BAB I

PENDAHULUAN

1.1 Latar Belakang

Berbagai media informasi semakin berkembang pesat, diantaranya yaitu melalui lalu lintas jaringan internet dan sistem perangkat lunak (L. Zou dkk., 2023). Hal ini tidak menutup kemungkinan untuk tersisipkannya berkas yang berbahaya, baik itu *cyber attacks, malware distribution,* dan data yang tidak terotorisasi. Berbagai kejahatan tersebut akan mengganggu pada keamanan, optimasi performa internet, efisiensi *bandwitch*, dan fungsi pada suatu aplikasi atau sistem (Huang dkk., 2024).

Kejahatan internet semakin marak seiring dengan tingginya akses lalu lintas jaringan. Penelitian mengenai ancaman *malware* pada sistem operasi *Linux* yang dilakukan oleh tim Atlas VPN, menyebutkan bahwa pada tahun 2022 terjadi peningkatan *malware* pada sistem sebesar 50% dibandingkan tahun sebelumnya yaitu tahun 2021, dengan total 1,9 juta sampel *malware* (Germain, 2023). Hal ini didukung laporan dari *Cybersecurity Ventures* yang memperkirakan kerugian akibat serangan *ransomware* mencapai 20 miliar dolar AS pada tahun 2021. Serangan tersebut meningkat 8,2 miliar dolar AS dari awalnya sebesar 11,5 miliar dolar AS pada tahun 2019 (Xia dkk., 2020). Pada penelitian teks semantik yang dilakukan oleh Aslan mengenai kerentanan, ancaman, serangan, dan solusi keamanan siber menyatakan bahwa salah satu dari tiga organisasi mengalami serangan *malware* pada tahun 2020. Lebih dari 70% dari serangan tersebut adalah versi baru yang tidak dapat dideteksi oleh sistem keamanan yang ada (Aslan dkk.,

2023). Hal ini menunjukkan bahwa metode umum seperti *antivirus* dan *firewall* tidak lagi cukup untuk melindungi sistem dari pertumbuhan dan keragaman ancaman *malware* yang semakin canggih.

Malware atau *malicious software* mampu merugikan berbagai pihak yang terinfeksi olehnya. Pembuatan model deteksi *malware* banyak menerapkan berbagai arsitektur baik untuk deteksi statis ataupun dinamis (Putra Wijaya & Santoso, 2021). Pada penelitian mengenai analisis serangan siber dan evaluasi sistem deteksi intrusi menunjukkan bahwa teknik *deep learning* dan *machine learning* lebih baik dalam mendeteksi dan mengklasifikasikan berbagai jenis serangan siber (B. Abushark dkk., 2022). Perancangan desain sistem yang efisien dan kokoh semakin krusial untuk terus dikembangkan (L. Zou dkk., 2023). Salah satu upaya untuk mengembangkan sistem tersebut yaitu dengan pembuatan model yang optimal dan akurat dalam menganalisis pergerakan aktivitas *malware*.

Metode *deep learning* terus dikembangkan untuk mendeteksi *malware* pada lalu lintas jaringan diantaranya menggunakan arsitektur *CNN* dan *Transformer*. Hal ini didukung dan didasarkan penelitian terdahulu, yaitu Model *CNN* konvensional yang diusulkan (Kamboj dkk., 2023) mencapai akurasi 99,18%. Penelitian ini berkonsentrasi pada ekstraksi fitur lokal tanpa mempertimbangkan hubungan *sequence* pada data. Penelitian (Rahman, Ahmed, Khan, Mahin, Kibria, Karim, dkk., 2023) mengenai perbandingan antara *CNN* dengan *Transformer* menggunakan dataset *binary images* menghasilkan nilai akurasi sebesar 97,43% pada *Transformer*, sedangkan pada *CNN* sebesar 99,44%. Penelitian tersebut

menunjukan bahwa nilai akurasi menggunakan *CNN* cukup tinggi dibandingkan dengan *Transformer*.

