Komunikasi Aman Untuk Layanan Internet Of Thing (Iot)

1st Diva Sofy Novianandа Saputra
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
divasofy@student.telkomuniversity.ac.id

2nd Prajna Deshanta Ibnugraha
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
prajna@staff.telkomuniversity.ac.id

3rd Muhammad Ikhsan Sani
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
ikhsansani@staff.telkomuniversity.ac.id

***Abstrak* — Pesatnya perkembangan teknologi membuat banyak aspek kehidupan menjadi lebih mudah, termasuk pekerjaan sehari-hari. Di era globalisasi, *Internet of Things* (*IoT*) menghubungkan perangkat fisik ke jaringan terintegrasi, memungkinkan komunikasi dan pertukaran data yang efisien. Namun, hal ini juga menimbulkan tantangan dalam hal perlindungan data dan privasi. Solusi efektif untuk masalah ini adalah dengan menggunakan *Virtual Private Network* (VPN), yang menyediakan saluran terenkripsi melalui jaringan publik seperti Internet. Tugas akhir ini bertujuan untuk menggunakan *WireGuard* VPN pada server MikroTik dan klien ESP32 untuk memastikan komunikasi dan enkripsi yang aman ke layanan *IoT*. *WireGuard* terkenal dengan kecepatan, keamanan, dan kemudahan penggunaannya. Proyek akhir ini berfokus pada penggunaan VPN pada router dan ESP32 untuk menyediakan fitur keamanan komunikasi dan mengembangkan sistem kendali jarak jauh yang aman. Menggunakan *WireGuard* VPN, proyek ini berupaya meningkatkan keamanan pengguna dan memudahkan pengelolaan perangkat *IoT*.**

Kata kunci*— ESP32, *Internet Of Things* (*IoT*), Keamanan, *Wireguard

I. PENDAHULUAN

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.

II. KAJIAN TEORI

A. *TINJAUAN Pustaka*

Internet Of Things (IoT) telah menjadi salah satu teknologi yang berkembang pesat, menghadirkan berbagai manfaat dalam berbagai sektor. Namun, keamanan masih menjadi tantangan utama dalam implementasi IoT. Keamanan IoT sangat penting karena perangkat ini sering kali terhubung ke jaringan yang sangat rentan dan dapat menimbulkan kerentanan dan risiko keamanan yang signifikan jika tidak diamankan dengan benar[4]. Hal ini memerlukan solusi keamanan yang kuat untuk melindungi data dan menjaga integritas sistem.

Lebih lanjut penelitian yang telah mengkaji *Internet Of Things* (IoT) yang berjudul ”Sistem Keamanan Rumah Berbasis *Internet Of Things*”. Penelitian sebelumnya telah menggunakan SMS gateway pada sistem keamanan rumah, namun teknologi ini telah diperluas hingga mencakup mikrokontroler dan sistem berbasis IoT yang terdiri dari sensor IR dan komponen pendukung lainnya. Sistem juga dilengkapi dengan pengambilan gambar sebagai alat notifikasi. Hasil penelitian menunjukkan bahwa sensor IR efektif mendeteksi sesuatu dan pesan dikirimkan ketika sensor mendeteksi gerakan. Sistem ini bekerja dengan baik dalam jarak jauh selama Anda terhubung ke internet[5].

Dalam era digital yang terus berkembang, salah satunya dalam bidang keamanan dan privasi data. Penggunaan Virtual Private Network (VPN) sebagai solusi untuk meningkatkan keamanan dan privasi dalam komunikasi data. Terdapat penelitian yang telah dilakukan. Mengangkat topik terkait penerapan VPN yaitu ” Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik”. Terdapat peningkatan ketergantungan pada teknologi informasi untuk aktivitas online, yang menyebabkan tuntutan yang lebih tinggi terhadap keamanan dan efisiensi informasi. Proses otentikasi pada jaringan publik rentan terhadap kebocoran data sehingga diperlukan koneksi yang aman seperti VPN. *WireGuard,* yang menggunakan enkripsi tingkat lanjut, dipilih karena kecepatan dan keamanannya. Pengembangan sistem ini menggunakan tools seperti metodologi PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) dan Unified Modeling Language.

