ROUTERS: Jurnal Sistem dan Teknologi Informasi
Vol. 2, No. 2, Juli 2024, pp. 79-84
ISSN: 2962-1224, DOI: 10.25181/rt.v2i2.3446

Analisis terhadap Enkripsi Data SSL di MySQL: Menguji Keamanan In-Transit

Antoni Haikal[1], Septafiansyah Dwi Putra[2] , Nelmiawati[3]
[1] Rekayasa Keamanan Siber, Politeknik Negeri Batam
[2] Teknologi Rekayasa Internet, Politeknik Negeri Lampung
[3] Rekayasa Keamanan Siber, Politeknik Negeri Batam

INFORMASI ARTIKEL

Diterima 25 Januari 2024
Direvisi 25 Januari 2024
Diterbitkan 29 Januari 2024

Kata kunci:

Data In-Transit;
SSL;
MySQL;
Enkripsi;

ABSTRAK

Keamanan transmisi data menjadi titik penting dalam manajemen basis data, terutama dalam menanggapi ancaman siber yang berkembang. Studi ini mengkaji satu aspek kritis keamanan data: enkripsi data in-transit menggunakan Secure Sockets Layer (SSL) dalam MySQL. Fokus utama penelitian ini adalah pada pengujian enkripsi data dengan menggunakan Wireshark, alat analisis jaringan yang mampu menangkap dan menampilkan paket data yang ditransmisikan. Proses pengujian terdiri dari dua skenario: pertama, transmisi data dengan SSL diaktifkan pada server MySQL; kedua, transmisi data tanpa penggunaan SSL. Hasil menunjukkan kontras yang signifikan antara kedua skenario tersebut. Dalam skenario dengan SSL, paket data yang diintersepsi oleh Wireshark terlihat tidak terbaca, menandakan bahwa enkripsi berhasil mencegah eksposur isi data. Sebaliknya, tanpa SSL, paket data dapat dibaca sebagai teks biasa, menunjukkan ketiadaan enkripsi dan risiko keamanan yang tinggi. Penelitian ini berfokus pada aspek keamanan enkripsi data in-transit di MySQL dan tidak mengeksplorasi implikasi terkait performa atau konfigurasi SSL lebih lanjut. Analisis ini memberikan pandangan yang berguna bagi administrator basis data dalam upaya peningkatan keamanan data, dengan mengidentifikasi SSL sebagai alat penting untuk memastikan keamanan data in-transit.

Analysis of SSL Data Encryption in MySQL: Testing In-Transit Security

ARTICLE INFO

Received January 25, 2024
Revised January 25, 2024
Published January 29, 2024

Keyword:

Data In-Transit;
SSL;
MySQL;
Encryption;

ABSTRACT

Data transmission security has become a pivotal point in database management, especially in response to the evolving cyber threats. This study examines a critical aspect of data security: the in-transit data encryption using Secure Sockets Layer (SSL) within MySQL. The main focus of the research is on testing data encryption by employing Wireshark, a network analysis tool capable of capturing and displaying transmitted data packets. The testing process consisted of two scenarios: first, data transmission with SSL enabled on the MySQL server; second, data transmission without the use of SSL. The results show a significant contrast between the two scenarios. With SSL, the data packets intercepted by Wireshark appeared unreadable, indicating that encryption was successful in preventing data content exposure. Conversely, without SSL, the data packets could be read as plain text, demonstrating a lack of encryption and a high security risk. This research delves only into the aspect of in-transit data encryption security in MySQL and does not explore the implications related to SSL performance or configuration further. This analysis offers a useful perspective for database administrators in efforts to enhance data security, identifying SSL as a crucial tool to ensure the security of in-transit data.

