

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pembangunan pelayanan publik menjadi salah satu titik strategis untuk menciptakan *good governance* yang efektif dan efisien. Hal ini dikarenakan pelayanan publik melibatkan kepentingan semua unsur pemerintahan. Di Indonesia, penyelenggaraan urusan pemerintahan berbasis digital atau yang dikenal sebagai *e-government* sudah mulai diterapkan. Masalah terbesar dari pemanfaatan teknologi Informasi dan Komunikasi (TIK) ialah persoalan keamanan. Keamanan pada sektor publik terutama dalam penerapan sistem *e-government* merupakan hal yang perlu diperhatikan oleh pemerintah karena merupakan hal sensitif sebab rentan disalahgunakan oleh pihak yang tidak mempunyai hak akses dan akan berpengaruh kepada kepercayaan publik pada pelaksanaannya. *E-government* merupakan suatu dukungan bagi penerapan revolusi industri 4.0 yang menjadi suatu inovasi dalam dunia pemerintahan sebagai bukti atas kemajuan TIK di Indonesia (TAMSIR ARIYADI et al., 2024)

Keamanan akses data terhadap sebuah sumber daya merupakan salah satu faktor penting dalam dunia teknologi dan informasi. Pada saat ini belum banyak organisasi dan instansi yang sangat serius dalam mengatasi masalah keamanan jaringan. Tetapi ketika sumber daya dalam hal ini *server* mendapat serangan melalui jaringan dan terjadi kerusakan sistem, sehingga akan banyak memakan biaya yang harus dikeluarkan untuk melakukan perbaikan sistem, barulah sebuah organisasi dan instansi mulai bergerak untuk lebih serius dalam menghadapi masalah keamanan

sistem. Untuk itu sudah seharusnya investasi dibidang keamanan lebih diperhatikan, untuk mencegah pencurian data, dan dari ancaman serangan yang akan terjadi di masa depan. Terutama ketika komputer *server* terhubung dengan internet maka kemungkinan serangan pun akan semakin meningkat.(Novianto et al., 2022)

Keamanan data saat mengakses secara jarak jauh menjadi hal yang sangat penting karena adanya resiko tinggi yang harus dipertimbangkan. Karyawan yang bekerja di tempat umum seperti di rumah, ruang kerja bersama, café atau tempat umum lainnya dengan menggunakan jaringan WI-FI Publik memungkinkan penyusup melakukan pencurian data. Dalam laporan yang diterbitkan oleh *Global advisory and Accounting Network*, masalah keamanan dunia maya menunjukkan bahwa hampir 65% organisasi mengumumkan bahwa mereka telah terkena serangan siber selama bekerja secara jarak jauh. Hal ini dapat terjadi karena organisasi tersebut tidak dapat menerapkan semua metode perlindungan keamanan informasi dalam menjaga informasi di kantor pada saat WFA (*Work From Anywhere*). Disisi lain perusahaan juga tidak memiliki kesiapan dalam keamanan siber. Pencurian data saat bekerja saat jarak jauh juga berdampak pada individu dan perusahaan seperti kehilangan data penting, penurunan produktivitas, kerugian finansial, serta dapat membuat organisasi tersebut kehilangan reputasi dan kepercayaan. Oleh karena itu, sangat penting untuk memikirkan upaya dalam memastikan keamanan informasi jika terjadi WFA.(Haeruddin et al., 2023)

Virtual Private Network (VPN) adalah sebuah teknologi yang memungkinkan untuk dapat terhubung ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local. Penggunaan VPN merupakan salah

salah satu cara untuk membangun jalur komunikasi yang aman melalui jaringan publik. Melalui VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi pada internet menjadi standar utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsi dan tunneling.(Fikri & Rifqi, 2023)

