ANALISIS PENGAMANAN JARINGAN REMOTE SITE BERBASIS PROTOKOL PPTP PADA JARINGAN VIRTUAL PRIVATE NETWORK

Sugiyono

Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda
sugiyono@uinsi.ac.id

Abstrak

Penelitian ini bertujuan untuk menganalisis pengamanan jaringan remote site berbasis protokol PPTP pada jaringan VPN di Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda. Metode penelitian ini berjenis kualitatif dengan peroleh data berdasarkan hasil observasi dan studi literatur terhadap penggunaan protokol PPTP. Penelitian ini menganalisis dan mengidentifikasi serangkaian serangan yang berpotensi mengganggu jaringan menggunakan protokol PPTP dan upaya mitigasi untuk memperkuat keamanan jaringan *remote site* menggunakan protokol tersebut. Hasil penelitian menunjukkan bahwa penggunaan protokol PPTP pada jaringan VPN di Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda sebagaimana merujuk pada berbagai literatur berpotensi terjadinya celah keamanan yang dapat membahayakan jaringan lokal universitas. Oleh karenanya upaya mitigasi meliputi penggunaan teknologi pengamanan tambahan, seperti enkripsi yang lebih kuat, otentikasi yang ditingkatkan sangat di sarankan. Penelitian ini juga diharapkan dapat memberikan pengetahuan dan wawasan berharga kepada administrator jaringan dan praktisi keamanan informasi tentang potensi kerentanan dan risiko yang terkait dengan penggunaan protokol PPTP dalam jaringan *remote site*. Dengan pemahaman yang lebih baik tentang kelemahan keamanan yang ada, maka dapat diantisipasi langkah-langkah mitigasi yang dapat diterapkan untuk meningkatkan keamanan jaringan secara keseluruhan.

Kata Kunci: Pengamanan jaringan, *Remote site*, Protokol PPTP, Analisis keamanan, Mitigasi risiko.

Abstract

This study aims to analyze the PPTP protocol-based remote site network security on the VPN network at Sultan Aji Muhammad Idris State Islamic University Samarinda. This research method is a qualitative type by obtaining data based on observations and literature studies on the use of the PPTP protocol. This research analyzes and identifies a series of attacks that have the potential to disrupt networks using the PPTP protocol and mitigation efforts to strengthen remote site network security using this protocol. The results showed that the use of the PPTP protocol on the VPN network at the Sultan Aji Muhammad Idris Samarinda State Islamic University, as referred to in various literature, has the potential to create security holes that could harm the university's local network. Therefore mitigation efforts include the use of additional security technologies, such as stronger encryption, enhanced authentication is highly recommended. This research is also expected to provide valuable knowledge and insights to network administrators and information security practitioners about the potential vulnerabilities and risks associated with using the PPTP protocol in remote site networks. With a better understanding of existing security weaknesses, mitigation measures can be anticipated that can be implemented to improve overall network security.

Keywords: *Network security, Remote site, PPTP Protocol, Security analysis, Risk mitigation.*

PENDAHULUAN

Di era globalisasi dan teknologi informasi yang terus berkembang pesat, jaringan komputer menjadi infrastruktur yang diandalkan oleh banyak organisasi. Jaringan komputer digunakan untuk menghubungkan perangkat-perangkat remote dengan server pusat yang memungkinkan akses dan pertukaran dan distribusi data dengan efektif dan efisien. Karenanya dalam upaya mengantisipasi beragam tindak kejahatan yang melibatkan akses dan distribusi data ini, maka perlu diterapkan sistem pengamanan jaringan yang handal. Salah satu metode yang bisa digunakan dalam mengamankan koneksi jaringan *remote site* adalah dengan menggunakan protokol PPTP (*Point-to-Point Tunneling Protocol*). Protokol PPTP adalah protokol jaringan yang memungkinkan pembentukan saluran aman (*tunnel*) antara perangkat remote dengan server pusat melalui jaringan publik, seperti jaringan internet. Dengan menggunakan protokol PPTP, data yang dikirimkan melalui jaringan dapat dienkripsi, sehingga memastikan kerahasiaan dan integritasnya. Namun, meskipun protokol PPTP ini telah digunakan secara luas, beberapa kasus kelemahan dan celah keamanan yang melibatkan protokol ini masih sering terjadi.