Penelitian terbaru mengenai *SeMalBERT* mengkolaborasikan *BERT* dengan *ConvLSTM-AM* untuk analisis sentimen pada deteksi *malware* menggunakan dataset *EMBER* dari penelitian (Catak & Yazı, 2021) menghasilkan nilai akurasi sebesar 98,81%. Pada penelitian *SeMalBERT* juga telah dilakukan eksperimen yang mengkombinasikan *BERT* dan *CNN* dengan hasil nilai akurasi sebesar 97.36% (Liu et al., 2024). Hal ini menunjukkan masih adanya peluang untuk meningkatkan akurasi lebih lanjut.

Transfer learning sebagai salah satu pendekatan *machine learning* yang memungkinkan untuk menjadi alternatif solusi dalam pemanfaatan pengetahuan dari model yang telah dilatih pada tugas atau domain berbeda untuk meningkatkan akurasi dan performa pada tugas baru, didukung oleh penelitian *Malware Traffic Classification (MTC)* yang menunjukkan bahwa pendekatan *few-shot classification* berbasis *transfer learning* mampu mencapai akurasi hingga 95,23% hanya dengan 20 sampel per kelas pada klasifikasi lalu lintas *malware* (M. Qin dkk., 2023). Hal ini menunjukkan keunggulannya dalam kondisi data terbatas. Selain itu, pendekatan serupa yang mengubah *file* lalu lintas jaringan menjadi representasi visual menggunakan model *CNN* yang telah dilatih sebelumnya dan menerapkan prinsip *transfer learning* juga berhasil mencapai akurasi sebesar 94,71% (S. Kumar dkk., 2024). Penelitian ini mengindikasikan bahwa *transfer learning* mampu mempertahankan performa tinggi meskipun tanpa pelatihan dari awal dengan dataset besar.

Berdasarkan pernyataan tersebut, terdapat gap penelitian dalam pengembangan model deteksi *malware*, seperti tingkat akurasi yang masih dapat ditingkatkan serta adanya ruang eksplorasi dalam menciptakan model yang mampu menggabungkan keunggulan berbagai arsitektur *neural network* menjadi sebuah model *hybrid* dengan *transfer learning* sebagai pendekatan untuk meningkatkan generalisasi dan efisiensi pelatihan model. Gap ini membuka peluang untuk mengembangkan model deteksi *malware* yang lebih adaptif dan akurat. Pendekatan *hybrid* dengan dukungan *transfer learning* juga diharapkan dapat memanfaatkan pengetahuan dari model pra-latih untuk mempercepat konvergensi dan mengurangi kebutuhan data pelatihan dalam jumlah besar, sehingga menghasilkan sistem deteksi *malware* yang lebih andal dan efisien dalam berbagai skenario jaringan nyata.

Dalam konteks evaluasi model deteksi *malware*, penggunaan metrik evaluasi yang komprehensif diperlukan karena karakteristik keamanan siber yang kompleks. Ketergantungan pada metrik akurasi saja tidak cukup merepresentasikan performa model secara menyeluruh, terutama dalam situasi ketidakseimbangan kelas serta potensi dampak signifikan dari kesalahan klasifikasi. *F1-Score* diperlukan untuk memberikan keseimbangan antara *precision* dan *recall*, terutama ketika menghadapi dataset yang tidak seimbang antara kelas *malicious* dan *benign*, dimana kesalahan klasifikasi dapat berdampak signifikan pada keamanan sistem (Panda dkk., 2025). *Confusion matrix* memberikan pemahaman mendalam tentang jenis kesalahan yang dibuat model, hal ini memungkinkan analisis *false positive* dan *false negative* yang kritis dalam sistem deteksi *malware* (Fahim dkk., 2025). Selain itu, Selain akurasi, efisiensi komputasi merupakan komponen penting dalam evaluasi

performa model deteksi malware. Parameter seperti *Giga Floating Point Operations per Second (GFLOPs)* dan waktu inferensi memberikan gambaran mengenai beban komputasi yang diperlukan selama proses deteksi. Pengukuran ini menjadi relevan dalam konteks optimasi sumber daya, terutama ketika model diimplementasikan pada sistem dengan keterbatasan kapasitas pemrosesan atau ketika menghadapi volume lalu lintas jaringan yang besar (Li dkk., 2025).

