INTISARI

OPTIMASI KINERJA DETEKSI INTRUSI PADA LALU LINTAS JARINGAN MENGGUNAKAN *NEURAL NETWORK*: PENDEKATAN *HYPERPARAMETER TUNING*

Oleh
Maulana Aji Satrio
23/525774/PPA/06618

Lalu lintas jaringan HTTP merupakan fondasi utama infrastruktur digital modern, sehingga keamanan data pada lalu lintas jaringan menjadi aspek yang krusial dan menuntut sistem deteksi intrusi yang akurat serta efisien. Deteksi intrusi dalam lalu lintas jaringan diperlukan untuk mengidentifikasi dan menangkal ancaman keamanan. Penelitian ini mengembangkan dan mengevaluasi model deteksi intrusi berbasis *Feedforward Neural Network* (FNN) menggunakan dataset CIC-IDS2019 dengan pendekatan optimasi *hyperparameter* yang sistematis, meliputi tahapan *preprocessing* data berupa normalisasi, encoding fitur, dan imputasi nilai, lalu perancangan arsitektur model, serta optimasi *hyperparameter* yang mencakup jumlah *neuron per layer*, jumlah *hidden layer*, tingkat *dropout*, dan *batch size*. Proses pelatihan dan evaluasi dilakukan menggunakan pustaka PyTorch dengan pembagian dataset ke dalam *train*, *validation*, dan *test set*, serta dievaluasi berdasarkan metrik performa deteksi yaitu akurasi, *precision*, *recall*, dan *f1-score*, serta aspek efisiensi komputasi yang mencakup penggunaan CPU, memori, dan waktu pengujian. Hasil pengujian menunjukkan bahwa kombinasi *hyperparameter* terbaik pada model FNN, yaitu 500 *batch size*, 2 *hidden layer*, 64 *neuron per layer*, dan 10% *dropout rate*, mampu mencapai akurasi sebesar 99,9950% dan *recall* sebesar 99,9974% pada tahap pengujian. Dibandingkan dengan *Random Forest* yang diuji pada spesifikasi perangkat keras dan lingkungan komputasi yang sama, model FNN menunjukkan performa deteksi yang lebih efisien dengan penggunaan CPU sekitar 12% lebih rendah dan konsumsi memori sekitar 56% lebih rendah. Meskipun terdapat perbedaan waktu inferensi antara kedua model, selisih tersebut berada pada skala mikrodetik dan relatif sangat kecil sehingga tidak signifikan dalam konteks implementasi praktis. Temuan ini menunjukkan bahwa optimasi *hyperparameter* berperan penting dalam meningkatkan keseimbangan antara performa deteksi dan efisiensi komputasi, sehingga penelitian ini memberikan kontribusi dalam pemahaman pengaruh *hyperparameter* terhadap kinerja dan efisiensi model FNN serta menjadi dasar pengembangan sistem deteksi intrusi jaringan yang adaptif dan efisien untuk implementasi nyata.

Kata Kunci: Deteksi Intrusi, Keamanan Jaringan, Feedforward *Neural Network*, Deep Learning, Lalu Lintas Jaringan, Optimasi Hyperparameter

ABSTRACT

OPTIMIZATION OF INTRUSION DETECTION PERFORMANCE IN NETWORK TRAFFIC USING NEURAL NETWORK: A HYPERPARAMETER TUNING APPROACH

by
Maulana Aji Satrio
23/525774/PPA/06618

HTTP network traffic constitutes the core foundation of modern digital infrastructure, making data security a critical aspect that requires accurate and efficient intrusion detection systems. This study develops and evaluates an intrusion detection model based on a Feedforward Neural Network (FNN) using the CIC-IDS2019 dataset with a systematic hyperparameter optimization approach, including data preprocessing (normalization, feature encoding, and value imputation), model architecture design, and hyperparameter tuning covering the number of neurons per layer, number of hidden layers, dropout rate, and batch size. Model training and evaluation were conducted using the PyTorch library with the dataset divided into training, validation, and testing sets. Performance was assessed using classification metrics, particularly accuracy and recall, as well as computational efficiency metrics including CPU usage, memory consumption, and testing time. The best hyperparameter configuration with 500 batch size, 2 hidden layers, 64 neurons per layer, and 10% dropout rate, achieved a testing accuracy of 99.9950% and a recall of 99.9974%. When evaluated under the same hardware specifications and computational environment, the optimized FNN demonstrated higher computational efficiency than the Random Forest model, with approximately 12% lower CPU usage and 56% lower memory consumption. Although there was a difference in inference time between the two models, the gap was only at the microsecond scale and therefore not significant in practical implementation. These findings indicate that hyperparameter optimization plays a crucial role in achieving a balanced trade-off between detection performance and computational efficiency, providing a foundation for the development of adaptive and efficient network intrusion detection systems for real-world deployment.

Keywords: Intrusion Detection, Network Security, Feedforward Neural Network, Deep Learning, Network Traffic, Hyperparameter Tuning