ABSTRAK

Syahputra, Yoga. 2025. *Deteksi Serangan Phishing berbasis URL dengan Variational Autoencoder dan Convolutional Neural Network (VAE-CNN),* Skripsi. Tanjungpinang: Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Pembimbing I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Pembimbing II: Novrizal Fattah Fahmitra, S.Kom., M.Kom.

Phishing merupakan ancaman berbahaya dalam keamanan siber yang mengelabui pengguna dengan menyamarkan konten berbahaya sebagai sesuatu yang sah. Penelitian ini mengusulkan metode deteksi anomali berbasis pembelajaran tidak terawasi yang menggabungkan *Variational Autoencoder* (VAE) dan *Convolutional Neural Network* (CNN) untuk mengidentifikasi URL *phishing*. Model menggunakan CNN sebagai *encoder* untuk mengekstrak fitur dari URL, melakukan *sampling* ruang laten secara probabilistik melalui trik reparameterisasi, dan merekonstruksi input melalui *decoder*. Model dilatih menggunakan 7.000 URL *legitimate* dan diuji pada 3.000 URL, terdiri dari 1.500 *legitimate* dan 1.500 *phishing* dari total 10.000 data yang tidak seimbang. Hasil evaluasi menunjukkan performa yang seimbang dengan nilai presisi, *recall*, dan *F1-score* sebesar 0,82 dengan ambang batas optimal 0,0049 berdasarkan analisis *reconstruction loss*. Temuan ini menunjukkan potensi model VAE-CNN dalam meningkatkan deteksi *phishing* melalui pembelajaran tidak terawasi dan berkontribusi terhadap pengembangan strategi pengendalian risiko keamanan siber dengan menawarkan kemampuan terhadap data yang tidak seimbang dan pola serangan yang belum terlihat sebelumnya.

Kata kunci: *Variational Autoencoder* (VAE), *Convolutional Neural Network* (CNN), deteksi *phishing*, deteksi anomali, pembelajaran tidak terawasi, URL

ABSTRACT

Syahputra, Yoga. 2025. *URL-Based Phishing Detection via Variational Autoencoder and Convolutional Neural Network (VAE-CNN),* Undergraduate Thesis. Tanjungpinang: Department of Informatics Engineering, Faculty of Engineering and Maritime Technology, Universitas Maritim Raja Ali Haji. Advisor: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Co-advisor: Novrizal Fattah Fahmitra, S.Kom., M.Kom.

Phishing is a serious cybersecurity threat that tricks users by hiding harmful content as legitimate. This study proposes an unsupervised anomaly detection method using a hybrid deep learning model that combines Variational Autoencoder (VAE) and Convolutional Neural Network (CNN) to identify phishing URLs. The model employs CNN as an encoder to extract features from URLs, applies probabilistic latent space sampling through the reparameterization trick, and reconstructs the input with a decoder. It was trained on 7,000 legitimate URLs and tested on 3,000 URLs, including 1,500 legitimate and 1,500 phishing, from an imbalanced data of 10,000 samples. Evaluation results show balanced performance, achieving a precision, recall, and F1-score of 0.82 with an optimal threshold of 0.0049 based on reconstruction loss analysis. These findings reveal the potential of VAE-CNN in enhancing phishing detection through unsupervised learning and contribute to the development of cybersecurity risk mitigation strategies by providing the capability to address data imbalance and unseen attack patterns.

Keywords: ***Variational Autoencoder (VAE), Convolutional Neural Network (CNN), phishing detection, anomaly detection, unsupervised learning, URL***