
Abstract

Internet of Things (IoT) is a tool that is able to communicate and transmit data over a network without human intervention and interaction. Along with the times, the use of information technology is increasingly being used and this affects the need for IoT devices which makes these devices increasingly widespread in use. In its development, issues in the field of privacy and security have become one of the most dangerous and must be the main focus. Examples of attacks that can attack IoT devices are dictionary attacks, DDoS, mitm, etc. Steps that can be taken to avoid these attacks are to use an Intrusion Detection System (IDS). The purpose of this study is to find the most optimal model to detect dictionary attacks and DDoS attacks using the naive Bayes machine learning (ML) algorithm method on the Internet of Things (IoT) which is simulated using red nodes. The naive Bayes algorithm was chosen because the Intrusion detection system (IDS) requires a fast level of performance and high accuracy. The results of this study are an optimal model built with a naive Bayes machine learning algorithm that can be applied to Intrusion detection systems (IDS) on the Internet of Things (IoT) with accuracy results for the datasets taken in this study 99.30% for DDoS and for dictionary. attack 99.74% while for the dataset taken from [19][20] for DDoS 82.38% and for dictionary attack 79.88%.

Keywords: IoT, IDS, *dictionary attack*, DDoS, naive bayes.
