Penerapan Autentikasi *One Time Password* berbasis Blockchain pada Protokol MQTT di Jaringan *Internet of Things* untuk Mencegah Serangan *Man in The Middle*

Naufal Zahid Yoga Pratama[1], Vera Suryani[2]

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]naufalyogap@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id

Abstrak

***Message Queue Telemetry Transport* (MQTT) merupakan salah satu protokol yang banyak digunakan pada perangkat *Internet of Things* (IoT) karena ringan dan fleksibel. Protokol MQTT menggunakan model *publish* dan *subscribe* dengan menggunakan broker untuk mengatur pengiriman data. Namun, dalam penggunaannya, protokol MQTT masih rentan terhadap serangan. Serangan yang bisa terjadi pada protokol MQTT salah satunya yaitu serangan *Man in The Middle* (MITM). Karena hal tersebut, diperlukan pengembangan keamanan pada jalannya komunikasi protokol MQTT. Pada penelitian ini, dilakukan pengembangan keamanan dengan menerapkan sistem autentikasi *One Time Password* (OTP) berbasis blockchain pada perangkat IoT untuk melakukan autentikasi antar *client* yang saling terhubung. Kemudian dilakukan pengujian serangan MITM berupa penyusupan data palsu yang dikirim oleh pihak ketiga atau *attacker*. Hasil pengujian yang telah dilakukan, menunjukkan bahwa serangan MITM terhadap perangkat IoT yang menerapkan skema autentikasi OTP berbasis blockchain dapat dicegah dan teridentifikasi. Selain pengujian keamanan, dilakukan juga pengukuran besar kapasitas *memory* yang terpakai. Besar *memory* yang digunakan untuk menerapkan skema autentikasi OTP berbasis blockchain tidak jauh berbeda dengan sistem normal. Hal tersebut ditunjukkan dari pengukuran *memory* berdasarkan waktu saat sistem dijalankan. Penerapan skema autentikasi menghasilkan rata-rata penggunaan *memory* sebesar 3,7910155 MB dan tanpa penerapan skema autentikasi sebesar 3,790039 MB.**

Kata kunci : MQTT, *One Time Password*, Autentikasi, Blockchain, *Man in The Middle*

Abstract

Message Queue Telemetry Transport (MQTT) is one of the protocols that is widely used in Internet of Things (IoT) devices because it is lightweight and flexible. The MQTT protocol uses a publish and subscribe model by using a broker to manage data transmission. However, in its use, the MQTT protocol is still vulnerable to attacks. One of the attacks that can occur on the MQTT protocol is the Man in the Middle (MITM) attack. Due to this, security development is needed in the course of MQTT protocol communication. In this research, security development is carried out by implementing a blockchain-based One Time Password (OTP) authentication system on IoT devices to authenticate between connected clients. Then the MITM attack is tested in the form of fake data sent by a third party or attacker. The test results show that MITM attacks on IoT devices that implement blockchain-based OTP authentication schemes can be prevented and identified. In addition to testing the security of the system, the test also measures the amount of memory used. The amount of memory used to implement the blockchain-based OTP authentication system is not much different from the normal system. This is shown by the memory measurement based on the time the system is running. Average memory usage is 3,7910155 MB with authentication and 3,790039 MB without authentication.

Keywords: MQTT, One Time Password, Authentication, Blockchain, Man in The Middle

1. Pendahuluan

Latar Belakang

Internet of Things (IoT) merupakan jaringan objek fisik atau benda yang digunakan untuk menghubungkan dan melakukan pertukaran data dengan perangkat lain melalui internet [1] . IoT digunakan untuk sensor, *software*, sistem tertanam, dan teknologi lainnya. Sampai saat ini IoT memiliki beberapa protokol, salah satunya yaitu MQTT (*Message Queue Telemetry Transport*). Protokol MQTT merupakan salah protokol IoT yang paling populer, karena protokol MQTT merupakan protokol jaringan yang ringan dalam pengaplikasiannya dan fleksibel dalam dukungan skenario aplikasi yang memberikan keseimbangan untuk para pengembang IoT. MQTT menggunakan model *publish-subscribe* sebagai klien dan broker sebagai penghubung antara klien *publish-subscribe*. Broker berfungsi untuk menerima dan mengirim data dari semua klien *publish* dan klien *subscribe*. Namun, dalam penggunaannya, protokol MQTT ini masih rentan terhadap serangan [2], [3].