

ABSTRAK

Serangan *phishing* menjadi ancaman keamanan siber yang signifikan dan terus berkembang. Untuk mengatasi tantangan ini, penelitian ini mengusulkan pengembangan model deteksi *phishing* berbasis *ensemble learning* dengan metode Soft Voting Classifier. Penelitian ini bertujuan untuk meningkatkan akurasi dan mengurangi tingkat *false positive* dengan memanfaatkan kekuatan prediksi dari beberapa model klasifikasi. Metodologi yang diterapkan meliputi pengumpulan 10.000 URL *phishing* dari PhishTank.org dan 5.000 URL *legitimate* dari Cisco Umbrella, yang kemudian diekstraksi menjadi 15 fitur utama. Model klasifikasi tunggal seperti Logistic Regression, K-Nearest Neighbor, Random Forest, dan Naive Bayes diimplementasikan, bersamaan dengan berbagai kombinasi *Soft Voting* dari model-model tersebut. Hasil evaluasi menunjukkan bahwa model Random Forest sebagai model tunggal mencapai akurasi tertinggi sebesar 87.60%. Sementara itu, kombinasi *Soft Voting* dari Logistic Regression, K-Nearest Neighbor, dan Random Forest menunjukkan performa yang sangat kompetitif dengan akurasi 87.47%, recall yang tertinggi (0.9175). Penelitian ini menyimpulkan bahwa meskipun *Soft Voting Classifier* tidak secara signifikan meningkatkan performa dibandingkan model tunggal terbaik, pendekatan ini berhasil mencapai kinerja yang setara dan memberikan profil performa yang stabil. Keseimbangan antara presisi dan *recall* yang dihasilkan menjadikannya solusi yang andal dan relevan untuk mitigasi ancaman *phishing* yang kompleks.

Kata Kunci: Deteksi Phishing, soft voting classifier, ensemble learning, machine learning, keamanan siber.