INTISARI

PENGEMBANGAN SISTEM DETEKSI KEAMANAN APLIKASI ANDROID BERBASIS *MACHINE LEARNING* MENGGUNAKAN ANALISIS STATIK *ANDROID PERMISSIONS*

Steven Tanadi

21/477962/SV/19227

Ancaman yang dihadapi aplikasi Android terus berkembang dalam skala dan kecanggihan, membuatnya semakin sulit dideteksi. Hal ini mendorong kebutuhan solusi keamanan untuk menghadapi ancaman tersebut, seperti sistem deteksi keamanan untuk aplikasi Android berbasis *machine learning* menggunakan analisis statik *Android permissions* yang dirancang khusus untuk mengetahui tingkat keamanan beberapa aplikasi Android. Penggunaan *machine learning* penting dalam mendeteksi aplikasi Android yang berbahaya maupun aman karena kemampuan dalam membaca pola izin aplikasi Android dari puluhan ribu aplikasi berbahaya dan aman sehingga *machine learning* mampu membangun model prediksi dengan tingkat akurasi yang tinggi. Sistem deteksi keamanan ini bertujuan untuk memprediksi tingkat keamanan berkas aplikasi Android dalam jumlah banyak dan besar dengan akurasi tinggi yang memanfaatkan 3 model *machine learning* untuk memprediksi tingkat keamanan berkas aplikasi Android, yaitu *Random Forest, LightGBM,* dan *Extra Trees*. Hasil pengujian yang dilakukan oleh model *machine learning* menunjukkan adanya variasi tingkat akurasi prediksi pada setiap model yang digunakan. Berdasarkan hasil *testing accuracy*, model dengan akurasi tertinggi adalah *Random Forest* dengan akurasi 0,9758. Diikuti oleh *LightGBM* dan *Extra Trees* yang sama-sama memiliki akurasi 0,9755. Model *machine learning* kemudian di-*deploy* menggunakan *framework Streamlit* sebagai antarmuka *web* interaktif, yang terintegrasi dengan *Mobile Security Framework (MobSF)* untuk analisis statik serta *VirusTotal API* untuk validasi reputasi berkas. Hasil perbandingan ini menunjukkan bahwa penerapan *machine learning* tertentu mampu

meningkatkan efektivitas akurasi deteksi keamanan berkas aplikasi Android. Dengan adanya sistem ini, diharapkan pengguna dapat mengetahui tingkat keamanan berkas-berkas aplikasi Android sebelum dijalankan di dalam perangkat pengguna, memberikan perlindungan yang lebih baik terhadap potensi ancaman *malware*.

Kata kunci : Android, *malware detection*, keamanan aplikasi, *MobSF*, analisis statik, *machine learning*.

ABSTRACT

Development of a Machine Learning Based Android Application Security Detection System Using Static Android Permissions Analysis

Steven Tanadi
21/477962/SV/19227

The threats faced by Android applications continue to evolve in scale and sophistication, making them increasingly difficult to detect. This has led to the need for security solutions to address these threats, such as a machine learning-based security detection system for Android applications that uses static analysis of Android permissions specifically designed to determine the security level of several Android applications. Machine learning plays an important role in distinguishing malicious and benign Android applications by identifying permission patterns from tens of thousands of samples, thereby enabling the construction of highly accurate predictive models. The proposed system aims to predict the security level of large volumes of Android application files with high accuracy using three machine learning models: Random Forest, LightGBM, and Extra Trees. Experimental results show variations in prediction accuracy among the models, with Random Forest achieving the highest testing accuracy of 0.9758, followed by LightGBM and Extra Trees with 0.9755 each. The models were deployed using the Streamlit framework as an interactive web interface integrated with the Mobile Security Framework (MobSF) for static analysis and the VirusTotal API for reputation validation. The results demonstrate that employing appropriate machine learning models can improve the effectiveness and accuracy of Android application security detection, enabling users to assess the security level of Android applications before installation and providing better protection against potential malware threats.

Keywords: Android, malware detection, application security, MobSF, static analysis, machine learning.