Corresponding Author:
Antoni Haikal, Rekayasa Keamanan Siber, Politeknik Negeri Batam
Email: antoni@polibatam.ac.id

1. PENDAHULUAN

Di era digital saat ini, perlindungan data sensitif menjadi hal esensial. Entah itu informasi pribadi, catatan keuangan, atau bentuk lain dari data rahasia, memastikan keamanannya adalah hal yang krusial[1]. Salah satu cara untuk mencapai hal ini adalah dengan menggunakan enkripsi SSL di MySQL. Metode ini tidak hanya membantu mengamankan pengiriman data antara server dan klien tetapi juga memberikan lapisan perlindungan tambahan untuk mencegah akses tidak sah dan intersepsi informasi sensitif. Dalam bagian berikut, kita akan menggali lebih dalam konsep enkripsi SSL di MySQL dan mengeksplor manfaat serta teknik implementasinya.

Keamanan data adalah masalah kritis dalam sistem apa pun yang menangani informasi sensitif[2], [3]. Salah satu pendekatan untuk meningkatkan keamanan data adalah dengan menerapkan enkripsi SSL di MySQL. Enkripsi SSL adalah metode untuk mengamankan pengiriman data antara server dan klien menggunakan protokol SSL/TLS[4], [5]. Protokol SSL/TLS memastikan bahwa data yang dikirim antara server MySQL dan klien dienkripsi dengan aman, sehingga sangat sulit bagi pengguna yang tidak sah untuk mencegat dan menguraikan informasi tersebut. Dengan menerapkan enkripsi SSL di MySQL, organisasi dapat secara signifikan mengurangi risiko pelanggaran data dan akses tidak sah. Selain itu, enkripsi SSL memberikan lapisan keamanan tambahan dengan memverifikasi identitas server, memastikan bahwa klien berkomunikasi dengan server MySQL yang sah dan bukan penipu jahat. Proses autentikasi ini menambah tingkat perlindungan lain terhadap potensi ancaman keamanan[6], [7].

Implementasi enkripsi SSL di MySQL melibatkan konfigurasi server untuk menggunakan sertifikat SSL dan mengaktifkan dukungan SSL dalam konfigurasi database. Proses ini memerlukan pembuatan sertifikat SSL, konfigurasi MySQL untuk menggunakan sertifikat, dan verifikasi koneksi aman antara server dan klien[4], [8]. Selain implementasi teknis, penting bagi organisasi untuk menetapkan kebijakan dan praktik keamanan yang komprehensif untuk mengelola enkripsi SSL di MySQL[6], [9]. Hal Ini termasuk memperbarui sertifikat SSL secara rutin, memantau dan mencatat koneksi SSL, dan melakukan audit keamanan berkala untuk memastikan kepatuhan dengan praktik terbaik dan standar industri[10], [11].

Dengan menerapkan enkripsi SSL di MySQL dan mengadopsi langkah-langkah keamanan yang kuat, organisasi dapat memperkuat perlindungan data sensitif mereka, menumbuhkan kepercayaan dengan klien mereka, dan menunjukkan komitmen untuk menjaga informasi rahasia.

Perlindungan data selama perpindahannya melintasi jaringan—dikenal sebagai data in-transit—merupakan aspek kritis di era digital yang sarat dengan tantangan keamanan siber. Dengan peran kunci sistem manajemen basis data relasional (RDBMS) seperti MySQL dalam infrastruktur teknologi informasi perusahaan, jaminan atas kerahasiaan dan integritas data yang bergerak menjadi prioritas utama. Protokol Secure Sockets Layer (SSL), serta penggantinya Transport Layer Security (TLS), dikembangkan sebagai mekanisme kriptografi untuk mengamankan komunikasi data melalui jaringan. Penerapan protokol ini dalam mengamankan koneksi server MySQL telah menjadi norma umum untuk menghadapi ancaman keamanan data yang semakin kompleks. Meski SSL/TLS telah menjadi tulang punggung keamanan data in-transit, masih terdapat kebutuhan akan pemahaman yang lebih mendalam tentang keefektifannya dalam konteks MySQL. Studi ini dirancang untuk mengisi kekosongan tersebut dengan memanfaatkan Wireshark[12], [13], [14], sebuah alat analisis jaringan yang mumpuni, guna menganalisis perbedaan keamanan paket data ketika SSL diimplementasikan dibandingkan dengan ketika tidak digunakan di MySQL.

