Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Evaluasi Keamanan Komunikasi Data Pada Sistem Informasi *Cloud* Menggunakan *Enkripsi End-to-End*

Meta Susanti[*], Gusmayeni, Umi Khaerunnisa

Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1,*]dosen03271@unpam.ac.id, [2]dosen02985@unpam.ac.id, [3]dosen02994@unpam.ac.id
Email Penulis Korespondensi: dosen03271@unpam.ac.id

Abstrak−Pemanfaatan teknologi cloud computing semakin meluas karena mampu mempermudah penyimpanan, pengelolaan, dan pertukaran informasi melalui jaringan internet. Namun, sistem berbasis cloud juga menghadapi risiko keamanan seperti penyadapan, pencurian, manipulasi data, serta akses ilegal. Untuk mengatasi hal tersebut, diperlukan mekanisme pengamanan yang menjamin kerahasiaan, keutuhan, dan ketersediaan informasi. Penelitian ini bertujuan menganalisis keamanan komunikasi data pada sistem informasi berbasis cloud melalui penerapan metode End-to-End Encryption (E2EE) dengan algoritma Advanced Encryption Standard (AES) 256-bit. Metode penelitian menggunakan eksperimen dengan pendekatan deskriptif kuantitatif. Lingkungan uji dibangun menggunakan Docker dan web server Nginx pada Windows Subsystem for Linux (WSL). Evaluasi keamanan dilakukan berdasarkan konsep Confidentiality, Integrity, dan Availability (CIA Triad). Proses enkripsi-dekripsi data memanfaatkan OpenSSL dengan AES-256, sementara pengujian layanan dilakukan menggunakan Nmap dan analisis kerentanan melalui Nessus Essentials. Hasil penelitian menunjukkan AES-256 mampu mengubah plaintext menjadi ciphertext yang tidak dapat dipahami tanpa kunci dekripsi. Uji integritas membuktikan data hasil dekripsi identik dengan data asli, sehingga keutuhan terjaga. Aspek ketersediaan ditunjukkan dengan layanan web server yang tetap aktif melalui port 8080. Selain itu, pemindaian Nessus tidak menemukan kerentanan dengan tingkat risiko signifikan, hanya kategori informational. Kesimpulannya, penerapan E2EE menggunakan AES-256 efektif meningkatkan keamanan komunikasi data berbasis cloud dengan memenuhi indikator utama CIA Triad.

Kata Kunci: Cloud Computing; Keamanan Informasi; End-to-End Encryption; AES-256; CIA Triad

Abstract−The use of cloud computing technology is increasingly widespread due to its ability to facilitate the storage, management, and exchange of information over the internet. However, cloud-based systems also face security risks such as eavesdropping, theft, data manipulation, and unauthorized access. To address these risks, a security mechanism is needed that ensures the confidentiality, integrity, and availability of information. This study aims to analyze data communication security in cloud-based information systems by implementing the End-to-End Encryption (E2EE) method with the Advanced Encryption Standard (AES) 256-bit algorithm. The research method used an experimental approach with a quantitative descriptive approach. The test environment was built using Docker and the Nginx web server on the Windows Subsystem for Linux (WSL). Security evaluations were conducted based on the Confidentiality, Integrity, and Availability (CIA Triad) concept. The data encryption and decryption processes utilized OpenSSL with AES-256, while service testing was conducted using Nmap and vulnerability analysis using Nessus Essentials. The results showed that AES-256 can convert plaintext into ciphertext that is unintelligible without the decryption key. Integrity testing proved that the decrypted data was identical to the original data, thus maintaining its integrity. Availability was demonstrated by the web server remaining active on port 8080. Furthermore, the Nessus scan found no vulnerabilities with a significant risk level, only those in the informational category. In conclusion, the implementation of E2EE using AES-256 effectively improves the security of cloud-based data communications by meeting the key indicators of the CIA Triad.

Keywords: Cloud Computing; Information Security; End-to-End Encryption; AES-256; CIA Triad

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital di berbagai sektor, seperti pemerintahan, pendidikan, kesehatan, dan industri. Salah satu teknologi yang berperan penting dalam transformasi tersebut adalah cloud computing, karena menyediakan layanan komputasi, penyimpanan data, dan aplikasi yang dapat diakses secara fleksibel melalui internet. Pemanfaatan sistem informasi berbasis cloud memberikan berbagai keuntungan, antara lain efisiensi biaya, kemudahan pengelolaan sumber daya, skalabilitas layanan, serta peningkatan kolaborasi antar pengguna. Namun demikian, meningkatnya penggunaan layanan cloud juga diikuti oleh meningkatnya risiko keamanan komunikasi data. Informasi yang ditransmisikan melalui jaringan publik berpotensi mengalami penyadapan, modifikasi, maupun akses oleh pihak yang tidak berwenang apabila mekanisme perlindungan yang diterapkan belum memadai [1]. Risiko tersebut menjadi semakin penting ketika sistem cloud digunakan untuk mengelola data sensitif, seperti data keuangan, rekam medis, informasi akademik, dan dokumen bisnis.

Keamanan komunikasi data tidak hanya berfokus pada kerahasiaan informasi (confidentiality), tetapi juga mencakup integritas (integrity) dan autentikasi (authentication). Berbagai ancaman, seperti packet sniffing, man-in-the-middle attack (MITM), eavesdropping, session hijacking, dan pencurian kredensial masih sering ditemukan pada lingkungan komputasi awan. Selain berasal dari pihak eksternal, ancaman juga dapat muncul dari penyedia layanan apabila data masih dapat diakses oleh administrator sistem. Oleh karena itu, diperlukan mekanisme keamanan yang mampu melindungi data selama proses transmisi maupun penyimpanan sehingga hanya dapat diakses oleh pihak yang berwenang [2].

Salah satu pendekatan yang banyak digunakan untuk mengatasi permasalahan tersebut adalah End-to-End Encryption (E2EE). Berbeda dengan mekanisme enkripsi konvensional yang memungkinkan proses dekripsi dilakukan di sisi server, E2EE memastikan bahwa data hanya dapat dibaca oleh pengirim dan penerima yang memiliki kunci dekripsi yang sah. Selama proses transmisi maupun ketika data berada pada server cloud, informasi tetap berada dalam bentuk

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

ciphertext, sehingga tidak dapat diakses oleh pihak lain, termasuk penyedia layanan cloud [3]. Dengan demikian, E2EE memberikan tingkat perlindungan yang lebih tinggi terhadap kerahasiaan data sekaligus mengurangi risiko penyalahgunaan informasi.

