Impact Factor: 9.9 ISSN-L: 2544-980X

Comparative Evaluation of Static and Dynamic Malware Analysis for Android Using AI Techniques

Z. Rakhimov [1], M. Mukhtoriddinov [2], Q. Hudoynazarov [3]

Abstract: With the rapid proliferation of Android devices, the volume and sophistication of Android-based malware have increased significantly. Traditional signature-based detection systems are insufficient to combat evolving threats. This paper presents a comparative evaluation of two core malware detection approaches: static and dynamic analysis. Emphasis is placed on the integration of artificial intelligence (AI) techniques such as machine learning and deep learning within these analysis methods. We explore their advantages, limitations, performance metrics, and practical applicability, culminating in a comprehensive comparative assessment to inform researchers and security practitioners.

Keywords: Android malware, static analysis, dynamic analysis, machine learning, artificial intelligence, behavior analysis, hybrid detection.

Introduction. The Android operating system, being open-source and widely adopted, has become a primary target for malware developers. Malicious Android apps can lead to data leakage, unauthorized access, and service disruption. To combat such threats, static and dynamic analysis techniques have been developed, both increasingly augmented by AI technologies. Static analysis inspects app code and structure without execution, while dynamic analysis observes behavior during execution. The integration of AI enhances pattern recognition, classification accuracy, and zero-day malware detection.

Static Malware Analysis. Static analysis involves decompiling APK files and examining components like the AndroidManifest.xml, class files, and resource directories. Common static features include requested permissions, API call sequences, intent filters, and opcode n-grams. AI models, especially supervised machine learning classifiers like Support Vector Machines (SVM), Random Forests (RF), and Gradient Boosting, are trained using these features. Static analysis is efficient and can be deployed pre-installation, making it ideal for app marketplaces. However, it is vulnerable to code obfuscation, packing, and dynamic code loading techniques used by advanced malware.

Dynamic Malware Analysis Dynamic analysis monitors an application's runtime behavior in a sandboxed environment, capturing API calls, system logs, network traffic, and file operations. Tools like DroidBox and TaintDroid simulate real-world usage to observe hidden or delayed behaviors. AI techniques process behavioral logs to identify anomalies or malicious patterns. Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models are effective for modeling time-series behavioral data. Although dynamic analysis reveals runtime behavior resistant to obfuscation, it is resource-intensive and time-consuming, requiring controlled environments.

Table-1. Comparative Analysis

Criteria	Static Analysis	Dynamic Analysis
Execution Requirement	Not required	Required (in sandbox or emulator)
Speed	Fast	Slower due to execution overhead
Resource Usage	Low	High

[1] Fergana state technical university Assistant of the Department of Software Engineering and Cybersecurity
[2] Fergana state technical university Assistant of the Department of Software Engineering and Cybersecurity
[3] Fergana state technical university student of information security

Obfuscation Resistance	Low	High
Zero-day Detection	Medium with AI	High with behavior analysis
AI Techniques Applied	SVM, RF, Decision Trees, CNNs	RNNs, LSTMs, Behavioral Pattern Learning
Real-time Suitability	Suitable for app store scanning	Less suitable for large-scale analysis

This table highlights the strengths and weaknesses of each method. Static analysis is more scalable but less resilient to sophisticated threats, while dynamic analysis offers deeper behavioral insights at the cost of complexity.

AI has revolutionized malware detection by enabling data-driven, adaptive learning systems. In static analysis, deep learning models like Convolutional Neural Networks (CNN) can analyze opcode images or permission vectors. In dynamic analysis, LSTM-based models track behavioral sequences. Hybrid models combine both feature sets to leverage the speed of static analysis and the robustness of dynamic monitoring. Studies show hybrid models achieving accuracy rates above 97%, outperforming standalone approaches. Key challenges include evasion techniques (e.g., anti-emulation checks), high computational costs of dynamic analysis, and adversarial AI attacks. Future research may focus on lightweight AI models for on-device detection, explainable AI for transparency, and federated learning to enhance privacy. Furthermore, improved datasets and benchmarking standards are needed for fair evaluation.

Conclusion. Both static and dynamic analysis methods are vital for Android malware detection, and their effectiveness is significantly enhanced by AI techniques. Static analysis is faster and scalable, while dynamic analysis provides behavioral depth. A hybrid approach, supported by intelligent algorithms, represents the most promising solution for comprehensive and resilient malware defense.

References

1. Arp, D. et al. (2014). DREBIN: Effective and Explainable Detection of Android Malware. NDSS.
2. METHODS OF ASSESSING THE POSSIBILITY OF EXCLUSIONS IN INFORMATION PROTECTION KK Sadirova Best Journal of Innovation in Science, Research and Development 2 (12), 43-46
3. ТЕХНОЛОГИЧЕСКИЕ ИННОВАЦИИ И РАЗВИТИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ М Хусанова, Ш Ганиева, Х Садирова Conference on Digital Innovation:" Modern Problems and Solutions.
4. Sadirova, X. X. (2025). IDS ORQALI TARMOQDA BO ‘LADIGAN HUJUMLARNI AQINLASH USULLARI VA TAHLILI. Miasto Przyszłości, 56, 298-302.
5. Садирова, Х. Х. (2024). Ахборотни Ҳимоялашда Четлаб Ўтишнинг Мумкин Бўлган Эхтимоллик Холатини Бахолаш Усуллари. Miasto Przyszłości, 55, 195-201.
6. Turdimatov, M., Xusanova, M., Sadirova, X., Abdurakhmonov, S., & Bilolov, I. (2024, November). On the method of approximation and quantization of information transmission through communication channels. In E3S Web of Conferences (Vol. 508, p. 03007). EDP Sciences.
7. Xusanova, M. Q., & G'aniyeva, S. N. (2021). YURAK-QON TOMIR KASALLIKLARINI ELEKTROFIZIOLOGIK DIAGNOSTIKASI UCHUN RAQAMLI SIGNALLARNI QAYTA ISHLASH ALGORITMLARIDAN FOYDALANISH. Интернаука, (6-2), 93-94.
8. Qurbonaliyevna, X. M. (2024). TARMOQ QURILMALARIDA DEMILITARIZATSIYALANGAN ZONA (DMZ) NI SOZLASH ORQALI XAVFSIZLIKNI TA’MINLASH. Al-Farg’oniy avlodlari, (4), 236-239.