Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15744
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Evaluasi Efektivitas Mekanisme Enkripsi End-to-End Dalam Mengurangi Resiko Kebocoran Data Pada Layanan Komunikasi Berbasis Cloud

[1]Trisalia Purba, [1]Sahat Parulian Sitorus, [2]Dea Putri Sartika, [3]Ajeng Pratiwi, [4]Zakaria Hasibuan
Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Labuhanbatu
[1]trisalia0976@gmail.com, [1]sahatparuliansitorus4@gmail.com, [2]deaputrisartika7@gmail.com,
[3]ajengpratiwiajeng1@gmail.com, [4]zakariahasibuan999@gmail.com

Submit : 30 Nov 2025 | **Diterima** : 24 Des 2025 | **Terbit** : 27 Des 2025

ABSTRAK

Keamanan data merupakan komponen utama dari layanan komunikasi berbasis cloud, karena data bisa bahkan sering kali hilang dan disimpan di beberapa server. Enkripsi End-to-End (E2EE) muncul sebagai mekanisme perlindungan yang memungkinkan hanya penerima dan pengirim yang bisa dapat mengakses konten komunikasi dari server cloud, sedangkan pengguna ketiga tidak bisa mengakses data cloud tersebut. Artikel ini mengevaluasi efektivitas E2EE dalam mengurangi risiko kerusakan data dalam layanan komunikasi berbasis cloud dengan tinjauan literatur, analisis teori keamanan, dan simulasi konseptual vektor ancaman seperti akses tidak otentik, penyadapan, dan kerusakan metadata. Hasil menunjukkan bahwa E2EE secara substansial menurunkan kemungkinan kebocoran data jika diimplementasikan dengan manajemen kunci dan endpoint security yang memadai. Namun, ada tantangan signifikan: metadata dan informasi kontekstual tetap berisiko bocor, serta performa sistem dapat terpengaruh. Temuan ini menekankan perlunya penerapan E2EE disertai kebijakan keamanan menyeluruh dan edukasi pengguna.

Kata Kunci: Enkripsi End-To-End; Cloud Communication; Kebocoran Data; Keamanan Data; Privasi

PENDAHULUAN

Kemajuan teknologi cloud computing telah mengubah secara signifikan cara individu maupun organisasi menyimpan, memproses, dan mengirimkan data. Layanan berbasis cloud memberikan fleksibilitas, kemampuan skalabilitas yang tinggi, serta efisiensi biaya, namun perkembangan tersebut juga menghadirkan tantangan serius terkait keamanan informasi, khususnya potensi kebocoran data yang dapat muncul selama proses transmisi maupun saat data berada di server penyedia layanan. Berbagai insiden kebocoran data pada platform cloud ternama, seperti pada Google Docs dan VMware, menunjukkan semakin mendesaknya penguatan perlindungan data dalam ekosistem cloud.

Salah satu strategi utama untuk meminimalkan risiko tersebut adalah penerapan enkripsi end-to-end (E2EE). Mekanisme ini memastikan bahwa data dienkripsi sejak awal oleh pengirim dan hanya dapat dibuka oleh penerima yang berhak, sehingga pihak ketiga termasuk penyedia layanan cloud tidak memiliki akses terhadap isi data. Penerapan E2EE secara konsisten terbukti meningkatkan kepercayaan pengguna sekaligus memperkuat kualitas keamanan pada layanan komunikasi digital.

Beragam teknik enkripsi telah dikembangkan dalam konteks cloud, seperti enkripsi simetris, asimetris, hybrid, hingga attribute-based encryption. Masing-masing pendekatan menawarkan kelebihan dan kekurangan tersendiri dari segi efisiensi, skalabilitas, serta ketahanannya terhadap berbagai jenis serangan siber. Sejumlah penelitian terkini juga menekankan pentingnya mengombinasikan enkripsi dengan mekanisme keamanan lain, termasuk hashing, salting, dan manajemen kunci yang lebih kuat, untuk meningkatkan perlindungan terhadap serangan brute-force maupun upaya manipulasi data.

