BAB 1 PENDAHULUAN

1.1 Latar Belakang

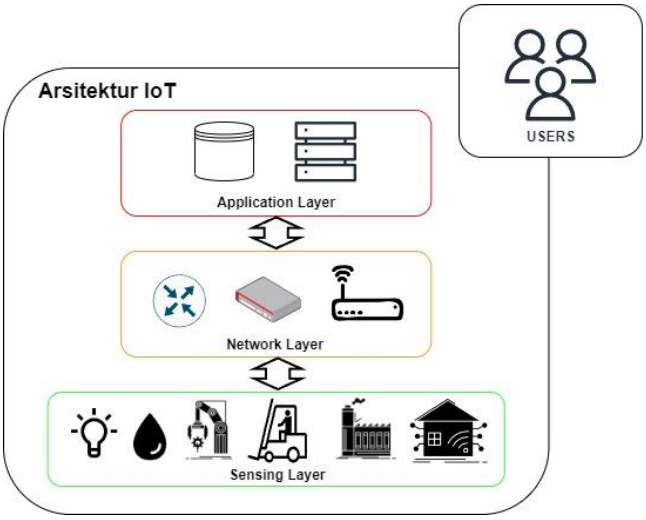
Saat ini kita berada pada era dimana saat suatu teknologi berkembang maka terdapat ancaman terhadap teknologi tersebut. Salah satu dari teknologi tersebut adalah Internet of Things (IoT), beberapa ancaman dapat terjadi pada IoT. IoT secara umum memiliki konsep kumpulan dari banyak objek, layanan, manusia, dan perangkat yang saling berhubungan yang dapat berkomunikasi, berbagi data, dan informasi untuk mencapai tujuan bersama di berbagai bidang dan aplikasi [1]. Pada tahun 2017, terjadi peningkatan serangan terhadap perangkat IoT sebesar 600% [2]. Hal tersebut dapat terjadi dikarenakan sebagian besar perusahaan yang memproduksi perangkat IoT tidak mempertimbangkan faktor keamanan dari sebuah perangkat namun lebih menekankan pada ukuran , biaya, dan kegunaan [2]

Beberapa bentuk ancaman pada teknologi IoT dapat berupa orang yang tidak berwenang mendapatkan akses untuk mengakses sebuah data dan menyalahgunakan informasi yang bersifat personal, penyerang membuat sistem mudah untuk diserang, serta ancaman kepada keselamatan pengguna [3]. Maka dari itu, diperlukan pengamanan yang dilakukan untuk mencegah hal tersebut terjadi. Salah satu upaya pengamanan tersebut adalah dengan mengamankan jaringan menggunakan *Virtual Private Network* (VPN) [4]. Dengan VPN, komunikasi atau transfer data lebih aman karena adanya sistem *tunneling* (terowongan) yang membuat data tersebut terenkripsi.

Sebelumnya terdapat penelitian terdahulu yang telah dilakukan dengan judul “Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi” [4]. Penelitian tersebut mengembangkan dan menerapkan sistem VPN pada IoT menggunakan simulasi GNS3 dan VM sebagai gambaran perangkat IoT. Penelitian ini menguji kinerja dan keamanan jaringan IoT dengan menggunakan empat jenis VPN, yaitu PPTP, L2TP, IPsec, dan L2TP IPsec. Jika dibandingkan dengan penelitian ini, perbedaan yang dilakukan dengan penelitian sebelumnya adalah protokolnya. Protokol yang digunakan untuk menguji kinerja dan keamanan jaringan IoT adalah *GRE over IPSec* dimana protokol Generic Routing Encapsulation (GRE) dikonfigurasikan

bersama protokol IP Security (IPSec) dalam satu jaringan yang sama sehingga komunikasi antar perangkat lebih aman.