Virtual Private Network (VPN) merupakan salah satu solusi dalam meningkatkan keamanan komunikasi jaringan dengan membentuk jalur terenkripsi antara pengguna dan jaringan internal instansi. OpenVPN, sebagai salah satu implementasi VPN berbasis *open-source*, menawarkan tingkat keamanan tinggi dengan metode autentikasi TLS/SSL. Metode ini memastikan bahwa hanya perangkat yang memiliki sertifikat yang sah yang dapat mengakses jaringan, sehingga mengurangi risiko akses tidak sah.(Ramesh et al., 2022)

Penerapan OpenVPN dengan autentikasi TLS/SSL memiliki keunggulan dalam hal enkripsi yang kuat dan sistem verifikasi berbasis sertifikat digital, sehingga lebih aman dibandingkan metode autentikasi konvensional seperti *username* dan *password* saja. Namun, masih terdapat kendala dalam penerapannya, seperti kurangnya pemahaman teknis dalam konfigurasi OpenVPN serta potensi kesalahan dalam pengelolaan sertifikat digital yang dapat menghambat efektivitas sistem keamanan (Saputra et al., 2023)

Meskipun memiliki banyak keunggulan, penerapan OpenVPN dengan autentikasi TLS/SSL tidak terlepas dari tantangan. Beberapa kendala yang sering dihadapi antara lain kurangnya pemahaman teknis dalam konfigurasi OpenVPN, serta potensi kesalahan konfigurasi yang dapat menghambat efektivitas sistem

keamanan. Oleh karena itu, dibutuhkan pendekatan yang tepat agar implementasi OpenVPN dapat berjalan optimal. (Ram, 2025)

AES-256 (*Advanced Encryption Standard 256-bit*) merupakan algoritma enkripsi simetris yang dikenal karena tingkat keamanannya yang tinggi. Dengan panjang kunci 256-bit, algoritma ini sangat sulit untuk diretas menggunakan serangan *brute force*, menjadikannya pilihan utama dalam berbagai sistem keamanan, termasuk OpenVPN. Enkripsi AES-256 bekerja dengan cara mengubah data menjadi bentuk terenkripsi yang hanya dapat dibuka dengan kunci yang sesuai, sehingga memastikan bahwa informasi yang dikirimkan tetap terlindungi dari akses yang tidak sah. (Firdaus & Santika, 2022)

Selain keamanannya yang tinggi, AES-256 juga memiliki keunggulan dalam hal efisiensi dan kompatibilitas dengan berbagai perangkat dan sistem operasi. Algoritma ini telah menjadi standar global dalam enkripsi data dan banyak digunakan dalam berbagai aplikasi keamanan, termasuk komunikasi VPN. Dengan penerapan AES-256 dalam OpenVPN, organisasi seperti Dinas Kesehatan Provinsi Sumatera Barat dapat memastikan bahwa komunikasi internal tetap aman dan data sensitif terlindungi dari ancaman siber (Guo et al., 2022)

Selain itu, *Virtual Private Network* (VPN) merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data yang telah dienkripsi antara dua atau lebih pengguna jaringan yang resmi. Untuk mengatasi masalah keamanan setiap komunikasi data yang dilakukan melalui jaringan publik (*public network*), maka diperlukan suatu mekanisme yang memungkinkan koneksi antar *workstation* berjalan secara *private*. Jaringan VPN memiliki enkripsi paling baik diperoleh pada metode OpenVPN, dengan data dienkripsi secara acak meskipun membutuhkan

waktu lebih lama dibandingkan metode lain seperti PPTP, L2TP, dan SSTP. Keuntungan VPN adalah data yang dikirimkan melalui VPN terenkripsi sehingga cukup aman, karena data tersebut dikirim melalui jalur tunneling. Tunneling sendiri merupakan metode untuk transfer data dari suatu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Saat dilakukan pengujian tunneling dengan serangan DoS, protokol VPN seperti PPTP dan L2TP mencatatkan waktu pengiriman sekitar 100 ms dengan jumlah paket data tertentu, sementara metode SSTP dan OpenVPN menunjukkan pengiriman data yang lebih cepat yaitu sekitar 2 ms dengan paket data sejumlah 28 paket. (Fayoumi et al., 2022)

