RINGKASAN

IMPLEMENTASI *MESSAGE AUTHENTICATION CODE* DAN ALGORITME *ADVANCED ENCRYPTION STANDARD* PADA PROTOKOL KOMUNIKASI MQTT

Hamzah Diza Santoso

Penggunaan *internet of things* (IoT) terus meningkat dari waktu ke waktu. IoT saat ini digunakan di berbagai lingkungan karena menawarkan banyak manfaat dan kemudahan penggunaan. *Message Queuing Telemetry Transport* merupakan protokol yang paling populer pada IoT. Peningkatan jumlah sektor yang dapat disisipi dengan MQTT juga mempengaruhi variasi perangkat atau pengembangan perangkat di IoT. Namun, peningkatan penggunaan MQTT juga mempengaruhi keamanan komunikasi MQTT. Tidak jarang menghadapi ancaman keamanan saat menggunakan MQTT. Penelitian ini bertujuan untuk meningkatkan keamanan komunikasi jaringan MQTT dengan mempertimbangkan parameter keamanan: *confidentiality, integrity,* dan *authentication*. Selain itu, penelitian ini juga bertujuan untuk menentukan, melalui proses analisis *overhead*, apakah variasi metode yang diusulkan cocok untuk diterapkan pada perangkat IoT yang memiliki sumber daya yang terbatas. Penelitian ini menggunakan AES sebagai metode enkripsi data. Variasi AES yang digunakan adalah AES128 dan AES256. Dan menggunakan MAC untuk memverifikasi data. Jenis MAC yang digunakan adalah HMAC dengan variasi SHA256, SHA512, SHA3-256, dan SHA3-512. Berdasarkan percobaan yang dilakukan, kombinasi metode AES dan MAC mampu mengamankan komunikasi antar perangkat dalam protokol MQTT dan memastikan *confidentiality, integrity,* dan *Authentication*. Ini dibuktikan dengan hasil percobaan *sniffer* tidak dapat melihat pesan asli dalam proses *sniffing*, nilai MAC dan *Key* MAC dapat divalidasi dengan benar di sisi penerima. Untuk analisis *overhead* secara keseluruhan, variasi keamanan AES128-HMAC-SHA256 memiliki frekuensi pengiriman paling besar yaitu 197 data dan memiliki waktu *generate* dan pengiriman data paling kecil yaitu 0,914 ms. Sedangkan variasi keamanan AES256-HMAC-SHA3_512 memiliki frekuensi pengiriman paling besar yaitu 163 data dan memiliki waktu *generate* dan pengiriman data paling besar yaitu 1,104 ms.

Kata Kunci: Keamanan data, Internet of Things, *Message Queuing Telemetry Transport,* AES*,* MAC, HMAC.

SUMMARY

IMPLEMENTATION OF MESSAGE AUTHENTICATION CODE AND ADVANCED ENCRYPTION STANDARD ALGORITHM IN MQTT COMMUNICATION PROTOCOL

Hamzah Diza Santoso

The Internet of Things (IoT) continues to expand rapidly. IoT is currently used in various environments because it offers many benefits and ease of use. Message Queuing Telemetry Transport is the most popular protocol in IoT. The increasing number of sectors that can be using with MQTT also affects device variety or device development in IoT. However, the increased use of MQTT also affects the security of MQTT communications. It is not uncommon to face security threats when using MQTT. This study aims to improve the security of MQTT network communication by considering the security parameters: confidentiality, integrity, and authentication. In addition, this study also aims to determine, through an overhead analysis, whether the proposed method variations are suitable to be applied to IoT devices that have limited resources. This study uses AES as a data encryption method. Variations of AES used are AES128 and AES256. And use MAC to verify data. The MAC type used is HMAC with variations of SHA256, SHA512, SHA3-256, and SHA3-512. Based on the results of the experiments, the combination of AES and MAC methods can secure communication between devices in the MQTT protocol and ensure confidentiality, integrity, and Authentication. It is evidenced by the results of the sniffer experiment not being able to see the original message in the sniffing process, the MAC value and MAC key can be validated correctly on the receiving side. For the overall overhead analysis, the security variation of AES128-HMAC-SHA256 has the largest transmission frequency of 197 data and has the smallest data generation and delivery time of 0.914 ms. Meanwhile, the security variation AES256-HMAC-SHA3_512 has the highest transmission frequency, that is 163 data, and has the largest data generation and delivery time of 1.104 ms.

Keywords: *Data security, Internet of Things, Message Queuing Telemetry Transport, AES, MAC, HMAC.*