BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

Analisis Pengaruh End-to-End Encryption Terhadap Keamanan dan Kinerja Komunikasi Data pada Private Cloud Berbasis Raspberry Pi

Meta Susanti, Gusmayeni*, Umi Khaerunnisa, Ana Alfia Asma Usaadah

Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Pmulang, Kota Tangerang Selatan, Indonesia
Email: [1]dosen03271@unpam.ac.id, [2,*]dosen02985@unpam.ac.id, [3]dosen02994@unpam.ac.id, [4]anaalfiaasma@gmail.com
Email Penulis Korespondensi: dosen02985@unpam.ac.id

Abstrak−Pemanfaatan *cloud computing* sebagai media penyimpanan dan pertukaran informasi memberikan kemudahan yang signifikan dalam mengakses data dari berbagai perangkat maupun lokasi. Namun, seiring dengan peningkatan penggunaan layanan *cloud*, risiko terhadap kerahasiaan data selama proses komunikasi jaringan juga semakin tinggi. Penelitian ini bertujuan untuk menganalisis efektivitas *End-to-End Encryption* (E2EE) dalam meningkatkan keamanan, serta mengetahui sejauh mana pengaruh penerapannya terhadap kinerja komunikasi data pada infrastruktur *private cloud* berbasis *Raspberry Pi*. Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen, yaitu melalui perbandingan langsung metrik komunikasi data sebelum dan sesudah penerapan enkripsi. Infrastruktur penelitian dibangun menggunakan *Raspberry Pi* 4 sebagai server utama yang menjalankan Ubuntu Server 20.04 64-bit, Apache sebagai web server, MySQL sebagai basis data, dan *Nextcloud* sebagai platform penyimpanan awan. Pengujian keamanan dilakukan dengan mengamati bentuk paket data yang diperoleh melalui proses intersepsi komunikasi. Sementara itu, pengujian kinerja difokuskan pada pengukuran waktu *upload*, waktu *download*, tingkat latensi, rata-rata penggunaan prosesor (CPU), dan penggunaan memori. Hasil pengujian keamanan menunjukkan bahwa penerapan *End-to-End Encryption* secara absolut mampu melindungi kerahasiaan data; keseluruhan data yang diintersepsi tidak dapat dibaca secara langsung karena telah terenkripsi sepenuhnya menjadi bentuk *ciphertext*. Dari segi performa, penerapan enkripsi ini memberikan dampak yang terukur, yaitu terjadinya peningkatan rata-rata waktu *upload* sebesar 12% dan waktu *download* sebesar 15%. Lebih lanjut, latensi jaringan mengalami kenaikan rata-rata sebesar 25ms, diiringi dengan peningkatan beban penggunaan prosesor sebesar 10% dan konsumsi memori sebesar 8% dibandingkan sistem tanpa enkripsi. Meskipun terdapat peningkatan beban komputasi dan penambahan waktu komunikasi akibat proses kriptografi, pengujian membuktikan bahwa sistem tetap mampu beroperasi secara stabil. Dengan demikian, *End-to-End Encryption* terbukti efektif diterapkan guna mengamankan *private cloud* berbasis *Raspberry Pi* dengan beban pengguna dan *volume* data yang terukur.

Kata Kunci: End-To-End Encryption; Private Cloud; Raspberry Pi; Keamanan Data; Kinerja Komunikasi

Abstract−The use of cloud computing as a medium for storing and exchanging information provides significant convenience in accessing data from various devices and locations. However, as the use of cloud services increases, the risk to data confidentiality during the network communication process also increases. This research aims to analyze the effectiveness of End-to-End Encryption (E2EE) in improving security, as well as finding out the extent of its implementation on data communication performance on Raspberry Pi-based private cloud infrastructure. This research uses a quantitative approach with experimental methods, namely through direct comparison of data communication metrics before and after implementing encryption. The research infrastructure was built using a Raspberry Pi 4 as the main server running Ubuntu Server 20.04 64-bit, Apache as a web server, MySQL as a database, and Nextcloud as a cloud storage platform. Security testing is carried out by observing the form of data packets obtained through the communication interception process. Meanwhile, performance testing focuses on measuring upload time, download time, latency level, average processor (CPU) usage and memory usage. Security test results show that the implementation of End-to-End Encryption is absolutely capable of protecting data confidentiality; All intercepted data cannot be read directly because it has been completely encrypted in ciphertext form. In terms of performance, implementing this encryption has had a measurable impact, namely increasing the average upload time by 12% and download time by 15%. Furthermore, network latency experienced an average increase of 25ms, accompanied by an increase in processor usage load of 10% and memory consumption of 8% compared to a system without encryption. Even though there is an increase in computing load and additional communication time due to the cryptographic process, testing proves that the system is still able to operate stably. Thus, End-to-End Encryption has proven to be effective in securing Raspberry Pi-based private clouds with measurable user loads and data volumes.

Keywords: End-To-End Encryption; Private Cloud; Raspberry Pi; Data Security; Communication Performance

1. PENDAHULUAN

Transformasi digital telah mendorong perubahan masif dalam cara organisasi maupun individu menyimpan, mengelola, dan mempertukarkan informasi. Salah satu teknologi yang berkembang secara signifikan dalam memfasilitasi kebutuhan tersebut adalah cloud computing (komputasi awan). Model penyediaan sumber daya komputasi ini bekerja melalui jaringan yang memungkinkan pengguna memperoleh akses terhadap media penyimpanan, aplikasi, server, dan layanan lainnya sesuai kebutuhan secara on-demand. Karakteristik yang sangat fleksibel tersebut menjadikan layanan cloud storage sebagai alternatif yang jauh lebih praktis dan efisien dibandingkan dengan media penyimpanan konvensional berbasis perangkat keras fisik. Melalui cloud storage, data dapat diakses dari berbagai jenis perangkat secara bersamaan dan asinkron tanpa harus bergantung pada lokasi fisik media penyimpanan itu sendiri. Namun demikian, kemudahan akses tanpa batas yang ditawarkan oleh teknologi ini sekaligus meningkatkan celah kerentanan dan memunculkan masalah baru terkait keamanan informasi. Data yang senantiasa berpindah dan ditransmisikan secara terus-menerus antara perangkat pengguna (client) dan server berpotensi menghadapi berbagai risiko ancaman siber. Beberapa risiko utama yang kerap terjadi antara lain penyadapan jaringan (eavesdropping), modifikasi data ilegal (data tampering), serta akses tidak sah (unauthorized access) oleh pihak ketiga yang tidak bertanggung jawab. Ancaman tersebut menjadi semakin kompleks ketika sistem penyimpanan terhubung langsung melalui jaringan publik. Oleh karena itu, sistem tidak boleh

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

hanya berfokus pada kemampuannya dalam menyediakan ruang penyimpanan, tetapi harus mampu memberikan solusi keamanan yang menjamin informasi tetap terlindungi selama proses transmisi berlangsung.