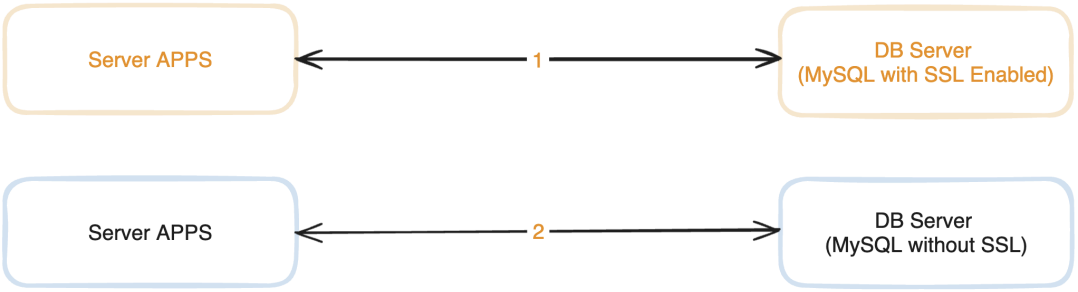
Urgensi penelitian ini diperkuat oleh peningkatan insiden pelanggaran data dan serangan siber yang bertujuan pada data in-transit. Di tengah meningkatnya tuntutan regulasi perlindungan data seperti General Data Protection Regulation (GDPR) dan California Consumer Privacy Act (CCPA), hasil dari penelitian ini sangat relevan dan tepat waktu[3], [15], [16], [17]. Dengan fokus pada pengaruh SSL dalam memastikan keamanan transmisi data MySQL, tulisan ini bertujuan untuk menambah wawasan ke dalam literatur keamanan data dan memberikan data empiris bagi para administrator basis data serta ahli keamanan untuk mendukung strategi keamanan mereka.

2. METODE

Penelitian ini menggunakan pendekatan empiris untuk menganalisis keamanan data in-transit pada MySQL dengan dan tanpa implementasi SSL. Metode yang diadopsi melibatkan penggunaan Wireshark, sebuah alat analisis jaringan yang luas digunakan, untuk merekam dan menganalisis paket data yang ditransmisikan.

2.1. Konfigurasi Sistem

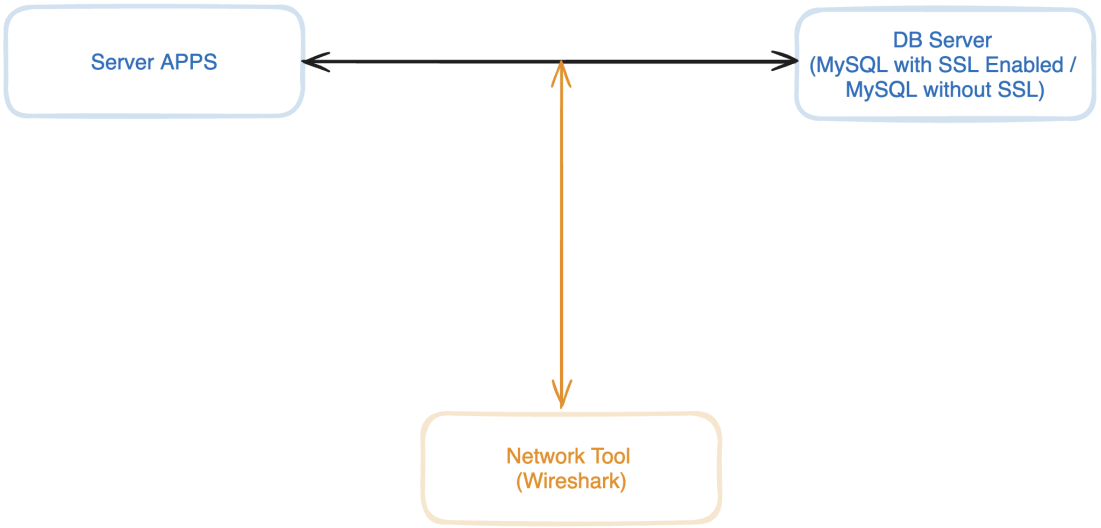
Dalam penelitian ini, konfigurasi sistem dilakukan pada lingkungan yang berbeda untuk membandingkan penggunaan SSL. Pertama, server aplikasi dihubungkan ke server basis data MySQL dengan SSL diaktifkan (ditunjukkan oleh jalur 1 dalam diagram) untuk menilai transmisi data yang terenkripsi. Kedua, server aplikasi yang sama dihubungkan ke server basis data MySQL kedua, kali ini tanpa SSL diaktifkan (ditunjukkan oleh jalur 2 dalam diagram), untuk memungkinkan pengamatan data yang tidak terenkripsi. Proses ini menjamin bahwa analisis komparatif dapat dilakukan antara keamanan transmisi data yang dilindungi SSL dan yang tidak.



