

ABSTRAK

Penggunaan kriptografi dalam pembuatan proyek *Internet of Things* (IoT) masih tergolong rendah sehingga dapat menimbulkan ancaman privasi bagi penggunanya. Perlu adanya sistem yang menjamin aspek keamanan pada lalu lintas jaringan IoT. Algoritma kriptografi modern digunakan dalam sistem pemantauan konsumsi daya listrik untuk mengamankan data berupa arus listrik dari ancaman berupa penyadapan oleh pihak yang tidak diinginkan.

Sistem pemantauan konsumsi daya listrik menggunakan sensor SCT-013-000 yang bersifat *non-invasive* dan diproses pada Wemos D1 ESP8266 menggunakan algoritma enkripsi *Advanced Encryption Standard* (AES) mode *Cipher Blocker Chaining* (CBC) dengan panjang kunci 128, 192, dan 256 bit yang terintegrasi dengan layanan *Amazon web server*.

Nilai rata-rata *Avalanche effect* untuk setiap panjang kunci 128, 192, dan 256 bit adalah 46% dengan konsumsi listrik sebesar 36 miliAmpere. AES mengalokasikan memori sebesar 128, 192, dan 256 bit untuk menyimpan tiap-tiap panjang kunci dengan lama waktu proses sebesar 830,11 μ s, 850,87 μ s, dan 883,26 μ s untuk panjang kunci 128, 192, dan 256 bit. Nilai rata-rata QoS mikrokontroler Wemos D1 ESP8266 dari/ke cloud server untuk setiap panjang kunci berbeda yaitu *Delay* sebesar 0,34 detik dan *Throughput* sebesar 2244,2 bit/s.

Kata Kunci: *Internet of Things, Advanced Encryption Standard, Amazon web server, SCT-013-000, Wemos D1 ESP8266*