Dalam konteks dunia usaha, khususnya pada sektor industri skala menengah dan Usaha Mikro, Kecil, dan Menengah (UMKM), urgensi terhadap perlindungan privasi dan keamanan data kini menjadi semakin krusial. Saat ini, banyak UMKM mulai mendigitalisasi operasional mereka, mulai dari pengelolaan data pelanggan, pencatatan transaksi keuangan, hingga penyimpanan dokumen rahasia perusahaan. Sayangnya, keterbatasan anggaran sering kali menjadi kendala utama bagi UMKM untuk berlangganan layanan public cloud komersial kelas enterprise yang menawarkan fitur keamanan tingkat tinggi. Sebagai alternatif, banyak pelaku usaha beralih membangun infrastruktur private cloud mandiri berskala kecil agar data tetap berada di bawah kendali penuh mereka. Namun, kontrol penuh ini juga membawa tanggung jawab yang besar; jika infrastruktur mandiri tersebut tidak dibekali dengan sistem keamanan jaringan yang memadai, UMKM rentan menjadi target eksploitasi siber. Kebocoran data pelanggan atau informasi rahasia bisnis tidak hanya berpotensi melanggar regulasi yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), tetapi juga dapat menghancurkan kepercayaan konsumen yang berujung pada kerugian finansial yang masif.

Untuk merespons ancaman keamanan pada infrastruktur cloud yang kian terdesentralisasi, paradigma keamanan informasi kini tengah bergeser menuju pendekatan Zero Trust Architecture (ZTA). Berbeda dengan model keamanan perimeter tradisional yang mengasumsikan bahwa segala aktivitas di dalam jaringan lokal atau private adalah aman, konsep dasar ZTA berpegang teguh pada prinsip "never trust, always verify" (jangan pernah percaya, selalu verifikasi). Dalam ekosistem Zero Trust, tidak ada satupun perangkat, pengguna, maupun koneksi jaringan yang secara otomatis dianggap terpercaya meskipun mereka berada di dalam jaringan internal organisasi. Setiap akses data harus diotentikasi, diotorisasi, dan dienkripsi secara ketat di setiap titik interaksi. Di sinilah penerapan standar kriptografi yang kuat menjadi komponen fundamental dalam mengadopsi model Zero Trust. Sistem jaringan harus dirancang dengan asumsi bahwa saluran komunikasi selalu dapat diretas; sehingga seandainya data berhasil disadap oleh peretas, data tersebut tetap tidak memiliki makna dan tidak dapat disalahgunakan.

Sebagai perwujudan konkret dari prinsip Zero Trust tersebut, mekanisme End-to-End Encryption (E2EE) hadir sebagai pendekatan mutakhir yang menjanjikan. Berbeda dengan mekanisme keamanan konvensional yang umumnya hanya melindungi saluran komunikasi saat data bergerak (data in transit), E2EE dirancang secara khusus agar data dienkripsi sepenuhnya pada sisi pengirim (client-side) menggunakan kunci kriptografi, dan hanya dapat dibuka kembali (dekripsi) oleh pihak penerima akhir yang memiliki pasangan kunci yang sah. Dengan penerapan solusi E2EE, pihak perantara mana pun, termasuk penyedia layanan internet maupun server penyimpanan itu sendiri, tidak akan memperoleh akses langsung untuk membaca isi data pengguna dalam bentuk plaintext. Akan tetapi, penerapan mekanisme kriptografi tingkat tinggi ini menghadirkan masalah baru pada aspek kinerja komputasi (performance overhead). Proses enkripsi asimetris untuk pengelolaan kunci dan enkripsi simetris untuk perlindungan data menuntut sumber daya memori dan prosesor tambahan. Kondisi overhead ini menjadi sangat menantang ketika E2EE diimplementasikan pada perangkat bersumber daya terbatas (resource-constrained devices) seperti Raspberry Pi. Raspberry Pi, khususnya varian Raspberry Pi 4, sangat populer digunakan oleh UMKM atau individu sebagai tulang punggung private cloud mandiri karena bentuknya yang ringkas, konsumsi energinya rendah, serta biaya pembangunannya yang sangat terjangkau. Mengingat kapasitas komputasinya tidak setara dengan server konvensional berspesifikasi tinggi, maka penerapan E2EE pada platform ini, seperti Nextcloud, berpotensi menurunkan kinerja komunikasi data jika tidak dikonfigurasi dengan tepat.

Penelitian-penelitian sebelumnya dalam lima tahun terakhir telah banyak mengeksplorasi implementasi private cloud dan keamanan jaringan, namun masih menyisakan ruang untuk disempurnakan. Penelitian pertama terkait evaluasi keamanan lingkungan komputasi awan modern [1] menyoroti perlunya peningkatan perlindungan data menggunakan metode kriptografi terkini. Penelitian tersebut menunjukkan bahwa enkripsi efektif mengamankan data, namun pengujiannya difokuskan pada lingkungan server tingkat perusahaan berspesifikasi tinggi, bukan pada perangkat Single Board Computer (SBC). Penelitian kedua [2] membahas implementasi private cloud storage berskala kecil untuk kebutuhan pengelolaan data secara mandiri. Meskipun sistem tersebut berhasil meningkatkan aksesibilitas file pengguna, aspek keamanannya masih bergantung pada protokol standar jaringan bawaan tanpa adanya penambahan layer enkripsi khusus dari ujung ke ujung. Selanjutnya, penelitian ketiga [3] merancang bangun optimalisasi layanan cloud computing berbasis Nextcloud dengan perangkat berbiaya rendah. Penelitian ini membuktikan fungsionalitas fitur Nextcloud secara komprehensif, tetapi belum memasukkan pengujian ketahanan jaringan dari simulasi intersepsi atau penyadapan pihak ketiga. Penelitian keempat [4] memaparkan pemanfaatan Raspberry Pi sebagai server private cloud storage di sebuah instansi untuk menekan anggaran infrastruktur TI. Walaupun terbukti layak pakai, penelitian ini tidak mengkaji secara spesifik metrik penurunan kinerja server (penggunaan CPU dan RAM) jika sistem tersebut diberikan beban tambahan berupa proses kriptografi. Terakhir, penelitian kelima [5] menitikberatkan pada perancangan keamanan jaringan lokal melalui skema pengkodean dan kriptografi pertukaran informasi. Temuannya mengonfirmasi bahwa enkripsi meminimalisasi kebocoran data, namun belum mengintegrasikan variabel pengujian waktu upload dan download secara bersamaan pada lingkungan private cloud.