Gambar 1. Konfigurasi Sistem

2.2. Pengumpulan Data

Data dikumpulkan dengan menjalankan serangkaian kueri SQL yang identik di server MySQL dalam kedua mode operasi tersebut. Wireshark diatur untuk memonitor lalu lintas jaringan yang relevan dan menangkap paket data yang ditransmisikan selama proses kueri.



Gambar 2. Pengujian dan Pengumpulan Data

2.3. Analisis Data

Analisis dilakukan pada paket data yang ditangkap untuk mengidentifikasi apakah isi dari paket tersebut terenkripsi atau tidak. Indikator utama yang digunakan dalam analisis ini adalah kemampuan untuk membaca teks dalam paket data. Dalam mode SSL, paket-paket diharapkan

tidak dapat dibaca, sementara dalam mode non-SSL, paket-paket tersebut harus terlihat sebagai teks biasa.

2.4. Variabel Penelitian

Fokus utama penelitian ini terletak pada identifikasi keberadaan enkripsi dalam paket data yang ditransmisikan. Variabel penelitian yang diteliti adalah karakteristik enkripsi paket data saat SSL diaktifkan dibandingkan saat tidak diaktifkan. Hal ini dievaluasi dengan menganalisis kemampuan untuk mendeteksi teks yang terbaca dalam paket data yang ditangkap oleh Wireshark. Dengan demikian, penelitian ini mengukur efektivitas SSL dalam mengamankan isi data selama transmisi tanpa mempertimbangkan faktor-faktor performa seperti waktu respons atau beban jaringan.

2.5. Etika Penelitian

Penelitian ini dilakukan dengan mematuhi etika penelitian yang ketat, termasuk menjamin bahwa semua data sensitif yang digunakan dalam pengujian telah dianonimkan dan tidak ada informasi pribadi yang terungkap.