Tujuan dari penelitian ini adalah dalam rangka melakukan analisis dan mengidentifikasi berbagai celah kemananan dan potensi ancaman atas penerapan protokol PPTP (*Point-to-Point Tunneling Protocol*) pada jaringan *Virtual Private Network* (VPN) pada sistem *remote server* pada jaringan Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda. Dengan mengetahui kelemahan dan berbagai celah keamanan yang berpotensi menyerang dan membahayakan jaringan data dan sistem informasi, diharapkan bisa diambil langkah-langkah antisipatif sebagai upaya prefentif yang merupakan bagian dari mitigasi resiko keamananan pada jaringan komputer universitas.

Beberapa penelitian terdahulu yang melibatkan penggunaan protokol PPTP menunjukkan adanya kerentanan pada protokol ini dalam berbagai bentuk serangan seperti pencurian data, pemalsuan identitas, dan serangan DoS (*Denial of Service*). Serangan-serangan ini dapat menyebabkan kerugian serius bagi organisasi, termasuk kebocoran data sensitif dan gangguan operasional. Diantaranya penelitian tentang *Security Analysis of PPTP Protocol for Remote Site Networks*. Penelitian ini mengidentifikasi kerentanan utama dalam implementasi protokol PPTP dan menganalisis risiko yang terjadi. Hasil penelitian menunjukkan adanya serangkaian serangan potensial yang dapat dieksploitasi, termasuk serangan pencurian data dan serangan pemalsuan identitas. Penelitian ini mengusulkan beberapa langkah mitigasi untuk memperkuat keamanan jaringan *remote site* yang menggunakan protokol PPTP.(K. Karuna Jyothi & B. Indira Reddy, 2018) Sementara pada penelitian lainnya yang berjudul *Evaluation of PPTP Protocol Security in Remote Access Scenarios* yang bertujuan untuk mengevaluasi keamanan protokol PPTP dalam skenario akses remote dengan menggunakan pendekatan analisis keamanan, penelitian ini mengidentifikasi adanya kelemahan pada protokol PPTP yang dapat dimanfaatkan oleh penyerang. Hasil penelitian menyoroti kerentanan terhadap serangan seperti serangan DoS, serangan *Man-in-the-Middle,* dan serangan kebobolan kredensial. Penelitian ini juga mengusulkan solusi alternatif untuk memperkuat keamanan jaringan *remote site,* termasuk penggunaan protokol VPN yang lebih aman.(Jahan et al., 2017) Sementara dalam penelitian yang berjudul *Enhancing PPTP Security for Remote Site Networks*, yang berfokus pada peningkatan keamanan protokol PPTP dalam jaringan *remote site*. Penelitian ini menganalisis kelemahan yang ada pada protokol PPTP dan mengusulkan perubahan dan peningkatan untuk mengatasi masalah keamanan tersebut. Salah satu solusi yang diajukan adalah penggunaan metode enkripsi yang lebih kuat untuk melindungi data yang dikirimkan melalui jaringan. Dalam penelitian ini juga menyoroti pentingnya penerapan kebijakan otentikasi yang kuat dan pemantauan lalu lintas jaringan sebagai langkah-langkah tambahan untuk memperkuat keamanan jaringan *remote site* yang menggunakan protokol PPTP.(Rana, 2013)

