

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan aspek krusial yang harus diperhatikan dalam era digital yang semakin berkembang, karena hal ini penting untuk melindungi data dan sistem dari akses yang tidak sah. Banyak organisasi, baik kecil maupun besar, bergantung pada infrastruktur jaringan untuk menjalankan operasional sehari-hari, menyimpan data penting, dan berkomunikasi secara efektif. Namun, penggunaan jaringan komputer tanpa perlindungan yang memadai dapat menyebabkan berbagai ancaman, baik secara fisik maupun logis, termasuk pencurian data, kerusakan perangkat keras, dan gangguan operasional yang dapat berakibat fatal (Tahir *et al* 2023:1). Sistem keamanan jaringan komputer perlu dirancang agar tahan terhadap berbagai bentuk serangan dan pemindaian yang dilakukan oleh pihak yang tidak berwenang. Seiring meningkatnya ketergantungan pada jaringan komputer dalam bidang pendidikan, pekerjaan, hingga hiburan, potensi ancaman terhadap keamanan jaringan pun semakin besar. Banyaknya akses jaringan tersedia membuka peluang bagi tindakan kriminal siber atau aktivitas peretasan yang dapat merusak sumber daya server secara signifikan (Dwiyanto et al., 2025).

Undang-Undang Dasar 1945 Pasal 28F dalam konteks keamanan siber menyatakan bahwa setiap orang berhak untuk berkomunikasi dan memperoleh informasi serta mengembangkan diri melalui media apapun, sedangkan Pasal 28G ayat (1) menegaskan hak individu atas perlindungan diri, keluarga, kehormatan, dan harta benda, serta hak atas rasa aman dari ancaman yang mengganggu. Regulasi ini mencerminkan tanggung jawab pemerintah untuk melindungi hak-hak setiap warga

negara dalam era digital yang penuh tantangan. Keamanan jaringan dan dunia siber sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi (MPR, 2002). Salah satu ancaman serius yang sering terjadi adalah serangan *Man in The Middle* (MitM), yaitu terjadi ketika pihak ketiga yang tidak sah berhasil menyusup ke dalam komunikasi antara dua pihak, dengan tujuan untuk menyadap atau bahkan mengubah informasi yang dipertukarkan tanpa diketahui oleh kedua pihak yang berkomunikasi (Tahir et al., 2024). Untuk mengatasi masalah ini, implementasi *Secure Sockets Layer* (SSL) melalui *Transport Layer Security* (TLS) menjadi solusi yang efektif. Protokol SSL/TLS berfungsi untuk memastikan bahwa data yang dikirim antara server dan klien tetap terenkripsi secara aman, sehingga menyulitkan pihak yang tidak berwenang untuk mencegat maupun membaca informasi tersebut. Dengan menerapkan enkripsi SSL/TLS, risiko terjadinya pelanggaran data dan akses ilegal dapat dikurangi secara signifikan oleh suatu organisasi (Haikal et al., 2024). Maka dari itu, penerapan SSL untuk pencegahan MITM attack pada FTP Server tidak hanya melindungi data pengguna, tetapi juga sejalan dengan upaya pemerintah untuk menjaga integritas dan privasi warga negara sesuai dengan ketentuan yang dijamin oleh undang-undang.

Laporan monitoring keamanan siber pada tahun 2023 yang dirilis oleh Badan Siber dan Sandi Negara mencatat lebih dari 403 juta trafik anomali di seluruh Indonesia, dengan jenis ancaman tertinggi berupa *Generic Trojan RAT* yang mengindikasikan adanya komunikasi *backdoor* menuju *domain* berbahaya milik *threat actor*. Selain itu, terdapat lebih dari 4 juta aktivitas *Advanced Persistent Threat* (APT) dan lebih dari 1 juta serangan *ransomware*. Data ini menegaskan bahwa serangan siber tidak hanya mengancam sektor finansial dan pemerintah,

tetapi juga mengakibatkan kebocoran data yang signifikan. BSSN juga mencatat 1.674.185 temuan data *exposure* yang berdampak pada ratusan stakeholder di Indonesia, serta insiden *web defacement* yang semakin meningkat. Kondisi ini menggambarkan betapa rentannya keamanan digital Indonesia terhadap berbagai jenis ancaman siber yang semakin kompleks, dan menekankan pentingnya penguatan proteksi siber guna menjaga kestabilan dan keamanan nasional di era digital (BSSN, 2023).