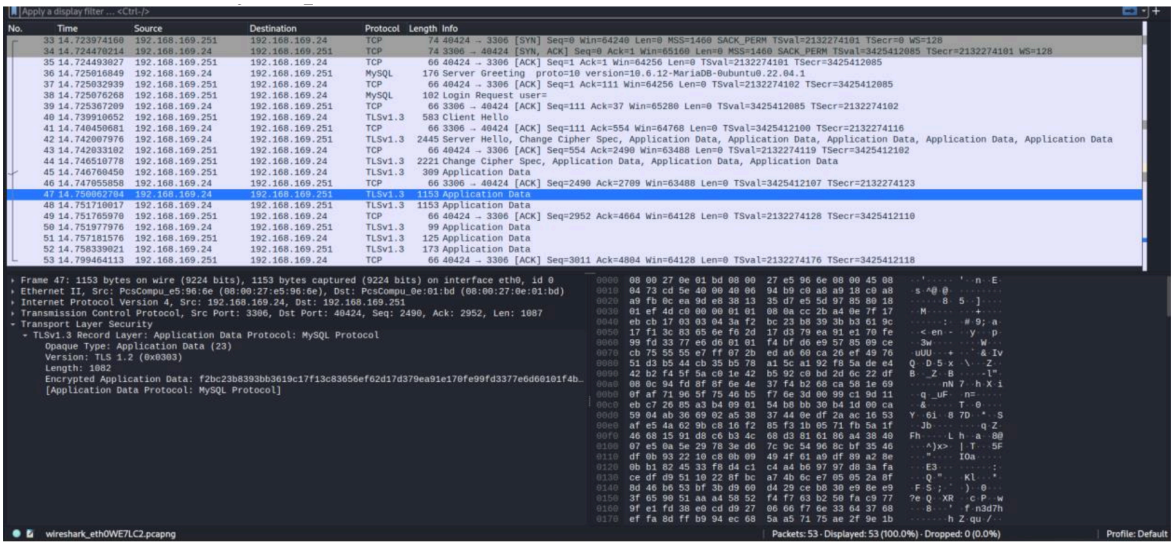
3. HASIL DAN PEMBAHASAN

3.1. Hasil Pengujian

Dalam pelaksanaan pengujian ini, Wireshark digunakan untuk menangkap dan merekam lalu lintas data transmisi antara server aplikasi dan server basis data MySQL. Pengujian menghasilkan dua kelompok data yang berbeda.

3.1.1. Data dengan SSL aktif

Kelompok pertama diperoleh saat SSL diaktifkan pada server MySQL, di mana Wireshark berhasil merekam paket-paket data yang menunjukkan karakteristik enkripsi yang kuat. Dalam kelompok data ini, isi paket tampak sebagai rangkaian karakter acak, yang mengindikasikan bahwa teks asli dari transmisi telah dienkripsi secara efektif, sehingga menjadikannya tidak dapat dibaca atau diinterpretasikan tanpa kunci dekripsi yang tepat.

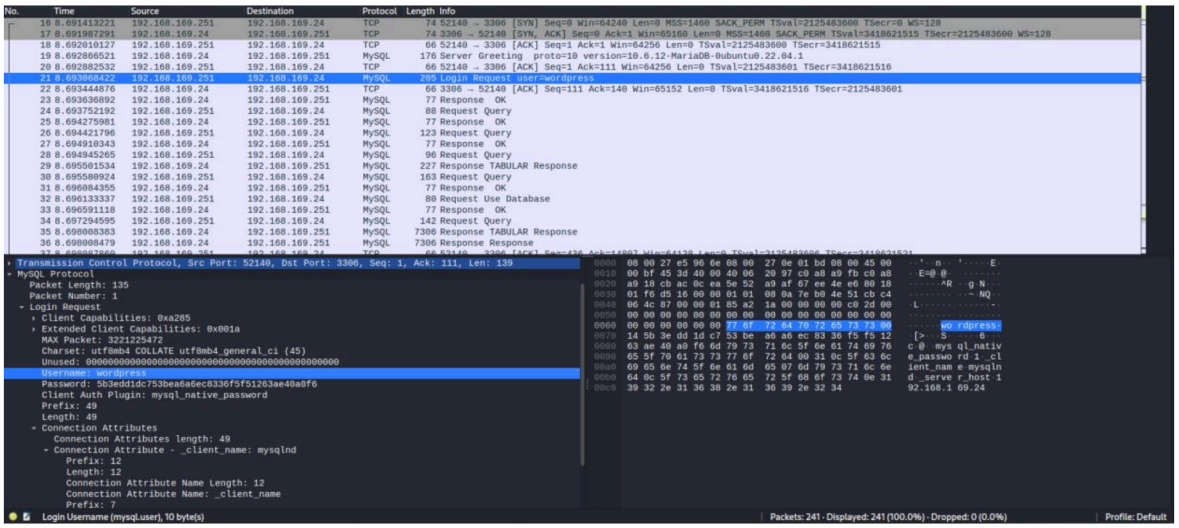


Gambar 3. Data dengan SSL aktif

3.1.2. Data tanpa SSL

Sebaliknya, kelompok kedua diperoleh dari kondisi di mana SSL tidak diaktifkan. Dalam kondisi ini, paket data yang ditangkap oleh Wireshark menunjukkan konten yang sangat berbeda. Data yang ditransmisikan tampak jelas dan dapat dibaca sebagai teks biasa, termasuk detail kueri SQL dan data yang dikembalikan oleh server basis data. Kelompok data ini memberikan bukti langsung

bahwa tanpa enkripsi SSL, informasi yang ditransmisikan rentan terhadap ancaman keamanan seperti penyadapan dan pengaksesan oleh pihak tidak berwenang.