WireGuard VPN berjanji untuk membuat data yang dikirimkan lebih aman dan memungkinkan Anda membuat koneksi secara pribadi antara jaringan jarak jauh melalui Internet publik[6].
Pada penelitian yang berjudul ”Analisa Virtual Private Network Menggunakan OpenVPN dan Point To Point Tunneling Protocol”. Pemrosesan data menjadi lebih efisien jika satu server mengumpulkan seluruh data dan menyediakan server jaringan VPN untuk semua pengguna. VPN menggunakan Point-to-Point Tunneling Protocol (PPTP) dan OpenVPN untuk memberikan akses mudah dan cepat ke sistem informasi melalui internet kapan saja dan di mana saja. Kecepatan dan keamanan VPN mencegah kebocoran data. Implementasi dimulai dengan menginstal Ubuntu Server 14.04 pada dua mesin virtual sebagai server VPN. Pengujian meliputi kinerja (kehilangan paket, transmisi bolak-balik, dan WinSCP) serta keamanan (panggilan dan sniffing layanan). Hasil pengujian menunjukkan bahwa OpenVPN lebih unggul dibandingkan PPTP dalam hal kinerja dan keamanan[1].

Selain itu, ada penelitian lain dengan judul ”Implementasi Keamanan Jalur Internet Menggunakan Ip Tunneling pada OpenVPN Access Server dengan Protokol OpenVPN dan Protokol DNS Over HTTPS”. Penelitian ini menggabungkan protokol OpenVPN dengan protokol DNS Over HTTPS (DOH). Keamanan dan stabilitas akses melalui OpenVPN memiliki kualitas layanan (QoS) yang mendekati akses langsung, dengan perbedaan sekitar 1,7% antara paket keluar dan masuk. Ketika protokol OpenVPN dan DOH digunakan bersamaan, perbedaan rata-rata kehilangan paket meningkat menjadi 1,8%. Akses DNS menggunakan OpenVPN+DOH memiliki waktu respon lebih lama dibandingkan akses DNS langsung ke ISP Anda, namun tidak ada dampak nyata pada kecepatan akses. Penelitian ini bertujuan untuk menganalisis keamanan akses Internet dengan menggabungkan protokol OpenVPN dan DNS Over HTTPS[7].

Penelitian yang pernah dilakukan dengan judul “Rancangan Prototype Smart Home Untuk Jarak Jauh Pada Perangkat Rumah dengan Mikrokontroler ESP32”. Penelitian ini memanfaatkan ESP32 untuk mengontrol peralatan rumah tangga dari mana saja dan kapan saja, bahkan jika diperlukan koneksi internet. Sistem dikembangkan dengan pendekatan prototyping menggunakan mikrokontroler node MCU ESP32, konektivitas Internet (Wi-Fi), serta aplikasi web dan Android sebagai media kontrol. Pengujian menunjukkan bahwa sistem dapat mengontrol lampu, TV, kipas angin, alarm, dan kunci pintu sebagaimana mestinya[8].

Dalam penelitian yang berjudul “Kendali Otomatis Pintu Gerbang dengan ESP32 dan RFID”. Tujuan dari penelitian ini adalah untuk mengembangkan sistem kendali gerbang otomatis menggunakan mikrokontroler ESP32 dan teknologi RFID. Sistem yang diusulkan menggunakan RFID untuk mengidentifikasi akses pengguna dan otomatisasi gateway kontrol. Integrasi ESP32 memungkinkan pengguna mengontrol gateway secara nirkabel dan mengelola akses dengan lebih efisien[9].

B. *Dasar Teori*

1. Virtual Private Network (VPN)

VPN adalah teknologi komunikasi yang memungkinkan pengguna untuk mengakses jaringan lokal melalui jaringan publik, seperti internet, dengan menciptakan koneksi yang aman dan terenkripsi[10]. Dengan menggunakan VPN pengguna dapat memiliki hak akses dan pengaturan seolah-olah mereka terhubung langsung ke jaringan lokal, mereka dapat mengakses informasi dan sumber daya di jaringan tersebut[11]. VPN digunakan untuk meningkatkan keamanan dan privasi saat berkomunikasi melalui jaringan tidak aman seperti Internet.

2. ESP32

ESP32 adalah mikrokontroler berbasis sistem SOC (*system-on-chip*) dari perusahaan China Espressif Systems. ESP32 adalah penerus ESP8266 dan menawarkan fitur yang diperluas dan lebih canggih[12]. ESP32 menampilkan arsitektur dual-core Xtensa LX6 dengan kecepatan clock hingga 240 MHz dan mendukung berbagai fitur seperti Witd-Fi, BLE (Bluetooth Low Energy), periferal I/O yang kaya, dan kemampuan pengolahan yang lebih baik[13]. ESP32 digunakan sebagai perangkat kontrol untuk terhubung ke server MikroTik VPN melalui *WireGuard* VPN, memungkinkan komunikasi yang aman untuk mengontrol perangkat lain.