Oleh karena itu, penelitian ini mengusulkan *Trans Neural Network* sebagai sebuah model deteksi *malware* dengan mengintegrasikan arsitektur *Transformer* dan *Convolutional Neural Network (CNN)* sebagai sebuah arsitektur *hybrid* yang memadukan keunggulan *Transformer* dalam menangkap hubungan sekuensial jangka panjang dan global, serta *CNN* dalam mengekstraksi fitur spasial dari data lalu lintas jaringan. Model ini dirancang untuk meningkatkan performa deteksi lalu lintas *benign* dan *malicious* pada klasifikasi lalu lintas jaringan yang lebih adaptif dan representatif dengan harapan mampu mengatasi keterbatasan pendekatan terdahulu yang berfokus mengandalkan satu jenis arsitektur.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, rumusan masalah utama pada penelitian ini yaitu:

a. Bagaimana proses pengembangan model *Trans Neural Network* untuk deteksi *malware* yang mengkombinasikan Arsitektur *Transformer* dan *Convolutional Neural Network (CNN)* secara *hybrid*?

b. Bagaimana performa model deteksi *malware hybrid Trans Neural Network* yang mengkombinasikan arsitektur *Transformer* dan *Convolutional Neural Network (CNN)* berdasarkan hasil analisis evaluasi?

1.3 Tujuan Penelitian

Berdasarkan permasalahan yang sudah dirumuskan, terdapat tujuan penelitian sebagai berikut:

a. Mengembangkan model *Trans Neural Network* untuk deteksi *malware* yang mengkombinasikan Arsitektur *Transformer* dan *Convolutional Neural Network (CNN)* secara *hybrid*.
b. Melakukan analisis terhadap performa model *Trans Neural Network* untuk deteksi *malware* dengan mengujinya menggunakan metrik evaluasi seperti akurasi, *loss function, precision, recall, F1-score*, *Giga Floating Point Operations per Second* (*GFLOPs*), serta waktu inferensi.

1.4 Manfaat Penelitian

a. Manfaat akademik

Penelitian ini berkontribusi dalam pengembangan ilmu di bidang sistem inteligen dan keamanan siber dengan menghadirkan model deteksi *malware* berbasis Arsitektur *Transformer* dan *CNN* yang bernama *Trans Neural Network*. Hasil penelitian ini dapat menjadi referensi bagi akademisi dalam mengembangkan model deteksi *malware* pada klasifikasi lalu lintas jaringan yang lebih efektif dan serta menganalisis pengaruh kombinasi *Transformer* dan *CNN* terhadap peningkatan akurasi dalam arsitektur *hybrid*.

b. Manfaat Praktis

Penelitian ini memberikan solusi bagi praktisi sistem inteligen serta keamanan siber dalam mendeteksi aktivitas malware dengan model yang lebih optimal. Melalui penggabungan arsitektur *Transformer* dan *Convolutional Neural Network* dengan pendekatan *transfer learning*, arsitektur *hybrid Trans Neural Network* yang dikembangkan dapat menangkap pola kompleks dalam lalu lintas jaringan secara lebih komprehensif, sehingga meningkatkan kemampuan identifikasi ancaman siber yang canggih. Hasil penelitian ini juga dapat menjadi dasar dalam pengembangan sistem deteksi ancaman yang lebih adaptif dan responsif terhadap serangan siber yang terus berkembang.

