ABSTRACT

Internet of things is a complex system that has been widely applied in various aspects to facilitate human life. Because it is composed of a complex system, IoT has many security risk loopholes, so an encryption system is needed to maintain the security of user data. Selection of the type of encryption that suits your needs is essential to get good performance. Due to these circumstances, the NSA launched an encryption algorithm for IoT named Simon and Speck. A study is proposed to test this encryption algorithm to compare the Simon-Speck and AES encryption algorithms and their effect on system performance on IoT devices.

The focus of this research is to examine the effect of the encryption algorithm on the performance of IoT devices so that the data generated is dummy data generated by the ubuntu server as a publisher. Furthermore, the data will be encrypted using the Simon-Speck algorithm and AES, then sent to the MQTT broker which has been implemented in Google Cloud Platform (GCP). After that, the subscriber will retrieve and decrypt the data. The parameters in this test are delay, throughput, packet loss, the efficiency of memory usage from the encryption algorithm, and the value of the avalanche effect. The test results show that the Speck algorithm has the lowest delay and memory usage. The amount of delay affects the throughput so that the Speck algorithm owns the best throughput value. Although not much different from Speck, Simon's algorithm has a higher avalanche effect value in the avalanche effect parameter. As for packet loss, all encryption algorithms have a packet loss of 0%. Based on these results, it can be concluded that the Speck and Simon algorithms are better implemented on IoT devices because it has smaller delay and memory usage efficiency but greater avalanche effect and throughput than the AES algorithm.

Keywords: System performance, Internet of Things, Simon-Speck encryption algorithm, AES encryption algorithm, MQTT