IJARSCT

ISSN (Online) 2581-9429

IJARSCT

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 1, November 2024

An Efficient Network Intrusion Detection and Classification System using Machine Learning

Prof. Shashikant V Golande[1], Sanket Vaidya[2], Aniket Pardeshi[3],
Vivekanand Katkade[4], Vedant Pawar[5]
Department of Information Technology[1,2,3,4,5]
Sinhgad Institute of Technology Lonavala, Pune, India

Abstract*:* *In today's digital landscape, network security is of paramount importance, with intrusion detection systems (IDS) playing a crucial role in protecting sensitive data from malicious attacks. Traditional IDS, often reliant on signature-based methods, struggle with high false positive rates, difficulty in adapting to novel threats, and significant computational demands. This paper explores the development of an efficient network intrusion detection and classification system utilizing machine learning techniques to address these challenges. By leveraging datasets such as NSL-KDD and UNSW-NB15, our study employs a combination of supervised learning algorithms, including Support Vector Machines (SVM), Random Forests, and Neural Networks, alongside comprehensive data preprocessing and feature engineering strategies. The evaluation of our models through metrics like accuracy, precision, recall, and ROC-AUC demonstrates a marked improvement in detection capabilities and computational efficiency. Our findings suggest that machine learning-based IDS can significantly enhance network security by reducing false positives and adapting to emerging threats more effectively than traditional systems. This research not only underscores the potential of advanced machine learning techniques in IDS but also provides a robust framework for future developments in the field.*

In the rapidly evolving landscape of cybersecurity, effective network intrusion detection and classification systems are critical for safeguarding sensitive data and maintaining operational integrity. This paper presents a novel approach utilizing machine learning techniques to enhance the efficiency and accuracy of intrusion detection systems (IDS). By employing a combination of supervised and unsupervised learning algorithms, our system can identify and classify both known and unknown threats in real-time. We leverage advanced feature selection methods to optimize the performance of our models, ensuring high detection rates with minimal false positives. Our experimental results, validated on benchmark datasets, demonstrate significant improvements in detection accuracy and processing speed compared to traditional IDS solutions. The proposed system not only strengthens network defenses but also provides a scalable and adaptive framework for future cybersecurity challenges..

Keywords: Intrusion Prevention, Feature Selection, Real-time Detection, Threat Detection, Network Intrusion Detection

DOI: 10.48175/IJARSCT-22045