

## ABSTRAK

*Intrusion Detection System* (IDS) berbasis *Machine Learning* (ML), khususnya pendekatan *Deep Learning* (DL), pada lingkungan *Internet of Things* (IoT) menghadapi tantangan utama berupa tingginya ketidakseimbangan kelas (*class imbalance*) serta banyaknya fitur yang bersifat redundan pada dataset Bot-IoT. Kondisi tersebut dapat menyebabkan model memiliki akurasi tinggi, namun kurang mampu dalam mengenali perilaku pada lalu lintas normal maupun lalu lintas berbahaya. Penelitian ini bertujuan untuk meningkatkan kinerja sekaligus aspek interpretabilitas *anomaly-based IDS* melalui pendekatan seleksi fitur berbasis analisis korelasi menggunakan *Pearson Correlation Coefficient* (PCC) terhadap kelas target, yang dikombinasikan dengan perhitungan standar deviasi dan perubahan absolut standar deviasi untuk menentukan jumlah fitur optimal. Fitur terpilih selanjutnya digunakan sebagai *input* pada model klasifikasi menggunakan *Bidirectional Gated Recurrent Unit* (BiGRU) untuk klasifikasi biner (*normal* dan *attack*). Untuk memperoleh performa optimal, dilakukan proses *hyperparameter tuning* dengan mengeksplorasi berbagai kombinasi parameter model, yang memanfaatkan kapasitas komputasi besar guna mengevaluasi konfigurasi secara sistematis dan intensif. Hasil evaluasi model *Deep Learning* (DL) tanpa integrasi aturan menunjukkan nilai *macro precision* 99%, *macro recall* 97%, dan *macro F1-score* 98%. Selanjutnya, interpretabilitas fitur terpilih dimanfaatkan untuk merancang mekanisme filtering awal berbasis aturan (*rule-based filtering layer*) sebelum proses inferensi model dilakukan, sehingga membentuk pendekatan *hybrid* antara penyaringan berbasis *threshold* dan DL. Evaluasi tambahan terhadap pendekatan *hybrid* menunjukkan peningkatan sensitivitas deteksi melalui penurunan *false negative* hingga nol pada skenario pengujian, meskipun disertai sedikit peningkatan *false positive*. Temuan ini menunjukkan bahwa integrasi seleksi fitur yang interpretatif dengan model DL dapat menghasilkan sistem deteksi yang lebih seimbang, efisien, dan berpotensi aplikatif untuk implementasi nyata pada lingkungan IoT.

**Kata kunci** : *Intrusion Detection System, Bot-IoT, Feature Selection, Pearson Correlation Coefficient, BiGRU, Macro Average, Hybrid IDS*