Abstrak

Deteksi anomali jaringan sangat penting untuk memperkuat sistem keamanan siber modern, terutama karena ancaman siber seperti serangan zero-day semakin kompleks. Penelitian ini membahas penggunaan Reinforcement Learning (RL), khususnya Q-Learning dan Deep Q-Learning (DQN), untuk membangun sistem deteksi intrusi adaptif yang mampu menemukan pola serangan yang sudah dikenal maupun yang baru. Dataset UNSW-NB15 digunakan dalam penelitian ini, dan simulasi zero-day dibuat dengan menghilangkan jenis serangan "Fuzzers" dan "Reconnaissance" dari data pelatihan. Pra-pemrosesan data mencakup pemilihan fitur, pengkodean, normalisasi, dan penyeimbangan kelas menggunakan SMOTE-Tomek untuk mengatasi ketidakseimbangan data. Kedua algoritma dibandingkan dengan berbagai metode hyperparameter tuning. Hasil kinerja menunjukkan bahwa DQN memberikan performa lebih baik dibandingkan Q-Learning pada semua metrik evaluasi yang digunakan. DQN mencatat akurasi pengujian sebesar 99,09% dan skor F1 sebesar 0,9918 pada skenario data normal. Model ini juga tetap stabil di bawah kondisi adanya serangan zero-day, dengan penurunan akurasi yang hanya sedikit (0,07%). Temuan ini menunjukkan bahwa model RL berbasis neural lebih unggul dalam mempelajari representasi abstrak dari serangan.

Kata Kunci

Deteksi Anomali, Reinforcement Learning, Q-Learning, Deep Q-Learning, Sistem Deteksi Intrusi, Serangan Zero-Day, Keamanan Jaringan