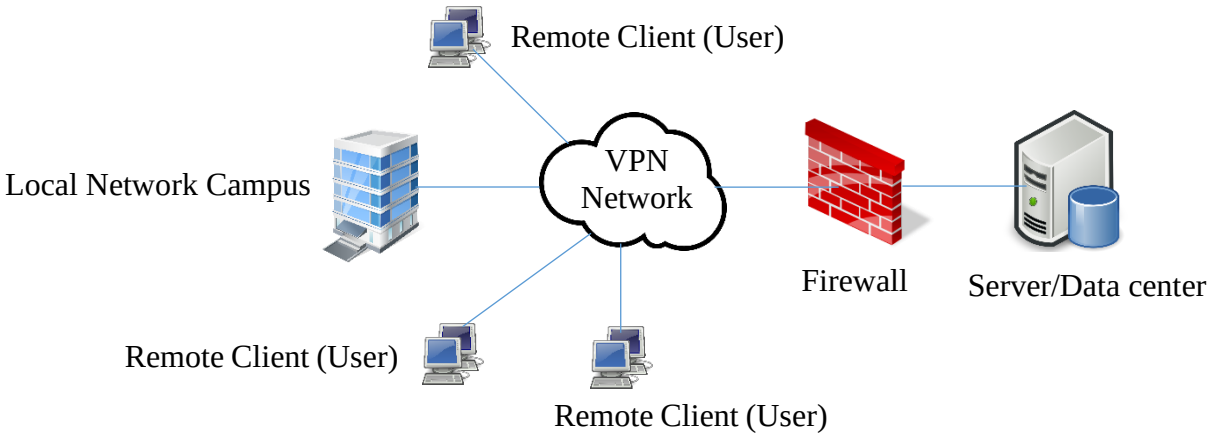
Dalam konteks ini maka penting dilakukan analisis mendalam terhadap pengamanan jaringan *remote site* berbasis protokol PPTP ini. Dengan menganalisis kelemahan dan risiko yang terkait dengan penggunaan PPTP, maka dapat diambil langkah-langkah mitigasi yang tepat yang dapat diterapkan untuk memperkuat keamanan jaringan sebuah organisasi. Melalui penelitian ini sekaligus akan dilakukan identifikasi serangkaian potensi serangan terhadap jaringan *remote site* yang menggunakan protokol PPTP. Disamping itu juga akan dilakukan evaluasi upaya mitigasi yang dapat diimplementasikan untuk mengurangi risiko yang terkait dengan penggunaan protokol ini. Diharapkan hasil penelitian ini akan memberikan wawasan dan pengetahuan yang bermanfaat bagi administrator jaringan dan profesional keamanan informasi dalam meningkatkan keamanan jaringan *remote site* pada institusinya masing-masing.

METODE

Metode penelitian yang digunakan dalam penelitian ini berjenis kualitatif, yang mengkaji secara komprehensif tentang protokol PPTP, pengamanan jaringan, dan kerentanan yang terkait dengan penggunaan PPTP dalam konteks jaringan *remote site* di Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda. Penelitian Kualitatif menurut Erickson dalam Albi Anggito merupakan penelitian yang berusaha menemukan dan menggambarkan secara naratif terhadap kegiatan yang dilakukan serta dampak atas tindakan yang dilakukan terhadap kehidupan mereka.(Albi Anggito & Johan Setiawan, 2018) Dalam penelitian ini data akan dikumpulkan melalui berbagai cara seperti melakukan observasi, serta menggali dari beragam referensi (studi literatur) dari berbagai penelitian terdahulu yang relevan serta rujukan dari berbagai buku. Adapun dalam pelaksanaannya penelitian ini akan dibagi ke dalam empat tahapan. Tahap pertama adalah mengumpulkan permasalahan dari berbagai sumber yang terkait kerentanan yang telah diidentifikasi sebelumnya beserta potensi serangan yang mungkin terjadi dan upaya mitigasi yang akan dijalankan. Tahap kedua menganalisis secara mendalam atas kemungkinan adanya celah pada protokol PPTP sehingga dapat diidentifikasi kelemahan keamanan yang ada. Ini dilakukan dengan melibatkan pemeriksaan spesifikasi protokol, metode enkripsi yang digunakan, mekanisme otentikasi, dan praktik keamanan lainnya yang terkait dengan PPTP. Dalam analisis kelemahan, selanjutnya dapat diidentifikasi berbagai kerentanan yang dapat dimanfaatkan untuk melakukan serangan seperti pencurian data, pemalsuan identitas, atau serangan DoS. Tahap kedua, setalah diketahui kerentanan pada protokol PPTP kemudian dilakukan penilaian risiko yang dimaksudkan untuk mengidentifikasi dampak dan probabilitas serangan terhadap jaringan *remote site* yang menggunakan protokol PPTP. Aktivitas ini melibatkan proses mengidentifikasi ragam aset berharga yang dimiliki organisasi yang selayaknya perlu dilindungi, mengidentifikasi kerentanan yang dapat menyebabkan dapat tereksposnya aset tersebut, mengevaluasi kemungkinan terjadinya serangan, dan menilai dampak yang mungkin terjadi jika serangan berhasil dilakukan. Tahap ketiga adalah melakukan simulasi Serangan dengan menggunakan skenario yang mungkin terjadi dalam jaringan *remote site* yang menggunakan protokol PPTP. Simulasi serangan dapat melibatkan pemodelan serangan seperti pencurian data, pemalsuan identitas, atau serangan DoS dan melihat bagaimana protokol PPTP bereaksi terhadap serangan tersebut. Hal ini membantu dalam mengidentifikasi kelemahan yang spesifik dan menguji keefektifan langkah mitigasi yang diusulkan. Tahap keempat adalah evaluasi mitigasi, dengan mengusulkan langkah-langkah mitigasi yang efektif berdasarkan hasil analisis dan penilaian risiko sebelumnya. Evaluasi mitigasi melibatkan kegiatan mengidentifikasi solusi keamanan tambahan yang dapat diterapkan, seperti penggunaan protokol VPN yang lebih aman, implementasi enkripsi yang lebih kuat, atau peningkatan mekanisme otentikasi. Langkah-langkah mitigasi ini harus dievaluasi untuk memastikan bahwa mereka efektif dalam melindungi jaringan *remote site* dari serangan yang diidentifikasi.