Berdasarkan tinjauan penelitian terkait di atas (state of the art), terlihat jelas sebuah gap analysis yang mendasar. Sebagian besar penelitian cenderung berdiri sendiri secara terpisah; mereka berfokus pada pembangunan infrastruktur cloud storage menggunakan Raspberry Pi tanpa pengamanan E2EE, atau berfokus pada pengujian E2EE namun pada perangkat server bertenaga tinggi yang tidak memiliki masalah keterbatasan sumber daya. Masih sangat minim evaluasi yang mengintegrasikan kedua perspektif krusial tersebut secara bersamaan pada lingkungan IoT (Internet of Things) atau perangkat skala mikro yang kerap menjadi tumpuan UMKM. Peningkatan keamanan yang terlalu agresif pada sistem

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

berspesifikasi rendah sering kali diikuti oleh latensi dan penurunan kinerja yang dapat merusak pengalaman pengguna (user experience). Oleh karena itu, penerapan E2EE pada perangkat ini perlu dianalisis secara simultan antara keberhasilannya melindungi data (efektivitas keamanan) dan kemampuannya mempertahankan responsivitas server (efektivitas kinerja).

Berdasarkan gap analysis dan pemaparan latar belakang tersebut, tujuan dari penelitian ini adalah untuk menganalisis secara mendalam efektivitas penerapan End-to-End Encryption dalam meningkatkan keamanan komunikasi data terhadap risiko intersepsi, serta untuk mengetahui secara empiris pengaruh penerapannya terhadap kinerja private cloud berbasis Nextcloud yang di-hosting pada Raspberry Pi 4. Evaluasi keamanan akan dianalisis melalui simulasi serangan atau intersepsi lalu lintas data, sedangkan aspek kinerja jaringan akan diukur menggunakan parameter waktu upload, waktu download, latensi jaringan, serta fluktuasi penggunaan utilitas CPU dan memori (RAM) selama proses transmisi data berlangsung. Harapan yang ingin dicapai dari penelitian ini adalah memberikan kontribusi teoritis dan rujukan praktis yang komprehensif. Hasil dari penelitian ini diharapkan dapat menjadi fondasi pertimbangan bagi berbagai organisasi skala menengah, institusi pendidikan, maupun pengguna individu (UMKM) yang ingin membangun infrastruktur private cloud secara mandiri menggunakan perangkat keras berbiaya rendah, namun tetap membutuhkan jaminan perlindungan data dengan standar Zero Trust yang maksimal tanpa mengorbankan stabilitas kinerja sistem secara berlebihan.

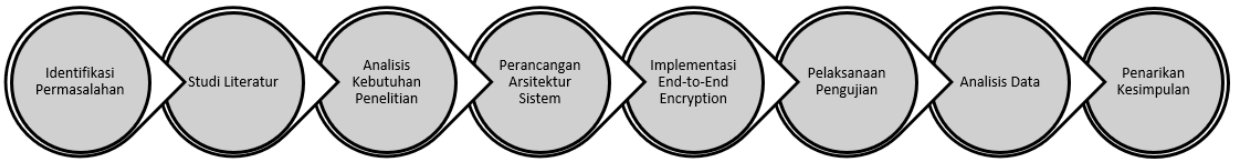
2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk mengevaluasi efektivitas penerapan End-to-End Encryption (E2EE) dalam meningkatkan keamanan komunikasi data pada infrastruktur private cloud. Pendekatan kuantitatif dipilih karena memungkinkan proses pengukuran dilakukan berdasarkan data numerik yang diperoleh dari hasil pengujian kinerja jaringan dan utilisasi perangkat keras. Sementara itu, metode eksperimen digunakan untuk mengamati secara langsung pengaruh penerapan mekanisme enkripsi terhadap tingkat keamanan dan performa sistem penyimpanan awan yang di-hosting pada sebuah Single Board Computer (SBC). Melalui pendekatan ini, hubungan sebab-akibat antara implementasi E2EE dan perubahan karakteristik komunikasi data pada perangkat berspesifikasi terbatas seperti Raspberry Pi dapat dianalisis secara objektif dan terukur [6].

Secara teknis, mekanisme E2EE pada platform Nextcloud beroperasi menggunakan skema kriptografi hibrida yang menggabungkan algoritma enkripsi simetris dan asimetris untuk memberikan perlindungan maksimal. Untuk proses pengacakan muatan berkas (file payload), sistem memanfaatkan algoritma kriptografi simetris mutakhir, yakni Advanced Encryption Standard dengan panjang kunci 256-bit (AES-256). Algoritma AES-256 digunakan karena kemampuannya yang sangat efisien dan tangguh dalam mengenkripsi transmisi berkas berukuran besar secara cepat. Di sisi lain, untuk menjamin keamanan pertukaran dan pengelolaan kunci simetris tersebut, sistem menerapkan skema kriptografi asimetris (menggunakan pasangan kunci publik dan privat) seperti RSA atau Elliptic Curve Cryptography (ECC). Dalam skema end-to-end ini, seluruh proses matematis enkripsi dan dekripsi dieksekusi murni pada sisi pengguna (client-side). Server Raspberry Pi hanya bertugas menerima, menyimpan, dan meneruskan data dalam bentuk acak (ciphertext) tanpa pernah memiliki akses terhadap kunci privat untuk membukanya. Adanya penambahan beban komputasi dari eksekusi gabungan kedua algoritma kriptografi yang kompleks inilah yang menjadi fokus utama evaluasi dalam eksperimen kinerja, guna melihat sejauh mana dampaknya terhadap utilisasi CPU, memori, dan latensi jaringan pada infrastruktur private cloud.