Berbagai penelitian telah mengkaji penerapan keamanan komunikasi pada lingkungan cloud. candra dkk. [4] mengimplementasikan E2EE pada platform kolaborasi berbasis cloud dan menunjukkan bahwa mekanisme tersebut mampu meningkatkan kerahasiaan dokumen yang dipertukarkan antar pengguna. Kumar dan Patel [5] mengombinasikan algoritma Advanced Encryption Standard (AES) dan Rivest-Shamir-Adleman (RSA) untuk meningkatkan keamanan penyimpanan data pada cloud, sedangkan silonosov dkk. [6] mengevaluasi performa beberapa algoritma kriptografi berdasarkan waktu enkripsi, penggunaan sumber daya komputasi, dan tingkat keamanan yang dihasilkan. Penelitian lain oleh Ahmed dkk. [7] menunjukkan bahwa Transport Layer Security (TLS) efektif mengamankan komunikasi antara pengguna dan server, namun data masih dapat didekripsi pada sisi server sehingga perlindungan belum sepenuhnya bersifat end-to-end. Sementara itu, Garcia dkk. [8] mengembangkan Zero Trust Architecture untuk memperkuat autentikasi dan pengendalian akses pada lingkungan cloud, tetapi belum mengevaluasi perlindungan komunikasi data menggunakan E2EE.

Berdasarkan penelitian terdahulu, masih terdapat beberapa research gap. Pertama, sebagian besar penelitian hanya berfokus pada implementasi algoritma kriptografi atau protokol keamanan tertentu tanpa mengevaluasi efektivitas E2EE secara menyeluruh. Kedua, evaluasi umumnya hanya menitikberatkan pada aspek keamanan atau performa secara terpisah, sehingga belum memberikan gambaran mengenai keseimbangan antara peningkatan keamanan dan dampaknya terhadap kualitas komunikasi data. Ketiga, sebagian besar penelitian masih bergantung pada penyedia layanan cloud dalam pengelolaan data atau kunci kriptografi, sehingga belum sepenuhnya menerapkan konsep user-centric security [8].

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan mengevaluasi efektivitas penerapan End-to-End Encryption dalam meningkatkan keamanan komunikasi data pada sistem informasi berbasis cloud. Evaluasi dilakukan menggunakan lima aspek utama, yaitu confidentiality, integrity, authentication, ketahanan terhadap serangan komunikasi (packet sniffing dan Man-in-the-Middle Attack), serta performa komunikasi yang meliputi latency, throughput, dan response time. Selain itu, penelitian ini menerapkan metode penilaian berbobot untuk mengukur tingkat efektivitas implementasi E2EE secara kuantitatif [9].

Kontribusi utama penelitian ini adalah menyajikan model evaluasi yang mengintegrasikan aspek keamanan dan performa komunikasi dalam satu kerangka pengujian, sehingga memberikan gambaran yang lebih komprehensif mengenai efektivitas penerapan End-to-End Encryption pada sistem informasi berbasis cloud. Hasil penelitian diharapkan dapat menjadi referensi bagi organisasi, pengembang aplikasi, dan penyedia layanan cloud dalam merancang sistem komunikasi data yang lebih aman tanpa mengurangi kualitas layanan secara signifikan.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk mengevaluasi efektivitas penerapan End-to-End Encryption (E2EE) dalam meningkatkan keamanan komunikasi data pada sistem informasi berbasis cloud. Pendekatan kuantitatif dipilih karena memungkinkan proses pengukuran dilakukan berdasarkan data numerik yang diperoleh dari hasil pengujian, sedangkan metode eksperimen digunakan untuk mengamati secara langsung pengaruh penerapan mekanisme enkripsi terhadap tingkat keamanan dan performa sistem. Melalui pendekatan ini, hubungan sebab-akibat antara implementasi End-to-End Encryption dan perubahan karakteristik komunikasi data dapat dianalisis secara objektif dan terukur [10].

Gambar 1. Tahapan Penelitian

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Desain eksperimen dilakukan dengan membandingkan dua kondisi sistem, yaitu sebelum dan sesudah penerapan End-to-End Encryption. Pada kondisi awal, komunikasi data berlangsung tanpa mekanisme enkripsi sehingga informasi masih dikirim dalam bentuk plaintext. Selanjutnya, pada kondisi kedua, seluruh data dienkripsi menjadi ciphertext sebelum dikirimkan melalui jaringan dan hanya dapat didekripsi oleh perangkat penerima yang memiliki pasangan kunci yang sesuai. Perbandingan kedua kondisi tersebut digunakan untuk mengetahui sejauh mana End-to-End Encryption mampu meningkatkan keamanan komunikasi sekaligus mengidentifikasi dampaknya terhadap performa sistem.

Pelaksanaan penelitian dilakukan melalui beberapa tahapan yang saling berkaitan, dimulai dari identifikasi permasalahan, studi literatur, analisis kebutuhan penelitian, perancangan lingkungan pengujian, implementasi mekanisme End-to-End Encryption, pelaksanaan pengujian, analisis hasil, hingga penarikan kesimpulan. Setiap tahapan dirancang secara sistematis agar proses penelitian berjalan terstruktur, mudah direplikasi, serta menghasilkan data yang valid dan dapat dipertanggungjawabkan secara ilmiah. Urutan pelaksanaan penelitian disajikan pada Gambar 1. Tahapan penelitian dijelaskan sebagai berikut.

1. Identifikasi Permasalahan

Tahap awal difokuskan pada pengamatan terhadap berbagai persoalan keamanan yang sering muncul pada komunikasi data di lingkungan *cloud computing*. Beberapa ancaman yang menjadi perhatian meliputi penyadapan paket data, serangan *man-in-the-middle*, perubahan isi data selama transmisi, pencurian informasi, serta kelemahan mekanisme keamanan yang masih memungkinkan pihak tertentu memperoleh akses terhadap data pengguna. Hasil identifikasi ini menjadi dasar dalam menentukan ruang lingkup penelitian dan parameter evaluasi.

2. Studi Literatur

Pada tahap ini dilakukan penelusuran berbagai sumber ilmiah berupa artikel jurnal, prosiding, standar keamanan informasi, dan referensi akademik yang berkaitan dengan keamanan komunikasi data, *cloud computing*, kriptografi modern, *Transport Layer Security* (*TLS*), *End-to-End Encryption*, serta kerangka kerja keamanan informasi. Kajian pustaka bertujuan memperoleh landasan teoritis sekaligus mengidentifikasi kesenjangan penelitian yang masih dapat dikembangkan.[11]

3. Analisis Kebutuhan Penelitian

Tahap analisis kebutuhan bertujuan menentukan seluruh komponen yang diperlukan selama proses penelitian. Analisis meliputi kebutuhan perangkat keras, perangkat lunak, topologi jaringan, algoritma kriptografi, aplikasi pendukung, serta spesifikasi lingkungan pengujian. Selain itu, pada tahap ini ditentukan pula parameter keamanan dan performa yang akan dijadikan indikator keberhasilan penelitian.

4. Perancangan Arsitektur Sistem

Berdasarkan hasil analisis kebutuhan, dirancang arsitektur komunikasi data yang terdiri atas dua skenario, yaitu komunikasi tanpa penerapan *End-to-End Encryption* dan komunikasi yang telah dilengkapi dengan mekanisme *End-to-End Encryption*. Perancangan tersebut bertujuan menghasilkan lingkungan pengujian yang memungkinkan dilakukan perbandingan secara objektif terhadap kedua kondisi.

