



Analisis Manfaat Dan Tantangan Dalam Implementasi Keamanan Web HTTP Dan HTTPS

Daffa Sholah Islamey^{1*}, Muhammad Muwafi², Musthafa Anggoro³, Muhammad Fathan Ramadhan⁴, Hasan Wijaya⁵, Anna Dina Kalifia⁶

¹Fakultas Sains dan Teknologi, Program Studi Informatika, Universitas Teknologi Yogyakarta, Sleman, Indonesia

Email: ^{1*}daffasholah26@gmail.com, ²mo4laas@gmail.com, ³Musthafaanggoro07@gmail.com,
⁴muhhammad.fathan0813@email.com, ⁵hasan.5210411075@student.utv.ac.id,
⁶anna.dina.kalifia@staff.utv.ac.id

(* : coresponding author)

Abstrak – Perkembangan teknologi internet telah mendorong peningkatan kebutuhan akan keamanan data dalam komunikasi web. Protokol HTTP (Hypertext Transfer Protocol) dan HTTPS (Hypertext Transfer Protocol Secure) adalah dua protokol utama yang digunakan untuk mengakses informasi di web. Artikel ini membahas secara komprehensif manfaat dan tantangan dalam implementasi HTTPS dibandingkan dengan HTTP, dengan fokus pada aspek keamanan, kinerja, dan kepercayaan pengguna. HTTPS menyediakan enkripsi data yang signifikan untuk melindungi informasi sensitif dari ancaman siber seperti man-in-the-middle attacks dan data interception. Selain itu, penggunaan HTTPS dapat meningkatkan peringkat SEO (Search Engine Optimization) dan membangun kepercayaan pengguna melalui indikasi keamanan seperti ikon gembok di browser. Namun, implementasi HTTPS juga menghadapi tantangan, termasuk kebutuhan akan sertifikat SSL/TLS, peningkatan beban komputasi server, dan potensi masalah kompatibilitas dengan sistem lama. Melalui analisis literatur dan studi kasus, penelitian ini menemukan bahwa meskipun terdapat hambatan dalam adopsi HTTPS, manfaat yang diperoleh dalam hal keamanan dan kepercayaan pengguna jauh melebihi biaya dan upaya yang diperlukan.

Kata Kunci: HTTP; HTTPS; Keamanan Web; Enkripsi Data; Sertifikat SSL/TLS; SEO; Kepercayaan Pengguna.

Abstract – The development of internet technology has led to an increased need for data security in web communications. HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) protocols are the two main protocols used to access information on the web. This article comprehensively discusses the benefits and challenges in implementing HTTPS compared to HTTP, focusing on the aspects of security, performance, and user trust. HTTPS provides significant data encryption to protect sensitive information from cyber threats such as man-in-the-middle attacks and data interception. In addition, the use of HTTPS can improve SEO (Search Engine Optimization) rankings and build user trust through security indications such as the padlock icon in the browser. However, HTTPS implementation also faces challenges, including the need for SSL/TLS certificates, increased server computing load, and potential compatibility issues with legacy systems. Through literature analysis and case studies, this research found that despite the barriers to HTTPS adoption, the benefits gained in terms of security and user trust far outweigh the cost and effort required.

Keywords: HTTP; HTTPS; Web Security; Data Encryption; Certification SSL/TLS; SEO; User Trusting.

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi dan penetrasi internet, keamanan informasi menjadi aspek krusial dalam pengelolaan dan penyampaian data *online*. Protokol komunikasi web seperti HTTP (Hypertext Transfer Protocol) dan HTTPS (Hypertext Transfer Protocol Secure) berperan vital dalam proses ini. HTTP, yang telah lama digunakan sebagai standar untuk transfer data di web, kini menghadapi tantangan signifikan terkait keamanan.