Indonesia menghadapi lonjakan ancaman di sektor keamanan siber, yang mencerminkan tingginya kerentanan sistem digital di berbagai bidang. Berdasarkan laporan SAFEnet yang dikutip oleh CNN Indonesia (2024), tercatat sebanyak 61 insiden keamanan digital hanya dalam tiga bulan pertama tahun 2024, hampir dua kali lipat dibandingkan periode yang sama pada tahun sebelumnya. Insiden tersebut mencakup berbagai bentuk serangan, seperti peretasan akun media sosial milik tokoh publik, misalnya akun Instagram mantan calon wakil presiden Mahfud MD yang diretas pada Januari, serta penangguhan akun Twitter @veenarooth pada Februari. Selain itu, ancaman digital juga menyasar kalangan akademisi, seperti yang dialami Guru Besar Psikologi UGM, Koentjoro Soeparno, yang mendapatkan teror melalui pesan WhatsApp setelah terlibat dalam aksi sosial. Serangan siber yang berskala lebih besar pun terjadi, termasuk serangan *Distributed Denial of Service* (DDoS) terhadap situs resmi Komisi Pemilihan Umum (KPU) pada hari pemungutan suara, dan meningkatnya aktivitas *ransomware* yang menargetkan sektor finansial maupun pemerintahan. Salah satu kasus paling menonjol terjadi pada Juni 2024, ketika Pusat Data Nasional Sementara (PDNS) di Surabaya diserang oleh grup peretas LockBit yang menuntut tebusan sebesar 8 juta dolar AS.

Rentetan peristiwa ini menegaskan pentingnya peningkatan keamanan siber di Indonesia guna melindungi infrastruktur vital dan data strategis dari ancaman yang semakin kompleks dan terorganisir.

Ancaman terhadap keamanan jaringan mendorong perlunya regulasi yang mengatur keamanan informasi dan jaringan. Regulasi di Indonesia mencakup sejumlah undang-undang, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diperbarui melalui Undang-Undang Nomor 1 Tahun 2024. Amandemen ini memperkuat perlindungan terhadap sistem elektronik, termasuk jaringan komputer, dari ancaman siber seperti peretasan (*hacking*), *malware*, dan serangan *Denial of Service* (DoS). Selain itu, terdapat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang juga mengatur kewajiban penyelenggara sistem elektronik untuk menjaga keamanan jaringan. Regulasi ini menggarisbawahi pentingnya penerapan standar keamanan yang lebih ketat guna menjaga integritas, kerahasiaan, dan ketersediaan data, serta melindungi aset digital dan pengguna jaringan dari ancaman yang terus berkembang di era digital. Di tengah urgensi regulasi dan perlindungan data tersebut, salah satu aspek teknis yang sangat penting untuk diamankan adalah protokol transfer file yang digunakan dalam jaringan.

Protokol transfer file yang tepat sangat penting dalam lingkungan jaringan modern, terutama di era digital yang terus berkembang, di mana kebutuhan untuk bertukar data secara efisien semakin meningkat. Salah satu metode yang paling banyak digunakan adalah *File Transfer Protocol* (FTP). *File Transfer Protocol* (FTP) adalah protokol yang berfungsi sebagai sarana untuk bertukar file atau data

dalam suatu jaringan berbasis koneksi TCP (Sahren, 2021). *File Transfer Protocol* (FTP) memungkinkan pengguna untuk menyimpan dan berbagi data dengan mudah. FTP memberikan kemudahan dalam pengelolaan file, memungkinkan pengguna untuk meng-upload, mendownload, dan mengatur file di *Server* dengan efisien. Melalui kemampuan ini, FTP menjadi solusi yang ideal untuk organisasi yang memerlukan transfer data secara rutin.

