INTISARI

IMPLEMENTASI DAN ANALISIS KINERJA MODEL DETEKSI *EMAIL PHISHING* BERBASIS *MULTI-FORMAT INPUT*

Fairuz Afnan Tsaqif

22/498654/SV/21232

Perkembangan pesat teknologi digital turut membuka celah bagi meningkatnya ancaman keamanan siber, khususnya serangan *phishing* melalui media *email*. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), tercatat aktivitas *phishing* sepanjang tahun 2024 yang telah terdeteksi sebanyak 26.771.610, dimana aktivitas tersebut masih menjadi tantangan serius dalam keamanan digital nasional. Penelitian ini membangun sistem deteksi *email phishing* berbasis *multi-format input* yang mampu memproses tiga jenis *input*, yaitu teks *email* langsung, berkas EML, serta tangkapan layar yang diekstraksi menggunakan *Optical Character Recognition* (OCR). Lima model klasifikasi diimplementasikan, meliputi *Logistic Regression*, *Support Vector Machine*, XGBoost, *Deep Neural Network*, dan DistilBERT. Sistem dikembangkan dengan FastAPI dan Streamlit yang dilengkapi fitur *text highlighting*. Hasil Evaluasi menunjukkan model SVM dan DistilBERT mencapai performa terbaik yaitu 98% pada seluruh metrik, sementara pada pengujian *email* aktual, DNN dan *Logistic Regression* unggul dengan rata-rata akurasi 86,7%. XGBoost mencatat performa terendah yaitu 53,3%, terutama pada format EML yaitu 40%, akibat sensitivitas berlebihan terhadap pola kata tertentu, sehingga metadata teknis EML justru menjadi *noise*. Format teks menghasilkan rata-rata akurasi tertinggi yaitu 76%, diikuti format EML dan gambar yang masing-masing mencapai akurasi sebesar 74%, di mana *input* gambar turut terkendala keterbatasan ekstraksi OCR.

Kata Kunci : Deteksi *Phishing*, *Email Phishing*, *Multi-Format*, OCR.

ABSTRACT

IMPLEMENTATION AND PERFORMANCE ANALYSIS OF A MULTI-FORMAT INPUT-BASED PHISHING EMAIL DETECTION MODEL

Fairuz Afnan Tsaqif

22/498654/SV/21232

The rapid advancement of digital technology has opened vulnerabilities to the growing threat of cybersecurity attacks, particularly phishing through email. According to the report from Badan Siber dan Sandi Negara (BSSN), a total of 26,771,610 phishing activities were detected throughout 2024, indicating that this type of attack remains a serious challenge in the national digital security landscape. This study develops a multi-format input-based phishing email detection system capable of processing three types of input, namely direct email text, EML files, and screenshots extracted using Optical Character Recognition (OCR). Five classification models are implemented, including Logistic Regression, Support Vector Machine, XGBoost, Deep Neural Network, and DistilBERT. The system is developed using FastAPI and Streamlit, equipped with a text highlighting feature. Evaluation results show that the SVM and DistilBERT models achieved the best performance at 98% across all metrics, while in tests using actual emails, DNN and Logistic Regression performed best with an average accuracy of 86.7%. XGBoost recorded the lowest performance at 53.3%, particularly in the EML format at 40%, due to excessive sensitivity to specific word patterns, causing the EML's technical metadata to act as noise. Text format yielded the highest average accuracy of 76%, followed by EML and image formats, which each achieved an accuracy of 74%, where image input was also constrained by the limitations of OCR extraction.

Keyword : Phishing Detection, Phishing Email, Multi-format, OCR.