3. Wireguard VPN

WireGuard adalah teknologi VPN *open-source* yang dikenal karena performanya yang cepat, sederhana, dan efisien. Untuk menghindari *Single Point of Failure* (SPOF) dalam desain jaringan, diperlukan mekanisme cadangan jika jalur utama mengalami kegagalan[14]. Dengan mengintegrasikan sistem dengan VPN *WireGuard*, seluruh data yang dikirimkan dari sistem pemantau akan terenkripsi secara sempurna, sehingga hanya dapat dibaca oleh klien yang memiliki kunci dekripsinya. Hal ini memastikan bahwa data tetap aman dan tidak dapat diakses oleh pihak yang tidak bertanggung jawab, menjaga integritas dan kerahasiaan informasi dalam komunikasi jaringan[15].*Wireguard* VPN digunakan untuk menjamin keamanan dan enkripsi data kontrol yang dikirim antara ESP32 dan MikroTik, mencegah akses tidak sah, dan menjaga integritas data.

4. Mikrotik Hap Lite

Mikrotik adalah sistem operasi berbasis perangkat lunak yang dirancang untuk mengubah komputer menjadi jaringan berbasis linux[16]. Mikrotik dapat dikontrol dengan dua cara yaitu menggunakan perangkat lunak dan perangkat keras. Perangkat lunak yang digunakan adalah winbox, sedangkan perangkat keras yang digunakan RouterBOARD. MikroTik didesain khusus untuk memudahkan berbagai kebutuhan jaringan komputer, mulai dari perancangan hingga pembangunan sistem jaringan yang kompleks. Seiring dengan kemajuan teknologi, MikroTik terus berkembang dengan penambahan berbagai fitur baru, menjadikannya semakin diminati oleh pengguna[17]. MikroTik menyediakan infrastruktur jaringan yang aman dan stabil untuk komunikasi antara ESP32 dan perangkat kontrol lainnya melalui *WireGuard* VPN.

5. Wireshark

Wireshark merupakan alat analisis jaringan yang biasa digunakan untuk menangkap dan menganalisis paket data yang melewati suatu jaringan. *Wireshark* memungkinkan peneliti memantau lalu lintas jaringan dengan cermat, mengidentifikasi masalah kinerja, dan mengevaluasi implementasi. [18]. *Wireshark* memantau dan menganalisis lalu lintas jaringan VPN Anda untuk memastikan bahwa koneksi dan komunikasi antara ESP32 dan MikroTik Anda berfungsi dengan baik dan untuk mengidentifikasi potensi masalah pada lalu lintas.

6. Relay

Relay adalah komponen elektronik yang berfungsi sebagai saklar magnetik, yang beroperasi ketika arus listrik mengalir melaluinya[19]. Relay adalah kawat tembaga yang menghasilkan gaya magnet untuk menarik pelat ke dalam sehingga menyebabkan saklar pindah ke posisi “*On*”. Dalam penerapannya relay memerlukan tegangan input atau vcc agar bisa aktif, biasanya 12 volt atau lebih tergantung kebutuhan. Pada sistem pembuatan gerbang otomatis, relay berperan

penting dalam menghidupkan motor DC yang menggerakan gerbang[20]. Relay bertindak sebagai antarmuka ke ESP32 dan dikontrol melalui koneksi VPN yang aman.

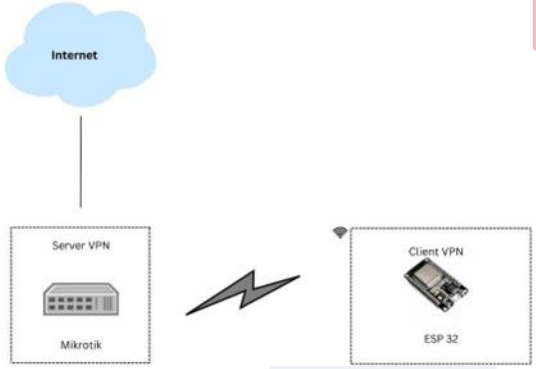
Ketika perintah kontrol dikirim melalui *WireGuard* VPN, ESP32 mengaktifkan atau menonaktifkan relay sesuai dengan instruksi yang diterimanya.

