RADemics

AI Powered Cybersecurity Frameworks for Intrusion Detection and Threat Intelligence in Smart Infrastructure

Manimaran M, S. Ranganathan, C. Gethara Gowri
EASWARI ENGINEERING COLLEGE, DEEMED TO BE UNIVERSITY, RAJALAKSHMI INSTITUTE OF TECHNOLOGY

AI Powered Cybersecurity Frameworks for Intrusion Detection and Threat Intelligence in Smart Infrastructure

[1]Manimaran M, Cyber Security/ Assistant Professor, Easwari Engineering College, 162, Bharathi Salai, Ramapuram, Chennai, Tamil Nadu 600089, Email ID: drmanimaranm@gmail.com

[2]S. Ranganathan, Professor /Department of Marine Engineering, Academy of Maritime Education and Training. Deemed to be University, Kanathur - 603112, Tamil Nadu, Chennai, Mail ID: ranganathan.s@ametuniv.ac.in

[3]C. Gethara Gowri, Assistant Professor, Computer Science & Engineering, Rajalakshmi Institute of Technology, Poonamalle, Chennai -600124, Mail ID: gowri.smak@gmail.com

Abstract

The exponential growth of smart infrastructure systems, encompassing critical sectors such as energy, transportation, healthcare, and urban management, has introduced a new era of operational efficiency and automation. The interconnected and dynamic nature of these systems has simultaneously exposed them to a wide array of evolving cyber threats. Traditional rule-based cybersecurity mechanisms are increasingly inadequate in addressing the complex, high-velocity, and adaptive attack patterns targeting smart infrastructure. In response to this challenge, the integration of Artificial Intelligence (AI) into cybersecurity frameworks has emerged as a pivotal advancement, enabling intelligent threat detection, contextual threat analysis, and proactive defense strategies. This chapter presents a comprehensive exploration of AI-powered cybersecurity frameworks designed for intrusion detection and threat intelligence in smart infrastructure environments. The discussion encompasses the foundational concepts of threat intelligence, the role of machine learning, deep learning, and reinforcement learning in real-time threat prediction, and the architectural evolution of context-aware and multimodal security systems. Emphasis is placed on low-latency AI implementations through edge and fog computing, ontology-driven threat modeling, and adaptive decision-making capabilities. The chapter examines current implementation challenges, such as data imbalance, model interpretability, adversarial robustness, and computational efficiency, while proposing strategies for their resolution. Through detailed technical analysis and synthesis of current research trends, this chapter contributes to the understanding and development of resilient, scalable, and intelligent cybersecurity solutions tailored for the demands of smart infrastructure. The insights offered are intended to guide future innovations in securing cyber-physical ecosystems against advanced and persistent threats.

Keywords: Smart Infrastructure, Threat Intelligence, Intrusion Detection, Artificial Intelligence, Edge Computing, Reinforcement Learning.

Introduction

The proliferation of smart infrastructure has significantly reshaped the landscape of modern digital ecosystems by enabling intelligent automation, real-time monitoring, and seamless communication between cyber-physical components [1]. These infrastructures span critical sectors such as energy, transportation, healthcare, utilities, and public administration, forming the backbone of contemporary urban and industrial environments [2]. Their operations are heavily dependent on interconnected systems that leverage IoT devices, cloud platforms, edge computing nodes, and big data analytics [3]. While these technologies contribute to operational efficiency and service personalization, they also introduce substantial vulnerabilities by expanding the attack surface and increasing exposure to both targeted and indiscriminate cyber threats [4]. As these systems evolve, so too do the tactics employed by cyber adversaries, necessitating a re-evaluation of conventional cybersecurity practices [5].

Traditional cybersecurity mechanisms, often based on static rule sets, predefined signatures, and manual threat analysis, are increasingly inadequate for protecting dynamic, heterogeneous smart infrastructures [6]. These methods lack the capability to recognize novel attack vectors, respond to emerging threats in real time, and adapt to contextual variations in system behavior [7]. The sheer volume, velocity, and diversity of data generated in smart systems render manual monitoring and rule-based intrusion detection inefficient and error-prone [8]. As attackers employ sophisticated techniques such as polymorphic malware, zero-day exploits, and multi-stage attack chains, the need for proactive, intelligent, and scalable security frameworks has become critical [9]. Current security infrastructures must be augmented with mechanisms that not only detect threats as they occur but also anticipate potential vulnerabilities based on behavioral trends and system anomalies [10].

Artificial Intelligence (AI) has emerged as a transformative technology in the realm of cybersecurity, offering advanced capabilities for learning, reasoning, and autonomous decision-making [11]. By leveraging machine learning, deep learning, and reinforcement learning algorithms, AI can analyze complex data streams to identify patterns, infer anomalies, and make predictions with minimal human intervention [12]. These capabilities are particularly valuable in the context of smart infrastructure, where real-time data processing and rapid response are essential for maintaining system integrity and continuity [13]. AI-powered intrusion detection systems can autonomously distinguish between benign and malicious activities, dynamically update threat models, and provide contextual intelligence that enhances the accuracy of detection and reduces false positives [14]. AI contributes to continuous monitoring, behavioral analysis, and attack prediction, enabling the creation of intelligent defense mechanisms tailored to the specific operational environment [15].