Salah satu fitur penting dalam OpenVPN adalah mekanisme *tls-crypt-v2*, yang memungkinkan penggunaan *pre-shared key* (PSK) untuk mengenkripsi saluran kontrol antara klien dan server. Dalam mekanisme ini, sebuah *client key* yang telah dibungkus (*wrapped*) dikirim ke *server* saat *tunnel* VPN dibentuk. Meskipun aman, kelemahannya adalah jika kunci *wrapping* server dikompromikan, maka seluruh *client key* harus diperbarui, yang tentu akan menyulitkan dari sisi manajemen sistem. Untuk mengatasi risiko tersebut, diperlukan pendekatan yang lebih kuat melalui penggunaan *Hardware Security Module* (HSM). HSM seperti YubiKey, Java Card, atau modul lain berbasis antarmuka PKCS#11 dapat digunakan untuk menyimpan dan memproses kunci kriptografi secara aman, sehingga membuat kunci server lebih sulit diekstrak oleh pihak yang tidak berwenang. Teknologi ini dapat diintegrasikan dengan OpenVPN melalui mekanisme plugin, dengan tambahan skema turunan kunci (*key derivation*) agar fungsi *tls-crypt-v2* tetap berjalan meskipun perangkat keras tersebut tidak secara

langsung mendukung semua operasi kriptografi yang dibutuhkan (Imalik Muhammad Alviendra et al., 2022)

Selain itu, penerapan teknologi OpenVPN juga semakin berkembang dalam berbagai sektor industri, termasuk di bidang pengawasan dan pemeliharaan peralatan berat. Salah satu contoh penerapannya adalah pada sistem pemantauan dan pemeliharaan crane jarak jauh berbasis teknologi OpenVPN. Sistem ini memanfaatkan PLC (*Programmable Logic Controller*) sebagai unit akuisisi dan pengolahan data di lokasi. WinCC sebagai perangkat lunak konfigurasi menggunakan OPC (*OLE for Process Control*) untuk berkomunikasi dengan PLC di lokasi, mengarsipkan data operasional crane ke dalam database SQL yang kemudian diunggah ke server cloud melalui teknologi OpenVPN. Penggunaan OpenVPN di sini memungkinkan komunikasi data yang aman antara perangkat di lokasi dan platform pemantauan jarak jauh yang dikembangkan menggunakan bahasa pemrograman Java. Meskipun sistem ini lebih fokus pada pemeliharaan peralatan berat, penerapan teknologi serupa di sektor kesehatan dapat meningkatkan pemantauan data kesehatan secara jarak jauh dengan keamanan yang lebih baik (Damanik, 2022)

Seiring dengan berakhirnya pandemi COVID-19 di Indonesia, banyak perkantoran yang terus melanjutkan pekerjaan dengan sistem *Work From Office (WFO)* dan *Work From Home (WFH)* untuk efisiensi biaya pengeluaran kantor. Walaupun sebagian besar pekerjaan dilakukan di luar kantor, sistem ini masih memerlukan akses yang aman untuk menjaga keberlanjutan proses perkantoran secara efisien. Dalam konteks ini, penerapan metode VPN (Virtual Private Network) dengan OpenVPN dapat menjadi solusi tepat untuk memungkinkan akses

jaringan kantor yang aman melalui internet publik. OpenVPN memungkinkan transmisi data yang terenkripsi antara perangkat yang terhubung ke jaringan internal kantor, meskipun dilakukan dari lokasi yang berbeda (Affandi, 2022)