7. Internet Of Things

Internet of Things (*IoT*) adalah teknologi yang memungkinkan *smart grid* untuk mengumpulkan, memantau, dan menganalisis status dan kinerja jaringan listrik, serta mengirimkan sinyal daya yang relevan[21]. Iot akan menciptakan lingkungan internet yang lengkap, sehingga masyarakat dapat lebih mudah mengakses berbagai teknologi cerdas yang terintegrasi dengan otomatisasi, sehingga dapat digunakan kapan saja dan di mana saja[22].

III. ANALISIS DAN PERANCANGAN

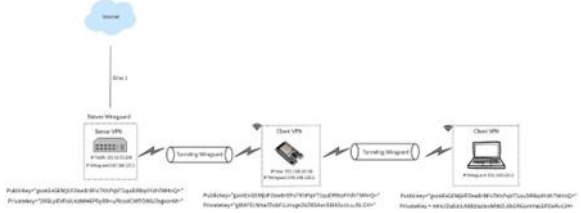
A. Gambaran Sistem Saat Ini



GAMBAR 3.1
Gambaran Saat Ini

Gambaran sistem saat ini ditunjukan pada gambar 3.1 yaitu Sistem ini menggambarkan koneksi antara Server VPN Mikrotik dan klien VPN ESP32 melalui jaringan internet. Mikrotik saat ini berfungsi sebagai server, akan tetapi belum menerapkan protokol WireGuard VPN untuk mengenkripsi data. ESP32 terhubung langsung ke jaringan WiFi menggunakan pengaturan SSID dan password yang telah dikonfigurasi untuk mendukung komunikasi dan kontrol jarak jauh, yang ditunjukkan dengan simbol petir sebagai representasi dari koneksi wireless. Karena sistem ini belum menggunakan VPN atau metode enkripsi lainnya, komunikasi antara ESP32 dan Mikrotik rentan terhadap ancaman keamanan seperti sniffing dan man-in-the- middle (MITM).

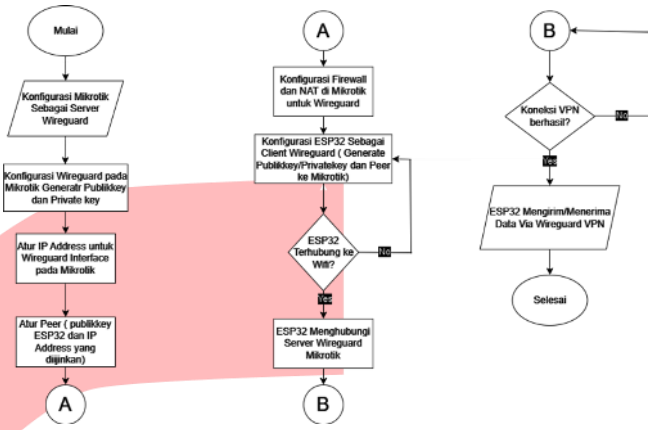
B. Gambaran Sistem Usulan



GAMBAR 3.2
Sistem Usulan

Gambaran sistem usulan ditunjukan pada gambar 3.2 yaitu menggambarkan arsitektur jaringan yang menggunakan sistem VPN WireGuard, di mana klien terhubung secara aman melalui tunneling VPN. Server VPN sebagai pengelola koneksi wireguard VPN. Klien pertama adalah ESP32 yang berfungsi sebagai perangkat kontrol yang menghubungkan ke server VPN menggunakan wireguard VPN. Klien kedua adalah laptop yang berfungsi untuk membuka web dan memastikan komunikasi menggunakan wireguard berjalan dengan baik. Masing- masing perangkat menggunakan kunci publik dan privat unik untuk autentikasi data, memastikan bahwa semua transmisi data berlangsung secara aman. Sistem ini menggambarkan bagaimana komunikasi antara klien dan server dapat dilakukan dengan aman melalui tunneling WireGuard, menjamin keamanan dan integritas data dalam jaringan.