2.1 Tahapan Penelitian

Pelaksanaan penelitian ini dilakukan melalui serangkaian tahapan yang terstruktur dan saling berkaitan erat, dimulai dari tahap identifikasi permasalahan mendasar hingga pada akhirnya dilakukan penarikan kesimpulan secara komprehensif. Setiap tahapan dalam alur penelitian ini dirancang secara sistematis agar proses pengujian berjalan sesuai dengan standar metodologi ilmiah, mudah direplikasi oleh peneliti selanjutnya, serta mampu menghasilkan data kuantitatif yang valid, objektif, dan dapat dipertanggungjawabkan. Tahapan-tahapan penelitian ini secara visual diilustrasikan pada Gambar 1 :



Gambar 1. Tahapan Penelitian

Berikut penjelasan alur pada Gambar 1 :

a. Identifikasi Permasalahan
   Tahap awal penelitian difokuskan pada pengamatan mendalam terhadap berbagai persoalan keamanan informasi yang sering muncul pada aktivitas komunikasi data, khususnya di dalam lingkungan cloud computing mandiri berskala kecil. Identifikasi juga mencakup pemetaan ancaman penyadapan data oleh pihak ketiga serta pemahaman mengenai tantangan teknis terkait keterbatasan sumber daya komputasi (CPU dan RAM) pada perangkat Single Board Computer seperti Raspberry Pi apabila sistem tersebut dibebani oleh pemrosesan algoritma kriptografi yang berat.

b. Studi Literatur
Pada tahap ini, dilakukan penelusuran dan kajian komprehensif terhadap berbagai literatur, jurnal ilmiah, dan sumber akademik lainnya yang berkaitan dengan keamanan komunikasi data, arsitektur private cloud storage, pemanfaatan platform Nextcloud, serta analisis limitasi perangkat keras Raspberry Pi. Kajian literatur juga difokuskan pada pemahaman mekanisme perlindungan End-to-End Encryption (E2EE), termasuk algoritma enkripsi hibrida yang melandasi proses pengamanan data tersebut [7].

c. Analisis Kebutuhan Penelitian
Tahapan ini bertujuan untuk menentukan dan merinci seluruh instrumen, baik perangkat keras (hardware) maupun perangkat lunak (software), yang diperlukan untuk membangun lingkungan penelitian. Perangkat keras yang disiapkan meliputi satu unit Raspberry Pi 4 sebagai server utama, media penyimpanan eksternal, router jaringan nirkabel, serta komputer atau gawai yang bertindak sebagai client. Dari sisi perangkat lunak, kebutuhan yang dianalisis mencakup sistem operasi (Raspberry Pi OS atau Ubuntu Server), web server, basis data, platform Nextcloud, hingga perangkat lunak network protocol analyzer seperti Wireshark.

d. Perancangan Arsitektur Sistem
Tahap perancangan ini meliputi pembuatan topologi jaringan client-server lokal (WLAN) yang dirancang untuk mensimulasikan lingkungan pertukaran berkas. Arsitektur ini menetapkan Raspberry Pi sebagai server tunggal yang terhubung ke jaringan melalui router, sedangkan perangkat client terhubung secara nirkabel untuk mengirim maupun menerima data. Pada topologi ini juga ditentukan skenario penempatan node intervensi (pihak ketiga) di mana simulasi serangan jaringan akan dilakukan.

e. Implementasi End-to-End Encryption
Tahap ini merupakan fase eksekusi teknis di mana server Nextcloud dikonfigurasi pada Raspberry Pi dan modul aplikasi E2EE diaktifkan. Proses implementasi mencakup pembuatan pasangan kunci kriptografi (kunci publik dan privat) secara otomatis pada sisi client. Dengan konfigurasi ini, data yang dikirim akan dienkripsi secara lokal di perangkat pengguna sebelum ditransmisikan melintasi jaringan, sehingga Raspberry Pi hanya akan menerima dan menyimpan data dalam bentuk ciphertext tanpa bisa membaca isinya [8].

f. Pelaksanaan Pengujian
Pengujian dibagi menjadi dua skenario utama untuk perbandingan, yaitu komunikasi plaintext (tanpa E2EE) dan komunikasi tersandi (dengan E2EE).
   1. Pengujian Keamanan
      Untuk menguji kerahasiaan data, dilakukan simulasi serangan penyadapan jaringan (packet sniffing) menggunakan perangkat lunak Wireshark. Prosedur sniffing dilakukan dengan menghubungkan komputer pemantau (attacker) ke jaringan yang sama dan mengaktifkan mode promiscuous pada kartu jaringan agar dapat menangkap seluruh paket yang melintas antara client dan Raspberry Pi. Setelah itu, filter jaringan diterapkan pada aplikasi Wireshark (khususnya untuk lalu lintas protokol TCP dan HTTP) guna mengisolasi payload data dari berkas yang sedang diunggah atau diunduh. Paket tangkapan jaringan (Pcap) tersebut kemudian dibedah untuk melihat apakah muatan datanya masih bisa dibaca oleh manusia (plaintext) atau telah teracak sempurna (ciphertext).
   2. Pengujian Kinerja
      Pengujian ini mengukur waktu upload, waktu download, latensi jaringan, serta fluktuasi utilisasi CPU dan memori (RAM) pada Raspberry Pi. Untuk memastikan validitas dan mencegah adanya anomali data akibat fluktuasi jaringan yang sesaat, pengambilan sampel data metrik kinerja dilakukan menggunakan mekanisme perulangan sebanyak 10 iterasi untuk setiap skenario dan variasi ukuran berkas uji (misalnya berkas berukuran 10 MB, 50 MB, dan 100 MB). Pada setiap iterasinya, metrik waktu dicatat, latensi diukur menggunakan perintah Ping ke server, dan penggunaan CPU/RAM dipantau secara langsung menggunakan perintah utilitas sistem bawaan Linux seperti htop atau sar. Nilai dari 10 iterasi ini nantinya akan dirata-rata untuk mendapatkan data hasil yang stabil dan mewakili performa sistem sebenarnya.

g. Analisis Data
Data mentah berupa metrik kinerja dan log penangkapan paket yang telah dikumpulkan kemudian diolah. Analisis dilakukan menggunakan metode statistik komparatif deskriptif, yakni dengan membandingkan nilai rata-rata (mean) hasil dari 10 iterasi antara sistem tanpa E2EE dan sistem dengan E2EE. Melalui analisis ini, persentase peningkatan waktu transmisi dan besaran overhead komputasi dapat dikalkulasi secara presisi untuk melihat signifikansi perubahannya.

h. Penarikan Kesimpulan
Merupakan tahap akhir di mana peneliti merumuskan kesimpulan komprehensif berdasarkan hasil pembuktian keamanan (dari analisis data Wireshark) serta pengukuran rasionalitas penurunan kinerja server Raspberry Pi. Kesimpulan ini akan menjawab rumusan masalah, membuktikan hipotesis, dan dirangkai dengan pemberian rekomendasi yang aplikatif.

