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

Abstrak

Dokumen ini menyajikan Analisis Overhead terhadap penggunaan mekanisme tanda tangan digital (*digital signature*) dalam protokol *Message Queue Telemetry Transport* (MQTT) untuk tiga kelas perangkat terbatas. Karena sumber daya yang disediakan oleh perangkat dibatasi sangat terbatas, tujuan dari Analisis Overhead ini adalah untuk membantu mencari tahu kelebihan dan kekurangan pada masing-masing kelas perangkat terbatas (*constrained-device*) setelah mekanisme keamanan dilakukan diterapkan, yaitu dengan menerapkan mekanisme tanda tangan digital. Tujuan menggunakan mekanisme tanda tangan digital ini adalah untuk memberikan integritas, bahwa pada saat *payload* dikirim dan diterima tujuannya masih asli dan tidak berubah selama proses transmisi. Aspek Analisis Overhead yang dilakukan diantaranya menganalisis waktu dekripsi, performa verifikasi tanda tangan, waktu pengiriman pesan, penggunaan memori dan flash di tiga kelas perangkat terbatas (*constrained-device*) yang berbeda. Berdasarkan hasil Analisis Overhead, dapat dilihat bahwa untuk waktu dekripsi dan perfoma verifikasi tanda tangan, perangkat *Class-2* adalah yang tercepat. Untuk waktu pengiriman pesan, waktu terkecil diperlukan untuk menerima *payload* adalah perangkat *Class-1*. Untuk penggunaan memori, perangkat *Class-2* menyediakan sisa memori dan kapasitas flash tersedia yang terbesar.

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