ABSTRACT

The increase in evolving malware attacks shows the inadequacy of conventional detection methods such as antivirus and firewalls. Research on malware detection models continues to be developed, but previous studies have primarily focused on implementing a single architecture, resulting in limitations in accuracy. This study proposes a Trans Neural Network (TNN). This hybrid malware detection model integrates Transformer and Convolutional Neural Network (CNN) architectures with a transfer learning approach to detect malicious and benign network traffic more accurately. The research was conducted using the USTC-TFC2016 dataset, which focuses on parallel feature extraction, where the Transformer captures temporal dependencies and the CNN extracts local spatial features. The TNN model achieved an accuracy of 99.57%, precision of 99.58%, recall of 99.58%, and F1-Score of 99.59%. With 88.342 million parameters and a complexity of 40.770 GFLOPs, the model demonstrated fast convergence with a loss reduction from 0.0421 to 0.0096 in 35 epochs, an inference time of 11.86 ms per batch, and a stable validation accuracy of 99.57% to 99.60% without overfitting. This research makes a significant contribution and explores the development of network security system models using a hybrid method capable of addressing the evolution of malware with greater accuracy.

Keywords: *CNN, Hybrid Model, Malware, Neural Netwok, Transformer*

ABSTRAK

Peningkatan serangan *malware* yang terus berevolusi menunjukkan ketidakcukupan metode deteksi konvensional seperti *antivirus* dan *firewall*. Berbagai penelitian model deteksi *malware* terus dikembangkan, namun penelitian terdahulu didominasi fokus pada implementasi arsitektur secara tunggal, sehingga masih memiliki keterbatasan dalam akurasi. Penelitian ini mengusulkan *Trans Neural Network (TNN),* sebuah model deteksi *malware hybrid* yang mengintegrasikan arsitektur *Transformer* dan *Convolutional Neural Network (CNN)* dengan pendekatan *transfer learning* untuk mendeteksi lalu lintas jaringan *malicious* dan *benign* secara lebih akurat. Penelitian yang dilakukan menggunakan dataset *USTC-TFC2016* dengan berfokus pada ekstraksi fitur paralel dimana *Transformer* menangkap dependensi temporal dan *CNN* mengekstrak fitur spasial lokal. Model *TNN* mencapai akurasi 99,57%, presisi 99,58%, *recall* 99,58%, dan *F1-Score* 99,59%. Dengan 88,342 juta parameter dan kompleksitas 40.770 *GFLOPs*, model menunjukkan konvergensi cepat dengan penurunan *loss* dari 0,0421 menjadi 0,0096 dalam 35 *epoch*, waktu inferensi 11,86 ms per *batch*, dan *validation accuracy* stabil 99,57 sampai 99,60% tanpa *overfitting*. Penelitian ini memberikan kontribusi signifikan dan membuka eksplorasi pengembangan model sistem keamanan jaringan dengan metode *hybrid* yang mampu menanggulangi evolusi *malware* dengan lebih akurat.

Kata Kunci: *CNN, Malware,* Model *Hybrid, Neural Netwok, Transformer*