ABSTRAK

Penelitian ini mengusulkan teknik klasifikasi untuk mendeteksi serangan *malware Mirai* pada arsitektur perangkat *Internet of Things*. *Hackers* menargetkan *Internet of Things* untuk dijadikan objek serangan, oleh karena itu diperlukan metode deteksi untuk melindungi perangkat dari serangan *hackers*. Proses deteksi *Malware Mirai* dilakukan menggunakan pembelajaran tanpa pengawasan dengan deteksi anomali. Pengujian dilakukan sebanyak 5 skenario menggunakan berbagai jenis serangan dan jenis perangkat untuk menemukan kinerja yang optimal dari metode yang diusulkan. Jumlah data uji diseimbangkan terlebih dahulu dengan pengambilan sampel dan fitur pada dataset diseleksi menggunakan kriteria *Gini index*, untuk menghasilkan nilai optimal sebelum melakukan proses pemodelan. Hasil percobaan menunjukkan algoritma *Random Forest* mencapai kinerja optimal dengan nilai rata-rata akurasi sebesar 95,01%, *recall* sebesar 90,82%, *F-Measure* sebesar 93,85% dan *precision* sebesar 99,23%. Algoritma *Random Forest* cocok untuk memproses data yang sangat besar. Kontribusi dari penelitian ini adalah model yang diusulkan untuk klasifikasi jenis serangan dan deteksi malware Mirai.

Kata Kunci: Algoritma *Random Forest*, Deteksi Anomali, *Internet of Things*, *Machine Learning, Malware Mirai*