IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, January 2025 Impact Factor: 7.67

Adversarially Robust Ensemble Models for Defending Against Evasion and Poisoning Attacks in IDS/IPS Systems

Arram Sriram[1] and Dr. Gyanendra Kumar Gupta[2]
[1]Research Scholar, Department of Computer Science and Engineering
[2]Supervisor, Department of Computer Science and Engineering
NIILM University, Kaithal, Haryana

Abstract: *Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play a critical role in safeguarding modern network infrastructures. However, the increasing adoption of machine learning (ML) in IDS/IPS has exposed them to adversarial threats such as evasion and poisoning attacks. This paper proposes an adversarially robust ensemble learning framework designed to enhance the resilience of IDS/IPS systems. By integrating diverse base learners, adversarial training, and anomaly-aware weighting mechanisms, the proposed model improves detection accuracy while maintaining robustness against adversarial manipulations. Experimental results demonstrate that the ensemble approach significantly outperforms traditional single-model IDS in both clean and adversarial environments.*

Keywords: Hybrid Models, Anomaly Detection, Zero-Day Attacks, Threat Detection