# ABSTRAK

Perkembangan teknologi informasi saat ini telah membawa banyak kemajuan di berbagai bidang, termasuk pada perangkat bergerak yaitu *smartphone*. *Android* menjadi sistem operasi seluler yang mendominasi pasar dengan persentase 71,54% lebih besar dibandingkan sistem operasi lainnya pada September 2022. Seiring dengan tingginya jumlah pengguna *Android*, hal tersebut justru dapat menjadikan mereka sebagai target utama serangan *malware*. *Malware* merupakan perangkat lunak berbahaya yang dirancang untuk menyebabkan kerusakan pada sistem, mencuri data, dan mendapatkan akses tanpa izin pada suatu sistem. Berdasarkan ancaman tersebut, identifikasi dan analisis lebih dalam perlu dilakukan mengingat risiko dan dampak negatif yang ditimbulkan oleh serangan *malware* cukup besar. Pendekatan dengan algoritma *machine learning* dalam melakukan identifikasi *malware android*, menjadi fokus penelitian yang signifikan pada beberapa dekade terakhir. Penelitian ini akan berfokus pada klasifikasi serangan *malware android* berdasarkan analisis fitur dinamis menggunakan pendekatan algoritma *Random Forest.* Tahapan dalam penelitian meliputi *preparation data, preprocessing data*, pengembangan model dan evaluasi model. Performa model klasifikasi dengan algoritma *Random Forest* menunjukkan hasil yang sangat baik dengan mendapatkan nilai *accuracy, precision, recall,* dan *f1-score* sebesar 98%. Berdasarkan hasil evaluasi *confusion matrix*, dapat diambil kesimpulan bahwa model mampu mengidentifikasi setiap kelas atau kategori malware dengan baik, hal tersebut dapat dilihat dari nilai *True Positive* (TP) yang hampir seimbang dari setiap kelas.

**Kata Kunci:** *Android, Malware,* Klasifikasi, *Machine Learning*, *Random Forest*, *Confusion Matrix*.

## *ABSTRACT*

*The current development of information technology has brought many advances in various fields, including mobile devices, namely smartphones. Android is the mobile operating system that dominates the market with a percentage 71.54% greater than other operating systems in September 2022. Along with the high number of Android users, this can actually make them the main target for malware attacks. Malware is malicious software designed to cause damage to a system, steal data, and gain unauthorized access to a system. Based on these threats, deeper identification and analysis needs to be carried out considering that the risks and negative impacts posed by malware attacks are quite large. Approaches using machine learning algorithms in identifying Android malware have become the focus of significant research in the last few decades. This research will focus on classifying Android malware attacks based on dynamic feature analysis using the Random Forest algorithm approach. Stages in the research include data preparation, data preprocessing, model development and model evaluation. The performance of the classification model with the Random Forest algorithm shows very good results by getting accuracy, precision, recall and f1-score values of 98%. Based on the results of the confusion matrix evaluation, it can be concluded that the model is able to identify each class or category of malware well, this can be seen from the True Positive (TP) values which are almost equal for each class.*



***Keywords:*** *Android, Malware, Classification, Machine Learning, Random Forest, Confusion Matrix.*