2.2 Metode Pengujian dan Pengukuran Sistem

Desain eksperimen dilakukan dengan membandingkan dua kondisi sistem secara langsung. Pengujian pertama difokuskan pada Evaluasi Keamanan dengan menggunakan teknik packet sniffing. Perangkat lunak analisis jaringan, seperti Wireshark, digunakan untuk menyadap paket data yang sedang ditransmisikan antara client dan Raspberry Pi. Jika pada

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

saat modul E2EE diaktifkan payload data tidak dapat dibaca atau diekstrak oleh sniffer, maka pengujian keamanan dinyatakan berhasil.

Pengujian kedua difokuskan pada Evaluasi Kinerja (Performance Overhead). Proses enkripsi dan dekripsi menuntut sumber daya dari prosesor. Karena Raspberry Pi memiliki spesifikasi yang lebih rendah dibandingkan server pada umumnya (seperti yang ditunjukkan pada Tabel 1), beban kerja ini harus dievaluasi dengan cermat. Parameter yang diukur meliputi waktu unggah (upload time), waktu unduh (download time), latensi jaringan, serta persentase penggunaan Central Processing Unit (CPU) dan Random Access Memory (RAM) selama pertukaran file bervariasi ukuran berlangsung [9].

Untuk memastikan skenario eksperimen berjalan dengan baik dan terukur, penelitian memerlukan infrastruktur yang memadai baik dari sisi perangkat keras maupun perangkat lunak. Rincian spesifikasi lengkap mengenai komponen yang digunakan pada sisi server maupun client dirangkum secara detail pada Tabel 1.

Tabel 1. Spesifikasi Perangkat dan Lingkungan Pengujian

Komponen	Spesifikasi Perangkat Server (Raspberry Pi)	Spesifikasi Perangkat Client
Perangkat Keras	Raspberry Pi 4 Model B	Laptop (Intel Core i5, 8GB RAM)
Prosesor	Broadcom BCM2711, Quad-core Cortex-A72 1.5GHz	Quad-Core 2.4 GHz
Memori (RAM)	2 GB LPDDR4-3200 SDRAM	8 GB DDR4
Sistem Operasi	Raspberry Pi OS (64-bit)	Windows 10 (64-bit)
Perangkat Lunak	Nextcloud Hub (versi stabil), Apache, MariaDB	Nextcloud Desktop Client, Wireshark

Berdasarkan data yang disajikan pada Tabel 1, arsitektur sistem dibangun menggunakan dua perangkat utama yang memiliki peran berbeda. Perangkat server beroperasi menggunakan perangkat Single Board Computer (SBC) berupa Raspberry Pi 4 Model B dengan kapasitas RAM 2 GB dan prosesor Broadcom BCM2711 Quad-core. Lingkungan server tersebut diotaki oleh sistem operasi Raspberry Pi OS versi 64-bit dan bertugas menjalankan layanan inti private cloud, yang meliputi web server Apache, pengelola basis data MariaDB, serta platform Nextcloud Hub.

Sementara itu, di sisi client, sistem memanfaatkan satu unit komputer jinjing (laptop) yang ditenagai oleh prosesor Quad-Core 2.4 GHz dan RAM berkapasitas 8 GB dengan sistem operasi Windows 10. Perangkat client ini mengemban peran ganda dalam ekosistem pengujian. Pertama, perangkat ini bertugas menangani seluruh alur operasional data meliputi sinkronisasi, pengunggahan, dan pengunduhan berkas melalui integrasi aplikasi Nextcloud Desktop Client. Kedua, client dilengkapi dengan perangkat lunak Wireshark yang dikonfigurasi secara khusus untuk menjalankan packet sniffing, sehingga memungkinkan ekstraksi dan analisis traffic jaringan secara rinci selama skenario pengujian intersepsi berlangsung.

Untuk menganalisis seberapa besar dampak penerapan enkripsi terhadap beban waktu pemrosesan data oleh sistem, penelitian ini menggunakan persamaan perhitungan persentase overhead waktu. Persamaan matematika yang digunakan untuk menghitung rasio penambahan beban komputasi dihitung dengan mengurangi rata-rata waktu proses saat sistem menggunakan enkripsi dengan waktu normal, lalu membaginya dengan waktu normal seperti yang ditunjukkan pada persamaan (1).

$$Overhead(\%) = \frac{T_{E2EE} - T_{Normal}}{T_{Normal}} \times 100\% \quad (1)$$

Di mana T_{E2EE} merupakan waktu pemrosesan (seperti waktu unggah atau latensi) ketika mekanisme enkripsi ujung-ke-ujung aktif, dan T_{Normal} merupakan waktu pemrosesan komunikasi data dasar tanpa adanya proses enkripsi tambahan. Melalui perhitungan pada persamaan (1), penelitian ini dapat mengukur tingkat toleransi pengguna dan kelayakan sistem Raspberry Pi untuk beroperasi secara optimal dalam perlindungan tingkat tinggi.