Gambar 3. Data tanpa SSL

3.2. Pembahasan

3.2.1. Keamanan Data In-Transit

Hasil ini menunjukkan bahwa implementasi SSL pada server MySQL memberikan lapisan keamanan yang kuat melalui enkripsi data in-transit. Ini konsisten dengan prinsip-prinsip keamanan siber yang menganjurkan enkripsi sebagai sarana untuk melindungi integritas dan kerahasiaan data.

3.2.2. Implikasi Keamanan

Dalam konteks ancaman siber saat ini, penggunaan SSL harus dianggap sebagai persyaratan standar, bukan hanya pilihan, untuk semua transmisi data sensitif. Temuan ini menegaskan pandangan ini, memperlihatkan kerentanan yang jelas ketika SSL tidak digunakan.

3.2.3. Rekomendasi

Berdasarkan hasil ini, sangat disarankan bagi organisasi yang menggunakan MySQL untuk transmisi data mereka untuk mengimplementasikan SSL. Hal ini tidak hanya memenuhi kepatuhan regulasi tetapi juga menawarkan ketenangan pikiran bahwa data tidak akan mudah dikompromikan selama transmisi.

3.2.4. Keterbatasan dan Arah Penelitian Selanjutnya

Walaupun studi ini memberikan bukti yang jelas mengenai keefektifan SSL, penelitian lebih lanjut dapat dilakukan untuk mengukur dampak dari penggunaan SSL terhadap performa sistem secara keseluruhan. Selain itu, penelitian dapat diperluas untuk mencakup berbagai RDBMS lain dan teknologi enkripsi terkini.

4. KESIMPULAN

Penelitian ini dilakukan dengan tujuan untuk memahami dampak implementasi Secure Sockets Layer (SSL) terhadap keamanan data in-transit pada MySQL. Berdasarkan hasil yang telah dijelaskan pada bab "Hasil dan Pembahasan", dapat disimpulkan bahwa tujuan ini telah tercapai. Penelitian ini berhasil menunjukkan dengan jelas perbedaan keamanan data antara transmisi data yang dienkripsi dengan SSL dan yang tidak. Fitur SSL diaktifkan, data yang ditransmisikan melalui MySQL tidak dapat diinterpretasikan atau diakses oleh Wireshark, menandakan bahwa isi data terlindungi secara efektif selama proses transmisi. Ini memberikan validasi empiris terhadap keamanan yang ditawarkan oleh SSL, yang sesuai dengan prinsip-prinsip keamanan informasi yang dianjurkan dalam literatur keamanan siber. Di sisi lain, ketika SSL tidak digunakan, data yang ditransmisikan terbuka dan dapat diakses sebagai teks biasa, yang memperlihatkan kerentanan terhadap intersepsi. Kesimpulan ini menegaskan bahwa enkripsi SSL tidak hanya

penting tetapi juga harus menjadi standar dalam praktek keamanan untuk transmisi data sensitif. Mengingat pentingnya data yang aman dan regulasi yang berkaitan dengan privasi data, penelitian ini menyarankan dengan kuat implementasi SSL sebagai langkah wajib dalam konfigurasi server MySQL. Selanjutnya, penelitian ini juga membuka jalan bagi eksplorasi lebih lanjut dalam aspek keamanan data. Prospek pengembangan penelitian ini dapat meliputi penilaian terhadap overhead performa yang mungkin ditimbulkan oleh SSL, perbandingan dengan protokol enkripsi lainnya, serta adaptasi keamanan pada RDBMS lain di luar MySQL. Diharapkan, temuan dari penelitian ini dapat menjadi bahan pertimbangan dan inspirasi bagi peneliti selanjutnya untuk mengembangkan metode keamanan data yang lebih efektif dan efisien, serta mendorong pengembangan praktek keamanan siber yang lebih kuat dan resilien.

DAFTAR PUSTAKA

[1] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Security&privacy issues and challenges in NoSQL databases," *Computer Networks*, vol. 206, p. 108828, Apr. 2022, doi: 10.1016/j.comnet.2022.108828.