Meningkatnya ancaman keamanan siber membuat pengguna perlu mempertimbangkan aspek keamanan saat menggunakan FTP. Salah satu metode pengamanan yang efektif adalah penggunaan *Transport Layer Security* (TLS), yang merupakan penerus dari *Secure Socket Layer* (SSL). *Secure Socket Layer* (SSL) sendiri merupakan protokol kriptografi yang dahulu banyak digunakan untuk menjamin keamanan komunikasi melalui internet. Namun, sejak tahun 2015, SSL telah dinyatakan *deprecated* oleh *Internet Engineering Task Force* (IETF) dan secara resmi digantikan oleh TLS (Barnes et al., 2015). Istilah SSL/TLS masih sering digunakan secara umum dalam berbagai literatur untuk merujuk pada protokol keamanan ini.

SSL bekerja sebagai protokol berlapis, di mana setiap lapisan data mencakup informasi tentang panjang, deskripsi, dan isi. Data yang akan dikirim diproses dengan cara dipecah menjadi blok-blok teratur, dikompresi jika diperlukan, diberi kode autentikasi pesan (*Message Authentication Code/MAC*), dienkripsi, dan kemudian dikirim. Setelah tiba di tujuan, data tersebut didekripsi, diverifikasi, didekompresi, dan disusun ulang (Purwoko & Irmayani, 2020).

Peran SSL dalam komunikasi yang aman mirip dengan peran TCP dalam komunikasi biasa, yaitu menyediakan infrastruktur komunikasi standar yang

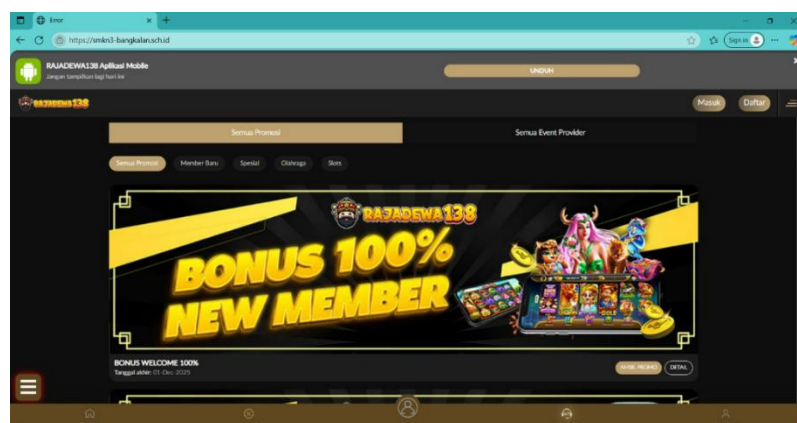
mempermudah aplikasi dalam menggunakannya secara efisien dan hampir tanpa disadari. *Secure Socket Layer/Transport Layer Security* (SSL/TLS) memberikan lapisan enkripsi yang membantu melindungi data yang ditransfer melalui FTP, sehingga menjamin bahwa informasi sensitif tetap aman dari akses tidak sah. Menggunakan SSL, pengguna dapat merasa lebih tenang karena data mereka dilindungi dari berbagai jenis serangan, termasuk serangan *Man In The Middle* (MITM). Salah satu jenis serangan yang secara khusus dapat dicegah dengan penerapan SSL/TLS adalah *Man In The Middle* (MITM), yang merupakan ancaman serius dalam komunikasi jaringan

Serangan *Man In The Middle* (MITM) adalah jenis serangan siber di mana penyerang secara diam-diam menyusup di antara dua pihak yang sedang berkomunikasi, tanpa disadari oleh keduanya (Zulkarnain, 2020). Dalam konteks pengujian, serangan ini sering diuji cobakan menggunakan teknik *sniffing*, yang memungkinkan penyerang untuk menangkap dan menganalisis data yang mengalir dalam jaringan. Melalui pemahaman cara kerja serangan ini, kita dapat lebih baik merancang langkah-langkah pencegahan yang diperlukan untuk melindungi sistem dari potensi kerugian yang diakibatkan oleh serangan siber. Untuk itu, sangat penting memastikan bahwa protokol transfer seperti FTP dibekali dengan perlindungan tambahan agar tidak menjadi sasaran empuk bagi serangan MITM.

