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].

Penelitian [2] membuat kategori serangan apa saja yang bisa terjadi pada protokol MQTT. Salah satu kategorinya yaitu *Tampering Data*, dimana penyerang dapat merusak integritas pesan dan dapat memodifikasi pesan tersebut dengan menggunakan serangan *Man in The Middle* (MITM). MITM merupakan suatu serangan dimana penyerang secara rahasia mengubah korespondensi antara dua pihak yang saling percaya bahwa mereka sedang berkomunikasi satu sama lain, atau dengan kata lain penyerang melakukan kegiatan eavesdropping (menyadap) kepada kedua pihak dan memungkinkan penyerang untuk mengirimkan, mengubah dan mengambil data [3], [4]. Karena protokol MQTT tersebut masih rentan terhadap serangan MITM, maka diperlukannya suatu solusi untuk mengatasi hal tersebut. Menurut penelitian yang dilakukan oleh [2] dan [5], Serangan MITM pada protokol MQTT dapat dicegah dengan menggunakan teknologi enkripsi dan autentikasi [2], [4]. Dalam kedua penelitian tersebut tidak menuliskan teknologi dan autentikasi seperti apa yang dapat mencegah serangan ini. Maka dari itu, diperlukannya suatu teknologi yang dapat digunakan untuk enkripsi dan autentikasi.

Salah satu teknologi terenkripsi yang dapat digunakan untuk mengenkripsi pesan yaitu dengan memanfaatkan Blockchain [6], [7], [8]. Blockchain dapat diaplikasikan pada perangkat IoT untuk peningkatan keamanan komunikasi karena blockchain merupakan jaringan terdistribusi yang dapat melakukan enkripsi pada komunikasi antar perangkat IoT [9]. Sebuah studi pernah dilakukan seperti pada penelitian [10] tentang pemanfaatan blockchain untuk peningkatan keamanan pada protokol MQTT. Namun, penelitian tersebut hanya berfokus pada enkripsi komunikasi data saja. Karena tidak adanya proses autentikasi, maka perangkat yang dibuat dalam penelitian tersebut masih rentan terhadap serangan MITM. Selain enkripsi, sebuah proses autentikasi juga diperlukan untuk menghindari serangan MITM, seperti yang ditulis pada penelitian [5].

Dalam penelitian ini, akan diterapkan sistem autentikasi berbasis blockchain yang dirancang oleh penelitian [11] dan digunakan untuk mengatasi kerentanan protokol MQTT terhadap serangan MITM. Penelitian [11] mengusulkan sebuah mekanisme peningkatan keamanan yang ringan dan sistem autentikasi yang kuat. Sistem yang dirancang oleh penelitian [11] yaitu autentikasi *One Time Password* (OTP) berbasis blockchain yang dirancang untuk autentikasi *client* pada protokol MQTT. Skema autentikasi yang diusulkan dan penyimpanan data ke dalam blockchain akan diimplementasikan ke dalam rancangan IoT dalam penelitian ini, dan kemudian dilakukan uji coba serangan MITM kepada sistem yang telah dibangun.

Topik dan Batasannya

Berdasarkan latar belakang, penelitian ini akan menerapkan sistem autentikasi OTP berbasis blockchain dan melakukan pengujian keamanan melalui serangan MITM. Batasan masalah pada penelitian ini adalah:

1. Uji coba serangan MITM menggunakan program Scapy.
2. Jaringan internet untuk menjalankan keseluruhan rancangan sistem dan pengujian menggunakan jaringan lokal.
3. Entitas *client* dalam sistem rancangan hanya dua, satu *publisher* (perangkat IoT) dan satu *subscriber* (Laptop).

Tujuan

Penelitian ini bertujuan untuk dapat mengimplementasikan sistem autentikasi OTP berbasis blockchain pada rancangan IoT yang dibuat. Melakukan analisis hasil perfomansi dari implementasi sistem autentikasi berdasarkan penggunaan *memory*. Serta melakukan uji serangan *Man in The Middle* (MITM) kepada rancangan IoT yang dibuat.

Organisasi Tulisan

Urutan penulisan dalam penelitian ini dimulai dengan studi terkait penelitian untuk menjadi acuan pada pengerjaan tugas akhir, kemudian dilanjutkan dengan perancangan sistem yang dibangun dan evaluasi hasil pengujian. Bagian terakhir dalam penelitian ini yaitu penarikan kesimpulan pada penelitian yang sudah dilakukan.

2. Studi Terkait

Penelitian oleh Bhanujyothi *et al.* [5] menggunakan mesin pencarian Shodan untuk mengumpulkan informasi ke semua perangkat yang rentan. Peneliti menggunakan *port* 1833 (*port* default broker MQTT) untuk mencari broker yang terdeteksi oleh mesin pencarian. Hasil penelitian ini menunjukkan bahwa perangkat dengan protokol MQTT standar dapat terdeteksi oleh mesin pencarian Shodan dan semua informasi dari perangkat tersebut terlihat. *Attacker* dapat menggunakan informasi tersebut untuk melakukan serangan pada perangkat korban. Penelitian ini memberikan informasi serangan apa saja yang dapat terjadi dalam protokol MQTT. Serangan yang dapat terjadi yaitu: Denial of Service (DoS), *Man in The Middle* (MITM), dan Intrusion.

Penelitian oleh Syed *et al.* [2] melakukan pengujian keamanan protokol MQTT dengan melakukan serangan *Denial of Service* (DoS) dan *flood attack*. Dari uji coba yang dilakukan, protokol MQTT sangat rentan terhadap serangan DoS. Peneliti melakukan kategorisasi serangan apa saja yang dapat terjadi dan membuat skenario serangannya. Kategori serangan yang dibuat yaitu: *Denial of Service* (DoS), *spoofing*, *Information disclosure*, *elevation of privileges*, dan *tampering data* menggunakan serangan MITM.