[2] M. dos S. Fantonelli *et al.*, "Organization and management of sensitive personal health data in electronic systems in countries with implemented data protection laws, lessons to Brazil: A brief systematic review," *Computer Law & Security Review*, vol. 51, p. 105872, Nov. 2023, doi: 10.1016/j.clsr.2023.105872.

[3] M. Mollaeefar and S. Ranise, "Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR," *Computers & Security*, vol. 129, p. 103206, Jun. 2023, doi: 10.1016/j.cose.2023.103206.

[4] M. L. Das and N. Samdaria, "On the security of SSL/TLS-enabled applications," *Applied Computing and Informatics*, vol. 10, no. 1, pp. 68–81, Jan. 2014, doi: 10.1016/j.aci.2014.02.001.

[5] M. Zhan, Y. Li, G. Yu, B. Li, and W. Wang, "Detecting DNS over HTTPS based data exfiltration," *Computer Networks*, vol. 209, p. 108919, May 2022, doi: 10.1016/j.comnet.2022.108919.

[6] F. F. Ashrif, E. A. Sundararajan, R. Ahmad, M. K. Hasan, and E. Yadegaridehkordi, "Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction," *Journal of Network and Computer Applications*, vol. 221, p. 103759, Jan. 2024, doi: 10.1016/j.jnca.2023.103759.

[7] Y. Ma, Y. Ma, Y. Liu, and Q. Cheng, "A secure and efficient certificateless authenticated key agreement protocol for smart healthcare," *Computer Standards & Interfaces*, vol. 86, p. 103735, Aug. 2023, doi: 10.1016/j.csi.2023.103735.

[8] Y. Wang *et al.*, "Identifying vulnerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis," *Journal of Systems and Software*, vol. 167, p. 110609, Sep. 2020, doi: 10.1016/j.jss.2020.110609.

[9] R. Oppliger, R. Hauser, and D. Basin, "SSL/TLS session-aware user authentication revisited," *Computers & Security*, vol. 27, no. 3, pp. 64–70, May 2008, doi: 10.1016/j.cose.2008.04.005.

[10] S. D. Putra, S. Sutikno, Y. Rosmansyah, and I. Asrowardi, "Integrated implementation of service and information security management system," in *2014 International Conference on ICT For Smart Society (ICISS)*, Sep. 2014, pp. 185–191. doi: 10.1109/ICTSS.2014.7013171.

[11] I. Asrowardi, S. D. Putra, E. Subyantoro, and N. H. M. Daud, "IT Service Management System Measurement using ISO20000-1 and ISO15504-8: Developing a Solution-Mediated Process Assessment Tool to Enable Transparent and SMS Process Assessment," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, Art. no. 5, Oct. 2018, doi: 10.11591/ijece.v8i5.pp4023-4032.

[12] R. Das and G. Tuna, "Packet tracing and analysis of network cameras with Wireshark," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, Apr. 2017, pp. 1–6. doi: 10.1109/ISDFS.2017.7916510.

[13] S. Sandhya, S. Purkayastha, E. Joshua, and A. Deep, "Assessment of website security by penetration testing using Wireshark," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Jan. 2017, pp. 1–4. doi: 10.1109/ICACCS.2017.8014711.

[14] S. Wang, D. Xu, and S. Yan, "Analysis and application of Wireshark in TCP/IP protocol teaching," in *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, Apr. 2010, pp. 269–272. doi: 10.1109/EDT.2010.5496372.

[15] O. Amaral, S. Abualhaija, M. Sabetzadeh, and L. Briand, "A Model-based Conceptualization of Requirements for Compliance Checking of Data Processing against GDPR," in *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*, Sep. 2021, pp. 16–20. doi: 10.1109/REW53955.2021.00009.

[16] M. Dutta and S. Dhal, "GDPR-Compliant Data Management Protocol: A Scalable Solution," in *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Jan. 2022, pp. 256–259. doi: 10.1109/COMSNETS53615.2022.9667791.

[17] R. Layton and S. Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices," in *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, Nov. 2019, pp. 1–6. doi: 10.1109/CMI48017.2019.8962288.