Abstrak

Deteksi intrusi dalam konteks *Internet of Things* (IoT) memiliki tujuan utama untuk mengidentifikasi dan merespons aktivitas yang dapat membahayakan keamanan sistem. Fokus penelitian ini adalah mengembangkan model deteksi intrusi yang efektif untuk jaringan IoT dengan membandingkan performa tiga model utama yaitu *Convolutional Neural Network* (CNN), (*L*ong Short-Term Memory LSTM), dan *Recurrent Neural Network* (RNN). Hasil penelitian menunjukkan bahwa model CNN mengungguli dengan akurasi tertinggi, mencapai 99.97%. Sementara LSTM dan RNN juga mencapai kinerja tinggi dengan akurasi masing-masing sebesar 99.76% dan 99.58%. Meskipun perbedaan akurasi antara model kecil, CNN secara konsisten menunjukkan performa yang sedikit lebih unggul dalam mengklasifikasi aktivitas mencurigakan. CNN memiliki nilai tertinggi pada semua metrik, termasuk akurasi (100%), presisi (100%), *recall* (99.99%), *F1-Score* (100%), dan *AUC score* (99.97%). Model LSTM dan RNN juga menunjukkan hasil yang sangat baik, walaupun sedikit lebih rendah dibandingkan dengan CNN. Secara keseluruhan, hasil ini menegaskan bahwa ketiga model mampu memberikan tingkat deteksi intrusi yang sangat tinggi dan memberikan kontribusi signifikan dalam pengembangan solusi keamanan untuk sistem IoT di masa depan.

Kata Kunci: deteksi intrusi, internet of things , convolutional neural network, long short-term memory, recurrent neural network