Abstrak

Keamanan data pada perangkat IoT merupakan hal yang sangat penting karena semakin berkembangnya perangkat yang menerapkan IoT semakin banyak pula data yang tersimpan setiap harinya. MQTT adalah salah satu protokol transmisi data yang ringan dan cocok dalam IoT, tetapi kurang memiliki keamanan yang baik dari segi kerahasiaan dan integritas data agar tetap sederhana dan ringan. Untuk mengamankan data dari dua segi tersebut bisa menggunakan algoritma kriptografi salah satunya algoritma Ascon yang diterapkan dalam perangkat IoT yaitu Orange Pi Zero 2. Prosesnya data dienkripsi dan didekripsi dengan mengikuti metode MQTT *publish-subscribe* sebagai transmisi datanya. Ascon memiliki dua varian yaitu 128 dan 128a yang akan saling dibandingkan dari segi performa waktu rata-rata, pemakaian CPU dan RAM. Untuk pesan pendek, Ascon 128 lebih unggul dari segi waktu dan pemakaian CPU, tapi untuk RAM terhitung sama yaitu sebesar 0B. Sedangkan untuk pesan satu juta *bytes*, Ascon 128a lebih unggul dari segi waktu dan pemakaian RAM. Hasil yang didapatkan menunjukkan kedua varian algoritma Ascon dapat mengatasi permasalahan tersebut.

Kata kunci: Ascon, IoT, MQTT, Orange Pi Zero 2