C. Flowchart



GAMBAR 3.3
Flowchart

Gambar flowchart 3.3 tersebut menggambarkan implementasi sistem komunikasi aman menggunakan WireGuard VPN diawali dengan mengkonfigurasi MikroTik dengan menginstal paket WireGuard dan membuat kunci enkripsi untuk antarmuka WireGuard. Selanjutnya ESP32 dikonfigurasi dengan menghubungkan WireGuard dengan Arduino IDE, dan mengatur kunci enkripsi untuk berkomunikasi dengan server MikroTik. Setelah itu, koneksi VPN dibuat dengan membuat kunci enkripsi dan mengatur peer pada MikroTik dan ESP32. Pengujian koneksi VPN dilakukan untuk memastikan ESP32 dapat terhubung ke MikroTik melalui Internet dengan benar. Pemantauan jaringan dilakukan dengan menginstal Wireshark di komputer untuk menangkap paket data, yang memungkinkan analisis mendalam terhadap lalu lintas data yang dienkripsi oleh WireGuard. Analisis paket data memastikan bahwa semua data yang dikirim dan diterima melalui VPN dienkripsi dengan benar, serta mengidentifikasi potensi kebocoran data atau masalah keamanan lainnya.

IV. IMPLEMENTASI DAN PENGUJIAN

A. Implementasi

Implementasi sistem komunikasi yang aman menggunakan teknologi WireGuard VPN dan IoT dilakukan dengan mengkonfigurasi MikroTik sebagai server dan ESP32 sebagai klien. Prosesnya dimulai dengan menyiapkan server VPN di MikroTik dan menginstal WireGuard di ESP32 untuk memastikan koneksi terenkripsi dan aman. Sistem dipantau menggunakan sniffing dengan Wireshark. Hal ini memungkinkan paket data yang dikirim dan diterima dianalisis untuk memastikan tidak ada kebocoran data dan komunikasi tetap terenkripsi dengan baik. Pemantauan jaringan ini memungkinkan Anda memantau kinerja dan keamanan sistem Anda secara real time, memberikan lapisan keamanan tambahan terhadap potensi ancaman.

1. Prototype

GAMBAR 4.1
Prototype Hardware

Gambar di atas menunjukkan prototipe perangkat keras yang terdiri dari dua komponen utama. Di sisi kiri terdapat mikrokontroler ESP32 yang terhubung ke relay. Relay ini digunakan untuk mengontrol perangkat dan ESP32 sebagai pengontrol utama yang mengirimkan sinyal untuk mengaktifkan atau menonaktifkan relay. Di sisi kanan ada router atau perangkat jaringan yang digunakan untuk menghubungkan ESP32 ke jaringan internet melalui WiFi. Router ini mendukung komunikasi jarak jauh, melalui VPN, memungkinkan mengontrol ESP32 dari jarak jauh dan mengoperasikan perangkat yang terhubung.

2. Tampilan

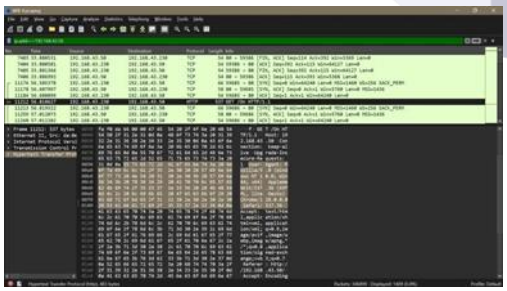
GAMBAR 4.2
Tampilan Web

Tampilan web ini untuk mengontrol ESP32 melalui jaringan dari jarak jauh. Tampilan ini menunjukan tombol On dan Off. Tampilan ini sebagai halaman kontrol utama yang dapat di akses melalui wifi atau VPN dari perangkat yang terhubung ke jaringan lokal.

B. Pengujian

1. Pengujian Tanpa Menggunakan VPN

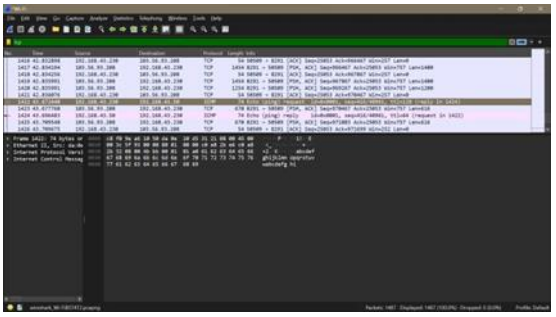
a. Kontrol On/Off



GAMBAR 4.4
Hasil Kontrol On/Off Tanpa VPN.

Gambar di atas menunjukan bahwa ada komunikasi antara server dan ESP32 di jaringan lokal. Terdapat pertukaran informasi menggunakan protokol HTTP. Semua ini dilakukan tanpa menggunakan VPN. Artinya alamat IP yang tertera adalah alamat Esp32 dan server sebenarnya di jaringan. Karena data tidak dilindungi oleh enkripsi, informasi sensitif dapat diakses dengan mudah oleh pihak yang tidak berwenang, membuat komunikasi jaringan ini tidak aman dan berisiko. Dengan menganalisis hasil perekaman jaringan yang dipilih, informasi jaringan yang ditangkap menggunakan program Wireshark dapat diperoleh[23].

