BAB I Pendahuluan

1.1 Latar Belakang

Seiring perkembangan zaman, banyak inovasi teknologi yang telah berkembang, salah satunya *Internet of Things* (IoT). *Internet of Things* merupakan inovasi teknologi dimana sebuah benda yang berada di sekeliling kita memiliki komponen yang dapat menyimpan suatu data atau informasi mengenai lingkungannya dan berkomunikasi dengan benda lain atau manusia yang terhubung dengan internet [1]. IoT memberikan banyak manfaat dan kemudahan ketika digunakan, sehingga sekarang ini IoT telah digunakan di berbagai lingkungan. Untuk lingkungan konsumen, biasanya IoT memiliki *smart sensor* seperti *smart watch*, *smart tv*, *health trackers*, dan perangkat IoT yang lain. Sedangkan untuk lingkungan industri, biasanya IoT dikembangkan dan digunakan untuk pekerjaan yang dilakukan secara otomatis untuk diberbagai bidang seperti otomotif, medis, dan yang lainnya.

Perangkat IoT membutuhkan protokol agar dapat berkomunikasi, bertukar data dengan perangkat yang lainnya. Meskipun sekarang ini sudah ada banyak protokol yang diciptakan, tidak sembarang protokol dapat diterapkan dalam jaringan IoT. Hal ini disebabkan karena, perangkat IoT pada umumnya memiliki spesifikasi yang terbatas. Salah satu protokol yang dapat digunakan untuk jaringan IoT adalah MQTT. MQTT merupakan protokol popular yang mekanismenya berupa publish/subscribe pesan antar perangkatnya. Protokol ini memiliki mekanisme publish/subscribe pesan antar perangkat dalam jaringannya. Kecilnya *bandiwidth*, transmsi yang ringan, dan penggunaan memori yang kecil merupakan alasan kenapa protokol ini sangat sering digunakan dalam jaringan IoT[2].

Penerapan IoT memang memudahkan dan membantu manusia dalam menyelesaikan suatu tugas. Tetapi ada hal yang perlu dipertimbangkan juga terkait keamanan pada jaringan IoT. Berdasarkan Book ISACA, terdapat tiga komponen mengenai keamanan informasi yaitu Data Confidentiality, Data Integrity, Data Availability. Selain itu, ada juga keamanan tingkat akses seperti *authentication*, *authorization*, dan *access control* [3]. Pada tahun ini banyak serangan siber yang ditargetkan ke perangkat IoT. Pada laporan RSA 2020, mesin *smart cleaning* menjadi target serangan *remote attack*, termasuk *Denial of Service* dan *camera hacks*. Selain itu, Bitdefender menemukan jenis botnet terbaru yang dijuluki Dark Nexus. Botnet ini terdiri lebih dari 1,372 bots yang tersebar di berbagai negara, seperti China, Korea Selatan, Thailand, Brasil, dan Rusia. Botnet ini mampu melakukan serangan *Distributed Denial of Service* (DDoS), *Self-propagation*, dan C&C *communication*.

Menurut [3], terbatasnya sumber daya perangkat, banyaknya jumlah perangkat yang terkoneksi pada suatu jaringan, dan kurangnya kesadaran masyarakat merupakan faktor jaringan IoT mudah terkena serangan siber. Protokol MQTT merupakan protokol yang memiliki banyak keunggulan untuk perangkat IoT, tetapi hal itu tidak menutupi kekurangannya dalam segi keamanan. Protokol MQTT pada umumnya menyediakan keamanan hanya berupa *username* dan *password* yang berbentuk plain text. Keamanan yang disediakan tidaklah cukup dalam membuat sebuah jaringan aman. Dengan autentikasi dasar MQTT, sebuah jaringan dapat mudah diserang dengan *sniffing* attack. Setelah penyerang berhasil melakukan sniffing attack, penyerang dapat melakukan serangan yang lain seperti seperti mengganti topik paket dari *publisher*, *denial of service*, *man – in – the middle attack* [3], [4].

Untuk mengurangi ancaman serangan siber, keamanan pada protokol dapat ditingkatkan dengan menambahkan mekanisme pada otentikasinya, seperti pada riset [5] yang mengimplementasikan *One – Time – Password* pada MQTT. Selain autentikasi, keamanan juga dapat ditingkatkan dengan menambahkan fitur autorisasi. *Authorization* merupakan mekanisme keamanan yang mengikat suatu perangkat dengan izin yang telah ditetapkan. Salah satu framework autorisasi yang pernah populer yaitu Framework OAuth 1.0a. Framework ini merupakan framework yang digunakan untuk *web servers*.

Pada riset [6], berhasil mengadaptasi framework OAuth1.0a agar dapat digunakan untuk jaringan IoT, yang kemudian dilanjutkan menjadi sebuah produk yang dinamakan Netpie. Dalam risetnya, menganalisis fungsionalitas fitur, penggunaan memori, dan time delay. Tetapi untuk analisis sekuritasnya masih berupa hipotesis terhadap beberapa serangan. Maka dari itu pada penelitian ini, penulis mengusulkan untuk meningkatkan keamanan protokol MQTT dengan menggunakan Netpie versi 2020 sebagai framework OAuth 1.0a sebagai fitur autorisasi. Kemudian, untuk menguji tingkat keamanannya dengan test case, *man – in – the middle attack* dan dilanjutkan dengan *eavesdropping* dan menguji memory consumption pada perangkat.

1.2 Rumusan Masalah

Masalah yang dibahas pada tugas akhir ini :

1. Bagaimana proses implementasi proses otorisasi Netpie pada protokol MQTT dalam jaringan IoT ?
2. Bagaimana hasil perfomansi Netpie pada protokol MQTT berdasarkan parameter *memory consumption*, dan hasil test case MiTM ARP Spoofing dan *eavesdropping* ?

1.3 Batasan Masalah

1. Perangkat IoT yang akan digunakan pada penelitian ini adalah NodeMCU dengan sensor LM35.
2. Perkakas yang akan digunakan untuk pengujian adalah Wireshark, arpspoof, airodump.
3. Platform MQTT yang akan digunakan adalah MQTT yang disediakan oleh Netpie.

1.4 Tujuan

Tujuan dari penelitian tugas akhir ini adalah :

1. Mengimplementasi mekanisme autorisasi dengan menggunakan Netpie pada protokol MQTT.
2. Menganalisis hasil performa memory consumption, dan test case serangan *man – in – the middle attack* ARP Spoofing dan *eavesdropping* pada protokol MQTT dengan terimplementasinya Netpie.