Seiring dengan meningkatnya penggunaan perangkat teknologi dan jaringan pada masa pandemi COVID-19, volume lalu lintas data yang mengalir melalui internet juga meningkat pesat. Hal ini membawa tantangan dalam memantau dan mengelola kualitas layanan (QoS) serta keamanan jaringan. Terutama, dengan meningkatnya penggunaan enkripsi data seperti VPN dan Tor Browser, pengelolaan lalu lintas jaringan terenkripsi menjadi tantangan besar. Oleh karena itu, dibutuhkan pendekatan yang efisien untuk mengklasifikasikan lalu lintas jaringan terenkripsi guna meningkatkan manajemen dan pengawasan kinerja jaringan. (Fayoumi et al., 2022)

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu:

“PERANCANGAN VIRTUAL PRIVATE NETWORK MENGGUNAKAN OPENVPN PADA ROUTER MIKROTIK DENGAN METODE AUTENTIKASI TLS/SSL DAN ENKRIPSI AES-256 UNTUK MENINGKATKAN KEMAMAN AKSES JARAK JAUH DI JARINGAN DINAS KESEHATAN PROVINSI SUMATERA BARAT”

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas dalam penelitian dapat dikemukakan beberapa rumusan masalah sebagai berikut:

1. Apakah dengan perancangan VPN menggunakan OPENVPN dapat menjadi salah satu alternatif dalam menjaga keamanan data di Dinas Kesehatan Provinsi Sumatera Barat?
2. Apakah dengan menerapkan autentikasi TLS/SSL dan enkripsi AES-256 dapat menunjang keamanan jaringan di Dinas Kesehatan Provinsi Sumatera Barat?
3. Apakah perancangan ini dapat mengatasi masalah ancaman kebocoran data, dokumen penting dari pihak yang tidak bertanggung jawab?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara yang disusun berdasarkan hasil pengamatan yang nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Hipotesa berfungsi sebagai jawaban awal terhadap rumusan masalah, yang menjadi dasar dalam menentukan arah dan fokus penelitian. Hipotesa berperan penting dalam mengarahkan penelitian untuk membuktikan efektivitas solusi yang akan ditawarkan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut:

1. Perancangan VPN menggunakan OPENVPN dapat menjadi salah satu alternatif dalam menjaga keamanan data di Dinas Kesehatan Provinsi Sumatera Barat.
2. Menerapkan autentikasi TLS/SSL dan enkripsi AES-256 dapat menunjang keamanan jaringan di Dinas Kesehatan Provinsi Sumatera Barat.
3. Perancangan ini dapat mengatasi masalah ancaman kebocoran data, dokumen penting dari pihak yang tidak bertanggung jawab.

1.4 Batasan Masalah

Batasan masalah yang akan dikemukakan dalam penelitian ini bertujuan untuk menghindari terjadinya penyimpangan pokok masalah dalam penyusunan penelitian, berikut adalah batasan-batasan yang akan diterapkan:

1. Penelitian berfokus pada perancangan dan pengujian sistem keamanan jaringan berbasis OpenVPN menggunakan metode autentikasi TLS/SSL dan enkripsi AES-256.
2. Proses implementasi tidak mencakup integrasi dengan sistem keamanan jaringan lainnya, melainkan pada pengembangan dan pengujian OpenVPN sebagai solusi keamanan akses jarak jauh.
3. Penelitian ini menguji keamanan koneksi dari sisi jaringan, tanpa membahas aspek keamanan fisik perangkat keras atau pelatihan pengguna terhadap ancaman keamanan siber.

1.5 Tujuan Penelitian

Tujuan penelitian merupakan salah satu komponen penting yang berfungsi untuk memberikan arah dan batasan yang jelas terhadap ruang lingkup pembahasan. Tujuan penelitian dirumuskan sebagai jawaban atas permasalahan yang telah dikemukakan sebelumnya, sehingga peneliti memiliki fokus yang terarah dalam pelaksanaan penelitian. Penelitian ini bertujuan untuk menyelidiki faktor-faktor yang mempengaruhi pada penelitian yang akan dilakukan. Penelitian yang akan dilakukan ini memiliki tujuan yang ingin dicapai diantaranya:

1. Penelitian ini bertujuan untuk merancang penggunaan OpenVPN dalam menjadi salah satu alternatif dalam menjaga keamanan data di Dinas Kesehatan Provinsi Sumatera Barat.