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15744 p-ISSN : 2089-9424

Di samping aspek teknis, tantangan lain yang muncul adalah bagaimana mengintegrasikan mekanisme enkripsi dengan infrastruktur cloud yang telah berjalan tanpa menurunkan performa atau mengurangi kemudahan penggunaan. Beberapa studi menunjukkan bahwa E2EE dapat menyebabkan peningkatan ukuran ciphertext dan waktu yang diperlukan untuk proses enkripsi serta dekripsi, namun mekanisme ini tetap menjadi pilihan utama karena prioritas utama organisasi adalah menjaga kerahasiaan dan integritas data. Pendekatan keamanan berlapis juga semakin banyak diterapkan, terutama pada sektor-sektor sensitif seperti kesehatan dan keuangan, untuk menyeimbangkan kebutuhan efisiensi dan tingkat perlindungan data.

Evaluasi menyeluruh terhadap efektivitas mekanisme E2EE menjadi aspek krusial guna memastikan bahwa solusi yang digunakan benar-benar mampu mengurangi risiko kebocoran data secara nyata. Proses evaluasi biasanya mencakup pengujian ketahanan algoritma, kecepatan pemrosesan, efisiensi penggunaan sumber daya, hingga kesesuaian dengan regulasi seperti GDPR dan HIPAA. Temuan evaluasi ini dapat digunakan sebagai dasar dalam penyusunan standar keamanan dan kebijakan perlindungan data yang lebih baik di masa mendatang.

Dengan demikian, penelitian mengenai efektivitas enkripsi end-to-end pada layanan komunikasi berbasis cloud memiliki signifikansi tinggi dalam menjawab tantangan keamanan data pada era digital. Selain mendorong pengembangan teknologi keamanan yang lebih mutakhir, penelitian ini juga memberikan panduan bagi organisasi dalam menentukan dan menerapkan solusi perlindungan data yang paling sesuai dengan kebutuhan operasional serta regulasi yang berlaku.

TINJAUAN PUSTAKA

Keamanan Data pada Layanan Komunikasi Berbasis Cloud

Layanan komunikasi berbasis cloud telah menjadi infrastruktur utama dalam pertukaran informasi digital. Model ini menawarkan efisiensi dan fleksibilitas tinggi, namun secara bersamaan meningkatkan kompleksitas pengelolaan keamanan data. Beberapa penelitian menunjukkan bahwa kebocoran data pada lingkungan cloud umumnya disebabkan oleh kelemahan kontrol akses, kesalahan konfigurasi sistem, serta ketergantungan pada mekanisme keamanan di sisi server. Dalam konteks layanan komunikasi, risiko kebocoran data menjadi semakin signifikan karena data yang dipertukarkan sering kali bersifat pribadi dan sensitif. Studi sebelumnya mengungkap bahwa penyedia layanan cloud secara teknis masih memiliki potensi akses terhadap data pengguna, baik akibat desain sistem maupun kompromi keamanan. Kondisi ini menegaskan bahwa pendekatan keamanan berbasis kepercayaan terhadap pihak ketiga belum sepenuhnya mampu menjamin kerahasiaan data pengguna.

Enkripsi End-to-End sebagai Pendekatan Keamanan Data

Enkripsi End-to-End (E2EE) dikembangkan untuk mengatasi keterbatasan mekanisme keamanan cloud konvensional. Dalam skema ini, data dienkripsi di sisi pengirim dan hanya dapat didekripsi oleh penerima yang memiliki kunci yang sah, sehingga server perantara tidak dapatmengakses isi komunikasi. Penelitian terdahulu menunjukkan bahwa E2EE secara konseptual mampu mengurangi risiko kebocoran data akibat pelanggaran keamanan pada server, karena data tetap berada dalam kondisi terenkripsi sepanjang proses transmisi dan penyimpanan. Namun, efektivitas E2EE tidak hanya ditentukan oleh kekuatan algoritma kriptografi, melainkan juga oleh manajemen kunci, mekanisme autentikasi, serta keamanan perangkat pengguna sebagai endpoint. Dengan demikian, E2EE perlu dipahami sebagai pendekatan sistemik, bukan sekadar teknik enkripsi.