HASIL DAN PEMBAHASAN

Kompleksitas transaksi digital dan sistem distribusi data yang terjadi di Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda dalam mendukung kegiatan operasional penyelenggaraan akademik, pendidikan dan pembelajaran membutuhkan tata kelola yang baik yang bisa memberikan jaminan kemananan terhadap informasi dan data yang handal didalamnya. Kebijakan Teknologi Informasi dengan sistem data terpusat yang diimplementasikan di universitas ini berimplikasi terhadap tingginya intensitas transaksi dan komunikasi data antara komputer client dengan *remote server* yang di alirkan melalui jaringan publik. Oleh karenanya agar terwujud sistem komunikasi data yang aman dan handal pada jaringan *Virtual Private Network* (VPN) berbasis protokol PPTP yang digunakan saat ini, maka perlu dilakukan analisis mendalam dan komprehensif dengan mempertimbangkan semakin meningkatkannya statistik kejahatan di bidang komputer sebagai implikasi dari perkembangan teknologi perangkat lunak, kompleksitas sistem, dan potensi temuan celah keamanan serta resiko yang ditimbulkan.(Afrianto & Setiawan, 2015)



Gambar 1.1 Model Jaringan *Virtual Private Network* berbasis protokol PPTP

Jaringan *Virtual Private Network* sendiri merupakan sebuah koneksi terenkripsi yang memungkinkan pengguna untuk mengakses jaringan privat atau sumber daya komputer secara remote melalui jaringan publik seperti internet. Dalam jaringan VPN, data yang dikirim antara perangkat pengguna dan jaringan target dienkripsi terlebih dahulu untuk tujuan meningkatkan keamanan dan privasi data yang di bawa. Jaringan VPN menciptakan saluran komunikasi pribadi melalui jaringan publik dengan menggunakan teknik enkripsi yang memungkinkan pengguna mengirimkan dan menerima data secara aman melalui koneksi yang terenkripsi, sehingga data yang dikirim melalui jaringan publik tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang.(Arafah & Gunawan, 2017) Jaringan VPN bekerja diatas protokol komunikasi berupa protokol PPTP (*Point-to-Point Tunneling Protocol*) yakni sebuah protokol yang digunakan untuk membuat koneksi jaringan pribadi virtual (VPN) melalui jaringan internet (publik). PPTP termasuk salah satu protokol VPN paling lama dan sudah umum digunakan. Konsep awal protokol PPTP dirancang untuk menyediakan koneksi yang aman dan terenkripsi antara dua titik akhir (*endpoints*) melalui jaringan publik dengan menggunakan saluran komunikasi yang terenkripsi untuk melindungi data yang dikirim antara pengguna dan server VPN.(Oktivasari & Utomo, 2016)

Tujuan penelitian ini adalah melakukan identifikasi dan menganalisis untuk mengetahui berbagai potensi celah kemanan pada jaringan VPN menggunakan protokol PPTP pada jaringan *remote server* di Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda serta