2. Penelitian ini bertujuan untuk menerapkan autentikasi TLS/SSL dan Enkripsi AES-156 dalam menunjang keamanan jaringan Dinas Kesehatan Provinsi Sumatera Barat.
3. Penelitian ini bertujuan dalam mengatasi masalah ancaman kebocoran data, dokumen penting dari pihak yang tidak bertanggung jawab

1.6 Manfaat Penelitian

Manfaat penelitian yang dilakukan oleh peneliti diharapkan dapat memberikan dampak yang lebih baik setelah melakukan penelitian ini. Adapun manfaat dari penelitian ini adalah:

1. Membantu Dinas Kesehatan Provinsi Sumatera Barat dalam meningkatkan keaamanan akses jarak jauh melalui perancangan OpenVpn.
2. Memberikan akes jaringan yang lebih aman dan terpercaya di Dinas Kesehatan Provinsi Sumatera Barat.
3. Menyediakan model perancangan yang dapat ditiru bagi instansi pemerintahan lainnya.

1.7 Gambaran Umum Objek Penelitian

1.7.1 Sekilas Tentang Dinas Kesehatan Provinsi Sumatera Barat

Dinas Kesehatan provinsi Sumatera Barat adalah sebuah instansi pemerintahan yang berada di kota Padang dan berfungsi untuk menyelenggarakan urusan pemerintahan di bidang kesehatan. Dinas kesehatan merupakan unsur pelaksana daerah di bidang kesehatan yang berkedudukan di bawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Kesehatan

mempunyai tugas pokok untuk melaksanakan urusan pemerintahan daerah di bidang kesehatan berdasarkan asas otonomi daerah.

Dinas Kesehatan didirikan berdasarkan peraturan daerah No.1/PP/DPRD/1997. Dinas kesehatan menjalankan kegiatannya berdasarkan perintah dari Departemen Kesehatan Pusat. Pada mulanya dinas kesehatan ini bernama Jawatan Kesehatan.

Pada saat pemerintahan di Indonesia khususnya di Kota Padang, saat itu pemerintahan Belanda mendirikan pelayanan kesehatan dan mendirikan poli teknik di Kota Padang dengan tujuan untuk memperluas jangkauan pelayanan kesehatan. Pemerintah mendirikan Rumah Sakit untuk melayani orang-orang Belanda

1.7.2 Visi dan Misi Dinas Kesehatan Provinsi Sumatera Barat

Visi dan Misi Dinas Kesehatan Provinsi Sumatera Barat ini berisi ide-ide yang telah ditetapkan oleh Pemerintah Provinsi Sumatera Barat. Ide-ide tersebut dapat dilihat sebagai berikut:

1. Visi

Dinas Kesehatan provinsi Sumatera Barat memiliki visi untuk
“Terwujudnya Pelayanan Berkualitas Dan Profesional ”.

2. Misi

- a. Melaksanakan Pelayanan publik sesuai standar.
- b. Melakukan upaya peningkatan mutu layanan melalui perbaikan saran dan prasarana.
- c. Melakukan monitoring dan evaluasi pelaksanaan pelayanan publik.
- d. Pengembangan kualitas sumber daya manusia dan sistem layanan berbasis informasi dan teknologi.

