ABSTRAK

Pertumbuhan pesat ekosistem *Internet of Things* (IoT) telah menimbulkan tantangan signifikan dalam bidang keamanan siber, khususnya terkait serangan *Distributed Denial of Service* (DDoS) dan berbagai serangan intrusi jaringan lainnya. Penelitian ini mengusulkan sistem deteksi intrusi berbasis anomali (*Anomaly-based Intrusion Detection System* / AIDS) yang mengintegrasikan metode seleksi fitur *Analysis of Variance* (ANOVA) F-test dengan arsitektur *deep learning Multilayer Perceptron* (MLP) dengan skenario klasifikasi serangan multikelas pada dataset Bot-IoT. Dari total 42 fitur, metode ANOVA berhasil memilih 10 fitur paling berpengaruh, sehingga mengurangi dimensi data sebesar 71,4% sekaligus mencapai nilai Macro *f1-score* sebesar 86,07%, yang mana lebih tinggi dibandingkan model yang menggunakan seluruh fitur dengan nilai 83,90%. Model yang diusulkan dengan total 46.085 parameter menunjukkan kinerja yang kompetitif dibandingkan metode seleksi fitur lainnya, serta hanya membutuhkan waktu komputasi fitur sebesar 1,4 detik dibandingkan dengan 772,9 detik pada pendekatan berbasis *wrapper*. Hasil penelitian ini menunjukkan bahwa seleksi fitur berbasis ANOVA memberikan keseimbangan yang baik antara performa klasifikasi dan efisiensi komputasi khususnya untuk lingkungan IoT dengan keterbatasan sumber daya.

Kata kunci : *Internet of Things, Intrusion Detection System,* ANOVA *Feature Selection, Multilayer Perceptron, Bot-IoT Dataset, Network Security.*