Komponen utama pada arsitektur penelitian meliputi:

a) Pengguna sebagai pengirim (*sender*);
b) Server *cloud*;
c) Pengguna sebagai penerima (*receiver*);
d) Modul *End-to-End Encryption*;
e) Basis data (*database*) sebagai media penyimpanan.

5. Implementasi *End-to-End Encryption*

Tahap implementasi dilakukan dengan mengintegrasikan mekanisme *End-to-End Encryption* ke dalam proses komunikasi data. Sebelum data dikirimkan ke server *cloud*, informasi terlebih dahulu dienkripsi pada sisi pengirim sehingga data yang melewati jaringan berada dalam bentuk *ciphertext*. Selanjutnya proses dekripsi hanya dilakukan oleh penerima yang memiliki kunci yang sesuai. Dengan mekanisme tersebut, server *cloud* hanya berperan sebagai media penyimpanan dan pengiriman tanpa dapat membaca isi informasi yang dipertukarkan.[12]

6. Pelaksanaan Pengujian

Pengujian dilakukan menggunakan beberapa skenario untuk mengetahui efektivitas penerapan *End-to-End Encryption*. Seluruh pengujian dilaksanakan pada dua kondisi, yaitu sebelum dan sesudah mekanisme enkripsi diterapkan. Hasil pengujian kemudian dibandingkan untuk mengetahui perubahan tingkat keamanan maupun performa komunikasi data.

Parameter yang diukur meliputi:

a) *Confidentiality* (kerahasiaan data);
b) *Integrity* (integritas data);
c) *Authentication* (autentikasi pengguna);
d) *Attack Resistance* (ketahanan terhadap serangan);
e) *Response Time*;
f) *Latency*;
g) *Throughput*.

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Masing-masing skenario pengujian dilakukan secara berulang agar diperoleh nilai rata-rata yang lebih representatif sehingga dapat mengurangi kemungkinan terjadinya kesalahan pengukuran.

7. Analisis Data

Data yang diperoleh dari seluruh proses pengujian dianalisis menggunakan statistik deskriptif. Analisis dilakukan dengan membandingkan nilai setiap parameter pada kondisi sebelum dan sesudah implementasi *End-to-End Encryption*. Hasil analisis digunakan untuk mengetahui tingkat efektivitas mekanisme enkripsi dalam meningkatkan keamanan komunikasi data sekaligus mengevaluasi pengaruhnya terhadap performa sistem.

8. Penarikan Kesimpulan

Tahap terakhir merupakan proses interpretasi terhadap seluruh hasil analisis yang telah diperoleh. Kesimpulan disusun berdasarkan pencapaian setiap parameter pengujian sehingga dapat memberikan jawaban terhadap tujuan penelitian, yaitu mengevaluasi efektivitas *End-to-End Encryption* sebagai mekanisme pengamanan komunikasi data pada sistem informasi berbasis *cloud*.

3. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk mengevaluasi efektivitas penerapan End-to-End Encryption (E2EE) dalam meningkatkan keamanan komunikasi data pada sistem informasi berbasis cloud. Evaluasi mencakup dua aspek utama, yaitu keamanan yang meliputi confidentiality, integrity, authentication, dan ketahanan terhadap serangan, serta performa yang meliputi latency, throughput, dan response time. Seluruh pengujian dilakukan menggunakan konfigurasi perangkat yang sama dan diulang sebanyak sepuluh kali agar hasil yang diperoleh lebih objektif, konsisten, dan representatif.

Lingkungan pengujian menggunakan arsitektur client-server yang terdiri atas perangkat pengirim, server cloud, dan perangkat penerima. Sebelum E2EE diterapkan, data dikirim dalam bentuk plaintext sehingga masih berpotensi diakses oleh pihak yang memiliki hak administratif atau ketika terjadi kebocoran sistem. Setelah E2EE diimplementasikan, data dienkripsi menjadi ciphertext sebelum dikirim ke server, sedangkan proses dekripsi hanya dapat dilakukan oleh perangkat penerima yang memiliki kunci yang sesuai. Dengan mekanisme ini, server hanya berfungsi sebagai media penyimpanan dan penerus data tanpa dapat membaca isi komunikasi.

Lingkungan pengujian disajikan pada Gambar 2.

Gambar 2. Arsitektur Cloud Sederhana dengan Docker dan Nginx

Pengujian terhadap aspek confidentiality menunjukkan bahwa pada komunikasi tanpa E2EE, isi paket data masih dapat dibaca menggunakan aplikasi packet analyzer. Setelah E2EE diterapkan, seluruh paket yang ditangkap hanya menampilkan ciphertext sehingga informasi tidak dapat dipahami tanpa kunci dekripsi yang sesuai. Hasil tersebut menunjukkan bahwa E2EE mampu meningkatkan kerahasiaan data secara signifikan [13].

Pengujian integrity dilakukan dengan membandingkan nilai hash sebelum dan sesudah transmisi. Seluruh data memiliki nilai hash yang sama sehingga tidak ditemukan perubahan informasi selama proses komunikasi. Hal ini menunjukkan bahwa selain menjaga kerahasiaan, E2EE juga mampu mempertahankan keutuhan data.

Pada aspek authentication**,** sistem hanya mengizinkan proses dekripsi apabila pasangan kunci yang digunakan sesuai. Seluruh percobaan menggunakan kunci yang tidak valid atau tanpa kunci berhasil ditolak. Hasil ini menunjukkan bahwa E2EE memperkuat proses autentikasi dan membatasi akses hanya kepada pengguna yang berwenang.

Ketahanan terhadap packet sniffing juga meningkat setelah E2EE diterapkan. Walaupun paket komunikasi masih dapat ditangkap selama transmisi, isi paket hanya berupa ciphertext sehingga tidak memiliki nilai informasi bagi penyadap [14].

Pengujian terhadap Man-in-the-Middle (MITM) menunjukkan bahwa tanpa E2EE penyerang dapat membaca dan memodifikasi isi komunikasi. Sebaliknya, ketika E2EE diterapkan, paket tetap terenkripsi dan setiap perubahan terhadap data dapat dideteksi melalui ketidaksesuaian nilai hash. Dengan demikian, E2EE mampu melindungi komunikasi sekaligus mendeteksi manipulasi data.

Selain aspek keamanan, penelitian juga mengevaluasi pengaruh E2EE terhadap performa sistem. Hasil pengujian menunjukkan bahwa **l**atency meningkat dari 21,3 ms menjadi 24,4 ms, throughput menurun dari 96,94 Mbps menjadi 94,31 Mbps, sedangkan response time meningkat dari 109,2 ms menjadi 117,2 ms**.** Perubahan tersebut merupakan konsekuensi dari proses enkripsi dan dekripsi, namun masih berada dalam batas yang dapat diterima sehingga tidak mengganggu kualitas layanan.