rekomendasi dan upaya mitagasi yang bisa dilakukan. Tahap awal penelitian dengan melakukan analisis mendalam terhadap potensi kerentanan keamanan pada protokol PPTP dari berbagai sumber. Kerentanan pertama adalah terkait metode autentikasi yang digunakan pada protokol PPTP. Ditemukan bahwa autentikasi berbasis MS-CHAP v2 (*Microsoft Challenge Handshake Authentication Protocol version 2*) yang merupakan metode yang paling umum digunakan dalam implementasi protokol PPTP memiliki kerentanan yang signifikan terhadap serangan *brute-force* dan pemulihan kata sandi (*password cracking*). Serangan *brute-force* dapat memanfaatkan kelemahan dalam protokol PPTP yang tidak membatasi jumlah percobaan login. Kerentanan pada protokol autentikasi MS-CHAPv2 yang digunakan dalam PPTP (*Point-to-Point Tunneling Protocol*) membuatnya rentan terhadap serangan *brute force*.(Goos et al., 1999) Pada tahun 2012, Moxie Marlinspike, seorang ahli keamanan, mempublikasikan serangan yang melibatkan kelemahan dalam MS-CHAPv2. Dalam serangan *brute force* pada MS-CHAPv2, penyerang mencoba semua kemungkinan kata sandi secara berulang untuk mencocokkan respon yang diterima dari server. Serangan tersebut memanfaatkan kelemahan dalam enkripsi yang digunakan oleh MS-CHAPv2 dan kecepatan komputasi yang tinggi yang tersedia saat ini. Serangan ini berhasil karena MS-CHAPv2 menggunakan metode enkripsi yang lemah dan algoritma *hashing* yang sudah usang. Algoritma *hashing* yang digunakan adalah MD4 (*Message Digest 4*), yang diketahui memiliki kelemahan keamanan. Serangan *brute force* pada MS-CHAPv2 mengungkapkan kerentanan yang signifikan dalam keamanan PPTP dan membuatnya tidak aman untuk digunakan. Oleh karena itu, disarankan untuk beralih ke protokol VPN yang lebih aman seperti OpenVPN, IPSec, atau IKEv2.(Jha & Dalal, 2010)

Kerentanan kedua adalah PPTP (*Point-to-Point Tunneling Protocol*) menggunakan protokol MPPE (*Microsoft Point-to-Point Encryption*) untuk enkripsi data yang dikirim melalui koneksi VPN. MPPE sebagai protokol enkripsi simetris yang dikembangkan oleh Microsoft memiliki kelemahan utama yang terletak pada panjang kunci enkripsi yang digunakan. MPPE menggunakan kunci 128-bit, yang saat ini dianggap relatif lemah terhadap serangan yang menggunakan kekuatan komputasi yang tinggi, terutama jika dibandingkan dengan enkripsi modern yang menggunakan kunci 256-bit atau lebih besar. Kunci 128-bit pada MPPE memiliki ruang kunci yang lebih terbatas dibandingkan dengan kunci yang lebih panjang. Ini berarti ada jumlah terbatas kombinasi kunci yang mungkin digunakan dalam enkripsi MPPE. Dengan kekuatan komputasi yang tinggi, serangan *brute forc*e atau metode lain yang menguji semua kemungkinan kunci dapat secara teoretis memecahkan enkripsi MPPE dan mendapatkan akses ke data yang dilindungi. Selain itu, karena MPPE menggunakan kunci yang relatif pendek, serangan dengan metode lain seperti serangan pencocokan pola atau analisis statistik juga dapat menjadi lebih efektif. Oleh karena itu, dari perspektif keamanan, kelemahan MPPE terletak pada ukuran kunci enkripsi yang relatif pendek. Dalam konteks serangan dengan sumber daya komputasi yang tinggi, kunci 128-bit yang digunakan dalam MPPE dapat menjadi lebih mudah dipatahkan dibandingkan dengan kunci enkripsi yang lebih panjang. Sebagai alternatif yang lebih aman, disarankan untuk menggunakan protokol VPN yang menggunakan enkripsi yang lebih kuat, seperti AES (*Advanced Encryption Standard*) dengan kunci 256-bit. Protokol VPN seperti OpenVPN atau IKEv2 dapat memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan PPTP dengan MPPE.(Alviendra, 2022)

Kerentatan ketiga bahwa protokol PPTP tidak dapat melintasi *firewall* terbaru, *Firewall* dan jaringan yang lebih modern sering kali menerapkan konfigurasi yang lebih ketat terkait penggunaan protokol PPTP (*Point-to-Point Tunneling Protocol*), yang dapat mengakibatkan masalah konektivitas. Beberapa *firewall* secara default memblokir PPTP karena adanya kerentanan keamanan yang diketahui dalam protokol tersebut. *Firewall* tersebut mengadopsi kebijakan yang membatasi jenis lalu lintas yang diizinkan, termasuk pemblokiran lalu lintas PPTP secara khusus. Selain itu, beberapa organisasi dan jaringan lebih memilih protokol VPN yang lebih aman dan kuat seperti OpenVPN, IPSec, atau IKEv2, dan *firewall* dan jaringan

