1. Introduction

Internet of Things (IoT) is a new paradigm that enables communication between electronic devices and sensors via the internet to facilitate human lives [1]. The development and growth of Internet of Things (IoT) devices are increasing time to time and it is projection that by 2025 there will be 41.6 billion IoT devices connected to the internet [2]. However, the increasing development and growth of IoT devices are not in line with the security applied on IoT devices. In fact, poor security on IoT devices is potential to be exploited by irresponsible parties that are able to access and use IoT devices for various purposes that can harm other parties. There are many types of attacks on IoT devices, one of which is botnet attack [3].

Botnet is a group of infected hosts remotely controlled via the Internet through the commands of the botmaster. Commonly it is used to facilitate any illegal activities such as keylogging, identity theft, malware distribution, cryptocurrency mining and, the most common one, distributed denial-of-service (DDoS) attack [4]. There are various types of botnet that attack IoT devices, one of which is Mirai botnet [3] - a kind of worm that spreads the copies of itself to IoT devices. Mirai infects IoT devices and turns them into bot [5]. Mirai botnet attacks IoT devices such as webcams, security cameras, and routers.

From the aforementioned problem, it is deemed necessary to have a system that is capable of detecting Mirai botnet attack on IoT devices. Through the application of detection system towards the Mirai botnet attack, it is expected that it is able to protect IoT device and fix security problems on this device. The detection system can be built using machine learning method and several models from machine learning. There have been several studies that have been carried out in detecting Mirai botnet attacks. In a study conducted by Jiyeon Kim et al, thedetection of Mirai botnet attack used several machine learning and deep learning models; however, the logistic regression model still had a low performance value [6]. Meanwhile, Zohaib Ahmed et al in their research used blockchain to protect IoT devices from Mirai botnet attack. However, it still had an increasing propagation delay with the increasing number of blockchain blocks [7].

The Support Vector Machine (SVM) model has good performance and accuracy in detecting an attack in consideration to that this model has a good generalization performance when the parameters are properly configured in modeling the training set [8]. Generalization is defined as the ability of a Support Vector Machine (SVM) model to classify a pattern, which does not include the data used in the learning phase of the method to minimize errors in the training-set [9]. For this reason, this study used the Support Vector Machine (SVM) model to detect Mirai botnet attack and analyzed its performance based upon the parameter of attack detection accuracy. Here, the dataset used was N-BaIoT [10].