IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, May 2025
Impact Factor: 7.67

Detection of Intranet Attacks Based on Behaviour by Machine Learning

B. Meenakshi[1], H. Lasya[2], B. Hanumanth[3]
Assistant Professor, Department of IT[1]
B.Tech Student, Department of IT[2,3]
Mahatma Gandhi Institute of Technology, Hyderabad, India

Abstract: *Realm of cybersecurity, the detection of intranet attacks poses a significant challenge due to the evolving nature of malicious behaviors. This paper proposes an advanced approach for detecting behavior-based intranet attacks utilizing machine learning techniques. By leveraging the power of machine learning algorithms, the proposed approach aims to effectively identify and mitigate intranet attacks based on their behavioral patterns. Through the analysis of network traffic and system logs, the model learns to distinguish between normal and anomalous behaviors, thereby enabling proactive threat detection and response mechanisms. The proposed approach offers a promising avenue for enhancing the security posture of intranet environments by providing real- time detection capabilities and adaptive defense mechanisms. Its effectiveness is demonstrated through empirical evaluations and comparative analyses, highlighting its potential to augment existing cybersecurity frameworks and fortify intranet defenses against emerging threats.*

Keywords: Cybersecurity, intranet attacks, machine learning, behavior-based detection, anomalous behaviors, network traffic, system logs, threat detection, adaptive defense, real-time detection

DOI: 10.48175/568