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, November 2024

Analysis of Malware Detection Using Various Machine Learning Approach

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 number one goal of this research is to decorate existing methodologies for malware detection via developing a robust and scalable version that robotically identifies malware via the analysis of difficult styles inside both records and code, moving beyond traditional signature-primarily based methods. constructing on previous studies that have efficaciously implemented more than a few devices getting to know techniques, this technique will integrate each supervised and unsupervised studying algorithm. especially, category strategies consisting of choice bushes, random forests, and help vector machines, which have validated accuracies starting from 85% to 95%, could be utilized along superior deep getting to know frameworks, which includes neural networks, which have said accuracies exceeding 96% in positive contexts. by means of education these fashions on an in depth and various dataset that consists of both benign and malicious files, this study aims to improve the version's generalization abilities, consequently allowing it to efficiently perceive new, previously unknown malware variants. The overall performance of the proposed model can be rigorously evaluated against installed benchmarks and metrics, consisting of accuracy, precision, bear in mind, and the false tremendous fee, making sure its efficacy in actual-time malware detection eventualities. This multifaceted technique not best seeks to develop the sphere of cybersecurity but also builds on the foundational paintings of others, offering a greater adaptive and proactive way of malware identification that aligns with present day developments in gadget studying and cybersecurity studies.*

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