WEBSITE PENDETEKSI *PHISHING WHATSAPP* BERDASARKAN ANALISIS 5 ALGORITMA *MACHINE LEARNING*

ELSA MAULINA SARI

ABSTRAK

Phishing merupakan ancaman keamanan siber yang semakin berkembang dengan teknik penipuan yang kompleks. WhatsApp sebagai *platform* komunikasi populer menjadi target utama serangan ini. Penelitian ini bertujuan mendeteksi anomali pada URL phishing menggunakan lima algoritma pembelajaran mesin, *Isolation Forest, Neural Network, Random Forest, Support Vector Machine* (SVM)*,* dan *XGBoost*. Dataset yang digunakan berasal dari Kaggle dengan total 11.430 URL, dibagi dalam rasio 80:10:10 untuk pelatihan, validasi, dan pengujian. Evaluasi dilakukan menggunakan empat parameter utama, yaitu akurasi, presisi, *recall*, dan *Area Under Curve* (AUC). Hasil menunjukkan bahwa *Neural Network* memiliki performa terbaik dengan akurasi 97% *(training)*, 92% (validasi), dan 93% (pengujian). Model ini diimplementasikan dalam aplikasi web menggunakan Flask, dengan ambang batas prediksi 0,5, URL dengan probabilitas di bawah nilai tersebut diklasifikasikan sebagai *legitimate*, dan sebaliknya sebagai *phishing*. Aplikasi mampu mengidentifikasi URL secara *real-time* dengan tingkat akurasi tinggi, efektif mendukung pencegahan *phishing* di WhatsApp.

Kata Kunci : Algoritma Pembelajaran Mesin, Deteksi *Phishing*, Flask, Hutan Acak, Hutan Isolasi, Jaringan SyarafTiruan, Mesin Pendukung Vektor, *XGBoost*.

WHATSAPP PHISHING DETECTION WEBSITE BASED ON THE ANALYSIS OF 5 MACHINE LEARNING ALGORITHMS

ELSA MAULINA SARI

ABSTRACT

Phishing is an evolving cybersecurity threat that employs increasingly complex deception techniques. WhatsApp, as a widely used communication platform, has become a prime target for such attacks. This study aims to detect anomalies in phishing URLs using five machine learning algorithms: Isolation Forest, Neural Network, Random Forest, Support Vector Machine (SVM), and XGBoost. The dataset, obtained from Kaggle, consists of 11,430 classified URLs and is divided using an 80:10:10 ratio for training, validation, and testing. The evaluation is based on four key performance metrics: accuracy, precision, recall, and Area Under Curve (AUC). The results show that the Neural Network algorithm outperforms the others, achieving 97% accuracy on the training set, 92% on validation, and 93% on testing. This model is implemented in a web-based application using the Flask framework, with a prediction threshold of 0.5—URLs with probabilities below this threshold are classified as legitimate, and those above are classified as phishing. The application is capable of identifying URLs in real time with high accuracy, effectively supporting phishing prevention on WhatsApp.

Keyword : *Algorithm Machine Learning, Detection Phishing, Flask, Isolation Forest, Neural Network, Random Forest, Support Vector Machine, WhatsApp, XGBoost.*