Penerapan FTP dalam transfer file memang memberikan kemudahan dalam pengelolaan dan distribusi data. Agar keamanan tetap terjamin, penggunaan SSL/TLS menjadi sangat diperlukan sebagai lapisan pengamanan tambahan. SSL/TLS memastikan bahwa data yang ditransfer tidak hanya dapat diakses dengan mudah, tetapi juga dilindungi dari berbagai ancaman, seperti serangan *Man In The*

Middle (MITM) atau penyadapan data. Mengombinasikan FTP dengan SSL/TLS merupakan langkah penting yang harus dilakukan untuk memastikan integritas dan kerahasiaan data. Selain itu, ini menjadi pondasi utama dalam membangun infrastruktur jaringan yang lebih aman, handal, dan mampu menghadapi ancaman keamanan siber yang semakin kompleks.

Sekolah memerlukan sistem keamanan yang kuat untuk melindungi informasi sensitif dan menjamin kelancaran operasional institusi. Data pribadi siswa, guru, dan staf seperti nama, alamat, dan data akademik merupakan informasi berharga yang wajib dijaga kerahasiaannya. Ketika sistem keamanan tidak memadai, data tersebut berisiko diakses dan disalahgunakan oleh pihak yang tidak berwenang, sehingga dapat melanggar hak privasi individu. Di samping itu, keamanan data juga penting dalam menjaga kelangsungan proses pendidikan, termasuk materi pembelajaran dan hasil evaluasi. Kehilangan atau kerusakan data akibat serangan siber dapat mengganggu proses belajar-mengajar dan merugikan berbagai pihak di lingkungan sekolah. Salah satu contoh kasus yang mencerminkan kerentanan keamanan siber di institusi pendidikan terjadi di SMKN 3 Bangkalan, di mana situs web sekolah diretas dan dialihkan ke situs lain, sebagaimana ditunjukkan pada Gambar 1.1.



Gambar 1. 1 Website SMK 3 Bangkalan di Retas

Serangan siber yang tidak ditangani secara serius berpotensi menimbulkan dampak yang lebih luas, seperti rusaknya reputasi sekolah di mata publik. Ketidakmampuan lembaga dalam menjaga keamanannya dapat mengakibatkan hilangnya kepercayaan dari orang tua, peserta didik, dan masyarakat. Peretasan semacam ini tidak hanya menurunkan kredibilitas sekolah, tetapi juga membuka peluang terhadap pelanggaran data yang lebih serius, termasuk pencurian identitas dan manipulasi informasi penting. Kejadian tersebut menjadi indikator kuat akan perlunya penguatan sistem keamanan siber guna menjaga integritas, kerahasiaan, dan kepercayaan publik terhadap lembaga pendidikan.

Penelitian terdahulu yang relevan yakni penelitian yang dilakukan oleh Sahren (2021) bertujuan untuk mengimplementasikan SSL sebagai langkah pencegahan terhadap serangan *Man In The Middle Attack* pada *FTP Server*. Hasil penelitian yang didapatkan adalah menunjukkan bahwa metode pengamanan dengan *Secure Socket Layer* (SSL) dapat diterapkan dengan efektif pada *FTP Server*. Implementasi SSL dalam *File Transfer Protocol* (FTP) terbukti mampu melindungi transmisi data pada *FTP Server* dari ancaman seperti penyadapan data atau serangan *Man In The Middle Attack*.

Penelitian terdahulu yang relevan yakni penelitian yang dilakukan oleh Akbar *et al.* (2022), bertujuan merancang dan mengimplementasikan sebuah *FTP Server* yang mampu mempercepat dan mempermudah proses pengiriman data, serta untuk memberikan solusi praktis dalam pengelolaan transfer file tanpa perlu menggunakan media fisik. Hasil penelitian yang didapatkan adalah menunjukkan bahwa dalam pembuatan *FTP Server*, diperlukan beberapa perangkat lunak seperti *FileZilla* dan browser Mozilla Firefox untuk mendukung kelancaran transfer data.

yang digunakan untuk menangkap paket data secara langsung dan menampilkan informasi secara detail maupun ringkas. Penggunaan *Transport Layer Security* (TLS) dalam konteks ini bertujuan untuk mengamankan proses transfer data di *FTP Server*, guna mencegah pencurian informasi dan menjaga integritas data yang dikirim.