Dalam penelitian ini, tidak menggunakan perangkat IoT sesungguhnya namun berfokus pada simulasi keamanan jaringan menggunakan VPN IPSec dan GRE dengan simulator GNS3 yang diskenariokan seperti lingkungan IoT. *Internet Protocol Security* atau IPSec adalah protokol untuk mengamankan komunikasi pada Internet Protocol/IP dengan autentikasi dan juga melakukan enkripsi di setiap paket IP. Dan definisi *Generic Routing Encapsulation* (GRE) adalah protokol yang menggunakan teknologi *tunneling* sehingga dapat melakukan enkapsulasi berbagai protokol untuk kebutuhan link *virtual point-to-point*. Nantinya akan dilakukan konfigurasi pada *Virtual PC Simulator* (VPCS) sebagai gambaran perangkat IoT. Kemudian, untuk memeriksa trafik data, aplikasi yang digunakan adalah *Wireshark*. Trafik data yang dianalisis berupa throughput dan ping rata - rata.



Gambar 1. 1 *Arsitektur lapisan IoT*

Pada arsitektur IoT yang ditunjukkan gambar 1.1 , terdapat *application layer*, *network layer*, dan *sensing layer*. *Application layer* merupakan lapisan yang menyediakan berbagai layanan dan fungsi untuk pengguna, seperti penyimpanan data, analisis data, visualisasi data, dan kontrol perangkat. Lapisan ini yang berinteraksi langsung dengan pengguna melalui aplikasi web atau aplikasi seluler. *Application layer* juga berinteraksi dengan lapisan jaringan untuk menerima dan mengirim data dari dan ke perangkat-perangkat IoT. Lapisan aplikasi biasanya

menggunakan protokol seperti HTTP dan MQTT. *Network layer* adalah lapisan yang menyediakan konektivitas dan transmisi data antara perangkat-perangkat IoT. *Network Layer* menggunakan berbagai teknologi jaringan, seperti Wi-Fi, Bluetooth, atau seluler, untuk menghubungkan perangkat-perangkat IoT dengan router. Pada lapisan ini, menggunakan protokol seperti IP, TCP, UDP, atau 6LoWPAN untuk mengatur alamat, rute, dan format data yang dikirim dan diterima. Terakhir, *Sensing layer* atau lapisan sensor yang bertanggung jawab untuk mengumpulkan data dari lingkungan fisik, seperti suhu, kelembaban, cahaya, gerakan, atau suara. Lapisan ini juga bertugas untuk mengirim data ke lapisan jaringan atau menerima instruksi dari lapisan aplikasi untuk mengontrol perangkat-perangkat IoT.

1.2 Rumusan Masalah

1. Bagaimana cara mengamankan jalur komunikasi jaringan IoT dengan Protokol IPSec dan GRE?

2. Bagaimana cara untuk menguji hasil implementasi protokol GRE dan IPSec?

3. Parameter apa yang di analisa setelah protokol GRE dan IPSec diterapkan ?

4. Bagaimana performa dari segi QoS sebelum menerapkan IPSec dan GRE dan setelah menerapkan IPSec dan GRE?

1.3 Tujuan dan Manfaat

Tujuan dibuatnya penelitian ini adalah menerapkan pengamanan jaringan menggunakan IPSec dan GRE pada IoT melalui simulasi di GNS3. Harapannya melalui simulasi ini, hasil pengamanan tersebut dapat di analisa terlebih dahulu sebelum nantinya akan di implementasikan langsung pada lapangan. Hal ini dapat meminimalisir biaya yang dikeluarkan jika dibandingkan dengan menerapkan tanpa menggunakan simulasi.

1.4 Batasan Masalah

Untuk mengarahkan pembahasan terhadap tujuan yang ingin dicapai, maka ditetapkan batasan – batasan masalah sebagai berikut :

1. Perangkat IoT yang disimulasikan berupa Virtual PC Simulator (VPCS)
2. Pengujian keamanan data menggunakan aplikasi *Wireshark*
3. Lingkungan IoT yang disimulasikan diwakilkan dengan 1 VPCS
4. Penelitian akan diterapkan pada studi kasus lingkungan pabrik