detection Systems, Smart Engineering Networks, IIoT, Threat Detection.

Introduction

Rapid digital transformation across engineering domains has accelerated the adoption of smart engineering networks, where interconnected devices, intelligent control systems, and real-time analytics operate in a unified ecosystem [1]. Industrial Internet of Things (IIoT) technologies, cyber-physical systems, and advanced communication infrastructures have enabled seamless interaction between physical processes and computational intelligence [2]. Such integration

supports automation, predictive maintenance, and efficient resource management across sectors such as manufacturing, energy, transportation, and healthcare [3]. Increasing reliance on distributed architectures and cloud-edge collaboration has reshaped traditional operational models into highly dynamic and data-driven environments. Continuous data exchange among sensors, controllers, and analytics platforms has created opportunities for enhanced situational awareness and decision-making precision. Growth in connectivity has expanded the functional capabilities of engineering systems while introducing new dimensions of complexity [4]. Interoperability among heterogeneous devices and protocols requires robust coordination and synchronization mechanisms. Large-scale deployment of smart components has transformed isolated systems into interconnected infrastructures with global reach. Evolution of these networks reflects a shift toward intelligent ecosystems where autonomy and adaptability define system performance. Such advancements establish a foundation for innovation while simultaneously introducing challenges that demand advanced technological solutions [5].

Expansion of connectivity and system complexity has significantly increased exposure to cybersecurity threats within smart engineering environments. Attack surfaces have grown due to the integration of legacy systems, wireless communication channels, and internet-facing interfaces [6]. Malicious actors exploit vulnerabilities in protocols, software, and hardware components to disrupt operations, manipulate data, or gain unauthorized access [7]. Threats such as distributed denial-of-service attacks, data injection, ransomware, and advanced persistent attacks target both cyber and physical layers of the system. Compromise of sensor data or control commands can directly influence physical processes, leading to operational failures or safety hazards [8]. Real-time dependencies within these networks amplify the impact of even minor disruptions, creating cascading effects across interconnected subsystems. Critical infrastructures such as power grids and industrial automation systems face heightened risks due to their societal and economic significance [9]. Increasing sophistication of attack strategies reflects a transition from isolated incidents to coordinated and multi-stage campaigns. Traditional security mechanisms based on static rules and signature detection struggle to address evolving attack patterns. Complex threat landscapes require adaptive and intelligent defense strategies capable of responding to dynamic adversarial behavior [10].