1.5 Batasan Masalah

Berikut merupakan batasan masalah yang diterapkan pada penelitian ini:

a. Ruang lingkup dataset yang digunakan adalah *USTC-TFC2016* dari penelitian (Wei Wang dkk., 2017) yang berisi rekap lalu lintas jaringan yang sudah dilakukan klasifikasi sebagai *malicious* dan *benign*.
b. Penelitian ini berfokus pada pengembangan model deteksi *malware* menggunakan arsitektur *Transformer* berupa *BERT* dan *Convolutional Neural Network* berupa *ResNet1D* secara *hybrid*, tanpa melakukan implementasi dalam bentuk *prototype*, ataupun produk aplikasi.
c. Evaluasi model dilakukan berdasarkan pada nilai akurasi, *loss function, precision, recall, F1-score*, *Giga Floating Point Operations per Second (GFLOPs)*, serta waktu inferensi.

c. Implementasi dan lingkungan pengujian model dilatih serta diuji dalam lingkungan komputasi berbasis *Graphics Processing Unit (GPU)* dengan menggunakan *framework PyTorch.*

1.6 Sistematika Penulisan

Sistematika penulisan pada laporan penelitian Tugas Akhir ini terdiri dari lima BAB sebagai berikut.

1. BAB I PENDAHULUAN

BAB I membahas mengenai latar belakang penelitian, perumusan masalah, tujuan, manfaat, serta batasan penelitian. Pembahasan dalam BAB I menjadi landasan dalam pengembangan model deteksi aktivitas *malware* bernama *Trans Neural Network* dengan menggabungkan arsitektur *CNN* dan *Transformer* pada klasifikasi lalu lintas jaringan. Selain itu, BAB I juga mencakup sistematika penulisan sebagai panduan dalam pelaksanaan penelitian ini.

2. BAB II LANDASAN TEORI

BAB II membahas teori-teori yang mendukung penelitian ini. Teori pendukung serta kajian penelitian terkait bertujuan untuk memahami dasar keilmuan dalam penggabungan arsitektur *Transformer* dan *CNN* untuk klasifikasi lalu lintas jaringan dalam mendeteksi aktivitas *malware*. Kajian terhadap teori dan penelitian sebelumnya akan menjadi landasan konseptual dalam pengembangan model yang dibahas pada BAB III.

3. BAB III METODOLOGI

BAB III menyajikan metodologi penelitian dengan menjelaskan alur penelitian yang dilakukan. Alur tersebut mencakup studi literatur, pengumpulan data, *pre-*

processing data, pemodelan *Trans Neural Network* berbasis *Transformer* dan *CNN* secara *hybrid*, serta evaluasi kinerja model dalam klasifikasi lalu lintas jaringan untuk mendeteksi aktivitas *malware*.

4. BAB IV HASIL DAN PEMBAHASAN

BAB IV membahas hasil penelitian yang telah dilakukan berdasarkan alur penelitian yang dijelaskan pada BAB III. Pembahasan disajikan secara rinci yang mencakup hasil dari proses pengumpulan data, *pre-processing* data, pemodelan *Trans Neural Network* berbasis *Transformer* dan *CNN* secara *hybrid*, serta evaluasi kinerja model dalam klasifikasi lalu lintas jaringan untuk mendeteksi aktivitas *malware*. Selain itu, pada BAB IV juga membahas mengenai ancaman terhadap validitas untuk mengetahui setiap ancaman atau kelemahan yang memungkinkan terjadi.

5. BAB V KESIMPULAN DAN SARAN

BAB V berisi kesimpulan dari seluruh rangkaian penelitian yang telah dilakukan dengan menyoroti kelebihan serta kelemahan model deteksi aktivitas *malware* yang bernama *Trans Neural Network* berbasiskan *Transformer* dan *CNN* secara *hybrid* pada klasifikasi lalu lintas jaringan. Selain itu, BAB V juga memberikan saran untuk pengembangan penelitian selanjutnya guna mengatasi keterbatasan yang ditemukan dan meningkatkan performa model di masa mendatang.