mereka dikonfigurasi untuk memprioritaskan dan mengizinkan lalu lintas protokol VPN yang lebih aman tersebut, sementara membatasi atau memblokir PPTP. Kendala kompatibilitas juga dapat menjadi faktor, di mana *firewall* dan jaringan modern menggunakan standar dan protokol yang lebih baru yang tidak mendukung atau berinteraksi langsung dengan PPTP. Dalam situasi seperti ini, pengguna PPTP dapat mengalami masalah konektivitas saat mencoba melakukan koneksi melalui *firewall* atau jaringan tersebut. Penting untuk memahami kebijakan keamanan dan konfigurasi jaringan yang ada untuk mengetahui apakah PPTP diizinkan atau diblokir. Jika PPTP tidak diizinkan, solusi yang lebih aman dan kompatibel adalah menggunakan menggunakan protokol lain seperti OpenVPN, IPSec, atau IKEv2 yang dapat digunakan sebagai alternatif yang lebih handal dan lebih dapat diandalkan.(Haeruddin, 2021)

Kerentatan keempat bahwa protokol PPTP tidak mendukung IPv6, Protokol PPTP (*Point-to-Point Tunneling Protocol*) tidak mendukung IPv6 (*Internet Protocol version 6*), yang merupakan versi protokol yang lebih baru dan berkembang pesat. PPTP didesain khusus untuk penggunaan dengan protokol IPv4 (*Internet Protocol version 4*). IPv6 menggunakan alamat IP yang lebih panjang dan menyediakan kapasitas yang lebih besar dalam menangani pertumbuhan perangkat yang terhubung ke internet. Namun, karena PPTP hanya mendukung IPv4, ini berarti bahwa PPTP tidak dapat digunakan dalam lingkungan jaringan yang hanya menggunakan protokol IPv6. Dalam era di mana adopsi IPv6 semakin meningkat, penggunaan PPTP menjadi semakin terbatas dan kurang relevan. Oleh karena itu disarankan menggunakan protokol VPN yang mendukung IPv6, apabila bekerja pada lingkungan jaringan yang menggunakan IPv6, seperti OpenVPN atau IKEv2, untuk memastikan kompatibilitas dan konektivitas yang baik dengan infrastruktur jaringan yang lebih modern.(Supendar, 2016)

Kerentanan kelima bahwa protokol PPTP sangat bergantung pada protokol TCP, Protokol PPTP (*Point-to-Point Tunneling Protocol*) sangat bergantung pada protokol TCP (*Transmission Control Protocol*) dalam operasinya. PPTP menggunakan TCP sebagai protokol transportasi untuk membentuk koneksi dan mentransmisikan data melalui jaringan. Hal ini dapat menyebabkan beberapa masalah terkait ketergantungan pada TCP. Salah satu masalah yang muncul adalah jika terjadi kehilangan paket atau keterlambatan dalam jaringan, hal ini dapat mempengaruhi kinerja PPTP. Jika paket-paket data hilang atau mengalami keterlambatan yang signifikan, maka koneksi PPTP dapat mengalami gangguan dan menyebabkan masalah konektivitas. Selain itu, karena PPTP menggunakan satu koneksi TCP untuk mengelola seluruh sesi VPN, jika koneksi tersebut terputus, misalnya karena gangguan jaringan atau pemutusan sambungan, maka semua sesi VPN yang terhubung melalui PPTP juga akan terputus. Hal ini dapat mengganggu kelancaran koneksi VPN dan menyebabkan gangguan bagi pengguna. Ketergantungan PPTP pada protokol TCP juga memiliki konsekuensi lainnya. Misalnya, protokol TCP memiliki overhead yang relatif tinggi dan cenderung lebih lambat dibandingkan dengan protokol transportasi yang lebih ringan seperti UDP (*User Datagram Protocol*). Hal ini dapat mempengaruhi kecepatan dan responsibilitas koneksi PPTP, terutama dalam situasi dengan latensi jaringan yang tinggi. Pada kesimpulannya, ketergantungan PPTP pada protokol TCP memiliki potensi untuk menghadirkan beberapa masalah terkait kinerja dan konektivitas jaringan. Oleh karena itu, dalam lingkungan jaringan yang mengalami gangguan atau memiliki persyaratan kinerja yang tinggi, mungkin lebih baik untuk mempertimbangkan penggunaan protokol VPN lain yang tidak terlalu tergantung pada protokol TCP, seperti OpenVPN yang dapat menggunakan UDP sebagai protokol transportasinya.(Halawa, 2021).

