Analisis Overhead pada Penerapan Digital Signature pada Protocol MQTT untuk Constrained Device di Sistem IoT

Andaresta Fauzan[1], **Parman Sukarno**[2], **Aulia Arif Wardana**[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[4]Divisi Digital Service PT Telekomunikasi Indonesia
[1]andarestafauzan@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstract

This paper presents an overhead analysis of the use of digital signature mechanisms in the Message Queue Telemetry Transport (MQTT) protocol for three classes of constrained-device. Because the resources provided by constrained-devices are very limited, the purpose of this overhead analysis is to help find out the advantages and disadvantages of each class of constrained-devices after a security mechanism has been applied, namely by applying a digital signature mechanism. The objective of using this digital signature mechanism is for providing integrity, that if the payload sent and received in its destination is still original and not changed during the transmission process. The overhead analysis aspects performed are including analyzing decryption time, signature verification performance, message delivery time, memory and flash usage in the three classes of constrained-device. Based on the overhead analysis result, it can be seen that for decryption time and signature verification performance, the Class-2 device is the fastest one. For message delivery time, the smallest time needed for receiving the payload is Class-1 device. For memory usage, the Class-2 device is providing the biggest available memory and flash.

Keywords: constrained-device, message queue telemetry transport, digital signature, overhead analysis