Untuk mendukung kelancaran operasional dan tercapainya tujuan bersama, diperlukan pembagian tugas dan tanggung jawab yang jelas bagi setiap pegawai. Berikut ialah uraian pekerjaan pada Dinas Kesehatan Provinsi Sumatera Barat:

1. Kepala Dinas Kesehatan Mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyusun dan merumuskan kebijakan serta program kerja Dinas Kesehatan.
 - b. Mengembangkan kompetensi dan kapasitas tenaga kesehatan melalui pelatihan
2. Sekretaris mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Mengelola dan menyusun administrasi Dinas Kesehatan, termasuk dokumen dan arsip.
 - b. Membantu kepala dinas dalam penyusunan rencana kerja tahunan dinas kesehatan.
 - c. Menyediakan layanan informasi dan administrasi kepada masyarakat terkait program kesehatan.
3. Kepala sub bagian keuangan dan aset mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyusun dan merencanakan anggaran tahunan untuk dinas kesehatan sesuai dengan program kerja yang telah ditetapkan.
 - b. Menyusun laporan keuangan bulanan dan tahunan untuk disampaikan kepada kepala dinas dan pihak terkait lainnya.
4. Kepala Bidang Kesehatan Masyarakat mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyusun rencana program kesehatan masyarakat yang berfokus pada pencegahan penyakit dan promosi kesehatan.

- b. Melakukan pengawasan terhadap pelaksanaan program kesehatan masyarakat dan melakukan evaluasi untuk mengetahui efektivitasnya.
- 5. Kepala Bidang Pelayanan Kesehatan mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyusun rencana strategis untuk pengembangan dan peningkatan layanan kesehatan di wilayah Dinas Kesehatan.
 - b. Melakukan pengawasan terhadap pelaksanaan layanan kesehatan untuk memastikan bahwa standar pelayanan dan kualitas kesehatan terpenuhi.
- 6. Kepala Bidang Sumber Daya Kesehatan mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyusun rencana strategis untuk pengelolaan dan pengembangan sumber daya manusia di sektor kesehatan.
 - b. Mengelola proses rekrutmen dan seleksi tenaga kesehatan untuk memastikan ketersediaan SDM yang berkualitas.
 - c. Mengumpulkan, menyimpan, dan menganalisis data terkait sumber daya manusia di bidang kesehatan.
- 7. Kepala Bidang Pencegahan dan Pengendalian Penyakit mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Merencanakan dan menyusun program-program pencegahan dan pengendalian penyakit, termasuk imunisasi dan skrining penyakit.

- b. Berkoordinasi dengan puskesmas, rumah sakit, dan fasilitas kesehatan lainnya untuk meningkatkan efektivitas program pencegahan.
8. UPTD Balai kesehatan olah raga masyarakat dan pelatihan kesehatan mempunyai tugas dan tanggung jawab sebagai berikut:
- a. Merancang dan melaksanakan program-program kesehatan yang berkaitan dengan olahraga dan pelatihan kesehatan masyarakat.
 - b. Menyelenggarakan kegiatan penyuluhan dan edukasi kepada masyarakat mengenai pentingnya olahraga dan gaya hidup sehat.
9. UPTD Laboratorium Kesehatan mempunyai tugas dan tanggung jawab sebagai berikut:
- a. Menyediakan layanan pemeriksaan laboratorium kesehatan untuk mendukung diagnosis dan pengobatan penyakit.
 - b. Melakukan pengujian berbagai jenis sampel, seperti darah, urin, dan sampel biologis lainnya, sesuai dengan prosedur standar.
 - c. Menyusun dan menyampaikan laporan hasil pemeriksaan kepada dokter dan pasien dengan tepat dan akurat.
10. UPTD Balai Kesehatan Indera Masyarakat mempunyai tugas dan tanggung jawab sebagai berikut:
- a. Menyediakan layanan pemeriksaan dan perawatan kesehatan bagi masyarakat yang berkaitan dengan indera, seperti penglihatan, pendengaran, dan kesehatan mulut.

- b. Menyelenggarakan program penyuluhan kepada masyarakat tentang pentingnya menjaga kesehatan indera dan melakukan pemeriksaan secara rutin.
- 11. RS Paru Lubuk Alung Mempunyai tugas dan tanggung jawab sebagai berikut:
 - a. Menyediakan layanan diagnosis, pengobatan, dan perawatan untuk pasien dengan penyakit paru, termasuk tuberkulosis dan gangguan pernapasan lainnya.