Berdasarkan berbagai temuan celah keamanan pada penerapan protokol PPTP (*Point-to-Point Tunneling Protocol*) pada jaringan *Virtual Privat Network* (VPN) berbasis *remote server* yang berupa : (a) Kerentanan protokol PPTP (*Point-to-Point Tunneling Protocol*) terhadap aktivitas serangan *brute force attack*, (b) Permasalahan panjang enkripsi pada protokol PPTP (*Point-to-Point Tunneling Protocol*) yang digunakan yang menyebabkan rentan dan mudahnya keamanan untuk ditembus, (c) Tidak kompatibelnya protokol PPTP (*Point-to-Point Tunneling*

Protocol) dengan jenis firewall model baru, dan (e) Protokol PPTP (*Point-to-Point Tunneling Protocol*) belum mendukung penggunaan internet protokol terbaru seperti IPV6, dan (f) Ketergantungan protokol PPTP (*Point-to-Point Tunneling Protocol*) terhadap protocol TCP. Oleh karena itu maka bagi Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda direkomendasikan beberapa langkah sebagai upaya mitigasi sekaligus antisipasi dengan mengganti protokol PPTP pada jaringan *Virtual Privat Network* (VPN) yang digunakan dengan protokol yang lebih kompatibel dan lebih aman seperti OpenVPN, IPSec, atau IKEv2.

Penelitian tentang analisis pengamanan jaringan *remote site* berbasis protokol PPTP (*Point-to-Point Tunneling Protocol*) yang menggambarkan secara mendalam mengenai keamanan jaringan *remote berbasis* protokol PPTP sudah banyak dilakukan para penelitin terdahulu. Secara umum pembahasan tentang protokol PPTP umumnya digunakan untuk membangun koneksi yang aman antara jaringan lokal dan *remote site* melalui jaringan publik seperti Internet. Sedangkan penelitian ini difokuskan pada identifikasi dan evaluasi potensi kerentanan serta kelemahan yang terkait dengan penggunaan protokol PPTP dalam konteks pengamanan jaringan *remote site*.

Sebagaimana temuan penelitian Mufida, dkk. dengan fokus pada pemanfaatan metode autentikasi dengan menggunakan protokol PPTP. Hasil penelitiannya menunjukkan bahwa metode autentikasi yang paling umum digunakan dalam implementasi PPTP adalah MS-CHAP v2 (*Microsoft Challenge Handshake Authentication Protocol version 2*). Penelitiannya menemukan bahwa metode ini memiliki kerentanan terhadap serangan *brute-force* dan pemulihan kata sandi. Keterbatasan dalam pembatasan jumlah percobaan login memberikan kesempatan bagi penyerang untuk mencoba kombinasi kata sandi yang berulang kali, yang dapat memungkinkan mereka untuk mendapatkan akses yang tidak sah ke jaringan.(Mufida et al., 2017)

Sementara pada penelitian lain yang mengulas penggunaan protokol PPTP. Dalam analisis penelitiannya menunjukkan bahwa metode enkripsi yang digunakan, seperti MPPE (*Microsoft Point-to-Point Encryption*), memiliki kelemahan yang dapat dimanfaatkan oleh penyerang. Dalam beberapa kasus, serangan *sniffing* terhadap aliran data dalam jaringan PPTP dapat mengungkapkan informasi sensitif, karena metode enkripsi yang digunakan relatif lemah. Dalam penelitian tersebut juga membahas kerentanan terhadap serangan *man-in-the-middle* (MITM) dalam konteks jaringan *remote site* berbasis PPTP. Bahwasanya serangan MITM dapat mengancam integritas dan kerahasiaan data yang dikirim melalui jaringan PPTP jika penyerang berhasil memanipulasi saluran komunikasi antara pengguna dan jaringan *remote site*. Pembahasan dalam penelitian ini mengidentifikasi potensi serangan MITM dan memberikan saran untuk langkah-langkah mitigasi yang dapat diambil untuk mencegah serangan semacam itu. Pembahasan penelitian ini menekankan pentingnya mengadopsi langkah-langkah pengamanan yang lebih kuat dan solusi yang lebih aman dalam pengaturan jaringan *remote site*. Rekomendasi yang diajukan meliputi penggunaan protokol yang lebih aman seperti IPsec (*Internet Protocol Security*) atau OpenVPN sebagai pengganti PPTP, penerapan kebijakan keamanan yang kuat, penggunaan autentikasi yang aman, penggunaan enkripsi yang lebih kuat, dan langkah-langkah mitigasi untuk mencegah serangan MITM. Secara keseluruhan, pembahasan penelitian ini menyediakan wawasan yang komprehensif mengenai potensi kerentanan dan kelemahan dalam penggunaan protokol PPTP dalam pengamanan jaringan *remote site*. Dengan memahami masalah ini, organisasi dapat mengambil langkah-langkah yang tepat untuk meningkatkan keamanan jaringan mereka dan melindungi data yang sensitif dari ancaman yang ada.(Bruce Scheier, 1998)

