

ANALISIS PENERAPAN SSL/TLS DALAM MENJAGA KEAMANAN TRANSMISI DATA PADA APLIKASI WEB

Andi Khairunnisa Ramadhani Saidiman¹, Siti Salwa Huwaidah Sugianto²,
Rakhmadi Rahman³

andikhairunnisaramadhanisaidiman.241031003@mahasiswa.ith.ac.id¹,
sitisalwahuwaidahsugianto.241031006@mahasiswa.ith.ac.id², rakhmadi.rahman@ith.ac.id³
Institut Teknologi Bacharuddin Jusuf Habibie Kota Parepare Sulawesi Selatan

ABSTRAK

Penggunaan aplikasi web yang terus meningkat menyebabkan intensitas pertukaran data melalui jaringan internet semakin tinggi. Kondisi tersebut menimbulkan risiko keamanan yang tidak dapat diabaikan, khususnya pada tahap pengiriman data dari klien ke server. Informasi yang ditransmisikan tanpa perlindungan berpotensi mengalami akses tidak sah, perubahan konten, maupun penyalahgunaan oleh pihak lain. Kajian ini bertujuan untuk menelaah penerapan Secure Socket Layer (SSL) dan Transport Layer Security (TLS) sebagai mekanisme pengamanan komunikasi data pada aplikasi web. Pendekatan yang diterapkan dalam penelitian ini dilakukan melalui penelaahan sumber pustaka, dengan penyajian pembahasan secara deskriptif berdasarkan keterkaitan antar konsep, disertai kajian konseptual terhadap perbedaan pola komunikasi data menggunakan protokol HTTP dan HTTPS. Hasil analisis menunjukkan bahwa penggunaan SSL/TLS mampu memperkuat keamanan transmisi data melalui penerapan enkripsi, verifikasi identitas, serta penjagaan keutuhan informasi. Penerapan mekanisme tersebut berkontribusi dalam menekan potensi ancaman keamanan jaringan dan meningkatkan tingkat kepercayaan pengguna terhadap layanan web. Oleh sebab itu, SSL/TLS merupakan elemen krusial dalam pengembangan aplikasi web yang berorientasi pada perlindungan data.

Kata Kunci: SSL/TLS, Keamanan Aplikasi Web, HTTPS, Transmisi Informasi, Perlindungan Data.

ABSTRACT

The continuous growth of web-based applications has resulted in an increasing volume of data transmission over internet networks. This situation introduces significant security risks, particularly during the data exchange process between clients and servers. Information transmitted without adequate protection may be accessed, altered, or misused by unauthorized entities. This study aims to examine the implementation of Secure Socket Layer (SSL) and Transport Layer Security (TLS) as mechanisms for securing data communication in web applications. A descriptive-analytical literature review approach is employed, complemented by a conceptual comparison of data communication patterns using HTTP and HTTPS protocols. The findings indicate that SSL/TLS implementation enhances data transmission security through encryption, identity verification, and data integrity protection. These mechanisms help reduce network security threats and strengthen user trust in web services. Therefore, SSL/TLS plays a vital role in the development of secure web-based systems.

Keywords: SSL/TLS, Web Application Security, HTTPS, Data Transmission, Information Protection.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong pemanfaatan aplikasi berbasis web secara luas dalam berbagai sektor, termasuk pendidikan, pemerintahan, dan kegiatan bisnis. Aplikasi web digunakan karena kemampuannya dalam menyediakan layanan yang mudah diakses serta fleksibel bagi pengguna. Namun, peningkatan penggunaan tersebut juga diikuti oleh meningkatnya tantangan dalam menjaga keamanan data yang dikelola oleh sistem web.

Proses pertukaran data pada aplikasi web berlangsung melalui jaringan internet yang memiliki sifat terbuka. Kondisi ini memungkinkan terjadinya intersepsi data oleh pihak tertentu apabila tidak disertai mekanisme perlindungan yang memadai. Data sensitif, seperti informasi autentikasi dan identitas pengguna, berisiko mengalami kebocoran yang dapat menimbulkan dampak negatif bagi pengguna maupun penyedia layanan.

Salah satu faktor yang memicu permasalahan keamanan web adalah penggunaan protokol komunikasi tanpa sistem pengamanan. Protokol HTTP, misalnya, mengirimkan data dalam format yang dapat dibaca secara langsung, sehingga rentan terhadap penyadapan. Kelemahan ini dapat dimanfaatkan dalam berbagai bentuk serangan siber yang mengancam keamanan informasi.

Untuk mengatasi permasalahan tersebut, diperlukan mekanisme pengamanan yang mampu melindungi data selama proses transmisi. SSL dan TLS merupakan solusi keamanan yang bekerja pada lapisan komunikasi dengan menerapkan teknik kriptografi dan autentikasi. Implementasi mekanisme ini pada aplikasi web ditunjukkan melalui penggunaan protokol HTTPS, yang saat ini telah menjadi standar keamanan pada layanan web modern. Dengan mempertimbangkan kondisi yang telah dipaparkan sebelumnya, penelitian ini difokuskan pada evaluasi penerapan SSL/TLS sebagai mekanisme pengamanan proses transmisi data pada aplikasi web.

METODE PENELITIAN

Pendekatan yang diterapkan dalam penelitian ini dilakukan melalui penelaahan sumber pustaka, dengan penyajian pembahasan secara deskriptif berdasarkan keterkaitan antar konsep. Kajian difokuskan pada pemahaman mekanisme pengamanan komunikasi data menggunakan SSL/TLS dengan merujuk pada berbagai referensi ilmiah yang relevan. Sumber kajian diperoleh dari publikasi akademik nasional dan internasional yang membahas keamanan jaringan serta sistem berbasis web.

