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, April 2025
Impact Factor: 7.67

Android Malware Detection using ML

Prof. Mangala Patil[1], Poornima[2], Pradhipa S[1], Indu A[3], Reena K[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Impact College of Engineering and Applied Sciences (ICEAS), Bengaluru, Karnataka, India

Abstract: *Android devices are more prone of malware attacks due to its open-source nature. This makes it easier for installing applications from various sources, which can lead to major security issues. Machine learning learns from examples. It studies data from apps both good and bad and understands its characteristics. Using Machine Learning in this case can help identify harmful malware installed in android devices. Detecting unknown malicious code by applying classification techniques on Opcode patterns, checks the use of Opcode n-gram patterns from disassembled files. Previously studies have proved that utilizing 2-gram of Opcode patterns, term frequency representation, and selecting 200 plus features based on document frequency gives higher performance in detecting unknown malware. In traditional method s this was considered a complex task. This project is focused on addressing the challenges of detecting the Android malware using a machine learning based approach, which improves upon traditional signature-based methods. By focusing on feature-based inputs rather than requiring users to upload APK files, this system enhances both privacy and usability*

Keywords: Data collection, De-compilation, Feature extraction, Classification algorithms, Malware detection model

DOI: 10.48175/IJARSCT-24885