Ancaman siber yang semakin canggih, seperti serangan *man-in-the-middle* dan pengintaian data, menuntut perlindungan lebih bagi data yang dikirim dan diterima melalui jaringan internet. HTTPS hadir sebagai solusi dengan menawarkan lapisan keamanan tambahan melalui enkripsi data menggunakan SSL/TLS (Secure Sockets Layer/Transport Layer Security). Protokol ini tidak hanya mengenkripsi data yang dikirim, tetapi juga memastikan bahwa data tersebut tidak dapat diubah atau diakses oleh pihak yang tidak berwenang selama proses transmisi. Selain manfaat



keamanan, HTTPS juga berkontribusi dalam peningkatan kepercayaan pengguna terhadap situs, yang ditunjukkan melalui indikator visual seperti ikon gembok pada *browser*, dan dalam peningkatan peringkat SEO (*Search Engine Optimization*) karena preferensi mesin pencari terhadap situs yang aman. Namun, implementasi HTTPS tidak bebas dari tantangan. Salah satu hambatan utama adalah kebutuhan untuk memperoleh dan memperbarui sertifikat SSL/TLS yang valid, yang dapat menambah biaya operasional bagi pengelola situs web. Selain itu, proses enkripsi dan dekripsi data dapat meningkatkan beban komputasi pada server, berpotensi memperlambat waktu *respons*, terutama pada situs dengan lalu lintas tinggi. Tantangan teknis lainnya termasuk masalah kompatibilitas dengan sistem lama yang belum mendukung protokol HTTPS sepenuhnya. Dalam konteks globalisasi dan digitalisasi, privasi dan integritas data menjadi sangat penting. Situs yang menggunakan HTTPS dapat menyediakan enkripsi data *end-to-end* yang lebih aman, sehingga memastikan bahwa data yang dikirimkan antar pengguna dan server tetap rahasia dan tidak dapat diubah oleh pihak ketiga. Selain itu, migrasi ke HTTPS juga mendukung prinsip-prinsip keamanan data yang diatur dalam berbagai regulasi internasional seperti *General Data Protection Regulation* (GDPR) di Eropa dan *Health Insurance Portability and Accountability Act* (HIPAA) di Amerika Serikat.

Berdasarkan penelitian sebelumnya, ditemukan bahwa situs web yang menggunakan HTTPS memiliki tingkat kepercayaan pengguna yang lebih tinggi dibandingkan dengan situs yang hanya menggunakan HTTP. Hal ini dikarenakan pengguna merasa lebih aman ketika berinteraksi dengan situs yang menyediakan enkripsi data, terutama saat memasukkan informasi sensitif seperti nomor kartu kredit, kata sandi, atau informasi pribadi lainnya. Selain itu, mesin pencari seperti Google juga memberikan peringkat lebih tinggi kepada situs yang menggunakan HTTPS, sehingga meningkatkan visibilitas dan aksesibilitas situs web tersebut di hasil pencarian.

2. METODE

2.1 Desain Penelitian

Penelitian ini menggunakan metode penelitian kuantitatif. Metode penelitian kuantitatif diartikan sebagai metode penelitian yang digunakan untuk meneliti pada sampel tertentu, analisis data bersifat statistik dengan tujuan untuk menguji hipotesis yang telah ditetapkan (Parjaman & Akhmad, 2019). Tipe penelitian adalah pengujian hipotesis dengan jenis kausalitas. Penelitian jenis kausalitas merupakan bentuk penelitian yang disusun untuk mencari penjelasan dalam bentuk hubungan sebab akibat antar beberapa variabel (Husain et al., 2020).

2.2. Alur Penelitian

Dalam naskah adapun penjelasan dari tahap alur penelitian sebagai berikut nomor kutipan secara berurutan dalam tanda kurung (Kumar, Kaur, & Kumar, 2019), juga tabel angka dan angka secara berurutan seperti yang ditunjukkan pada Tabel 1 dan Gambar 1.