KESIMPULAN

Berdasarkan hasil penelitian analisis pengamanan jaringan *remote site* berbasis protokol PPTP (*Point-to-Point Tunneling Protocol*) pada jaringan *Virtual Private Network* (VPM) di

Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda, dapat disimpulkan bahwa PPTP memiliki kelemahan dalam hal keamanan. Meskipun PPTP memungkinkan konektivitas jaringan yang mudah, metode enkripsi yang digunakan rentan terhadap serangan seperti *sniffing* dan *brute force attack,* yang dapat mengakibatkan pengungkapan data sensitif atau akses yang tidak sah ke jaringan. Oleh karena itu, disarankan untuk mempertimbangkan alternatif protokol VPN yang lebih aman seperti IPsec (*Internet Protocol Security*), OpenVPN, IKEv2 atau SSL/TLS (*Secure Sockets Layer/Transport Layer Security*). Implementasi langkah-langkah pengamanan tambahan seperti penggunaan sertifikat digital untuk otentikasi, penggunaan password yang kuat, dan pemantauan aktifitas jaringan juga penting. Selain itu, penting untuk selalu melakukan pembaruan perangkat lunak dan memelihara sistem secara rutin guna menjaga keamanan jaringan *remote site* secara optimal. Dengan demikian, pemahaman akan kerentanan keamanan pada jaringan *remote site* yang menggunakan protokol PPTP menjadi landasan untuk meningkatkan keamanan jaringan melalui pemilihan alternatif protokol yang lebih aman dan implementasi langkah-langkah pengamanan yang tepat.

DAFTAR PUSTAKA

Afrianto, I., & Setiawan, E. B. (2015). Kajian virtual private network (vpn) sebagai sistem pengamanan data pada jaringan komputer (studi kasus jaringan komputer unikom). *Majalah Ilmiah UNIKOM*, *12*(1). https://doi.org/10.34010/miu.v12i1.34

Albi Anggito & Johan Setiawan. (2018). *Metodologi Penelitian Kualitatif*. CV Jejak.

Alviendra, I. M. (2022). *Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi*. *11*(1).

Arafah, M., & Gunawan, A. (2017). Perancangan dan Simulasi Penerapan Virtual Private Network Menggunakan Metode PPTP (Studi Kasus Pada PT Pelindo IV Makassar). *Inspiration : Jurnal Teknologi Informasi dan Komunikasi*, *7*(2). https://doi.org/10.35585/inspir.v7i2.2450

Bruce Scheier. (1998). Cryptanalysis of Microsofi's Point-to-Point heling Protocol (PPTP). *Proceedings of the 5th ACM Conference*.

Goos, G., Hartmanis, J., Van Leeuwen, J., Schneier, B., Mudge, & Wagner, D. (1999). Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). In R. Baumgart, *Secure Networking—CQRE [Secure] ' 99* (Vol. 1740, pp. 192–203). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-46701-7_17

Haeruddin, H. (2021). Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 848. https://doi.org/10.30865/mib.v5i3.2979

Halawa, W. K. (2021). Analisis Perbandingan VPN PPTP Dan EOIP Menggunakan Metode AQM. *INFACT UKRIM*, *6*(1).

Jahan, S., Rahman, Md. S., & Saha, S. (2017). Application specific tunneling protocol selection for Virtual Private Networks. *2017 International Conference on Networking, Systems and Security (NSysS)*, 39–44. https://doi.org/10.1109/NSysS.2017.7885799

Jha, R. K., & Dalal, D. U. D. (2010). *A Journey on WiMAX and its Security Issues*. *1*.

K. Karuna Jyothi & B. Indira Reddy. (2018). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(5).

Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7

Oktivasari, P., & Utomo, A. B. (2016). *Analisa Virtual Private Network Menggunakan OpenVPN dan Point To Point Tunneling Protocol*. *20*(2), 185–202.

Rana, A. (2013). *Effective Tunnelling of Data and Traffic Management over Network using L2TP based on L2F*. *2*(5).

Supendar, H. (2016). Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. *BINA INSANI ICT JOURNAL*, *3*(1), 85–98.