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 1, July 2025
Impact Factor: 7.67

AI based Malware Detection

Prof. Parul Bhanarkar, Mansi Mahamuni, Snehal Jadhav
Professor, School of CSIT (Cybersecurity)
Student, School of CSIT (Cybersecurity)
Symbiosis Skills and Professional University, Kiwale, Pune

Abstract: *Malware remains one of the most prevalent and damaging forms of cyber threats today, compromising millions of devices globally. It can steal sensitive data, degrade system performance, encrypt critical files, and evade detection using advanced techniques. As malware continues to evolve rapidly, traditional detection methods often fall short, especially against previously unseen or zero-day variants. This growing challenge underscores the urgent need for intelligent, adaptive detection mechanisms. In response, this study proposes an advanced, AI-driven approach to malware detection that leverages dynamic deep learning and heuristic methods to identify and classify five prominent malware families: adware, Radware, rootkits, SMS malware, and ransomware. The paper reviews current detection technologies, highlights their limitations, and explores how artificial intelligence, particularly machine learning and deep learning, can enhance malware identification and response. Our analysis aims to guide future research in cybersecurity by advocating for self-learning, autonomous systems capable of handling real-time malware threats. By enhancing the resilience of digital infrastructures, AI-powered solutions can offer robust protection against the ever-growing sophistication of cyber-attacks, ensuring safer computing environments for users and organizations alike.*

Keywords: Malware Detection, Artificial Intelligence, Deep Learning, Heuristic Techniques, Cyber Security, Dynamic Analysis, Malware Classification.

DOI: 10.48175/IJARSCT-28402