ABSTRAK

Peningkatan penggunaan jaringan internet telah menyebabkan lonjakan jumlah data yang dikirimkan, meningkatkan kerentanan terhadap serangan siber seperti *DoS*, *DDoS*, *DNS Poisoning*, *Spoofing*, *SQL Injection*, dan *Sniffer*. Untuk mengatasi ini, diperlukan sistem deteksi anomali *traffic* jaringan yang efektif secara *real-time*. Penelitian ini bertujuan mengimplementasikan dan mengevaluasi tuning *hyper-parameter* pada algoritma *Random Forest* guna meningkatkan akurasi deteksi anomali menggunakan *NSL-KDD Dataset*.

Metode yang digunakan meliputi pengumpulan data, *preprocessing*, pembagian data, klasifikasi dengan *Random Forest* dengan dan tanpa *parameter tuning*, serta evaluasi model. Dalam tahap *preprocessing*, teknik seperti *Min-Max Normalization*, *Polynomial Features*, dan *One Hot Encoder* digunakan untuk mempersiapkan data.

Hasil penelitian menunjukkan bahwa penerapan *hyper-parameter tuning* pada *Random Forest* secara signifikan meningkatkan akurasi deteksi anomali dibandingkan dengan model yang tidak menggunakan *parameter tuning*. Evaluasi dilakukan menggunakan metrik-metrik seperti *Confusion Matrix*, akurasi, presisi, recall, dan F1-score. Selain itu, penelitian ini juga mengembangkan sebuah sistem yang mampu mendeteksi anomali secara *real-time*, yang ditunjukkan dengan kemampuan sistem untuk memproses dan menganalisis data *traffic* jaringan dengan cepat dan akurat.

Penelitian ini memberikan kontribusi dalam meningkatkan akurasi dan efisiensi sistem deteksi anomali *traffic* jaringan serta dapat menjadi referensi bagi penelitian selanjutnya dalam bidang keamanan jaringan dan *machine learning*. Diharapkan hasil penelitian ini dapat membantu pengembangan sistem keamanan jaringan yang lebih handal dan efisien.

Kata Kunci : Deteksi Anomali, *Random Forest*, *Hyper-parameter Tuning*, *Traffic* Jaringan, Serangan Siber, *Real-time*, *NSL-KDD Dataset*, Keamanan Jaringan, *Machine Learning*, Evaluasi Model