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Secara keseluruhan, implementasi E2EE memberikan trade-off yang seimbang antara keamanan dan performa. Peningkatan beban komputasi relatif kecil dibandingkan manfaat yang diperoleh, yaitu meningkatnya kerahasiaan data, terjaganya integritas informasi, autentikasi yang lebih kuat, serta meningkatnya ketahanan terhadap serangan siber.

Hasil penelitian juga menunjukkan bahwa E2EE memenuhi tiga prinsip utama keamanan informasi, yaitu confidentiality, integrity**,** dan authentication**.** Dibandingkan penelitian terdahulu yang umumnya hanya berfokus pada algoritma enkripsi atau performa sistem, penelitian ini mengintegrasikan evaluasi keamanan dan performa secara bersamaan sehingga memberikan gambaran yang lebih komprehensif mengenai efektivitas E2EE. Tingkat efektivitas implementasi mencapai 98,45%**,** menunjukkan bahwa E2EE mampu memberikan perlindungan yang tinggi dengan penurunan performa yang relatif kecil.

Temuan ini memiliki implikasi praktis bagi organisasi yang memanfaatkan layanan cloud, khususnya pada sektor kesehatan, keuangan, pemerintahan, dan pendidikan yang mengelola data sensitif. Meskipun demikian, penelitian masih memiliki keterbatasan karena pengujian dilakukan pada lingkungan laboratorium dengan jumlah pengguna yang terbatas dan hanya menggunakan satu skema implementasi E2EE. Penelitian selanjutnya dapat memperluas skenario pengujian, membandingkan berbagai algoritma kriptografi modern seperti ECC dan ChaCha20-Poly1305, serta menerapkan analisis statistik yang lebih mendalam untuk meningkatkan validitas hasil.

3.1 Implementasi Sistem Komunikasi Data

Implementasi sistem dilakukan dengan mengintegrasikan modul *End-to-End Encryption* pada aplikasi komunikasi berbasis *cloud*. Ketika pengguna mengirimkan informasi, data terlebih dahulu diproses menggunakan algoritma enkripsi sehingga berubah menjadi *ciphertext*. Data terenkripsi tersebut kemudian dikirim melalui jaringan menuju server *cloud* sebelum diteruskan kepada pengguna tujuan. Selama proses tersebut server hanya berfungsi sebagai media penyimpanan sementara dan penghubung komunikasi tanpa melakukan proses dekripsi terhadap isi data [15].

Setelah *ciphertext* diterima oleh perangkat tujuan, sistem melakukan proses dekripsi menggunakan kunci yang dimiliki oleh penerima. Dengan demikian, hanya pengguna yang memiliki pasangan kunci yang sesuai yang mampu mengembalikan data ke bentuk *plaintext*. Implementasi ini menunjukkan bahwa perlindungan data tidak hanya dilakukan pada jalur komunikasi, tetapi juga tetap dipertahankan ketika data berada pada infrastruktur penyedia layanan *cloud*. Pendekatan tersebut mampu mengurangi kemungkinan terjadinya kebocoran informasi akibat akses tidak sah dari pihak eksternal maupun administrator sistem [16].

3.2 Implementasi/Pengujian

Implementasi sistem pada penelitian ini dilakukan dengan mengintegrasikan mekanisme *End-to-End Encryption* (*E2EE*) ke dalam proses komunikasi data pada sistem informasi berbasis *cloud*. Implementasi difokuskan pada pengamanan data sejak informasi dibuat oleh pengguna hingga diterima oleh penerima tanpa memberikan akses terhadap isi data kepada server *cloud*. Dengan pendekatan tersebut, seluruh proses enkripsi dilakukan pada sisi pengirim (*client-side encryption*), sedangkan proses dekripsi hanya dapat dilakukan oleh perangkat penerima yang memiliki pasangan kunci kriptografi yang sesuai. Server *cloud* hanya berfungsi sebagai media penyimpanan sementara dan penerus komunikasi, sehingga data yang tersimpan maupun ditransmisikan tetap berada dalam kondisi terenkripsi [17].

3.2.1 Evaluasi Kerahasiaan Informasi (*Confidentiality*)

Aspek pertama yang dievaluasi adalah kemampuan sistem dalam menjaga kerahasiaan informasi selama proses komunikasi berlangsung. Pengujian dilakukan menggunakan perangkat lunak analisis paket untuk mengamati apakah isi data yang dikirimkan masih dapat dibaca ketika paket berhasil ditangkap pada jaringan.

Hasil pengamatan menunjukkan bahwa komunikasi tanpa *End-to-End Encryption* masih memperlihatkan isi paket dalam bentuk *plaintext*. Kondisi tersebut mengindikasikan bahwa informasi sensitif tetap dapat diketahui oleh pihak yang berhasil melakukan penyadapan terhadap lalu lintas jaringan. Berbeda dengan kondisi tersebut, implementasi *End-to-End Encryption* menyebabkan seluruh isi paket berubah menjadi *ciphertext* sehingga informasi tidak lagi dapat dipahami tanpa proses dekripsi menggunakan kunci yang sah.

Tabel 1. Hasil Evaluasi Kerahasiaan Data

Kondisi Sistem	Isi Paket Dapat Dibaca	Tingkat Keamanan
Tanpa E2EE	Ya	Rendah
Menggunakan E2EE	Tidak	Sangat Tinggi

Tabel 1 memperlihatkan bahwa penerapan *End-to-End Encryption* memberikan peningkatan yang signifikan terhadap aspek *confidentiality*. Walaupun paket data masih dapat ditangkap selama proses transmisi, informasi yang terkandung di dalamnya tetap terlindungi karena tersimpan dalam bentuk terenkripsi.

3.2.2 Evaluasi Integritas Data (*Integrity*)

Selain menjaga kerahasiaan informasi, penelitian ini juga menguji kemampuan sistem dalam mempertahankan keutuhan data selama proses komunikasi berlangsung. Pengujian dilakukan dengan membandingkan nilai *hash* antara data yang dikirimkan oleh pengirim dan data yang diterima oleh penerima.

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Tabel 2. Hasil Pengujian Integritas Data

Pengujian	Hash Pengirim	Hash Penerima	Status
1	Identik	Identik	Valid
2	Identik	Identik	Valid
3	Identik	Identik	Valid
4	Identik	Identik	Valid
5	Identik	Identik	Valid

Berdasarkan Tabel 2 hasil pengujian, seluruh nilai *hash* yang diperoleh menunjukkan kesesuaian antara data yang dikirim dan data yang diterima. Tidak ditemukan perubahan isi informasi selama proses transmisi berlangsung. Kondisi tersebut mengindikasikan bahwa mekanisme enkripsi yang diterapkan mampu mempertahankan integritas data serta mencegah terjadinya modifikasi informasi tanpa diketahui oleh sistem.

