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 2, May 2024

Detection of Cyber Attacks and Network Attacks using Machine Learning Algorithms

Ajit Wagh[1], Ravindra Pawar[2], Nilesh Wable[3], Sanket Wandhekar[4], Prof. M. S. Dighe[5]
Department of Computer Engineering[1,2,3,4,5]
Adsul's Technical Campus, Chas, Ahmednagar, India

Abstract: *With the escalating sophistication of cyber threats and the increasing complexity of network infrastructures, traditional rule-based intrusion detection systems (IDS) are proving inadequate in safeguarding against modern cyber attacks. Consequently, the integration of machine learning (ML) algorithms has emerged as a promising approach to fortify network security by enabling proactive detection and mitigation of cyber threats. This review paper comprehensively explores the application of ML algorithms in detecting various forms of cyber-attacks and network intrusions.*

The review begins by outlining the fundamental concepts of cyber attacks and network intrusions, providing context for the subsequent discussion on ML-based detection methodologies. It surveys the landscape of ML algorithms employed in cybersecurity, ranging from classical techniques like Support Vector Machines (SVM) and Random Forests to more advanced methods such as deep learning and ensemble models.

Furthermore, the paper explains the diverse datasets utilized for training and evaluating ML-based intrusion detection systems, highlighting their significance in ensuring robust and generalizable models. Additionally, it examines the challenges and limitations associated with ML-driven detection, including issues of data scarcity, adversarial attacks, and model interpretability.

Keywords: Cyber Attacks, Machine Learning, Datasets, Detection

DOI: 10.48175/IJARSCT-18161