RADemics

AI-Powered Cybersecurity Mechanisms for Intrusion Detection and Threat Intelligence in Smart Infrastructure Networks

K.P.Sangeetha, P.shasikala,
Madhavi Abhijit Mohite
ACS college of Engineering, Vishwakarma Institute of Technology

AI-Powered Cybersecurity Mechanisms for Intrusion Detection and Threat Intelligence in Smart Infrastructure Networks

[1]K.P.Sangeetha, Assistant professor, cyber security, ACS college of Engineering, Mail id:kpsangeetha20@gmail.com

[2]P.shasikala,Assistant professor / IOT, ACS college of engineering, Mail id: sasikalaglory123@gmail.com

[3]Madhavi Abhijit Mohite, Assistant Professor, Department of Engineering Sciences and Humanities, Vishwakarma Institute of Technology, Pune, Mail ID: Madhavi.mohite@vit.edu

Abstract

The rapid expansion of smart infrastructure networks and the proliferation of IoT devices have introduced unprecedented cybersecurity challenges, requiring advanced techniques for real-time threat detection and proactive defense. This chapter presents a comprehensive exploration of AI-driven methodologies for securing smart cities, industrial control systems, and interconnected IoT ecosystems. It examines the limitations of traditional security mechanisms in detecting sophisticated attacks such as advanced persistent threats, zero-day exploits, and ransomware, highlighting the critical role of artificial intelligence in enhancing network resilience. Key AI techniques, including machine learning, deep learning, hybrid models, reinforcement learning, and lightweight edge-based algorithms, are analyzed for their efficacy in intrusion detection, anomaly recognition, and adaptive threat prevention. The chapter also emphasizes AI-powered threat intelligence frameworks, incorporating big data analytics, natural language processing, knowledge graphs, and predictive modeling to enable multisource threat analysis and collaborative cybersecurity. Data acquisition, preprocessing, feature extraction, privacy-preserving aggregation, and handling of imbalanced datasets are presented as foundational steps for robust AI model development. Performance metrics, including accuracy, precision, recall, and latency, are discussed to ensure real-time and reliable detection in distributed and resource-constrained environments. By integrating theoretical foundations with practical applications, this chapter provides a roadmap for the development of intelligent, adaptive, and scalable cybersecurity systems tailored to the unique requirements of modern smart infrastructure.

Keywords: Smart Infrastructure, Artificial Intelligence, Intrusion Detection, IoT Security, Threat Intelligence, Predictive Modeling

Introduction

The rapid evolution of smart infrastructure networks has transformed urban landscapes and industrial operations, integrating IoT devices, sensors, and automated systems to optimize efficiency, resource utilization, and service delivery [1]. These interconnected systems generate

massive volumes of heterogeneous data, creating complex ecosystems that require continuous monitoring and management. While the digitalization of infrastructure enables advanced functionalities and real-time decision-making, it also introduces significant cybersecurity risks [2]. Attacks on such networks can compromise operational safety, disrupt essential services, and result in severe financial and societal consequences, necessitating advanced strategies for threat detection and mitigation [3, 4, 5].

Traditional cybersecurity mechanisms, including signature-based firewalls, antivirus solutions, and rule-driven intrusion detection systems, are insufficient in addressing the evolving threat landscape [6]. Advanced Persistent Threats, ransomware, and zero-day exploits employ sophisticated techniques to bypass conventional defenses, targeting both software and hardware vulnerabilities [7]. Static defenses fail to adapt to dynamic network behavior, leaving smart infrastructure exposed to emerging attack vectors [8]. The scale, heterogeneity, and distributed nature of IoT and industrial networks further complicate the implementation of conventional monitoring systems, highlighting the need for intelligent, adaptive approaches capable of real-time threat identification [9, 10].