Abstract

The development of the Internet of Things lately is very rapid, it can be seen from the increasing number of users of various IoT devices from time to time. IoT can connect various devices and exchange data with each other via the internet. However, in implementing this technology, there are various kinds of threats. One of the serious threats to IoT technology is DDOS attacks through Botnet intermediaries (Robot Network). These attacks have been the cause of a fairly serious security risk to the Internet network for several years. such as problems that often occur in privacy, security, system configuration, access control, and verification. Therefore, it is necessary to have a botnet attack detection system using the Random forest algorithm. Where Random forest was chosen because, the algorithm is very optimal in the process of detecting attacks with large amounts of data compared to other algorithms. In this final project, using a dataset originating from UNSW Canberra, namely the Bot-IoT UNSW-2018 dataset and the Random forest algorithm used in the botnet attack classification process. After testing, the Random Forest Algorithm can work well in detecting botnet attacks. Where in the attack feature, the accuracy value is 99.27%. Meanwhile, in the category feature, the accuracy value is 99.43%. and the subcategory feature has an accuracy value of 98.86%

Keywords : Botnet, Internet of Things, Machine Learning, Random Forest