INTISARI

PENDETEKSIAN DAN PENCEGAHAN EMAIL PHISHING MENGGUNAKAN METODE LONG-SHORT TERM MEMORY (LSTM)

Oleh

KADEK GUNAMULYA SUDARMA YASA
24/547500/PPA/06892

Penelitian ini bertujuan untuk mengembangkan model pendeteksian dan pencegahan dalam mendeteksi aktivitas *phishing* menggunakan metode *Long Short-Term Memory (LSTM)*. Fokus utama penelitian ini adalah pada pertimbangan waktu yang dibutuhkan oleh model dalam proses pendeteksian dan pencegahan serangan *phishing*. Untuk mendukung tujuan tersebut, penelitian ini menggunakan dua dataset, yaitu *CEAS* 08 dan *Spam Phishing Email* 2025.

Tahapan penelitian meliputi praproses teks email, pelatihan model *LSTM*, serta evaluasi kinerja model. Evaluasi dilakukan menggunakan beberapa metrik, yaitu akurasi, presisi, *recall*, *F1-score*, dan *inference speed*. Metrik-metrik tersebut digunakan untuk menilai kemampuan sistem dalam mendeteksi serangan *phishing* secara akurat sekaligus efisien dari sisi waktu pemrosesan.

Hasil penelitian menunjukkan bahwa metode *LSTM* merupakan algoritma yang paling adaptif pada kedua dataset yang digunakan. Pada dataset *CEAS* 08, sistem *IPS* mencapai akurasi sebesar 0.9946 dengan nilai *True Positive (TP)* sebanyak 2158, *False Positive (FP)* 9, *True Negative (TN)* 1737, dan *False Negative (FN)* 12. Selain itu, sistem juga menunjukkan performa yang efisien dengan *inference speed* sebesar 753.90 email per detik.

Kata-kata kunci : *Social Engineering, Phishing, Pendeteksian dan Pencegahan*

ABSTRACT

PHISHING EMAIL DETECTION AND PREVENTION USING THE LONG-SHORT TERM MEMORY (LSTM) METHOD

By

KADEK GUNAMULYA SUDARMA YASA
24/547500/PPA/06892

This study proposes an detection and Prevention for phishing email using the Long Short-Term Memory (LSTM) method. The study addresses a key limitation of existing approaches that primarily focus on detection accuracy while neglecting inference time, which is a critical factor for security systems. To evaluate the proposed approach, two benchmark datasets were utilized, namely CEAS 08 andSpam Phishing Email 2025.

The proposed framework consists of several stages, including email text preprocessing, LSTM model training, and performance evaluation. Model performance was assessed using accuracy, precision, recall, F1-score, and inference speed to measure both detection effectiveness and computational efficiency. These evaluation metrics provide a comprehensive assessment of the system's capability to detect phishing emails accurately while maintaining efficient processing time.

Experimental results indicate that the LSTM-based model outperforms other approaches across both datasets. On the CEAS 08 dataset, the proposed IPS achieved an accuracy of 0.9946, with 2158 True Positives (TP), 9 False Positives (FP), 1737 True Negatives (TN), and 12 False Negatives (FN), while maintaining an inference speed of 753.90 emails per second. These findings demonstrate that the proposed LSTM-based IDPS provides a robust and efficient solution for phishing email detection.

Keywords : *Social Engineering, Phishing, Detection and Prevention*