Selain kajian pustaka, penelitian ini dilengkapi dengan analisis konseptual terhadap perbedaan mekanisme komunikasi data pada protokol HTTP dan HTTPS. Analisis dilakukan untuk menggambarkan tingkat perlindungan data yang dihasilkan oleh masing-masing protokol, khususnya dari sisi keamanan transmisi informasi.

Tahapan penelitian dilakukan secara sistematis sebagai berikut:

1. Pengumpulan Sumber Referensi

Referensi dikumpulkan dari publikasi ilmiah yang membahas keamanan komunikasi web dan penerapan SSL/TLS.

2. Klasifikasi Informasi

Informasi yang diperoleh dianalisis dan dikelompokkan berdasarkan topik pembahasan, seperti karakteristik protokol HTTP dan HTTPS, mekanisme enkripsi, serta autentikasi server.

3. Analisis Mekanisme SSL/TLS

Tahap ini difokuskan pada kajian mekanisme kerja SSL/TLS dalam mengamankan transmisi data, termasuk proses pembentukan koneksi aman dan penggunaan sertifikat digital.

4. Perbandingan Protokol Komunikasi

Perbandingan dilakukan untuk menilai perbedaan tingkat keamanan antara HTTP dan HTTPS dalam komunikasi data aplikasi web.

5. Perumusan Kesimpulan

Tahap ini dilakukan dengan merangkum hasil analisis yang telah diperoleh guna menjawab fokus penelitian sekaligus menegaskan urgensi penerapan SSL/TLS dalam menjaga keamanan komunikasi data pada aplikasi web.

HASIL DAN PEMBAHASAN

Hasil kajian menunjukkan bahwa penerapan SSL/TLS memberikan pengaruh signifikan terhadap keamanan transmisi data pada aplikasi web. Analisis dilakukan dengan meninjau perbedaan karakteristik komunikasi data menggunakan protokol HTTP dan HTTPS serta peran SSL/TLS dalam menjaga keamanan informasi.

Pada protokol HTTP, data dikirimkan tanpa mekanisme perlindungan sehingga informasi dapat diakses secara langsung apabila terjadi penyadapan. Kondisi ini meningkatkan risiko kebocoran data, terutama pada aplikasi yang mengelola informasi sensitif pengguna. Oleh karena itu, penggunaan HTTP dinilai tidak sesuai untuk aplikasi web yang menuntut tingkat keamanan tinggi.

Sebaliknya, protokol HTTPS menerapkan SSL/TLS untuk melindungi data selama proses transmisi. Data yang dikirimkan melalui HTTPS berada dalam bentuk terenkripsi, sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci akses. Penerapan enkripsi ini secara efektif menurunkan risiko penyadapan data.

Selain enkripsi, SSL/TLS juga menyediakan mekanisme autentikasi server melalui sertifikat digital. Mekanisme ini memungkinkan pengguna untuk memastikan keaslian server yang diakses, sehingga risiko pemalsuan identitas dapat diminimalkan. Dengan demikian, penerapan SSL/TLS tidak hanya melindungi data secara teknis, tetapi juga meningkatkan rasa aman dan kepercayaan pengguna terhadap aplikasi web.

Implikasi penerapan SSL/TLS terlihat dari meningkatnya tingkat keamanan dan keandalan aplikasi web. Aplikasi yang menggunakan HTTPS memiliki perlindungan data yang lebih baik dibandingkan dengan aplikasi yang masih menggunakan HTTP. Hal ini menjadikan SSL/TLS sebagai komponen penting dalam pengembangan sistem web modern.

KESIMPULAN

Penerapan SSL/TLS terbukti memberikan kontribusi signifikan dalam memperkuat keamanan pertukaran data pada aplikasi web. Melalui penerapan enkripsi dan mekanisme verifikasi identitas, risiko terjadinya akses tidak sah serta perubahan data selama proses komunikasi dapat ditekan.

Penggunaan HTTPS sebagai bentuk implementasi SSL/TLS terbukti memberikan tingkat keamanan yang lebih baik serta meningkatkan kepercayaan pengguna terhadap layanan web. Oleh karena itu, penerapan SSL/TLS disarankan sebagai standar keamanan dalam pengembangan aplikasi web guna memastikan perlindungan data dan kualitas layanan yang optimal.

DAFTAR PUSTAKA

- Dharmawan, N., Indriyanta, G., & Senapatha, I. K. D. (2020). Analisis keamanan jaringan menggunakan SSL/TLS. *Jurnal Teknologi Informasi*.
- Onoja, E. D., Adewale, B. S., & Omopariola, V. (2022). Comparative analysis of SSL and TLS protocols in modern web environments. *International Journal of Scientific Research and Management*.
- Syahab, A. S., Ujianto, E. I. H., & Rianto. (2023). Analisis keamanan data website menggunakan protokol SSL/TLS. *Jurnal Informatika*, 7(2), 101–110.
- Wakoli, L. W. (2021). Secure sockets layer and transport layer security for web-based applications. *International Journal of Scientific Research and Management*, 9(4), 210–217.
- Wibowo, A., Pratama, D., & Hidayat, R. (2021). Implementation of TLS/SSL for securing web-based systems. *International Journal of Advanced Computer Science and Applications*, 12(6), 345–352.