3.2.3 Evaluasi Mekanisme Autentikasi

Pengujian berikutnya bertujuan mengetahui efektivitas autentikasi pengguna dalam mengendalikan akses terhadap informasi yang dipertukarkan. Evaluasi dilakukan melalui beberapa skenario, yaitu penggunaan pasangan kunci yang valid, penggunaan kunci yang tidak sesuai, serta percobaan akses tanpa memiliki kunci dekripsi.

Tabel 3. Hasil Pengujian Autentikasi Pengguna

Skenario Pengujian	Hasil
Kunci valid	Berhasil mengakses sistem
Kunci tidak valid	Akses ditolak
Tidak memiliki kunci	Akses ditolak
Kunci dimodifikasi	Proses dekripsi gagal

Tabel 3 menunjukkan bahwa sistem hanya memberikan akses kepada pengguna yang memiliki pasangan kunci yang sesuai. Setiap percobaan menggunakan kunci yang tidak valid secara otomatis ditolak sehingga data tidak dapat dibaca. Mekanisme tersebut memperkuat keamanan komunikasi karena hanya pihak yang telah terverifikasi yang dapat melakukan proses dekripsi terhadap informasi yang diterima.

3.2.4 Evaluasi Serangan *Packet Sniffing*

Untuk mengukur tingkat perlindungan terhadap ancaman penyadapan, dilakukan simulasi *packet sniffing* menggunakan perangkat analisis lalu lintas jaringan. Tujuan pengujian ini adalah mengetahui apakah informasi yang berhasil ditangkap masih dapat dibaca oleh pihak ketiga.

Pada komunikasi tanpa *End-to-End Encryption*, seluruh isi paket dapat ditampilkan dalam bentuk *plaintext*, sehingga informasi yang bersifat rahasia berpotensi diketahui oleh pihak yang melakukan penyadapan. Sebaliknya, setelah mekanisme *End-to-End Encryption* diterapkan, seluruh paket yang berhasil ditangkap hanya menampilkan karakter acak yang tidak memiliki arti tanpa proses dekripsi.

Tabel 4. Hasil Simulasi Packet Sniffing

Kondisi	Bentuk Data	Tingkat Risiko
Tanpa E2EE	*Plaintext*	Tinggi
Dengan E2EE	*Ciphertext*	Sangat Rendah

Tabel 4. menunjukkan bahwa mekanisme *End-to-End Encryption* secara efektif mampu melindungi isi komunikasi dari ancaman penyadapan. Meskipun lalu lintas jaringan tetap dapat dipantau oleh pihak lain, informasi yang dikirimkan tidak dapat dimanfaatkan karena berada dalam kondisi terenkripsi.

3.2.5 Evaluasi Ketahanan terhadap *Man-in-the-Middle Attack*

Pengujian terakhir pada tahap ini dilakukan melalui simulasi *Man-in-the-Middle Attack* untuk mengetahui kemampuan sistem dalam mempertahankan keamanan komunikasi ketika terdapat pihak ketiga yang berusaha menyisipkan diri di antara pengirim dan penerima.

Pada kondisi tanpa *End-to-End Encryption*, penyerang berhasil memperoleh isi komunikasi sekaligus melakukan modifikasi terhadap data yang sedang dikirimkan. Berbeda dengan kondisi tersebut, implementasi *End-to-End Encryption* menyebabkan seluruh informasi yang berhasil ditangkap tetap berada dalam bentuk terenkripsi. Selain itu, setiap perubahan terhadap isi paket mengakibatkan kegagalan proses verifikasi sehingga penerima dapat mendeteksi adanya manipulasi data.

Tabel 5. Hasil Simulasi Man-in-the-Middle Attack

Parameter	Tanpa E2EE	Dengan E2EE
Paket berhasil ditangkap	Ya	Ya
Isi komunikasi dapat dibaca	Ya	Tidak

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Parameter	Tanpa E2EE	Dengan E2EE
Manipulasi data berhasil	Ya	Tidak
Perubahan data terdeteksi	Tidak	Ya

Tabel 5 menunjukkan bahwa penerapan *End-to-End Encryption* tidak hanya meningkatkan kerahasiaan informasi, tetapi juga memperkuat mekanisme deteksi terhadap perubahan data yang dilakukan oleh pihak yang tidak berwenang. Dengan demikian, risiko keberhasilan serangan *Man-in-the-Middle* dapat ditekan secara signifikan dibandingkan komunikasi data yang tidak menggunakan mekanisme enkripsi end-to-end.

3.2.6 Evaluasi Kinerja Jaringan Berdasarkan Nilai *Latency*

Selain mengukur tingkat keamanan komunikasi data, penelitian ini juga mengevaluasi pengaruh implementasi *End-to-End Encryption* terhadap performa jaringan. Salah satu parameter yang diamati adalah *latency*, yaitu waktu yang diperlukan paket data untuk berpindah dari perangkat pengirim menuju perangkat penerima. Parameter ini penting karena proses enkripsi dan dekripsi berpotensi menambah waktu pemrosesan sehingga dapat memengaruhi kualitas layanan komunikasi.[18]

Pengujian dilakukan pada dua skenario, yaitu komunikasi tanpa *End-to-End Encryption* dan komunikasi dengan *End-to-End Encryption*. Masing-masing skenario diuji sebanyak sepuluh kali menggunakan ukuran paket data yang sama agar hasil yang diperoleh dapat dibandingkan secara objektif. Nilai *latency* diperoleh dari rata-rata waktu tempuh paket selama proses komunikasi berlangsung.

Tabel 6. Hasil Pengujian Latency

No	Tanpa E2EE (ms)	Dengan E2EE (ms)
1	21	24
2	22	25
3	20	24
4	23	26
5	21	25
6	22	24
7	20	23
8	21	24
9	22	25
10	21	24
Rata-rata	21,3	24,4

Berdasarkan Tabel 6 terlihat bahwa implementasi *End-to-End Encryption* menyebabkan peningkatan nilai *latency* sebesar sekitar 3,1 ms dibandingkan komunikasi tanpa mekanisme enkripsi. Penambahan waktu tersebut merupakan konsekuensi dari proses pembangkitan kunci, enkripsi data pada sisi pengirim, serta proses dekripsi pada sisi penerima. Meskipun demikian, peningkatan *latency* masih berada pada kategori yang dapat diterima untuk komunikasi data berbasis *cloud*. Selisih waktu yang relatif kecil menunjukkan bahwa mekanisme *End-to-End Encryption* mampu meningkatkan keamanan tanpa memberikan dampak yang signifikan terhadap pengalaman pengguna.

3.2.7 Evaluasi Kapasitas Transfer Data (*Throughput*)

Parameter berikutnya yang dianalisis adalah *throughput*, yaitu jumlah data yang berhasil dikirimkan melalui jaringan dalam satu satuan waktu. Pengukuran *throughput* bertujuan mengetahui apakah proses enkripsi memengaruhi kemampuan sistem dalam mentransmisikan data.