Penelitian terdahulu yang relevan yakni penelitian yang dilakukan oleh Tambunan *et al.* (2021) bertujuan utama penelitian ini adalah untuk membangun sistem keamanan yang efektif untuk *File Transfer Protocol* (FTP) dengan menggunakan *Secure Socket Layer* (SSL) pada *Server CentOS 7* demi melindungi data yang ditransfer dari akses pihak ketiga dan serangan siber. Hasil penelitian ini membuktikan bahwa implementasi SSL pada *FTP Server* terbukti efektif dalam melindungi data selama proses transmisi, sehingga sistem menjadi lebih terlindungi dari ancaman yang dapat membahayakan keamanan jaringan.

Berdasarkan permasalahan dari beberapa sumber yang diperoleh peneliti ingin melakukan penelitian dengan judul “Implementasi SSL Untuk Pencegahan *Man In The Middle Attack* Pada *FTP Server* Menggunakan *Transport Layer Security Protocol*”. Penelitian ini bertujuan untuk mengimplementasikan *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) sebagai upaya pencegahan terhadap serangan *Man In The Middle* (MITM) pada *FTP Server* di lingkungan sekolah. Penerapan protokol keamanan ini diharapkan dapat memberikan perlindungan terhadap data yang ditransfer melalui jaringan, sehingga mampu menjaga kerahasiaan, integritas, dan ketersediaan informasi. Dengan demikian, sistem jaringan sekolah dapat menjadi lebih aman, andal, dan terlindungi dari berbagai potensi ancaman siber.

1.2 Rumusan Masalah

Berdasarkan latar belakang dan identifikasi permasalahan diatas, maka rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana keamanan jaringan *FTP Server* di lingkungan sekolah dalam mencegah serangan *Man In The Middle* (MITM)?
2. Bagaimana kinerja penerapan *Secure Socket Layer* atau *Transport Layer Security* (SSL/TLS) dalam melindungi *FTP Server* dari serangan MITM?
3. Bagaimana tahapan implementasi protokol *Secure Socket Layer* atau *Transport Layer Security* (SSL/TLS) pada *FTP Server* untuk menjaga keamanan jaringan di lingkungan sekolah?.

1.3 Tujuan Penelitian Pengembangan

Berdasarkan pada rumusan masalah yang sudah dipaparkan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis tingkat keamanan jaringan *FTP Server* di lingkungan sekolah dalam mencegah serangan *Man In The Middle* (MITM).
2. Mengimplementasikan *Secure Socket Layer* atau *Transport Layer Security* (SSL/TLS) pada *FTP Server* sebagai upaya pencegahan terhadap serangan MITM.
3. Mendeskripsikan tahapan implementasi *Secure Socket Layer* atau *Transport Layer Security* (SSL/TLS) pada *FTP Server* dalam rangka menjaga keamanan jaringan di lingkungan sekolah.

1.4 Spesifikasi Produk yang diharapkan

Produk yang diharapkan dari penelitian Implementasi SSL Untuk Pencegahan *Man In The Middle Attack* Pada FTP Server Menggunakan *Transport Layer Security Protocol* antara lain sebagai berikut:

1. Penerapan Protokol SSL/TLS

FTP Server dikonfigurasi dengan protokol SSL/TLS untuk mengenkripsi komunikasi data, mencegah serangan *Man In The Middle* (MITM), serta menjaga kerahasiaan dan integritas data.

2. Penggunaan OpenSSL

OpenSSL digunakan untuk menghasilkan dan mengelola sertifikat digital yang akan memastikan autentikasi dan koneksi aman pada FTP Server.

3. Implementasi Sistem FTP Secure (FTPS)

Pengembangan FTP Server dengan dukungan SSL/TLS yang menghasilkan layanan FTPS, sebagai bentuk nyata dari pengamanan jalur komunikasi data dalam jaringan sekolah.

