ABSTRACT

The development of technology and the increase of internet usage create a numerous technological innovation that can help human life in every aspect. One of the technological innovation is the presence of Internet of Things or IoT. IoT devices has a lot of functions and can be applied on many sensors. Through the internet, IoT devices can communicate to another IoT devices or to a cloud servers. With IoT devices connected through the internet, it increases the cybersecurity risk in forms of a cyberattack. One of the latest cyberattack is Distributed Denial-of-Service or DDoS that attack through Robot Network or Botnet. DDoS can interfere and affects privacy, system configuration, security, access control and verification of IoT devices. Consequently, there is a need of Distributed Denial-of-Service attack detection system that can be utilize to detect, mitigate and control the risks. This thesis objective is to create DDoS attack detection system using Chicken Swarm Optimization algorithms to achieve better accuracy rate. The implementation of Chicken Swarm Optimization (CSO) contributes increasing the accuracy of the system to detect the attack by choosing features that positively contribute to the detection process.

Keywords: Distributed Denial-of-Service, Internet of Things, Machine Learning, Swarm Optimization, Chicken Swarm Optimization