ABSTRAK

Serangan *SQL Injection* merupakan salah satu ancaman paling umum dan berbahaya terhadap aplikasi web modern. Meskipun sistem deteksi intrusi berbasis tanda tangan seperti Suricata mampu mendeteksi pola serangan yang telah dikenal, metode ini memiliki keterbatasan dalam menghadapi serangan baru (*zero-day*). Di sisi lain, pendekatan *anomaly-based* dengan *deep learning* dapat mengenali pola tidak lazim, namun rentan terhadap *false positive*.

Penelitian ini mengusulkan sebuah sistem Hybrid Intrusion Detection System (IDS) yang menggabungkan Suricata sebagai detektor *signature-based* dengan model *deep learning* berbasis *Convolutional Neural Network-Gated Recurrent Unit* (CNN-GRU) untuk deteksi anomali. Dataset yang digunakan diperoleh dari Kaggle dan telah melalui proses normalisasi, tokenisasi, dan padding. Model CNN-GRU dilatih untuk mendeteksi serangan *SQL Injection* pada data berupa *query* URL, dengan optimasi menggunakan binary crossentropy dan Adam optimizer.

Pengujian dilakukan dengan dua skenario: pertama hanya menggunakan Suricata, dan kedua dengan pendekatan hybrid. Hasil evaluasi menunjukkan bahwa sistem hybrid mampu meningkatkan akurasi deteksi secara signifikan dibandingkan Suricata saja, dengan akurasi 99.5% pada model hybrid dan akurasi 73.5% pada Suricata. Penelitian ini menunjukkan bahwa pendekatan hybrid mampu menutupi kekurangan masing-masing metode dan memberikan hasil deteksi yang lebih baik.

Kata Kunci: *SQL Injection*, Intrusion Detection System, Suricata, CNN-GRU, Hybrid IDS