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 7, March 2024

An Analytical Research on Adversarial Machine Learning in Cybersecurity

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: *This research investigates the vulnerabilities of IDSs to evasion attacks and poisoning attacks, and evaluates the effectiveness of existing defense mechanisms such as adversarial training, input validation, robust optimization, and ensemble methods. Theoretical analysis and empirical evaluation demonstrate the significant impact of adversarial perturbations on IDS performance, highlighting the need for more robust methodologies. While existing defenses provide improved robustness compared to baseline models, their performance still degrades under stronger attacks. The findings underscore the importance of securing training data and developing resilient defense strategies to mitigate AML threats in cybersecurity*

Keywords: Adversarial machine learning, intrusion detection systems, evasion attacks, poisoning attacks, adversarial training, robust optimization, ensemble methods, cybersecurity

Copyright to IJARSCT
www.ijarsct.co.in