BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi memberikan fasilitas terhadap kita dalam segala hal, termasuk hal yang berkaitan dengan pekerjaan yang biasa dilakukan manusia[1]. Di era globalisasi dan kemajuan teknologi, *Internet of Things (IoT)* telah menjadi pendorong utama untuk menghubungkan perangkat fisik dalam jaringan terintegrasi. Hal ini memungkinkan konektivitas dan pertukaran data yang lebih efisien, membuka peluang baru di berbagai sektor. Akan tetapi peningkatan jumlah perangkat yang terhubung juga membawa tantangan baru terkait keamanan dan privasi data. Solusi terbaik dari permasalahan ini dengan menggunakan *Virtual Private Network* (*VPN*) yang sifatnya lebih aman. Dengan VPN jaringan yang digunakan seolah-olah privat. Sehingga menjadi pembatas untuk siapapun yang mengaksesnya[2].

VPN memberikan lapisan keamanan tambahan dengan menyediakan saluran terenkripsi melalui jaringan publik, seperti Internet. Menerapkan VPN pada perangkat ESP32, bisa menjadi solusi yang efektif. Salah satu protokol VPN yang saat ini banyak digunakan adalah *WireGuard*, yang dikenal karena kecepatan dan keamanannya. Keunggulan dari VPN *WireGuard* yaitu kemudahan dalam penggunaan dan kemampuan enkripsi yang baik dengan menggunakan kunci dari kedua pengguna. Selain itu, VPN ini juga memiliki mekanisme kombinasi untuk otentikasi. Protokol ini dapat menyembunyikan isi komunikasi di protokol HTTP pada sistem[3].

Oleh karena itu, tujuan proyek akhir ini bertujuan memberikan solusi yang aman dan efisien. Dengan menggunakan *WireGuard* VPN, komunikasi antara ESP32 dan server dapat dienkripsi dengan baik, sehingga data sensitif seperti perintah kontrol tetap aman dari akses yang tidak sah. Dengan demikian komunikasi aman untuk layanan

IoT merupakan langkah yang tepat dalam meningkatkan keamanan dan kenyamanan pengguna.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dibahas sub bab sebelumnya, salah satu masalah yang terjadi adalah masalah keamanan dan privasi data. Oleh karena itu, rumusan masalah dalam proyek akhir ini adalah Bagaimana cara mengimplementasikan *WireGuard* VPN pada server MikroTik dan klien ESP32 untuk memastikan komunikasi yang aman dalam layanan *IoT*?

1.3 Tujuan

Tujuan proyek akhir ini adalah sebagai berikut.

1. Mampu mengimplementasikan VPN pada perangkat router dan ESP32 untuk memberikan fitur keamanan komunikasi.
2. Mampu mengembangkan sistem kontrol jarak jauh yang memanfaatkan teknologi VPN untuk memastikan data yang terkirim dan diterima tetap terlindungi.

1.4 Batasan Masalah

Ruang lingkup batasan masalah dalam penulisan laporan proyek akhir ini hanya terbatas pada masalah-masalah sebagai berikut.

1. Fokus pada implementasi VPN pada perangkat router dan ESP32 dengan *Wireguard* VPN.
2. Keunggulan menggunakan VPN pada perangkat router dan ESP32.
3. Hanya menggunakan pengujian kinerja dari sistem sniffing.