RADemics

Cybersecurity Challenges and AI-Powered Intrusion Detection

Raafiya Gulmeher, V. Srinivasan
KHAJA BANDANAWAZ UNIVERSITY,
DAYANANDA SAGAR COLLEGE OF ENGINEERING

Cybersecurity Challenges and AI-Powered Intrusion Detection

[1]Raafiya Gulmeher, Assistant Professor, Computer Science and Engineering, Khaja Bandanawaz University, Gulbarga, Karnataka, India. dr.raafiyagulmeher@gmail.com

[2]V. Srinivasan, Associate Professor, Department of Computer Applications, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India. srinivasan-mcavtu@dayanandasagar.edu

Abstract

The rapid advancement of cyber threats and the increasing complexity of network environments have necessitated the evolution of cybersecurity strategies, particularly in the realm of intrusion detection systems (IDS). Traditional IDS methods, such as signature-based and heuristic approaches, often fall short in identifying novel and sophisticated attacks in real-time. Artificial Intelligence (AI) and Machine Learning (ML) techniques have emerged as transformative tools, offering enhanced accuracy, adaptability, and scalability for intrusion detection. This chapter explores the application of AI-powered IDS, focusing on key advancements in real-time threat detection, scalability challenges, and hybrid AI models. The integration of ensemble methods and edge computing for reduced latency and improved performance is discussed, highlighting their potential in mitigating network vulnerabilities. Additionally, the chapter addresses the ethical implications of AI in cybersecurity, emphasizing the need for explainability and transparency in AI-driven decision-making processes. By examining current challenges and exploring cutting-edge solutions, this chapter provides a comprehensive overview of how AI can be leveraged to enhance cybersecurity defenses against evolving threats. The insights presented offer a roadmap for the future of AI-based intrusion detection systems, with significant implications for the security of both organizational and critical infrastructure networks.

Keywords: Intrusion Detection Systems, Artificial Intelligence, Machine Learning, Real-Time Threat Detection, Scalability, Hybrid AI Models.

Introduction

The rapid expansion of digital networks and the increasing reliance on interconnected devices have introduced a host of new opportunities and challenges in the field of cybersecurity [1]. As organizations and individuals become more dependent on digital technologies for communication, commerce, and daily activities, the risks associated with cyberattacks have grown exponentially [2]. From advanced persistent threats (APTs) to ransomware and insider threats, the landscape of cyber threats is increasingly diverse and sophisticated [3]. Traditional methods of intrusion detection, which rely on predefined attack signatures or heuristic algorithms, often fail to detect new, unknown, or rapidly evolving threats [4]. This limitation has led to the need for more intelligent, adaptable security systems capable of identifying and mitigating threats in real-time. The development of AI-powered intrusion detection systems (IDS) represents a significant breakthrough in cybersecurity, offering a more robust, efficient, and proactive defense mechanism [5].

AI and Machine Learning (ML) techniques provide the ability to process and analyze large volumes of data quickly, enabling the detection of complex attack patterns that might be overlooked by traditional security systems [6]. These technologies allow intrusion detection systems to learn from past data, adapt to emerging threats, and make more accurate predictions about potential vulnerabilities and attacks [7]. Unlike traditional systems that rely heavily on human input for rule creation and updating [8], AI-driven IDS continuously improve their detection models through unsupervised learning, allowing them to identify anomalous behavior without the need for explicit programming [9]. This dynamic adaptability is essential in a landscape where cybercriminals are constantly developing new methods to bypass conventional defenses [10].

The scalability of AI-powered IDS is another critical advantage in modern cybersecurity [11]. As organizations increasingly deploy cloud-based infrastructures and IoT devices, the volume and complexity of network traffic grow exponentially [12]. Traditional IDS systems struggle to handle this increased load, often resulting in slow detection and higher rates of false positives [13]. In contrast, AI-based systems can scale more effectively, processing large amounts of network data in real time while maintaining high detection accuracy [14]. By utilizing advanced machine learning algorithms such as ensemble methods and deep learning, these systems can simultaneously analyze multiple data streams and detect a wide range of attacks. This scalability ensures that AI-powered IDS remain effective even as networks expand and evolve, making them particularly well-suited for organizations operating in dynamic, fast-changing environments [15].