ABSTRAK

Deteksi botnet berbasis siganture kesulitan untuk mendeteksi ancaman baru atau varian botnet yang belum terdokumentasi. Metode deteksi ini sering kali memiliki nilai false positif rate yang tinggi. Jenis deteksi ini kurang dapat diandalkan dalam lingkungan jaringan karena ketergantungannya pada pola-pola yang telah diketahui. Penelitian ini digunakan pendekatan berbasis deep learning dengan mengintegrasikan *Variational Autoencoder* (VAE) dan *Transformer* untuk mendeteksi *botnet* dalam jaringan komputer menggunakan dataset CTU-13. VAE memungkinkan pembelajaran representasi laten probabilistik dari lalu lintas jaringan, sementara Transformer, dengan mekanisme self-attention, meningkatkan kemampuan model dalam menangkap ketergantungan jarak jauh dalam data jaringan yang kompleks. Hasil eksperimen menunjukkan bahwa model VAE-Transformer memiliki akurasi 88,98% deteksi botnet dan tingkat false positive dengan nilai sebesar 1,560 . Hasil optimalisasi parameter terhadap penggunaan batch size menunjukan bahwa penggunaan batch size 32 lebih baik dengan akurasi 88,98% .

Kata Kunci: *Botnet*, *Variational Autoencoder-Transformer* (VAE-Transformer), Deteksi Anomali, Pembelajaran Mendalam (*Deep Learning*), Jaringan Komputer, False Positive.