ABSTRAK

Perkembangan teknologi dan peningkatan penggunaan internet membuat banyak inovasi di bidang teknologi yang dapat membantu kehidupan manusia di segala aspek. Salah satu dari banyak inovasi di bidang teknologi tersebut ialah kehadiran dari *Internet of Things* atau IoT. Perangkat IoT mempunyai banyak fungsi dan dapat diaplikasikan ke beberapa sensor. Melalu internet, perangkat IoT dapat berkomunikasi dengan perangkat IoT lain dan dengan *server cloud*. Dengan terhubungnya perangkat IoT ke jaringan internet, risiko keamanan siber yang salah satunya adalah serangan siber menjadi semakin meningkat. Salah satu bentuk serangan siber yang sering terjadi adalah serangan *Distributed Denial-of-Service* atau DDoS yang menyerang perangkat IoT melalui perantara Botnet atau *Robot Network*. Serangan DDoS dapat mengganggu konektivitas dan mempengaruhi aspek privasi, selain itu dapat menjadi ancaman bagi konfigurasi sistem, keamanan sistem, control akses dan verifikasi pada perangkat IoT. Akibatnya, dibutuhkan sebuah sistem deteksi serangan DDoS yang dapat diutilisasi untuk mendeteksi serangan tersebut, sehingga serangan dapat di mitigasi dan di kontrol. Tujuan tesis ini adalah untuk menciptakan sistem deteksi serangan DDoS menggunakan algoritma *Chicken Swarm Optimization* atau CSO yang diharapkan dapat meningkatkan tingkat akurasi deteksi serangan. Implementasi dari algoritma CSO tersebut berkontribusi positif meningkatkan akurasi dari sistem deteksi terhadap pendeteksian serangan DDoS.

Kata kunci: *Distributed Denial-of-Service, Internet of Things, Machine Learning, Swarm Optimization, Chicken Swarm Optimization*