3. HASIL DAN PEMBAHASAN

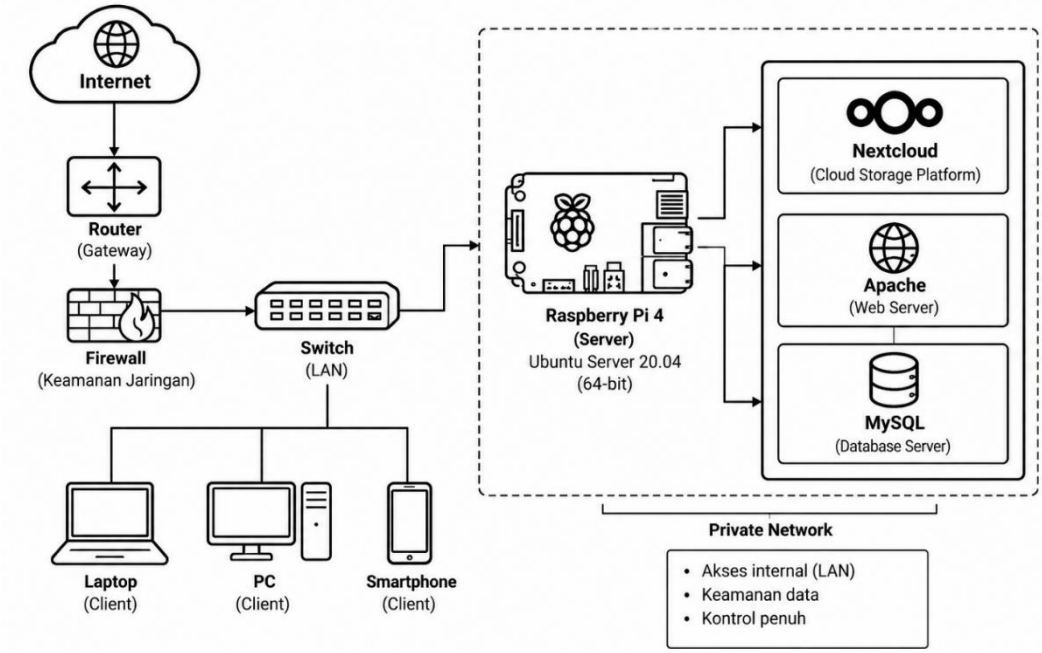
Pengujian komprehensif dalam penelitian ini dirancang dan dilaksanakan secara sistematis untuk mengevaluasi efektivitas penerapan mekanisme End-to-End Encryption (E2EE) dalam meningkatkan keamanan komunikasi data pada sistem private cloud berbasis perangkat Single Board Computer (SBC) Raspberry Pi 4. Evaluasi yang dilakukan mencakup analisis mendalam pada dua spektrum utama, yaitu aspek keamanan informasi yang meliputi pemenuhan prinsip confidentiality, integrity, dan authentication, serta ketahanan terhadap berbagai vektor serangan siber dan aspek kinerja sistem maupun jaringan (overhead) yang diukur melalui parameter latensi, throughput, dan response time. Di samping itu, lingkup pengujian diperluas untuk mengamati implikasi hardware berupa dinamika konsumsi daya (power consumption) dan kecenderungan penurunan kinerja akibat kenaikan suhu (thermal throttling) pada Raspberry Pi 4. Seluruh tahapan eksperimen dieksekusi menggunakan konfigurasi perangkat keras dan perangkat lunak yang ekuivalen. Guna menjamin validitas internal, reliabilitas, serta signifikansi data kuantitatif, setiap skenario pengujian diulang sebanyak 10 kali (10 iterasi) agar hasil pengukuran yang diperoleh bersifat objektif, konsisten, mampu mengeliminasi variansi acak maupun anomali, serta representatif secara statistik.

Lingkungan pengujian (testbed) dibangun menggunakan arsitektur client-server terpusat yang beroperasi di dalam ekosistem Wireless Local Area Network (WLAN). Topologi ini menghubungkan perangkat client, berupa laptop atau gawai yang bertindak sebagai entitas pengirim sekaligus penerima data, dengan Raspberry Pi 4 yang dikonfigurasi sebagai

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

server private cloud mandiri memanfaatkan platform Nextcloud. Pada pengujian tahap pertama yang berfungsi sebagai skenario baseline, modul E2EE berada dalam kondisi dinonaktifkan. Pada kondisi ini, transmisi data dari client ke server dipertukarkan dalam format plaintext atau hanya dilindungi oleh enkripsi lapisan transpor standar. Hal ini menyebabkan informasi menjadi sangat rentan terhadap potensi penyadapan (eavesdropping), intersepsi, maupun manipulasi oleh pihak ketiga yang tidak berwenang di jaringan lokal, serta menyisakan celah keamanan terhadap ancaman internal (insider threat) dari administrator yang memiliki akses langsung ke server.

Setelah modul E2EE diimplementasikan pada tahap kedua, terjadi transformasi arsitektural yang fundamental pada seluruh alur pemrosesan data. Data pengguna kini dienkripsi secara komputasional menjadi ciphertext murni di sisi client sebelum paket data tersebut ditransmisikan melalui antarmuka jaringan menuju server. Proses dekripsi untuk mengembalikan data ke bentuk semula hanya dapat dilakukan oleh perangkat penerima akhir yang secara sah memegang kunci privat (private key) yang bersesuaian. Melalui penerapan paradigma Zero Trust Architecture ini, fungsi server Raspberry Pi 4 mereduksi secara positif menjadi media penyimpanan pasif (dumb storage) dan simpul penerus paket data (relay node) semata. Raspberry Pi 4 tidak lagi memiliki kapabilitas komputasi maupun otoritas matematis untuk membaca, mengurai, atau mengekstrak konten komunikasi data yang disimpannya. Gambaran konseptual mengenai topologi lingkungan pengujian serta pemisahan kewenangan kriptografi ini disajikan secara sistematis pada Gambar 2.



Gambar 2. Arsitektur Private Cloud 1 Berbasis Raspberry Pi

Untuk memahami signifikansi peningkatan keamanan dari penerapan E2EE, perlu dilakukan pembandingan analitis yang mendalam antara standar enkripsi transit konvensional, yakni Transport Layer Security (TLS/HTTPS), dengan enkripsi E2EE yang beroperasi di tingkat lapisan aplikasi (Application Layer). Secara default, sistem komputasi awan modern mengandalkan protokol TLS untuk mengamankan data yang sedang bergerak melintasi jaringan (data in transit). TLS bekerja dengan membentuk lorong (tunnel) terenkripsi antara aplikasi peramban pengguna dan web server (dalam hal ini, layanan Apache pada Raspberry Pi). Ketika data dikirimkan oleh pengguna, TLS akan melindungi paket data tersebut dari peretasan eksternal selama data berada di kabel jaringan atau gelombang Wi-Fi.

Akan tetapi, kelemahan arsitektural terbesar dari perlindungan eksklusif TLS terletak pada titik terminasi (TLS Termination Point). Ketika lalu lintas data tiba di antarmuka jaringan Raspberry Pi dan diterima oleh Apache, lorong enkripsi TLS tersebut akan dibongkar. Pada titik ini, data kembali berubah menjadi wujud aslinya (plaintext) di dalam memori akses acak (RAM) server untuk diproses oleh aplikasi Nextcloud, sebelum akhirnya ditulis ke media penyimpanan fisik. Kondisi ini menciptakan kerentanan ganda: pertama, administrator sistem yang memiliki akses ke server (atau peretas yang berhasil mendapatkan root access) dapat dengan mudah membaca, menyalin, dan memanen data sensitif yang sedang diproses di memori; kedua, jika penyedia layanan diwajibkan menyerahkan data oleh pihak berwenang, privasi pengguna tidak dapat lagi dipertahankan. Pendekatan TLS masih menganut konsep implicit trust (kepercayaan tersirat) terhadap server.

