ABSTRAK

Serangan *phishing* merupakan ancaman siber dominan yang mengeksploitasi kelengahan pengguna, sementara metode deteksi konvensional berbasis *blacklist* sering terkendala latensi dan risiko privasi. Penelitian ini bertujuan mengembangkan sistem deteksi *phishing real-time* berbasis ekstensi Google Chrome yang bekerja sepenuhnya di sisi klien (*client-side*). Sistem mengadopsi pendekatan *hybrid machine learning* yang menggabungkan efisiensi *Logistic Regression* sebagai deteksi awal dan akurasi *Random Forest* untuk verifikasi lanjutan, menggunakan *dataset* PhiUSIIL dengan 22 fitur URL. Hasil eksperimen menunjukkan bahwa model *hybrid* berhasil meningkatkan akurasi deteksi dan meminimalkan *false negative* tanpa membebani kinerja peramban secara signifikan. Implementasi ini terbukti efektif memberikan peringatan dini yang akurat kepada pengguna, menawarkan solusi keamanan adaptif dan praktis bagi aktivitas penjelajahan web.

Kata Kunci: Deteksi *Phishing*, *Machine Learning*, Model *Hybrid*, Ekstensi Chrome, Keamanan Siber.

ABSTRACT

Phishing is a dominant cyber threat exploiting user negligence, while conventional blacklist-based detection methods often suffer from latency and privacy risks. This study aims to develop a real-time, fully client-side phishing detection system implemented as a Google Chrome extension. The system adopts a hybrid machine learning approach, combining the efficiency of Logistic Regression for initial detection and the accuracy of Random Forest for advanced verification, utilizing the PhiUSIIL dataset with 22 URL features. Experimental results demonstrate that the hybrid model successfully improves detection accuracy and minimizes false negatives without significantly burdening browser performance. This implementation proves effective in providing accurate early warnings to users, offering an adaptive and practical security solution for web browsing activities.

Keywords: *Phishing Detection, Machine Learning, Hybrid Model, Chrome Extension, Cybersecurity.*