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 5, June 2025
Impact Factor: 7.67

A Novel Technique for Malware Detection Analysis Using Hybrid Machine Learning Model

Vishal Borate[1], Dr. Alpana Adsul[2], Aditya Gaikwad[3], Akash Mhetre[4], Siddhesh Dicholkar[5]
Assistant Professor, Department of Computer Engineering[1]
Associate Professor, Department of Computer Engineering[2]
Department of Computer Engineering[3,4,5]
Dr. D. Y. Patil College of Engineering & Innovation Talegaon, Pune, India

Abstract: *The primary goal of this research is to improve existing malware detection methods by developing a robust and scalable model that can automatically identify malware through complex pattern analysis in both data and code. Unlike traditional signature-based techniques, which struggle to detect new and evolving threats, this approach leverages advanced machine learning techniques to enhance detection accuracy. Building on previous studies that have successfully applied machine learning for malware detection, this research integrates both supervised and unsupervised learning algorithms. Specifically, classification methods such as decision trees, random forests, and support vector machines (SVM)—which have demonstrated accuracies ranging from 85% to 95%—will be used alongside deep learning frameworks, including neural networks, which have achieved accuracy rates exceeding 96% in certain cases. By training these models on a comprehensive dataset containing both benign and malicious files, the aim is to enhance the model's ability to generalize and detect new, previously unknown malware variants. The effectiveness of the proposed model will be rigorously assessed using established benchmarks and key performance metrics such as accuracy, precision, recall, and false positive rates. This ensures that the system is reliable in real-time malware detection scenarios. This multi-faceted approach not only advances cybersecurity research but also builds on foundational work in the field, offering a more adaptive and proactive way to identify malware. By aligning with modern trends in machine learning and cybersecurity, this study seeks to create a more effective solution for combating emerging cyber threats*

Keywords: Machine Learning, Malwares, Analysis, Techniques, Risk Management, Algorithms, Framework, Malware Variants, Malware Classification

DOI: 10.48175/IJARSCT-27763