- a. Merumuskan Masalah Penelitian: Menentukan pertanyaan penelitian yang spesifik dan dapat diukur.
- b. Pengembangan Hipotesis: Merumuskan hipotesis yang jelas dan spesifik yang akan diuji.
- c. Desain Penelitian: Memilih desain penelitian yang sesuai, seperti survei, eksperimen, atau analisis korelasional.
- d. Pengumpulan Data: Menggunakan instrumen yang terstandarisasi, seperti kuesioner atau perangkat pengukur, untuk mengumpulkan data numerik.
- e. Analisis Data: Menggunakan teknik statistik untuk menganalisis data yang dikumpulkan dan menguji hipotesis.
- f. Kesimpulan: Menarik kesimpulan berdasarkan hasil analisis data dan memberikan rekomendasi untuk penelitian lebih lanjut atau aplikasi praktis.



3. ANALISA DAN PEMBAHASAN

3.1 Manfaat Implementasi HTTPS

a. Keamanan Data

HTTPS menggunakan protokol SSL/TLS untuk mengenkripsi data yang ditransfer antara server dan browser pengguna. Enkripsi ini membantu mencegah akses yang tidak sah terhadap informasi sensitif, seperti kata sandi, informasi kartu kredit, dan data pribadi lainnya.

b. Peningkatan Kepercayaan Pengguna

Pengguna sering kali memandang situs web yang menggunakan HTTPS sebagai lebih tepercaya dan aman. Ketika pengguna melihat ikon gembok hijau atau status "aman" di browser mereka, ini memberikan kepercayaan tambahan bahwa situs tersebut adalah sumber yang dapat dipercaya untuk berinteraksi secara online.

c. Peningkatan Peringkat SEO

Mesin pencari, seperti Google, memberikan peringkat yang lebih tinggi untuk situs web yang menggunakan HTTPS daripada HTTP. Hal ini karena Google memprioritaskan keamanan dan privasi pengguna, sehingga menggunakan HTTPS dapat memberikan keuntungan dalam hal peringkat pencarian dan visibilitas online.

3.2 Tantangan Implementasi HTTPS

a. Biaya Sertifikat SSL/TLS

Untuk menggunakan HTTPS, situs web perlu memiliki sertifikat SSL/TLS yang dikeluarkan oleh otoritas sertifikat tepercaya. Biaya untuk mendapatkan sertifikat ini bisa bervariasi tergantung pada penyedia sertifikat dan jenis sertifikat yang dipilih, yang bisa menjadi beban tambahan terutama bagi pemilik situs kecil atau startup.

b. Beban Komputasi Server

Proses enkripsi dan dekripsi yang terjadi saat menggunakan HTTPS dapat meningkatkan beban komputasi pada server. Ini bisa berdampak pada kinerja situs web, terutama saat menghadapi lalu lintas tinggi. Diperlukan pemantauan dan penyesuaian yang tepat untuk memastikan bahwa server mampu menangani beban tambahan dengan efisien.

c. Masalah Kompatibilitas

Implementasi HTTPS dapat menghadapi masalah kompatibilitas dengan perangkat lunak atau sistem yang lebih lama atau tidak mendukung standar enkripsi yang lebih baru. Ini memerlukan penyesuaian tambahan atau upgrade perangkat lunak dan infrastruktur untuk memastikan bahwa semua pengguna dapat mengakses situs web dengan aman.

3.3 Analisis Literatur dan Studi Kasus

a. Kelayakan Ekonomi

Meskipun investasi awal dan biaya operasional terkait dengan implementasi HTTPS bisa signifikan, banyak studi ekonomi telah menunjukkan bahwa manfaat jangka panjang dari keamanan data dan peningkatan reputasi situs web biasanya mengkompensasi biaya tersebut.

b. Efektivitas dalam Melindungi Data

Berbagai studi kasus telah mengonfirmasi bahwa implementasi HTTPS secara efektif mengurangi risiko serangan siber, seperti pencurian data dan peretasan, dengan menyediakan lapisan enkripsi yang kuat untuk data yang ditransfer.



c. Penerimaan Pengguna

Meskipun awalnya mungkin terdapat resistensi atau tantangan dalam adopsi HTTPS, peningkatan kesadaran akan keamanan online dan dukungan dari penyedia layanan web besar telah mendorong penerimaan luas terhadap protokol ini.

