ABSTRAK

Internet of things merupakan sistem kompleks yang sudah banyak diaplikasikan dalam berbagai aspek untuk memudahkan kehidupan manusia. Karena tersusun dari sistem yang kompleks, IoT memiliki banyak celah resiko keamanan sehingga diperlukan sebuah sistem enkripsi untuk menjaga keamanan data pengguna. Pemilihan jenis enkripsi yang sesuai kebutuhan sangat penting untuk mendapatkan performa yang baik. Karena keadaan ini, NSA meluncurkan algoritma enkripsi untuk IoT bernama Simon dan Speck. Untuk menguji algoritma enkripsi ini, diusulkan sebuah penelitian untuk membandingkan algoritma enkripsi Simon-Speck dan AES serta pengaruhnya terhadap performansi sistem pada perangkat IoT.

Fokus dari penelitian ini adalah menguji pengaruh algoritma enkripsi terhadap performansi perangkat IoT sehingga data yang dibangkitkan merupakan data *dummy* yang dihasilkan oleh ubuntu server sebagai publisher. Selanjutnya, data akan dienkripsi menggunakan algoritma Simon-Speck dan AES, lalu dikirimkan ke MQTT broker yang telah diimplementasikan pada *Google Cloud Platform* (GCP). Setelah itu, *subscriber* akan mengambil dan mendekripsi datanya. Parameter dalam pengujian ini berupa *delay*, *throughput*, dan *packet loss* serta efisiensi penggunaan memori dari algoritma enkripsi dan nilai *avalanche effect*nya. Dari hasil pengujian diperoleh bahwa delay dan penggunaan memori yang paling rendah yaitu pada algoritma Speck. Besar delay memengaruhi throughput sehingga nilai throughput yang paling baik dimiliki oleh algoritma Speck. Pada parameter avalanche effect, walaupun tidak berbeda jauh dari Speck, algoritma Simon memiliki nilai avalanche effect yang lebih tinggi. Sedangkan untuk packet loss, semua algoritma enkripsi memiliki packet loss sebesar 0%. Berdasarkan hasil tersebut, dapat disimpulkan bahwa algoritma Speck dan Simon lebih baik untuk diimplementasikan pada perangkat IoT karena memiliki delay yang lebih kecil serta avalanche effect, efisiensi penggunaan memori, dan throughput yang lebih besar daripada algoritma AES

Kata kunci : Performansi sistem, *Internet of Things*, algortima enkripsi Simon-Speck, algoritma enkripsi AES, MQTT