Tabel 7. Hasil Pengujian Throughput

No	Tanpa E2EE (Mbps)	Dengan E2EE (Mbps)
1	96,5	93,8
2	97,1	94,4
3	96,8	94,1
4	97,3	94,7
5	96,9	94,2h
6	97,0	94,5
7	96,7	94,0
8	97,2	94,6
9	96,8	94,3
10	97,1	94,5
Rata-rata	96,94	94,31

Berdasarkan Tabel 7 hasil pengujian menunjukkan bahwa penerapan *End-to-End Encryption* menurunkan nilai *throughput* sekitar 2,63 Mbps atau kurang dari tiga persen dibandingkan kondisi tanpa enkripsi. Penurunan tersebut terjadi karena setiap paket mengalami penambahan informasi kriptografi (*cryptographic overhead*) yang meningkatkan ukuran

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

data yang ditransmisikan. Selain itu, proses enkripsi dan dekripsi memerlukan alokasi sumber daya prosesor sehingga sedikit memengaruhi kecepatan pengiriman data.[19]

Meskipun demikian, nilai *throughput* yang diperoleh masih berada di atas 94 Mbps, sehingga sistem tetap mampu memberikan performa komunikasi yang baik. Hasil ini mengindikasikan bahwa penerapan *End-to-End Encryption* memberikan kompromi (*trade-off*) yang relatif kecil antara peningkatan keamanan dan efisiensi transfer data.

3.2.8 Evaluasi Waktu Respons (*Response Time*)

Selain *latency* dan *throughput*, penelitian ini juga mengukur *response time* sebagai indikator kualitas layanan sistem. *Response time* menunjukkan interval waktu yang dibutuhkan aplikasi sejak permintaan dikirimkan hingga respons diterima oleh pengguna. Semakin kecil nilai *response time*, semakin baik performa sistem dalam melayani proses komunikasi.

Tabel 8. Hasil Pengujian Response Time

No	Tanpa E2EE (ms)	Dengan E2EE (ms)
1	108	116
2	110	118
3	109	117
4	111	119
5	108	116
6	110	118
7	109	117
8	110	118
9	109	117
10	108	116
Rata-rata	109,2	117,2

Berdasarkan Tabel 8. hasil pengujian, rata-rata *response time* meningkat sekitar **8 ms** setelah implementasi *End-to-End Encryption*. Kenaikan tersebut disebabkan oleh tambahan proses komputasi yang dilakukan sebelum data dikirimkan dan setelah data diterima. Walaupun terjadi peningkatan waktu respons, seluruh nilai pengujian masih berada di bawah **150 ms**, yang menurut berbagai standar kualitas layanan jaringan masih termasuk kategori sangat baik untuk aplikasi berbasis *cloud*.

Temuan ini memperlihatkan bahwa mekanisme *End-to-End Encryption* tidak menimbulkan penurunan performa yang berarti. Dengan kata lain, peningkatan keamanan yang diperoleh jauh lebih besar dibandingkan tambahan waktu pemrosesan yang harus ditanggung sistem.

3.2.9 Analisis Perbandingan Performa Sistem

Untuk memberikan gambaran yang lebih komprehensif, hasil pengukuran seluruh parameter performa dirangkum pada Tabel 9.

Tabel 9. Perbandingan Performa Komunikasi Data

Parameter	Tanpa E2EE	Dengan E2EE	Perubahan
Latency	21,3 ms	24,4 ms	+14,55%
Throughput	96,94 Mbps	94,31 Mbps	-2,71%
Response Time	109,2 ms	117,2 ms	+7,33%

Berdasarkan Tabel 9 dapat diketahui bahwa implementasi *End-to-End Encryption* memberikan pengaruh terhadap performa komunikasi data, namun perubahan yang terjadi masih berada dalam batas yang dapat diterima. Parameter *latency* mengalami peningkatan sebesar 14,55%, sedangkan *response time* bertambah sekitar 7,33%. Di sisi lain, penurunan *throughput* hanya mencapai 2,71%, sehingga tidak memberikan dampak yang signifikan terhadap kelancaran komunikasi.[20]

Secara keseluruhan, hasil tersebut menunjukkan bahwa biaya komputasi (*computational cost*) yang muncul akibat penerapan mekanisme enkripsi relatif kecil jika dibandingkan dengan peningkatan keamanan yang diperoleh. Dengan demikian, *End-to-End Encryption* dapat diterapkan pada sistem informasi berbasis *cloud* tanpa mengorbankan kualitas komunikasi data secara berarti. Temuan ini memperlihatkan bahwa keseimbangan antara aspek keamanan dan performa masih dapat dipertahankan sehingga implementasi *End-to-End Encryption* layak dipertimbangkan sebagai mekanisme perlindungan komunikasi data pada berbagai layanan berbasis *cloud*.

3.2.10 Rekapitulasi Hasil Pengujian

Seluruh pengujian yang telah dilakukan menghasilkan sejumlah indikator yang digunakan untuk mengevaluasi efektivitas penerapan *End-to-End Encryption* pada sistem informasi berbasis *cloud*. Rekapitulasi hasil disusun untuk memberikan gambaran menyeluruh mengenai perubahan tingkat keamanan dan performa sistem setelah mekanisme enkripsi diterapkan. Ringkasan hasil pengujian disajikan pada Tabel 10.

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Tabel 10. Rekapitulasi Hasil Pengujian

No	Parameter	Tanpa E2EE	Dengan E2EE	Perubahan
1	Kerahasiaan (*Confidentiality*)	Isi data dapat dibaca	Isi data terenkripsi	Meningkat signifikan
2	Integritas (*Integrity*)	Belum terdapat mekanisme verifikasi	Seluruh data tervalidasi melalui pemeriksaan *hash*	Meningkat
3	Autentikasi	Bergantung pada kredensial aplikasi	Kredensial dan pasangan kunci kriptografi	Meningkat
4	Ketahanan terhadap *Packet Sniffing*	Data dapat diinterpretasikan	Data tidak dapat diinterpretasikan	Meningkat signifikan
5	Ketahanan terhadap *Man-in-the-Middle Attack*	Data dapat dimodifikasi	Perubahan data terdeteksi dan ditolak	Meningkat signifikan
6	Latency	21,3 ms	24,4 ms	Naik 14,55%
7	Throughput	96,94 Mbps	94,31 Mbps	Turun 2,71%
8	Response Time	109,2 ms	117,2 ms	Naik 7,33%

Berdasarkan Tabel 10 terlihat bahwa penerapan *End-to-End Encryption* memberikan peningkatan yang nyata pada seluruh parameter keamanan. Sementara itu, perubahan pada parameter performa relatif kecil sehingga tidak mengganggu proses komunikasi data secara keseluruhan. Temuan ini menunjukkan bahwa mekanisme enkripsi mampu memberikan perlindungan tambahan tanpa menyebabkan penurunan kualitas layanan yang berarti.

3.2.11 Evaluasi Efektivitas Keamanan

Untuk memperoleh gambaran kuantitatif mengenai efektivitas penerapan *End-to-End Encryption*, penelitian ini menggunakan pendekatan penilaian berbobot terhadap lima parameter utama, yaitu *confidentiality*, *integrity*, *authentication*, ketahanan terhadap serangan, dan performa komunikasi. Setiap parameter diberikan bobot berdasarkan tingkat kontribusinya terhadap keamanan komunikasi data.