4. Pemantauan Jaringan dengan Wireshark

Wireshark digunakan untuk menganalisis lalu lintas jaringan, mendeteksi potensi serangan MITM, dan memverifikasi keberhasilan enkripsi data.

1.5 Batasan Penelitian Pengembangan

Batasan masalah penelitian dalam penelitian Implementasi SSL Untuk Pencegahan *Man In The Middle Attack* Pada FTP Server Menggunakan *Transport Layer Security Protocol* antara lain sebagai berikut:

1. Penelitian ini difokuskan pada implementasi protokol keamanan *Secure Socket Layer* atau *Transport Layer Security* (SSL/TLS) pada *FTP Server* di SMK Negeri 3 Bangkalan, tanpa membahas protokol keamanan lainnya.
2. Fokus utama adalah pencegahan serangan *Man In The Middle* (MITM) dalam transfer data menggunakan *FTP Server*, dengan penekanan pada efektivitas SSL/TLS dalam melindungi data.
3. Penelitian hanya menganalisis dan mendeskripsikan tahapan implementasi dan hasil penerapan SSL/TLS pada *FTP Server*, tanpa membahas pengelolaan jaringan secara menyeluruh di lingkungan sekolah.
4. Ruang lingkup penelitian terbatas pada penggunaan *FTP Server* di lingkungan sekolah dan tidak mencakup aplikasi FTP di sektor lain.
5. Penelitian ini tidak membahas pemulihan data atau sistem setelah terjadi serangan siber, melainkan hanya fokus pada pencegahan melalui penerapan protokol keamanan.

1.6 Pentingnya Penelitian Pengembangan

Pentingnya penelitian dan pengembangan ini diharapkan dapat memberikan manfaat bagi semua pihak yang terlibat dalam pembelajaran:

1. Bagi Guru

Penelitian ini membantu guru meningkatkan pemahaman tentang keamanan jaringan, sehingga dapat mengajarkan siswa pentingnya melindungi data. Melalui pengetahuan yang lebih baik, guru dapat merancang metode pengajaran yang relevan dan meningkatkan keterlibatan siswa dalam belajar tentang keamanan siber.

2. Bagi Sekolah

Implementasi hasil penelitian berkontribusi pada perlindungan data siswa dan meningkatkan kepercayaan masyarakat terhadap sekolah. Kebijakan keamanan informasi yang kuat menciptakan lingkungan belajar yang aman dan nyaman bagi siswa dan staf.

3. Bagi Peneliti

Penelitian ini memberikan kontribusi pada pengembangan ilmu keamanan siber dan membuka peluang untuk penelitian lebih lanjut. Publikasi hasil penelitian juga membantu peneliti membangun jaringan profesional dan kolaborasi di bidang keamanan TI.

1.7 Definisi Istilah

Berikut adalah beberapa istilah yang digunakan dalam penelitian Implementasi SSL Untuk Pencegahan *Man In The Middle Attack* Pada FTP Server Menggunakan *Transport Layer Security Protocol*:

1. SSL (*Secure Socket Layer*) adalah Protokol kriptografi berbasis kunci publik yang memungkinkan dua pihak yang berkomunikasi menyamarkan data yang dikirimkan. Data tersebut hanya dapat dibaca oleh kedua pihak melalui kunci khusus yang mereka miliki (Utomo & Rokhmah, 2022).
2. *Transport Layer Security* (TLS) adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi paket data yang dikirim antara klien dan *Server*, sehingga isi paket data tersebut dapat terlindungi privasi dan kerahasiaannya, serta memastikan terjalinnya komunikasi yang aman pada jaringan internet (Putranto *et al* 2022).

3. *Man In The Middle Attack* (MITM) adalah salah satu jenis serangan siber di mana penyerang menyusup ke dalam komunikasi antara dua pihak tanpa diketahui oleh keduanya (Auliafitri *et al* 2024).
4. *FTP Server (File Transfer Protocol Server)* adalah *Server* yang menjalankan perangkat lunak untuk menyediakan layanan pertukaran file. *Server* ini selalu siap melayani permintaan (request) dari *FTP client* untuk melakukan transfer file (Rachmawati, R. N., & Christiana, T., 2021).