ANALYSIS OF MALWARE IN ANDROID FEATURES USING MACHINE LEARNING

Paraphrase

The research paper is focused on the detection of Android malware using machine learning techniques. The methodology outlined in the text comprises several key steps. First, data is collected, including both malicious and benign Android apps. Various features, such as app components (e.g., Activity, Services) and permissions, are extracted from these apps.

Next, a Genetic Algorithm is employed to select the most effective set of features, with the goal of reducing the dimensionality of the feature set. This feature selection process aims to optimize the performance of two machine learning classifiers: Support Vector Machine (SVM) and Neural Network (NN). SVM and NN are chosen due to their capabilities in handling classification and regression problems, with SVM excelling in linear and nonlinear problem-solving.

The workflow involves uploading the Android malware dataset, splitting it into training and testing sets, and running SVM and NN algorithms on the selected features. Genetic algorithms are used to enhance feature selection and reduce the dataset size, resulting in faster model training.

The results of the research highlight the significance of detecting malware in Android, given the platform's open-source nature and susceptibility to malicious apps. The text emphasizes the importance of reverse-engineering Android APK files to extract static characteristics and permissions for analysis. The research demonstrates that SVM and NN achieve high accuracy in malware detection, with SVM utilizing genetic algorithms for feature selection, resulting in shorter execution times, albeit with a slight trade-off in accuracy.

The text provides insights into the steps of a genetic algorithm, including initialization, population generation, fitness scoring, parent selection, crossover, and mutation. Visual representations, in the form of graphs, are used to illustrate the accuracy and execution time of different algorithms, showcasing the balance between accuracy and computational efficiency.

In conclusion, the research underscores the critical need for accurate malware detection on Android devices, particularly as threats continue to evolve. Machine learning approaches, such as SVM and NN, combined with Genetic Algorithms for feature selection, offer promising solutions for combating Android malware while streamlining classifier complexity. Future work may involve larger datasets and exploring the impact of these techniques on other machine learning methods, further advancing the field of Android malware detection.

References:
https://www.engpaper.com/analysis_of_malware_in_android_using_machinelearinging.html
paper for IEEE research