Dari analisis ini, dapat disimpulkan bahwa manfaat keamanan dan kepercayaan pengguna yang diperoleh melalui implementasi HTTPS jauh melebihi tantangan dan biaya yang terkait dengan adopsinya. Meskipun perlu dilakukan investasi yang cukup, keamanan data dan reputasi situs web yang ditingkatkan membuat implementasi HTTPS menjadi pilihan yang sangat dianjurkan bagi organisasi yang peduli terhadap keamanan dan pengalaman pengguna mereka.

4. KESIMPULAN

Perkembangan teknologi internet dari tahun ke tahun meningkatkan kebutuhan keamanan data dalam komunikasi web. Artikel ini membandingkan dua protokol utama, HTTP dan HTTPS, dengan berfokus pada manfaat dan tantangan implementasi HTTPS. HTTPS menawarkan enkripsi data yang signifikan untuk melindungi informasi sensitif dari ancaman cyber, serta dapat meningkatkan peringkat SEO dan kepercayaan pengguna melalui indikator keamanan seperti icon gembok di browser. Namun, dalam penerapan HTTPS terdapat beberapa tantangan, termasuk kebutuhan sertifikat SSL/TLS, peningkatan beban komputasi server, dan masalah kompatibilitas dengan sistem terdahulu.

Melalui analisis literatur dan studi kasus, ditemukan bahwa meskipun terdapat hambatan dalam penerapan HTTPS, manfaat yang diperoleh dari penggunaan HTTPS, terutama dalam hal keamanan dan kepercayaan pengguna, jauh melebihi biaya dan upaya yang diperlukan. Implementasi HTTPS tidak hanya memberikan perlindungan tambahan tetapi juga mendukung privasi dan integritas data, serta mematuhi regulasi keamanan data internasional. Oleh karena itu, meskipun HTTP masih banyak digunakan, penerapan HTTPS sangat dianjurkan bagi organisasi yang peduli terhadap keamanan dan pengalaman pengguna mereka. Keamanan data dan reputasi situs web yang ditingkatkan membuat HTTPS menjadi pilihan yang lebih unggul dibandingkan HTTP dalam konteks modern.

REFERENCES

- Alfin Syarifuddin Syahab, E. I. (2023). PENGGUNAAN WIRESHARK DAN NESSUS UNTUK ANALISIS SSL/TLS PADA KEAMANAN DATA PENGGUNA WEBSITE. *JIKA (Jurnal Informatika)*, 10.
- HUZAIRI, H. (2023). ANALISIS KEAMANAN FASILITAS JARINGAN (WI-FI) TERHADAP SERANGAN PACKET SNIFFING PADAPROTOCOL HTTP DAN HTTPS.
- Kurniawan, R. (2021). ANALISIS KEAMANAN FASILITAS JARINGAN (Wi-Fi) TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS. *UIR*, 71.
- Naikson Fandier Saragih, R. T. (2023). ANALISIS DAN IMPLEMENTASI SECURE CODE PADA PENGEMBANGAN SISTEM KEAMANAN WEBSITE FIKOM-METHODIST.COM MENGGUNAKAN PENETRATION TESTING DAN OWASP ZAP. *Jurnal TIMES*, 12.
- Nanang Sadikin, M. (2019). IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER UNTUK AKSES INTERNET MENGGUNAKAN KEY SECURITY. *Jurnal Maklumatika*, 8.
- Syarif Hidayatulloh, D. S. (2021). Penetration Testing Pada Website Universitas ARS Menggunakan open Web Application Security Project. *Jurnal Algoritma*.
- Winawang, Y. (2021). IMPLEMENTASI KEAMANAN JALUR INTERNET MENGGUNAKAN IP TUNNELING PADA OPENVPN ACCESS SERVERDENGAN PROTOKOL OPENVPN DAN PROTOKOL DNS OVER HTTPS. *InstituteJurnal Syntax Admiration*.
- Yacob Hae, W. S. (2021). Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen. *Jurnal Syntax Admiration*.