RADemics

AI-Based Cybersecurity and Predictive Intrusion Detection for Modern Digital Systems

J. Santhosh, B. Ramakantha Reddy
Sri Krishna Adithya College of Arts and Science,
Sri Venkateswara College of engineering

AI-Based Cybersecurity and Predictive Intrusion Detection for Modern Digital Systems

[1]J. Santhosh, Assistant Professor, Dept of Computer Applications, Sri Krishna Adithya College of Arts and Science, Coimbatore, India. santhoshj@skacas.ac.in

[2]B. Ramakantha Reddy, B. Tech, M. Tech. Ph. D, Associate Professor, Department of CSE (AI ML), Sri Venkateswara College of engineering, Tirupati, Andhra Pradesh, India. ramakanthareddy@gmail.com

Abstract

The rapid advancement of digital technologies has led to an unprecedented expansion of cyber threats, necessitating the evolution of cybersecurity solutions. Traditional methods of intrusion detection, primarily reliant on signature-based systems, are no longer sufficient to address the complexities and dynamic nature of modern cyber-attacks. Artificial Intelligence (AI), with its ability to learn from vast datasets, recognize patterns, and predict potential threats, offers a transformative solution to cybersecurity challenges. This chapter explores the integration of AI-driven predictive intrusion detection systems (IDS) in modern digital ecosystems, focusing on how machine learning, deep learning, and hybrid AI approaches can enhance threat detection and response capabilities. The chapter delves into the challenges associated with AI in cybersecurity, including resource limitations, the need for large-scale data, and the ethical considerations surrounding privacy and accountability. Special attention is given to data fusion techniques, which integrate multiple security data sources to improve model accuracy and reduce false positives. Furthermore, the role of transparency and accountability in AI decision-making is examined to ensure the ethical application of AI in security. As the digital threat landscape continues to evolve, AI-powered systems provide a proactive defense mechanism, moving beyond reactive strategies to anticipate and neutralize emerging risks in real-time. The chapter emphasizes the need for scalable, resource-efficient AI solutions to secure complex networks, such as IoT, cloud, and 5G environments, against increasingly sophisticated attacks.

Keywords: Artificial Intelligence, Predictive Intrusion Detection, Machine Learning, Deep Learning, Data Fusion, Cybersecurity.

Introduction

The rapid proliferation of digital technologies has revolutionized the way industries operate, creating an interconnected and data-driven world [1]. This digital transformation has also resulted in an exponential rise in cyber threats, which have become increasingly sophisticated and difficult to detect [2]. Traditional cybersecurity measures, such as signature-based intrusion detection systems (IDS), firewalls, and antivirus software, while effective against known threats, are inadequate in defending against novel, complex, or evolving attack vectors [3]. Cyber attackers continuously develop new methods to exploit vulnerabilities in digital systems, and the reliance on static, rule-based security frameworks has proven to be insufficient in addressing these dynamic and emerging risks [4]. Consequently, the need for advanced, adaptive, and proactive defense mechanisms has never been more critical [5].

Artificial Intelligence (AI) has emerged as a transformative tool in the cybersecurity domain, offering a paradigm shift from reactive to proactive threat detection and mitigation [6]. Unlike conventional methods, AI-based intrusion detection systems utilize machine learning (ML) and deep learning (DL) algorithms that can process large volumes of data, identify subtle patterns, and continuously adapt to new attack strategies [7]. These AI models are capable of detecting both known and previously unknown threats, providing a dynamic layer of defense that traditional systems cannot offer [8]. By learning from historical data, AI-driven systems can identify anomalies in network traffic, system behavior, or user actions, allowing for early detection of potential security breaches before they escalate into full-scale attacks [9]. This predictive approach significantly enhances the ability to prevent and mitigate damage, reducing the need for time-consuming manual interventions and strengthening the overall security posture of organizations [10].

One of the most promising aspects of AI in cybersecurity is its ability to integrate multiple sources of security data through techniques such as data fusion [11]. In complex, large-scale digital environments, such as cloud infrastructures, Internet of Things (IoT) networks, and hybrid systems, security data is generated across various endpoints and devices [12]. Traditional security systems often struggle to consolidate and analyze this data in real-time, leading to gaps in threat detection and response [13]. AI-powered predictive intrusion detection systems can seamlessly integrate data from various sources, including network traffic logs, system logs, user behavior data, and external threat intelligence feeds, providing a holistic view of potential threats [14]. By correlating these data points, AI models can recognize sophisticated attack patterns that span multiple layers of the network, offering a more comprehensive defense against multi-vector attacks and reducing the risk of undetected intrusions [15].