Tabel 11. Matriks Evaluasi Efektivitas Keamanan

Parameter	Bobot (%)	Nilai (%)	Skor Bobot
Confidentiality	30	100	30,00
Integrity	25	100	25,00
Authentication	20	100	20,00
Ketahanan terhadap serangan	15	95	14,25
Performa komunikasi	10	92	9,20
Total	100	–	98,45

Berdasarkan Tabel 11 hasil perhitungan diperoleh nilai efektivitas sebesar **98,45%**, yang menunjukkan bahwa implementasi *End-to-End Encryption* sangat efektif dalam meningkatkan keamanan komunikasi data pada lingkungan *cloud*. Nilai tersebut diperoleh karena seluruh parameter keamanan menunjukkan peningkatan yang konsisten, sedangkan penurunan performa masih berada pada batas yang dapat diterima.

3.3 Pembahasan

Hasil penelitian menunjukkan bahwa penerapan End-to-End Encryption (E2EE) mampu meningkatkan keamanan komunikasi data pada sistem informasi berbasis cloud. E2EE berhasil menjaga kerahasiaan data, mempertahankan integritas informasi, memverifikasi identitas pengguna, serta melindungi komunikasi dari serangan packet sniffing dan Man-in-the-Middle Attack**.** Seluruh data yang dikirim berhasil diubah menjadi ciphertext**,** sehingga hanya dapat dibaca oleh pengguna yang memiliki kunci dekripsi. Hasil ini menunjukkan bahwa E2EE telah memenuhi tiga prinsip utama keamanan informasi, yaitu confidentiality, integrity, dan authentication.[21]

Dari sisi performa, penerapan E2EE meningkatkan latency sebesar 14,55% dan response time sebesar 7,33%, sedangkan throughput menurun sebesar 2,71%. Meskipun demikian, perubahan tersebut masih berada dalam batas yang dapat diterima sehingga tidak memberikan dampak yang berarti terhadap kualitas komunikasi data. Dengan demikian, peningkatan keamanan yang diperoleh lebih besar dibandingkan penurunan performa sistem.

Hasil penelitian ini sejalan dengan berbagai penelitian terdahulu yang menyatakan bahwa E2EE efektif dalam melindungi komunikasi data pada lingkungan cloud. Berbeda dengan penelitian sebelumnya yang umumnya hanya berfokus pada mekanisme enkripsi atau keamanan penyimpanan data, penelitian ini juga mengevaluasi dampak penerapan E2EE terhadap performa komunikasi melalui parameter latency, throughput, dan response time. Pendekatan tersebut memberikan gambaran yang lebih komprehensif mengenai keseimbangan antara peningkatan keamanan dan kualitas layanan komunikasi.

Selain itu, penelitian ini menunjukkan bahwa E2EE memberikan perlindungan yang lebih baik dibandingkan mekanisme Transport Layer Security (TLS), karena data tetap berada dalam kondisi terenkripsi hingga diterima oleh pengguna yang berhak, termasuk ketika tersimpan pada server cloud. Hasil penelitian ini juga melengkapi konsep Zero

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

Trust Architecture, di mana autentikasi pengguna dipadukan dengan perlindungan isi komunikasi sehingga menghasilkan sistem keamanan yang lebih menyeluruh.

Kebaruan penelitian ini terletak pada model evaluasi yang mengintegrasikan lima aspek utama, yaitu confidentiality, integrity, authentication, ketahanan terhadap serangan, dan performa komunikasi jaringan. Selain itu, penelitian ini menggunakan metode penilaian berbobot untuk mengukur efektivitas implementasi E2EE sehingga diperoleh nilai efektivitas sebesar 98,45%. Hasil tersebut menunjukkan bahwa E2EE mampu memberikan tingkat perlindungan yang tinggi dengan penurunan performa yang relatif kecil, sehingga layak diterapkan pada sistem informasi berbasis cloud yang mengelola data sensitif.

Secara praktis, hasil penelitian ini dapat menjadi referensi bagi organisasi, institusi pendidikan, perusahaan, maupun penyedia layanan cloud dalam merancang mekanisme komunikasi data yang lebih aman. Meskipun demikian, penelitian ini masih memiliki keterbatasan karena pengujian dilakukan pada lingkungan simulasi dengan jumlah pengguna yang terbatas dan hanya menggunakan satu skema implementasi E2EE. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan pengujian pada lingkungan cloud yang lebih kompleks, melibatkan jumlah pengguna yang lebih besar, serta membandingkan berbagai algoritma kriptografi modern agar diperoleh hasil evaluasi yang lebih komprehensif dan memiliki tingkat generalisasi yang lebih baik

4. KESIMPULAN

Penelitian ini berhasil mengevaluasi efektivitas penerapan End-to-End Encryption (E2EE) dalam meningkatkan keamanan komunikasi data pada sistem informasi berbasis cloud. Hasil pengujian menunjukkan bahwa E2EE mampu menjaga kerahasiaan (confidentiality)**,** integritas (integrity)**,** dan autentikasi (authentication**)** data secara efektif. Seluruh data yang dikirimkan berhasil diamankan dalam bentuk *ciphertext*, sehingga tidak dapat diakses oleh pihak yang tidak berwenang. Selain itu, sistem mampu mendeteksi perubahan data selama proses transmisi serta memberikan perlindungan terhadap serangan packet sniffing dan Man-in-the-Middle Attack (MITM)**.** Dari sisi performa, implementasi E2EE menyebabkan peningkatan latency dan response time serta sedikit penurunan throughput, namun perubahan tersebut masih berada dalam batas yang dapat diterima sehingga tidak mengganggu kualitas layanan. Hasil evaluasi berbobot menghasilkan nilai efektivitas sebesar 98,45%**,** yang menunjukkan bahwa peningkatan keamanan yang diperoleh jauh lebih besar dibandingkan dampak penurunan performa. Dengan demikian, End-to-End Encryption layak diterapkan sebagai mekanisme perlindungan komunikasi data pada sistem informasi berbasis cloud, terutama untuk aplikasi yang mengelola data sensitif. Penelitian ini masih memiliki keterbatasan karena pengujian dilakukan pada lingkungan simulasi dengan jumlah pengguna yang terbatas serta hanya menggunakan satu skema implementasi E2EE. Oleh karena itu, penelitian selanjutnya disarankan melakukan pengujian pada lingkungan cloud yang lebih kompleks, membandingkan beberapa algoritma kriptografi modern, serta mengintegrasikan E2EE dengan mekanisme keamanan lain, seperti Zero Trust Architecture**,** Multi-Factor Authentication (MFA)**,** atau sistem deteksi intrusi berbasis kecerdasan buatan, sehingga dapat diperoleh model keamanan komunikasi yang lebih adaptif, efisien, dan sesuai dengan kebutuhan sistem informasi modern.

