Automating AI in Cybersecurity: A Comprehensive Literature Review

Kashish Shah

Department of School of Technology, Pandit Deendayal Energy University, Gujarat, India

Prachi Radadiya

Department of School of Technology, Pandit Deendayal Energy University, Gujarat, India

Nishant Doshi

Department of School of Technology, Pandit Deendayal Energy University, Gujarat, India

Abstract:

The increasing complexity of cyber threats necessitates innovative strategies to safeguard digital assets and infrastructure, as traditional cybersecurity measures often fail to match the scale and sophistication of modern attacks. This research examines the transformative potential of automating Artificial Intelligence (AI) in cybersecurity, leveraging machine learning and data analytics for real-time threat detection, predictive vulnerability management, and automated incident response. Key advantages include faster response times, scalability, and enhanced resource efficiency. Unlike existing literature, this paper introduces novel strategies for integrating ethical frameworks and addressing algorithmic biases while ensuring transparency and accountability in AI-driven systems. By analyzing case studies and future trends, it highlights practical solutions to challenges such as adversarial attacks, data quality issues, and integration complexities. This paper provides actionable recommendations for fostering adaptive and resilient cybersecurity ecosystems, emphasizing the critical balance between technological innovation and ethical governance.

Keywords:

AI, Cybersecurity, Automation, Threat Detection, Incident Response.