Abstract

Data security on IoT devices is very important because the more devices that implement IoT, the more data is stored every day. MQTT is one of the lightweight data transmission protocols and is suitable for IoT. Still, it lacks good confidentiality and data integrity security to keep it simple and light. Cryptographic algorithms can be used to secure data from these two aspects, one of which is the Ascon algorithm applied to IoT devices, namely Orange Pi Zero 2. The process of data is encrypted and decrypted by following the MQTT publish-subscribe method as the data transmission. Ascon has two variants, namely 128 and 128a, which will be compared in terms of average time performance and CPU and RAM usage. For short messages, Ascon 128 is superior in terms of time and CPU usage, but it is the same for RAM, which is 0B. As for one million bytes messages, Ascon 128a is excellent in time and RAM usage. The results obtained show that both variants of the Ascon algorithm can overcome these problems.

Keywords: Ascon, IoT, MQTT, Orange Pi Zero 2