ABSTRAK

Potensi serangan *cyber* terhadap teknologi *Internet of Things* (IoT) sangat besar. Berbagai macam serangan yang mengakibatkan gangguan dalam proses komunikasi diantaranya serangan *botnet mirai*. Untuk mendeteksi dan mengidentifikasi anomali dalam jaringan IoT, dipilih metode *machine learning* dengan menggunakan tiga algoritma yang berfungsi mengklasifikasi serangan *botnet mirai*, yaitu *Random Forest, K-Nearest Neighbor* dan *Decision Tree* dengan parameter *accuracy, precision, recall,* dan AUC. Pengujian dilakukan sebanyak tiga kali dengan nilai k-fold yang berbeda. Dari pengujian 1, 2 dan 3, algoritma *Random Forest, K-Nearest Neighbour*, dan *Decision Tree* menghasilkan rata-rata nilai pada parameter *accuracy, precision,* dan *recall* tidak terlihat perbedaan yang signifikan karena mendekati nilai 100%. Akan tetapi, pada parameter AUC algoritma *K-Nearest Neighbor* mendapatkan nilai paling tinggi yaitu dengan rata-rata nilai 1,000 yang menunjukkan lebih unggul dari algoritma *Random Forest* dan *Decision Tree*.

Kata Kunci: IoT, *Botnet Mirai, Machine Learning, Random Forest, K-Nearest Neighbor , Decision Tree*