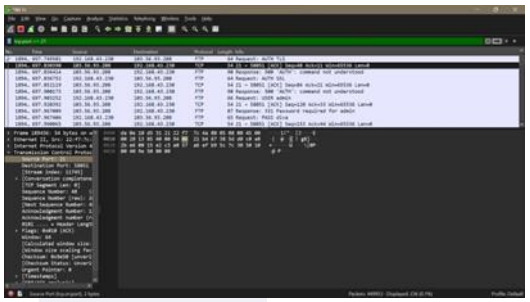
b. *Internet Control Message Protocol* (ICMP)



GAMBAR 4.5
Hasil ICMP Tanpa VPN

Gambar di atas menunjukan bahwa ada komunikasi antara server dan ESP32 di jaringan lokal. Terdapat pertukaran informasi menggunakan protokol ICMP. Alamat IP yang tertera adalah alamat sebenarnya di jaringan. Karena data tidak dilindungi, membuat komunikasi jaringan ini tidak aman dan berisiko.

c. File Transfer Protocol (FTP)

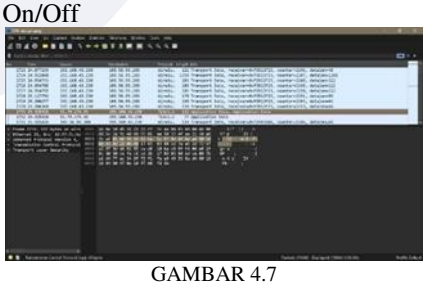


GAMBAR 4.6
Hasil FTP Tanpa VPN

Gambar di atas menunjukan bahwa ada komunikasi antara server dan ESP32 di jaringan lokal. Terdapat pertukaran informasi menggunakan protokol FTP. Semua IP dan info terlihat jelas, itu adalah informasi yang sebenernya di jaringan. Dikarenakan data tidak terlindungi membuat komunikasi jaringan ini tidak aman dan berisiko.

2. Pengujian Menggunakan VPN

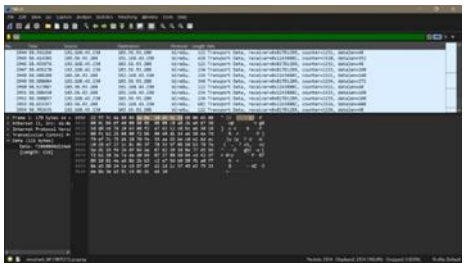
a. Kontrol On/Off



GAMBAR 4.7
Hasil Kontrol On/Off Menggunakan VPN

Gambar 4.9 menjelaskan bahwa Esp32 sedang berkomunikasi dengan server melalui protokol wireguard. Alamat IP yang tertera bukan alamat Esp32 dan server sebenarnya di jaringan. Komunikasi antara keduanya berjalan dengan baik, dan paket-paket dienkrepsi untuk menjaga keamanan komunikasi.

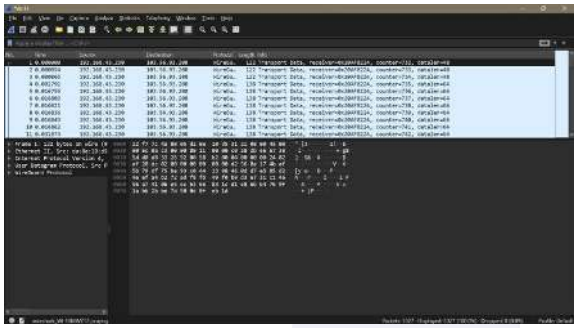
b. *Internet Control Message Protocol* (ICMP)



Gambar 4.8
Hasil ICMP Menggunakan VPN

Gambar 4.8 menjelaskan bahwa ESP32 sedang berkomunikasi dengan server melalui metode ICMP (Internet Control Message Protocol). Alamat IP yang tertera bukanlah alamat ESP32 dan server sebenarnya di jaringan, melainkan alamat IP yang dialokasikan oleh VPN WireGuard. Komunikasi antara keduanya berjalan dengan baik, dengan paket-paket ICMP yang dikirim bolak-balik untuk memastikan konektivitas dan stabilitas jaringan. Paket-paket ICMP ini juga dienkripsi oleh WireGuard untuk menjaga keamanan komunikasi, memastikan bahwa data yang dikirim dan diterima tetap aman dari gangguan pihak ketiga.

