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 10, April 2025
Impact Factor: 7.67

Machine Learning Based Intrusion Detection System

Dr. Deepika Ajalkar[1], Vrushali Chavan[2], Pratiksha Bhosle[3]
Professor, Department of Computer Science and Engineering (Cyber Security)[1]
Student, Department of Computer Science and Engineering (Cyber Security)[2,3]
G H Raisoni College of Engineering and Management ,Wagholi, Pune, Maharashtra, India

Abstract: *With the exponential growth in the size and sophistication of cyber attacks, the security of digital infrastructures has emerged as a critical issue for organizations and individuals. Conventional Intrusion Detection Systems (IDS) mainly rely on signature-based methods, which are plagued by the inability to detect unknown or zero-day attacks. To address these limitations, this paper introduces a Machine Learning-Based Intrusion Detection System (MLA IDS) that can intelligently scan network traffic and classify it into normal or malicious categories. The system uses supervised learning algorithms — Random Forest, Decision Tree, and Support Vector Machine (SVM)—trained on benchmark datasets like NSL-KDD and CICIDS2017. The project involves several phases: data collection, preprocessing, model training, evaluation, and real-time detection. The experimental results show high accuracy, lower false positives, and good adaptability to new intrusion types. It is scalable to fit deployment across enterprise, cloud, or IoT networks and is a cutting-edge approach to defending against cybersecurity.*

Keywords: Intrusion Detection System, Machine Learning, Cybersecurity, Random Forest, SVM, NSL-KDD, CICIDS2017

DOI: 10.48175/IJARSCT-25679