Analisis Overhead Penggunaan Digital Signature Pada Protokol MQTT

Husnul Hidayat[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]husnulhidayat@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardana@telkomuniversity.ac.id

Abstrak

Penelitian ini mengusulkan skema digital signature untuk mengamankan pesan yang dikirimkan oleh protokol *Message Queue Telemetry Transport* (MQTT) *publish* / *subscribe middleware* menggunakan *Advanced Encryption System* (AES) dan *Secured Hash Algorithm* (SHA) dengan metode *end-to-end* dan menganalisis *overhead* dari penerapan *digital signature*. Kekurangan dari MQTT secara *default* yaitu tidak adanya proses enkripsi pada payload yang memungkinkan seseorang untuk dapat mengetahui konten payload yang menyebabkan tidak adanya privasi dalam data. Integritas data juga merupakan masalah pada MQTT. Tujuan dari *digital signature* ini dalam sistem ini adalah untuk memverifikasi bahwa *payload* yang dikirim adalah asli, tidak berubah selama proses transmisi, serta menjamin kerahasiaan pada payload. Setelah evaluasi dan pengujian sistem yang diusulkan, program ini dapat mengamankan payload MQTT. Penambahan mekanisme keamanan di MQTT seperti proses enkripsi, dekripsi, hasil verifikasi menghasilkan *overhead* pada beberapa aspek. *Overhead* yang digunakan dalam penelitian ini adalah untuk mengukur ukuran *payload*, waktu pengiriman pesan, proses mekanisme keamanan *digital signature*, konsumsi memori, dan penggunaan CPU. Dalam analisis *overhead*, *overhead* dilakukan dengan memeriksa berbagai jenis kunci AES dan berbagai jenis SHA. Setelah dilakukan analisis, ada peningkatan ukuran untuk beberapa aspek yang telah disebutkan karena skema *digital signature*.

Kata kunci : middleware, payload, AES, SHA, digital signature, overhead.