Smart Android Malware Detection Using Machine Learning and Evolutionary Techniques

Abstract:
The rapid expansion of Android applications and the availability of third-party app stores have made the Android platform the primary target for cybercriminals. Traditional malware detection methods, such as signature-based approaches, fail to detect zero-day and obfuscated malware variants. Machine learning has been increasingly applied for Android malware detection; however, single classifiers often suffer from reduced accuracy, high-dimensional redundant features, and outdated datasets. To address these challenges, this work proposes an intelligent malware detection framework that integrates genetic algorithm-based feature selection with an ensemble learning model optimized through evolutionary algorithms. In the proposed system, static and dynamic features of Android applications are extracted, and a genetic algorithm is employed to identify the most discriminatory features, reducing dimensionality and improving computational efficiency. Multiple machine learning classifiers, including Support Vector Machine, Neural Network, Decision Tree, Logistic Regression, K-Nearest Neighbor, and Boosting models, are used as base learners. Their outputs are combined using a Random Forest meta-learner, whose parameters are further optimized with a genetic algorithm to maximize detection performance. Experimental validation on recent Android malware datasets demonstrates that the proposed framework achieves high detection accuracy, precision, and robustness while effectively mitigating zero-day threats. This hybrid GA-optimized ensemble approach thus provides a scalable and efficient solution for securing the Android ecosystem against evolving malware.