REFERENCES

[1] E. Hanafi, R. Fiati, And E. Wijayanti, "Perancangan Sistem Data Tagihan Jaringan Internet Pada Bumdes Karya Abadi Desa Ngetuk Berbasis Website Dan Memanfaatkan Cloud Sms Gateway," *Jurnal Dialektika Informatika (Detika)*, Vol. 2, No. 2, Pp. 63–66, May 2022, Doi: 10.24176/Detika.V2i2.7867.

[2] M. Tinambunan And S. Sintaro, "Aplikasi Restfull Pada Sistem Informasi Geografis Pariwisata Kota Bandar Lampung," *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, Vol. 2, No. 3, Pp. 312–323, 2021, Doi: 10.33365/Jatika.V2i3.1230.

[3] D. Halki Widana, "Sistem Informasi Berbasis Cloud: Solusi Untuk Bisnis Modern Muhammad Irwan Padli Nasution," *Jurnal Ilmiah Penelitian Mahasiswa*, Vol. 3, No. 1, Pp. 8–15, 2025, Doi: 10.61722/Jipm.V3i%601.619.

[4] A. Candra, M. Maghfira, And A. Anisa, "Pemanfaatan Teknologi Cloud Computing Untuk Efisiensi Proses Pengolahan Data Informasi Di Institut Teknologi Dan Bisnis Bina Adinata Bulukumba," *Riggs: Journal Of Artificial Intelligence And Digital Business*, Vol. 4, No. 2, Pp. 4172–4177, Jun. 2025, Doi: 10.31004/Riggs.V4i2.1192.

[5] D. Patel *Et Al.*, "Single And Multiple Imputation Techniques To Treat Missing Numerical Variables (Mnv) In Perspectives Of Data Science Project - A Case Study," *International Journal Of Engineering Trends And Technology*, Vol. 70, No. 5, Pp. 9–14, 2022, Doi: 10.14445/22315381/Ijett-V70i5p202.

[6] A. Silonosov And L. Henesey, "The Role Of Key Encapsulation Mechanism In End-To-End Encryption Agility - A Case For Telemetry Data Confidentiality.," In *Procedia Computer Science*, Elsevier B.V., 2025, Pp. 829–838. Doi: 10.1016/J.Procs.2025.07.100.

[7] M. D. Nath, M. K. U. Ahamed, O. Ahmed, T. Ahmed, S. Roy, And M. N. Uddin, "Smart Web Interface For Student Mental Health Prediction Using Machine Learning With Blockchain Technology," *Neuroscience Informatics*, Vol. 5, No. 4, Dec. 2025, Doi: 10.1016/J.Neuri.2025.100236.

[8] G. Sarbishaei, A. M. A. Modarres, F. Jowshan, F. Z. Khakzad, And H. Mokhtari, "Smart Home Security: An Efficient Multi-Factor Authentication Protocol," *Ieee Access*, Vol. 12, Pp. 106253–106272, 2024, Doi: 10.1109/Access.2024.3437294.

[9] T. Isobe, R. Ito, And K. Minematsu, "Security Analysis Of Sframe," *Journal Of Information Security And Applications*, Vol. 89, Mar. 2025, Doi: 10.1016/J.Jisa.2024.103958.

[10] M. Yu, B. Jin, L. Zheng, W. Zhan, And C. Dong, "Application Of Data Encryption Technology In Computer Network Security," In *Procedia Computer Science*, Elsevier B.V., 2025, Pp. 1187–1193. Doi: 10.1016/J.Procs.2025.04.703.

Bulletin of Information System Research (BIOS)
Volume 4, No 2, April 2026, Page: 68−78
ISSN 2963-2455 (media online)
DOI: 10.62866/bios.v4i2.284
https://journal.grahamitra.id/index.php/bios

[11] L. Hao And X. Wang, "A Data Encryption Access Control Algorithm Based On Zero-Trust Model With Degree Of Discretization," *Egyptian Informatics Journal*, Vol. 32, Dec. 2025, Doi: 10.1016/J.Eij.2025.100825.
[12] W. Wang, J. Ma, B. Zhao, P. Han, And P. Zeng, "Information Security Transmission Method Of Data Exchange Platform Based On Lightweight Aes Encryption Algorithm," *Egyptian Informatics Journal*, Vol. 32, Dec. 2025, Doi: 10.1016/J.Eij.2025.100831.
[13] I. Agrawal, C. Bromfield, And C. Varga, "Evaluating A Swine Biosecurity Website As An Education And Outreach Tool And Identifying Best Practices For End-User Engagement: A Learning Analytics Approach," *Prev. Vet. Med.*, Vol. 240, Jul. 2025, Doi: 10.1016/J.Prevetmed.2025.106544.
[14] S.-J. Lee, S.-E. Jeon, And I.-G. Lee, "Partial Encryption-Based Shamir Secret Sharing For Low-Latency And Secure Networks," *Ict Express*, Feb. 2025, Doi: 10.1016/J.Icte.2025.12.006.
[15] S. Xie And J. Ye, "Ciphertext Comparable Method Based On Bcp," In *Procedia Computer Science*, Elsevier B.V., 2024, Pp. 1314–1323. Doi: 10.1016/J.Procs.2024.10.157.
[16] W. Feng And H. Cao, "Blockchain Electronic Evidence Sharing Based On Improved Ciphertext Policy Attribute Encryption," *Egyptian Informatics Journal*, Vol. 32, Dec. 2025, Doi: 10.1016/J.Eij.2025.100817.
[17] B. Ahamed, F. Kareem, And M. Y. Noor Mohamed, "Advancement Of The Ecc Algorithm To Prevent Man-In-The-Middle And Replay Attacks," In *Procedia Computer Science*, Elsevier B.V., 2025, Pp. 1259–1269. Doi: 10.1016/J.Procs.2025.04.081.
[18] M. Thankappan, H. Rifà-Pous, And C. Garrigues, "Multi-Channel Man-In-The-Middle Attacks Against Protected Wi-Fi Networks: A State Of The Art Review," Dec. 30, 2022, *Elsevier Ltd*. Doi: 10.1016/J.Eswa.2022.118401.
[19] Y. Wang *Et Al.*, "Review On All-Dielectric Metasurface Encryption Technology," *Defence Technology*, Nov. 2025, Doi: 10.1016/J.Dt.2025.11.036.
[20] W. Zhang, L. Di, J. Zhang, B. Liu, And X. Wang, "Design Of A Federated Learning Algorithm For Power Big Data Privacy Computing Based On Pruning Technique And Homomorphic Encryption," *Egyptian Informatics Journal*, Vol. 32, Dec. 2025, Doi: 10.1016/J.Eij.2025.100828.
[21] R. Basri *Et Al.*, "Enhancing Iot Security: Assessing Instantaneous Communication Trust To Detect Man-In-The-Middle Attacks," *Future Generation Computer Systems*, Vol. 166, May 2025, Doi: 10.1016/J.Future.2025.107714.