IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, June 2024

Review on Adversarial Machine Learning in Cybersecurity: Evaluating Robustness and Vulnerabilities of Intrusion Detection Systems

Lanchi Jaiswal[1] and Dr. Savya Sachi[2]
Research Scholar, Department of CSE, Rajiv Gandhi Proudhyogiki Mahavidhyalaya Bhopal[1]
Associate Professor, Department of CSE, Rajiv Gandhi Proudhyogiki Mahavidhyalaya Bhopal[2]

Abstract: *Adversarial machine learning has emerged as a critical area of research in cybersecurity, particularly concerning the robustness and vulnerabilities of intrusion detection systems (IDS). This paper explores the landscape of adversarial machine learning within the context of cybersecurity, focusing on the challenges, techniques, and methodologies for evaluating the robustness and vulnerabilities of IDS. We delve into the mechanisms of adversarial attacks, analyze their impact on IDS performance, and discuss potential defense strategies. Additionally, we present experimental results and case studies to illustrate the effectiveness and limitations of current approaches in enhancing the resilience of IDS against adversarial threats.*

Keywords: Adversarial machine learning