c. File Transfer Protocol (FTP)



GAMBAR 4.9
Hasil FTP Menggunakan VPN

Gambar 4.9 menjelaskan bahwa ESP32 sedang berkomunikasi dengan server melalui metode FTP (File Transfer Protocol). Alamat IP yang tertera bukanlah alamat ESP32 dan server sebenarnya di jaringan, melainkan alamat IP yang dialokasikan oleh VPN WireGuard. Komunikasi antara keduanya berjalan dengan baik, dengan transfer file yang dilakukan melalui FTP untuk memastikan pertukaran data antara ESP32 dan server. Paket-paket FTP ini dienkripsi oleh WireGuard untuk menjaga keamanan komunikasi, sehingga file yang dikirim dan diterima terlindungi dari gangguan pihak ketiga dan tetap aman selama proses transmisi.

V. KESIMPULAN

A. Kesimpulan

Proyek ini berhasil mencapai tujuannya dalam membuktikan efektivitas penggunaan WireGuard VPN untuk meningkatkan keamanan komunikasi berbasis IoT serta mengembangkan sistem kontrol jarak jauh. Berikut adalah kesimpulan berdasarkan tiga metode kontrol yang digunakan:

1. Kontrol On/Off: ESP32 berhasil mengirim dan menerima instruksi kontrol on/off melalui VPN WireGuard ke server MikroTik. Hasilnya menunjukkan bahwa sistem mampu mengontrol perangkat secara efektif dan aman dengan menggunakan VPN, sehingga menjaga privasi dan keamanan komunikasi.
2. *Internet Control Message Protocol* (ICMP): Dengan menggunakan metode ICMP (Ping), ESP32 sebagai klien dan WireGuard VPN berhasil berkomunikasi dengan stabil dan aman. WireGuard VPN memastikan bahwa paket ICMP yang digunakan untuk pemantauan dan diagnosis tidak dapat disadap, sehingga kualitas jaringan tetap terjaga dan risiko penyadapan dapat diminimalisir.
3. File Transfer Protocol (FTP): ESP32 mampu mengirim dan menerima file melalui protokol FTP ke server melalui tunnel WireGuard. Data yang ditransmisikan melalui FTP terlindungi selama proses pengiriman, memastikan keamanan dan integritas file. Penggunaan FTP di bawah VPN membuktikan bahwa sistem mendukung transfer file yang aman dan efisien.

Secara keseluruhan, penggunaan WireGuard VPN pada ESP32 dan server MikroTik terbukti efektif melindungi komunikasi sistem kontrol jarak jauh berbasis IoT. VPN ini meningkatkan keamanan dan integritas data dibandingkan dengan sistem tanpa VPN. Selain mudah diimplementasikan dan dioperasikan, WireGuard mendukung integrasi yang baik dengan perangkat IoT seperti ESP32, menjadikannya solusi efisien untuk aplikasi kontrol jarak jauh.

B. Saran

Adapun saran-saran yang dapat disampaikan dalam penelitian ini adalah sebagai berikut :

1. Pengembangan Infrastruktur Jaringan: Meningkatkan infrastruktur jaringan untuk mendukung komunikasi yang lebih cepat dan stabil.
2. Optimalisasi Pengaturan Server: Melakukan optimasi konfigurasi server untuk memastikan performa dan keamanan yang lebih baik.

REFERENSI

[1] P. Oktivasari and A. Budhi Utomo Politeknik Negeri Jakarta JlProfDrGASiwabessy, “ANALISA VIRTUAL PRIVATE NETWORK MENGGUNAKAN OPENVPN DAN POINT TO POINT TUNNELING PROTOCOL ANALYSIS OF VIRTUAL PRIVATE NETWORK USING OPENVPN AND POINT TO POINT TUNNELING PROTOCOL.”

[2] J. Administrasi Jaringan Komputer et al., “Implementasi Interkoneksi Jaringan Dengan Virtual Private Network (Vpn) Berbasis Bridge Control Protocol (Bcp) Pada Mikrotik Di Kantor Upt Pondok Pesantren Darussalam Blokagung,” 2023.

[3] Arifwidodo B, “Mekanisme Keamanan Jaringan Menggunakan Protokol Wireguard Pada Jaringan Privat”.

