ABSTRAK

Dalam pesatnya perkembangan Internet terdapat salah satu pemanfaatan dari berkembangnya Internet yaitu munculnya konsep *Internet of Things* (IoT). Dalam penerapan konsep IoT ini ternyata banyak kasus yang ditemukan pada perangkat IoT yaitu menjadi target kejahatan siber, dengan terhubungnya perangkat kedalam jaringan internet maka disitu akan timbul kerentanan dalam jaringan IoT, maka dari itu disitulah menjadi tantangan terbesar untuk IoT ini

Dengan didapatkan permasalahan seperti itu, maka dikembangan sistem keamanan dengan merancang sistem keamanan pada jaringan IoT dengan mengadopsi algortima *advanced encryption standard* (AES) dan MD5. Penerapan algortima AES diimplementasikan pada saat terjadi pengiriman data dari perangkat IoT ke *server*, dengan melakukan enkripsi-dekripsi agar saat proses pengiriman data tetap terjaga kerahasian dan keabsahannya.

Sistem keamanan diuji dengan menggunakan skenario serangan DoS. Pengujian dilakukan untuk mengetahui performasi QoS dan CPU *usage* pada sistem yang dirancang. Hasil dari pengujian didaptakan delay sebesar 0,26284968s pada sistem keamanan tanpa adanya serangan, selisih delay anatara yang menerapkan sistem dan tanpa sistem dengan serangan DoS *tools* ApacheJMeter sebesar 10% dan dengan DoS *tools* LOIC sebesar 4%. Sedangkan untuk hasil dari peningkatan CPU *usage* mendapatkan selisih antara 9% pada sistem yang dirancang dengan serangan DoS dan tanpa serangan DoS.

Kata kunci : *Internet of Things (IoT), advanced encryption standard (AES),* MD5, DoS, QoS