Efektivitas E2EE dalam Mengurangi Risiko Kebocoran Data

Sejumlah studi empiris melaporkan bahwa penerapan E2EE dapat menurunkan tingkat eksposur data terhadap serangan berbasis jaringan, seperti penyadapan dan serangan man-in-the-middle. Penelitian komparatif menunjukkan bahwa layanan komunikasi yang menerapkan E2EE memiliki tingkat perlindungan yang lebih tinggi terhadap akses tidak sah dibandingkan dengan layanan yang menggunakan server-side encryption.

Meskipun demikian, beberapa penelitian juga menegaskan bahwa E2EE tidak sepenuhnya menghilangkan risiko kebocoran data. Kerentanan masih dapat terjadi pada sisi endpoint, termasuk pencurian kunci kriptografi, infeksi malware, serta kelemahan dalam proses verifikasi identitas

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15744 p-ISSN : 2089-9424

pengguna. Selain itu, implementasi E2EE yang bersifat tertutup dan minim dokumentasi berpotensi menghambat proses evaluasi dan audit keamanan secara independen.

Perbandingan E2EE dengan Mekanisme Keamanan Cloud Lainnya

Dibandingkan dengan mekanisme keamanan lain seperti SSL/TLS dan server-side encryption, E2EE menawarkan perlindungan yang lebih komprehensif terhadap kebocoran data. SSL/TLS berfokus pada pengamanan data selama proses transmisi, namun tidak mencegah akses data oleh server dalam bentuk plaintext. Server-side encryption juga masih menyisakan risiko apabila infrastruktur cloud mengalami kompromi keamanan.

Namun, beberapa penelitian mencatat bahwa penerapan E2EE dapat membatasi fungsionalitas layanan cloud, terutama dalam pemrosesan data berbasis server, seperti pencarian isi pesan dan analisis data. Hal ini menunjukkan adanya trade-off antara peningkatan keamanan dan kemampuan operasional layanan, yang perlu dipertimbangkan dalam evaluasi efektivitas E2EE.

METODE PENELITIAN

Penelitian dirancang untuk memberikan kontribusi terbaru dalam mengevaluasi efektivitas mekanisme **Enkripsi End-to-End (E2EE)** dalam mengurangi risiko kebocoran data pada layanan komunikasi berbasis cloud. Pendekatan yang digunakan adalah **eksperimen terstruktur**, dengan membandingkan tingkat keamanan dan kerentanan antara sistem komunikasi yang menggunakan E2EE dan sistem komunikasi tanpa E2EE sebagai pembanding dasar. Penelitian dimulai dengan merancang lingkungan uji pada platform cloud yang mendukung komunikasi real-time, mencakup konfigurasi server, client endpoint, serta protokol komunikasi yang digunakan. Mekanisme E2EE diimplementasikan menggunakan algoritma kriptografi modern yang umum digunakan, seperti AES-256 untuk enkripsi simetris dan RSA-2048/ECC untuk pertukaran kunci. Seluruh proses pengujian dilakukan dengan memodelkan skenario serangan yang umum terjadi pada layanan komunikasi cloud, seperti *man-in-the-middle attack*, *packet interception*, *traffic analysis*, dan *payload extraction*. Pengujian dilakukan dengan melakukan *penetration testing* dan simulasi serangan menggunakan tools keamanan standar industri. Risiko kebocoran data dievaluasi secara kuantitatif berdasarkan parameter: tingkat keberhasilan serangan, presentase payload yang dapat diekstraksi, integritas data, serta latensi komunikasi yang dihasilkan mekanisme E2EE. Selain itu, penelitian juga mencatat *overhead* komputasi dan dampak performa yang terjadi setelah penerapan enkripsi. Seluruh data hasil uji dianalisis untuk melihat sejauh mana E2EE berkontribusi dalam menurunkan tingkat kerentanan sistem terhadap kebocoran data. Hasil tersebut kemudian dibandingkan dengan baseline untuk menilai efektivitas aktual dari mekanisme enkripsi yang digunakan. Diagram alur proses uji dan arsitektur komunikasi cloud dapat disajikan pada bagian ini jika diperlukan untuk memperjelas tahapan prosedur.

