

Abstrak

Perkembangan *Internet of Things* belakangan ini sangatlah pesat, hal tersebut terlihat dari meningkatnya jumlah pengguna berbagai perangkat *IoT* dari waktu ke waktu. *IoT* dapat menghubungkan berbagai *device* dan saling bertukar data melalui jaringan internet. Namun dalam pengimplementasian teknologi tersebut, terdapat berbagai macam ancaman. Salah satu ancaman serius pada teknologi *IoT* yaitu serangan *DDOS* melalui perantara *Botnet (Robot Network)*. Serangan tersebut telah menjadi penyebab risiko keamanan yang cukup serius terhadap jaringan Internet selama beberapa tahun ini. seperti masalah yang banyak terjadi pada privasi, keamanan, konfigurasi sistem, kontrol akses, dan verifikasi. Oleh karena itu, perlu adanya sistem pendeteksi serangan *botnet* dengan menggunakan algoritma *Random forest*. Dimana *Random forest* dipilih karena, algoritma tersebut sangat optimal dalam proses deteksi serangan dengan jumlah data yang besar dibanding algoritma lainnya. Pada tugas akhir ini, menggunakan dataset yang berasal dari *UNSW Canberra* yaitu *Bot-IoT UNSW-2018* dataset dan *Algoritma Random forest* digunakan pada proses klasifikasi serangan *botnet*. Setelah dilakukan pengujian, *Algoritma Random Forest* dapat bekerja dengan baik dalam melakukan deteksi terhadap serangan *botnet*. Dimana pada fitur *attack* didapat nilai *accuracy* sebesar 99.27% sedangkan pada fitur *category* nilai *accuracy* sebesar 99.43% dan fitur *subcategory* nilai *accuracy* sebesar 98.86%, *category* 97.97% dan *subcategory* 83.77%, dengan pembagian data *train* 80%, *data test* 30% dan jumlah *n estimators* 200.

Kata Kunci : *Botnet, Internet of Things, Machine Learning, Random Forest*