Penerapan Metode Autentikasi Menggunakan JSON Web Token dan Enkripsi Menggunakan XXTEA pada IoT Berbasis MQTT

Fathan Abdul Shodiq[1], Parman Sukarno[2], Rizka Reza Pahlevi[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]fathanabduls@student.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]rizkarezap@telkomuniversity.ac.id

Abstrak

Konsep komunikasi *Internet of Things* (IoT) atau *Machine-to-Machine* (M2M) diharapkan menjadi salah satu dari solusi jaringan masa depan. Salah satu protokol yang sering digunakan dalam aplikasi IoT adalah *Message Queuing Telemetry Transport* (MQTT). MQTT menggunakan lebih sedikit bandwidth, ringan dalam komputasi, dan cepat dalam transmisi. Dengan demikian, MQTT dapat diterapkan pada perangkat terbatas. Namun, MQTT tidak memiliki metode keamanan bawaan sehingga memiliki beberapa kerentanan. Keretanan pertama yang dapat ditemui pada MQTT adalah autentikasi. Dengan tidak adanya autentikasi dapat menyebabkan *node* yang tidak sah untuk menggunakan sumber daya jaringan MQTT, sehingga bisa menyebabkan *over connections*. Penelitian ini menggunakan *JSON Web Token* (JWT) untuk membangun metode autentikasi berbasis token pada MQTT sebagai faktor autentikasi tambahan selain *username* dan *password*. Hal ini dilakukan untuk mencegah *node* yang tidak valid untuk masuk ke jaringan MQTT. Dari hasil pengujian, metode autentikasi yang dibangun dapat bertahan dari serangan *brute force* dan memastikan bahwa tidak ada node tidak valid yang dapat masuk ke jaringan MQTT. Kerentanan kedua yang dapat ditemui pada MQTT adalah privasi data yang disebabkan oleh tidak adanya metode enkripsi data bawaan pada MQTT. Hal tersebut dapat memudahkan penyerang untuk mendapatkan data yang dipertukarkan di jaringan MQTT, meskipun MQTT sudah dibangun menggunakan metode autentikasi tertentu. Oleh karena itu, penelitian ini juga menggunakan algoritma *Corrected Block Tiny Encryption Algorithm* (XXTEA) untuk melakukan enkripsi data pada MQTT. Dari hasil pengujian, metode enkripsi yang digunakan dapat bertahan dari serangan *sniffing*. Metode autentikasi dan enkripsi yang dibangun juga dapat dijalankan pada perangkat terbatas menggunakan 405912 *byte* memori (38% dari total penyimpanan program) pada *publisher node* dan 406856 *byte* memori (38% dari total penyimpanan program) pada *subscriber node* dengan perkiraan konsumsi daya sebesar 70.9mA untuk masing-masing *node*.

Kata kunci : *Internet of Things* (IoT), *Message Queuing Telemetry Transport* (MQTT), autentikasi, *JSON Web Token* (JWT), enkripsi, *Corrected Block Tiny Encryption Algorithm* (XXTEA), perangkat terbatas