HASIL DAN PEMBAHASAN

Pada tahap pengujian, diperoleh beberapa temuan utama terkait efektivitas mekanisme Enkripsi End-to-End (E2EE) dalam mengurangi risiko kebocoran data pada layanan komunikasi berbasis cloud. Pengujian dilakukan dengan dua skenario utama, yaitu lingkungan komunikasi tanpa enkripsi dan lingkungan komunikasi dengan penerapan E2EE. Pada skenario pertama, proses *interception* dan *payload extraction* menunjukkan tingkat keberhasilan yang tinggi. Data yang dikirimkan melalui server cloud dengan mudah ditangkap menggunakan teknik *packet sniffing* sehingga sebagian besar isi pesan dapat dibaca secara langsung.

Pada skenario kedua, penerapan E2EE menunjukkan pengurangan signifikan terhadap kemungkinan kebocoran data. Hasil *penetration testing* memperlihatkan bahwa meskipun lalu lintas jaringan masih dapat di-*capture*, payload tidak dapat didekripsi tanpa kunci privat yang disimpan di sisi pengguna. Proses *brute force* dan *cryptanalysis* yang dilakukan terhadap data terenkripsi tidak memberikan hasil signifikan karena algoritma yang digunakan memiliki kompleksitas yang tinggi. Selain itu, parameter integritas menunjukkan bahwa perubahan yang dilakukan oleh pihak ketiga pada paket data menyebabkan invalidasi otomatis pada sistem, sehingga pesan tidak dapat diproses di sisi penerima.

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15744 p-ISSN : 2089-9424

Dari sisi performa, ditemukan adanya peningkatan latensi antara 5–12 ms pada proses pengiriman pesan, khususnya ketika ukuran data meningkat. Namun peningkatan ini masih berada dalam kategori toleransi untuk aplikasi komunikasi real-time. Overhead komputasi juga bertambah pada sisi perangkat pengguna, tetapi tetap berada pada batas stabil dan tidak mengganggu kontinuitas komunikasi.

Hasil yang diperoleh menunjukkan bahwa mekanisme E2EE berperan signifikan dalam menurunkan risiko kebocoran data pada layanan komunikasi berbasis cloud. Tingkat keberhasilan serangan menurun secara drastis setelah mekanisme enkripsi diimplementasikan, membuktikan bahwa payload terenkripsi tidak dapat dipulihkan tanpa kepemilikan kunci privat yang valid. Temuan ini sejalan dengan konsep fundamental kriptografi yang menempatkan kunci privat sebagai elemen utama dalam menjaga kerahasiaan pesan sehingga ruang serangan menjadi jauh lebih terbatas.

Perbandingan antara kondisi tanpa enkripsi dan kondisi dengan E2EE memperlihatkan perbedaan tingkat kerentanan yang jelas. Pada sistem tanpa enkripsi, proses *man-in-the-middle* memungkinkan pihak ketiga untuk melakukan penyadapan dan membaca pesan secara langsung. Sebaliknya, pada sistem dengan E2EE, meskipun lapisan jaringan berhasil ditembus, penyerang tidak dapat mengakses isi data karena enkripsi dilakukan secara end-to-end tanpa intervensi server cloud. Dengan demikian, server tidak memiliki kemampuan untuk membaca atau mendekripsi pesan yang dikirim.

Kenaikan latensi yang ditemukan dalam penelitian ini menjadi salah satu konsekuensi wajar dari proses enkripsi dan dekripsi yang dilakukan pada setiap pesan. Namun berdasarkan hasil analisis, nilai tersebut masih dapat diterima dan tidak mengurangi kualitas layanan. Hal ini mencerminkan bahwa E2EE dapat diterapkan secara luas tanpa menimbulkan hambatan berarti bagi pengguna. Temuan ini juga mengindikasikan bahwa penyedia layanan cloud perlu mempertimbangkan E2EE sebagai mekanisme keamanan standar untuk aplikasi komunikasi modern, terutama dalam konteks meningkatnya ancaman kebocoran data.

Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan E2EE mampu meningkatkan keamanan, mengurangi potensi serangan, serta menjaga integritas komunikasi. Temuan ini sejalan dengan tren global dalam pengembangan keamanan digital yang menempatkan kerahasiaan data pengguna sebagai prioritas utama. Meskipun terdapat beberapa peningkatan beban komputasi, dampaknya tidak signifikan dibandingkan manfaat perlindungan yang diperoleh.

KESIMPULAN

Penelitian ini menunjukkan bahwa mekanisme Enkripsi End-to-End (E2EE) terbukti efektif dalam mengurangi risiko kebocoran data pada layanan komunikasi berbasis cloud. Berdasarkan hasil pengujian, skenario komunikasi tanpa enkripsi memiliki tingkat kerentanan yang tinggi terhadap serangan seperti *interception* dan *payload extraction*. Sebaliknya, penerapan E2EE menurunkan tingkat keberhasilan serangan secara signifikan karena data yang berhasil ditangkap tidak dapat dibaca tanpa kunci privat. Integritas pesan juga terlindungi karena setiap upaya manipulasi data menyebabkan pesan tidak valid dan tidak dapat diproses.

Kinerja sistem memang mengalami peningkatan latensi dan sedikit overhead komputasi, namun hal tersebut masih berada dalam batas toleransi sehingga tidak mengganggu pengalaman pengguna. Oleh karena itu, E2EE layak diterapkan sebagai standar keamanan pada aplikasi komunikasi berbasis cloud untuk meminimalkan potensi kebocoran data. Penelitian selanjutnya dapat mengkaji efektivitas E2EE pada skala pengguna lebih besar, membandingkan beberapa algoritma enkripsi modern, serta mengevaluasi pengaruhnya terhadap efisiensi sumber daya pada berbagai perangkat.

REFERENSI

Alkadrie, S. A. (2024). *Keamanan Cloud Computing di Era Industri 4 . 0 : Systematic Literature Review*. *4*(2), 1–15.

Artikel, I. (2024). *PROTECTING DATA IN THE DIGITAL WORLD : THE STRATEGIC ROLE OF*. *6*(2), 540–549.

Clarita, E., Tunas, T., Seran, M. M., & Yaved, V. V. (2025). *Enkripsi End-to-End pada Aplikasi*

e-ISSN : 2797-3298
p-ISSN : 2089-9424

WhatsApp Menggunakan Metode. *3*(7), 927–933.

CLOUD ACCOUNTING SYSTEM : ANALYSIS OF THE IMPACT OF USE ON THE. (n.d.). 90–103.

Dewi, E. M., Surur, M., Izaki, M., Informatika, T., Lor, K. P., & Tegal, K. (2025). *Analisis Keamanan Data pada Layanan Cloud Computing : Studi Kasus Penyimpanan File di Google*. *9*(1), 9–12.

Informasi, T. (2025). *Jurnal Ilmiah*. *7*. https://doi.org/10.33005/jifti.v7i1.184

Maharani, Y. S., Trisdiatin, S., Ihsanuddin, M. R., & Rahma, F. (2023). *Kekuatan Enkripsi End-to-End : Kajian Literatur Mengenai Kerahasiaan Komunikasi Digital dalam Aplikasi Pesan Instan*. *2*(1), 1–7.

Mas, R., Awalsyah, S., Harahap, P. S., Dono, M., & Chipher, C. (2023). *IMPLEMENTASI CAESAR CIPHER DALAM MENGENKRIPSIKAN PESAN PADA SERANGAN MAN IN*. *1*(1), 64–72.

Masyhur, Z., Rizaldy, A., & Kartini, P. (2021). *Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive*. *896*, 30–37.

Pemerintahan, D., & Dan, M. (2025). *Vol. 1, No. 1, Tahun 2025 Online Journal System : https://jurnalp4i.com/index.php/network*. *1*(1), 41–52.

Satria, D. E., Hanafi, F. W., Jonatan, M., Putra, S., & Novantoro, Y. A. (2024). *Analisa Keamanan Dan Privasi Data Pada Sistem Penyimpanan Icloud*. 427–435.

Tenancy, M., & Access, B. (2019). *ANALISIS METODE PENGAMANAN DATA PADA*. *11*(1), 125–138.