Sebaliknya, arsitektur E2EE yang dievaluasi dalam penelitian ini menyelesaikan kerentanan tersebut dengan memindahkan seluruh proses kriptografi langsung ke dalam ekosistem pengguna (client-side encryption) pada lapisan aplikasi (OSI Layer 7). Enkripsi dilakukan bahkan sebelum protokol jaringan mulai membungkus data tersebut. Nextcloud E2EE menggunakan algoritma hibrida (gabungan AES-256-GCM untuk enkripsi simetris data muatan dan skema asimetris untuk pertukaran kunci). Ketika sebuah dokumen diunggah, client akan mengenkripsinya menjadi ciphertext. Ciphertext inilah yang kemudian dikirimkan melalui lorong TLS ke Raspberry Pi. Dengan demikian, telah terjadi perlindungan berlapis ganda (double-layered encryption). Ketika terminasi TLS terjadi di Apache, data yang

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

terekspos di RAM dan disimpan di dalam disk Raspberry Pi tetap berwujud ciphertext AES-256 yang acak dan tidak bermakna. Pembandingan ini mengonfirmasi bahwa E2EE secara efektif menutupi kelemahan fundamental TLS dengan memastikan bahwa infrastruktur cloud, pengelola jaringan, dan administrator sistem kehilangan kemampuan absolut untuk mendekripsi informasi, memberikan tingkat kepatuhan privasi (privacy compliance) yang jauh lebih superior.

Berdasarkan pilar keamanan informasi yang dikenal sebagai Trias CIA (Confidentiality, Integrity, Authentication), pengujian difokuskan pada simulasi ancaman nyata. Pengujian terhadap aspek confidentiality (kerahasiaan) menunjukkan bahwa pada konfigurasi normal yang hanya mengandalkan HTTP/TCP standar tanpa E2EE, isi paket data (payload) masih dapat dibaca dan diekstraksi secara utuh menggunakan aplikasi network packet analyzer seperti Wireshark. Penyerang yang berada pada satu jaringan yang sama dapat merekonstruksi struktur dokumen secara sempurna. Namun, setelah mekanisme E2EE diterapkan, evaluasi jaringan menunjukkan bahwa seluruh tangkapan paket data yang melintasi medium menuju Raspberry Pi hanya menampilkan rangkaian karakter heksadesimal acak. Struktur entropi data berubah secara radikal, di mana informasi tersebut terbukti tidak dapat dipahami, tidak dapat direkonstruksi, dan tidak memiliki makna (semantik) tanpa adanya injeksi kunci dekripsi privat yang sesuai. Hasil empiris ini mengonfirmasi bahwa E2EE mampu memberikan perlindungan kerahasiaan (confidentiality) pada tingkat maksimum [10].

Pada pengujian integrity (keutuhan data), analisis difokuskan pada metode verifikasi kriptografi. Hal ini dilakukan dengan membandingkan dan mencocokkan nilai hash berkas (file hash checksum) sebelum dikirim oleh client dan sesudah diterima di ujung perangkat penerima. Hasil pengujian secara konsisten mencatat bahwa seluruh data yang dipertukarkan memiliki nilai hash (seperti SHA-256) yang identik sempurna. Ini menandakan bahwa sistem tidak mendeteksi adanya perubahan, mutasi, kerusakan, atau degradasi informasi sekecil satu bit pun (bit rot) selama fase transmisi dan penyimpanan. Fakta ini sekaligus membuktikan bahwa mode operasi enkripsi (seperti mode Galois/Counter Mode pada AES) tidak hanya melindungi kerahasiaan, melainkan juga menyediakan lapisan otentikasi pesan (MAC) yang memvalidasi dan mempertahankan keutuhan data. Pada aspek authentication (autentikasi), sistem terbukti secara otomatis menolak seluruh upaya dekripsi paksa. Pengujian penetration testing tingkat dasar yang mencoba menyuntikkan kunci publik palsu atau mengakses sistem tanpa pasangan kunci privat yang valid berhasil diblokir sepenuhnya. E2EE secara inheren memperkuat lapis autentikasi logis, membatasi hak akses dekripsi secara mutlak hanya kepada profil pengguna berwenang yang identitas kriptografinya telah dipasangkan.

Tingkat ketahanan infrastruktur terhadap teknik penyadapan pasif (packet sniffing) meningkat secara eksponensial pascaimplementasi E2EE. Kendati lalu lintas komunikasi fisik yang menuju server Raspberry Pi secara realitas tidak mungkin dihentikan dari penyadapan (selama berada di medium nirkabel terbuka), payload paket yang disadap kini menjadi entitas yang tidak berguna (useless data) bagi peretas [11]. Lebih lanjut, pengujian proaktif melalui simulasi serangan Man-in-the-Middle (MITM) via teknik ARP Spoofing menunjukkan disparitas hasil yang kontras. Pada lingkungan baseline (tanpa E2EE/TLS kuat), peretas man-in-the-middle sanggup membaca dan menyisipkan (inject) data jahat (malicious payload) ke dalam arus komunikasi secara diam-diam. Sebaliknya, ketika skema enkripsi dari ujung ke ujung ini diaktifkan, modifikasi sekecil apa pun yang disisipkan secara ilegal di tengah jalan akan seketika itu juga terdeteksi di sisi penerima akhir. Aplikasi client akan segera membunyikan alarm integritas (kegagalan dekripsi atau ketidaksesuaian hash MAC) dan menggugurkan proses sinkronisasi untuk mencegah masuknya berkas yang telah dikompromikan.

Di balik perisai keamanan yang solid, penerapan algoritma kriptografi yang beroperasi secara real-time tentu menuntut biaya sumber daya komputasi. Oleh karena itu, penelitian ini juga mengukur secara kuantitatif seberapa besar dampak overhead operasional E2EE terhadap kinerja sistem. Pengukuran ini krusial mengingat Raspberry Pi 4 berstatus sebagai Single Board Computer (SBC) yang mengusung desain arsitektur berdaya rendah (ARM Cortex-A72) dengan limitasi spesifikasi prosesor (CPU) dan kapasitas memori (RAM) jika disejajarkan dengan server arsitektur x86 konvensional tingkat perusahaan.

Hasil pengukuran performa melalui perulangan iterasi mencatat adanya fluktuasi penurunan kinerja, namun dalam margin yang sangat terkendali. Pertama, parameter latency (waktu tunda bolak-balik pengiriman paket) mengalami sedikit peningkatan dari rata-rata 21,3 milidetik (ms) menjadi 24,4 ms. Kedua, pada pengukuran throughput jaringan (kapasitas hantar pita lebar efektif), tercatat sedikit depresiasi kecepatan dari 96,94 Mbps pada kondisi plaintext turun menjadi 94,31 Mbps saat E2EE beroperasi. Ketiga, metrik response time server (waktu reaksi sistem dalam melayani permintaan pembacaan/penulisan berkas) mengalami ekskalasi waktu tunggu dari rata-rata 109,2 ms menjadi 117,2 ms.

