

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan model deteksi phishing menggunakan algoritma K-Nearest Neighbors (KNN) dan membandingkan kinerjanya dengan Decision Tree (DT). Dengan meningkatnya ancaman phishing, deteksi yang efektif sangat penting untuk melindungi data pengguna. Dalam penelitian ini, dataset yang terdiri dari 10.000 URL situs phishing dan situs yang sah digunakan. Setelah pra-pemrosesan data termasuk pembersihan, normalisasi, dan ekstraksi fitur, model KNN dan DT dilatih dan diuji. Hasil penelitian menunjukkan bahwa model KNN mencapai akurasi 95%, sedangkan DT mencapai akurasi 93%. KNN menunjukkan keunggulan dalam akurasi dan konsistensi, sedangkan DT memberikan interpretasi yang lebih baik melalui visualisasi pohon keputusan. Penelitian ini memberikan wawasan tentang keefektifan masing-masing metode dan mengidentifikasi fitur yang paling relevan dalam proses klasifikasi.

Kata kunci: Keamanan Siber, Deteksi *Phishing*, *K-Nearest Neighbor* (KNN), *Decision Trees* (DT), URL