[4] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, “Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi,” vol. 5, no. 2, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[5] M. S. Sungkar, T. Elektronika, P. Harapan, and B. Tegal, “SISTEM KEAMANAN RUMAH BERBASIS INTERNET OF THINGS,” vol. 9, no. 2, 2020,[Online]. Available: https://id.wikipedia.org/wiki/Keamanan.

[6] D. Novianto, Y. S. Japriadi, and L. Tommy, “Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik,” Jurnal Ilmiah Informatika Global, vol. 13, no. 2, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.

[7] Y. Winawang, “Implementasi Keamanan Jalur Internet Menggunakan IP Tunneling pada OpenVPN Access Server dengan Protokol OpenVPN dan Protokol DNS Over HTTPS,” Jurnal Syntax Admiration, vol. 2, no. 4, pp. 712–730, Apr. 2021, doi: 10.46799/jsa.v2i4.207.

[8] F. Ichsanuddin M, “RANCANGANPROTOTYPE SMART HOME UNTUK KONTROL JARAK JAUH PADA PERANGKAT RUMAH DENGAN MIKROKONTROLLER

ESP32".
[9] T. Surya Budi and T. Komputer, "Kendali Otomatis Pintu Gerbang dengan ESP32 dan RFID."
[10] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," Jurnal KomtekInfo, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.
[11] P. Wicaksana, "IMPLEMENTASI VPN SERVER MENGGUNAKAN PROTOKOL L2TP DAN METODE IPSEC," 2022.
[12] HUDA M, "PENERAPAN WIRELESS SENSOR NETWORK (WSN) UNTUK MONITORING DAYA LAMPU PENERANGAN JALAN UMUM (LPJU) MENGGUNAKAN THINGSPEAK," 2023.
[13] A. Arifin, "RANCANG BANGUN INFORMASI KETINGGIAN BANJIR MENGGUNAKAN SENSOR MAGNETIC FLOATING BERBASIS IOT PROTOKOL MQTT," 2023.
[14] O. T. Saputra, W. Andriyani, B. Purnomosidi, and D. Putranto, "Optimisasi Beban VPN menggunakan WireGuard pada koneksi Multi WAN," 2024, doi: 10.33322/petir.v17i1.2320.
[15] B. G. Pratama and M. F. Qodri, "SISTEM PEMANTAUAN LIMBAH CAIR BERBASIS INTERNET OF THINGS DAN TERPROTEKSI WIREGUARD," KURVATEK, vol. 8, no. 1, pp. 99–108, Apr. 2023, doi: 10.33579/krvtk.v8i1.4028.
[16] A. Mikola, A. C. Nurcahyo, T. Informasi, and S. Bhuana, "Analisis Load
Balancing Berbasis Mikrotik Dalam Meningkatkan Kemampuan Server di Institut Shanti Bhuana," JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY, vol. 2, no. 2, 2022.
[17] M. A. Wardana, A. Z. Nusri, and J. Juliandika, "Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng," Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI), vol. 5, no. 2, pp. 107–116, Oct. 2022, doi: 10.57093/jisti.v5i2.135.
[18] A. Wijaya, A. Abdullah, E. Windriyani, F. Citra Samaeni, M. Yusri Romdhan, and R. Ardiansah, "Implementasi Quality of Service (QoS) menggunakan Wireshark pada Jaringan Wireless LAN," vol. 4, no. 1, 2024, doi: 10.47709/digitech.v4i1.4030.
[19] Y. Purbowo, I. Joko Waluyo, and T. Hidayat, "Perancangan Mesin Shredder Limbah Botol Plastik Menggunakan Sensor Proximity Berbasis Arduino," 2022.
[20] S. D. Simarmata, I. Gunawan, I. P. Sari, S. Sumarno, and I. O. Kirana, "Sistem Kendali Pintu Gerbang Otomatis Menggunakan Koneksi Wireless Module Wifi Berbasis Mikrokontroler Arduino Uno," Jurnal Pendidikan dan Teknologi Indonesia, vol. 1, no. 7, pp. 297–308, Jul. 2021, doi: 10.52436/1.jpti.67.
[21] A. Tohir, A. Febriyo Febriyansyah, W. Istiana, and T. Komputer, "Fitur Protokol IoT Dalam Komunikasi Jaringan Cerdas."
[22] S. Megawati and A. Lawi, "Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia."
[23] R. Tri Novita, I. Gunawan, I. Marleni, O. Gregarius Grasia, and M. Nanda Valentika abcde Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, "Analisis Keamanan Wifi Menggunakan Wireshark," 2021. [Online]. Available: https://www.researchgate.net/publication/316464159_Analisis_Keama