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

Abstract

The concept of Internet of Things (IoT) or Machine-to-Machine (M2M) communication is expected to be one of the future network solutions. One of the protocols that is often used in IoT applications is Message Queuing Telemetry Transport (MQTT). MQTT uses less bandwidth, is light in computing, and fast in transmission. Thus, MQTT can be implemented on constrained devices. However, MQTT does not have a default security method so it has some vulnerabilities. The first vulnerability that can be encountered in MQTT is authentication. Lack of authentication can cause unauthorized nodes to use MQTT network resources, which can lead to over connections. This study uses JSON Web Token (JWT) to build a token-based authentication method on MQTT as an additional authentication factor besides username and password. This is done to prevent invalid nodes from logging into the MQTT network. From the test results, the authentication method built can withstand brute force attacks and ensure that no invalid nodes can enter the MQTT network. The second vulnerability that can be encountered in MQTT is data privacy which is caused by the absence of a default data encryption method in MQTT. This can make it easier for attackers to obtain data exchanged on the MQTT network, even if MQTT was built using certain authentication methods. Therefore, this study also uses the Corrected Block Tiny Encryption Algorithm (XXTEA) to encrypt data on MQTT. From the test results, the encryption method used can withstand sniffing attacks. The authentication and encryption methods built can also be run on constrained devices using 405912 bytes of memory (38% of the total program storage) on the publisher node and 406856 bytes of memory (38% of the total program storage) on the subscriber node with an estimated power consumption of 70.9mA for each node.

Keywords: Internet of Things (IoT), Message Queuing Telemetry Transport (MQTT), authentication, JSON Web Token (JWT), encryption, Corrected Block Tiny Encryption Algorithm (XXTEA), constrained devices