RANCANG BANGUN APLIKASI ANDROID PENDETEKSI PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING

Faiz Daffa Makarim

ABSTRAK

Phishing merupakan salah satu ancaman keamanan siber yang terus berkembang. Di saat yang sama, banyaknya penggunaan perangkat Android sebagai media layanan digital meningkatkan risiko serangan *phishing*. Penelitian ini bertujuan membandingkan performa algoritma *Long Short-Term Memory* (LSTM), *Random Forest*, dan *Extreme Gradient Boosting* (XGBoost) dalam mendeteksi URL *phishing* serta menganalisis performa layanan aplikasi Android yang mengimplementasikan model *machine learning* tersebut. Evaluasi model dilakukan menggunakan metrik akurasi, presisi, *recall*, dan *Area Under Curve* (AUC). Performa layanan aplikasi dievaluasi dengan parameter *response time*, *error rate*, dan *throughput*. Hasil penelitian menunjukkan bahwa XGBoost memberikan performa terbaik dengan akurasi 95,05%, presisi 96,78%, recall 93,20%, dan AUC 0,9902. Dari sisi layanan sistem Android, sistem mampu menangani seluruh skenario pengujian dengan error rate 0% dan tetap memberikan hasil deteksi *phishing* secara stabil. Hasil penelitian menunjukkan bahwa integrasi *machine learning* pada aplikasi Android dapat digunakan secara efektif untuk mendeteksi *phishing* dengan tingkat akurasi tinggi dan performa layanan yang baik.

Kata Kunci : Android, Deteksi *Phishing*, LSTM, *Machine Learning*, *Random Forest*, XGBoost.

DEVELOPMENT OF AN ANDROID-BASED PHISHING DETECTION APPLICATION USING THREE MACHINE LEARNING ALGORITHMS

Faiz Daffa Makarim

ABSTRACT

Phishing is one of the continuously evolving cybersecurity threats. At the same time, the use of Android devices as a platform for digital services increases the risk of phishing attacks. This study compares the performance of Long Short-Term Memory (LSTM), Random Forest, and Extreme Gradient Boosting (XGBoost) algorithms in detecting phishing URLs and to analyze the service performance of an Android application implementing these machine learning models. Model evaluation was conducted using accuracy, precision, recall, and Area Under the Curve (AUC) metrics. The application's service performance was evaluated using response time, error rate, and throughput parameters. The results show that XGBoost achieved the best performance with an accuracy of 95.05%, precision of 96.78%, recall of 93.20%, and an AUC score of 0.9902. From the Android system service perspective, the application successfully handled all testing scenarios with a 0% error rate and consistently delivered stable phishing detection results. The findings indicate that the integration of machine learning into Android applications can be effectively utilized for phishing detection, providing high classification accuracy and good service performance.

Keywords : *Android, Machine Learning, Phishing Detection, LSTM, Random Forest, XGBoost.*