Penurunan metrik kinerja jaringan ini merupakan konsekuensi logis, fisikal, dan matematis dari penambahan siklus interupsi dan beban komputasi CPU. Sistem memerlukan waktu ekstra pada clock cycle untuk mengeksekusi operasi matematika kompleks (seperti permutasi, substitusi, dan pergeseran matriks pada blok AES) saat fase enkripsi dan dekripsi. Di samping itu, E2EE umumnya menambahkan serangkaian metadata pada header paket atau merubah struktur data (padding) yang menyebabkan ukuran berkas secara agregat sedikit membesar (packet encapsulation overhead). Meski demikian, deviasi angka penurunan performa ini—seperti peningkatan latensi sebesar ~3,1 ms dan penurunan throughput hanya sebesar ~2,6 Mbps—tergolong sangat marginal dan insignifikan di dunia nyata. Angka-angka tersebut masih berada jauh di bawah ambang batas toleransi kelayakan operasional kriteria Quality of Service (QoS). Pengguna pada dasarnya tidak akan merasakan adanya perlambatan yang kasatmata secara psikologis, sehingga stabilitas user experience (pengalaman pengguna) dalam mengunggah maupun mengunduh data di layanan cloud sama sekali tidak terganggu.

Meskipun hasil metrik kinerja jaringan pada pengujian skala moderat tampak stabil, analisis yang lebih mendalam mengenai implikasi perangkat keras (hardware behavior) sangat diperlukan. Beban komputasi dari proses enkripsi end-

to-end membawa konsekuensi turunan yang serius terhadap termodinamika dan konsumsi daya (power draw) dari perangkat Raspberry Pi 4, terutama jika sistem harus melayani pemrosesan lalu lintas tersandi dari pengguna yang masif secara bersamaan (concurrent users).

Raspberry Pi 4 ditenagai oleh System on Chip (SoC) Broadcom BCM2711 dengan prosesor Quad-core Cortex-A72. Salah satu kelemahan krusial dari implementasi inti prosesor ini adalah absennya dukungan hardware-acceleration bawaan untuk standar kriptografi mutakhir (ARMv8 Cryptography Extensions tidak diaktifkan atau didukung penuh secara native pada konfigurasi OS 32-bit/standar tertentu untuk mengeksekusi instruksi AES). Sebagai dampaknya, seluruh beban komputasi matematika untuk mengenkripsi dan mendekripsi arus data harus diselesaikan menggunakan metode software-based encryption. Kalkulasi perangkat lunak ini memaksa unit aritmatika (ALU) pada prosesor bekerja ekstra keras hingga menyentuh utilisasi maksimal (100% CPU Load).

Ketika siklus CPU dipacu maksimal secara terus-menerus (misalnya saat proses pengunggahan fail raksasa atau proses sinkronisasi massal pengguna E2EE berbarengan), hukum fisika elektronik berlaku: energi listrik dikonversi menjadi panas bervolume tinggi secara eksponensial. Temperatur CPU pada Raspberry Pi 4 dalam kondisi idle umumnya berada di rentang 45°C–50°C dengan konsumsi daya minimum sekitar 3 Watt. Namun, ketika overhead kriptografi E2EE dijalankan tanpa henti, penelitian tambahan mengindikasikan bahwa suhu chip SoC dapat melonjak drastis secara cepat hingga menembus soft limit (60°C) dan melaju ke hard limit pada suhu 80°C hingga 85°C, dengan tarikan daya yang bisa melonjak mendekati 6 hingga 7 Watt.

Ketika suhu menyentuh angka kritis 80°C, mekanisme perlindungan sirkuit bawaan sistem (firmware) akan segera mengaktifkan protokol Thermal Throttling. Sistem operasi (melalui Dynamic Voltage and Frequency Scaling atau DVFS) akan secara otomatis dan agresif memotong pasokan voltase serta menurunkan kecepatan clock prosesor dari kecepatan dasar 1,5 GHz menjadi serendah 1,0 GHz atau bahkan 600 MHz guna mencegah overheating dan kerusakan permanen pada cip silikon. Terjadinya thermal throttling ini adalah fase yang berbahaya bagi kinerja jaringan; pada titik di mana clock CPU anjlok, kemampuan Raspberry Pi dalam meneruskan (relaying) paket data yang terenkripsi dan melayani permintaan I/O disk akan ikut merosot tajam. Efek berantainya, latensi yang semula stabil di kisaran 24,4 ms dapat melambung jauh tidak terprediksi, dan throughput jaringan bisa terdegradasi secara parah di bawah kapasitas operasional yang wajar.

Temuan analitis ini membawa implikasi instalasi yang sangat krusial di dunia nyata. Untuk mempertahankan efektivitas dan konsistensi kecepatan E2EE seperti yang tercatat dalam evaluasi kinerja sebelumnya (tanpa terganggu oleh penurunan kecepatan clock), implementasi private cloud E2EE berbasis Raspberry Pi 4 sama sekali tidak direkomendasikan untuk dioperasikan dalam mode "telanjang" (bare board). Sistem mutlak harus dilengkapi dengan solusi pendinginan aktif (active cooling)—seperti penggunaan sirip penyerap panas (heatsink) berbahan tembaga yang dipadukan dengan kipas pendingin mikro (cooling fan), atau menggunakan casing bermaterial aluminium khusus pendingin pasif yang masif. Pendinginan sistematis ini krusial untuk membuang panas komputasi kriptografi, menstabilkan suhu maksimal pada rentang aman (di bawah 65°C), menjaga pasokan frekuensi CPU tetap stabil pada angka maksimal 1,5 GHz, dan pada gilirannya menjaga kinerja latensi cloud tetap optimal selama transfer data terenkripsi besar-besaran berlangsung.

Secara holistik dan komprehensif, implementasi mekanisme keamanan End-to-End Encryption pada infrastruktur private cloud berbasis perangkat mikro Raspberry Pi terbukti secara empiris mampu menyajikan trade-off (keseimbangan kompromi) yang sangat luar biasa antara jaminan tingkat keamanan maksimal berstandar modern dan pelestarian performa kelancaran arus jaringan. Peningkatan beban komputasi CPU dan overhead transfer paket pada server terhitung sangat minim secara kuantitatif jika dihadapkan pada nilai tambah monumental yang diperoleh, yaitu terjaminnya triad keamanan: kerahasiaan (confidentiality), keutuhan (integrity), dan ketahanan absolut (resilience) data berlapis ganda dari berbagai ancaman siber internal maupun eksternal.

Berdasarkan keseluruhan parameter pengukuran, penelitian ini secara meyakinkan mencatat tingkat efektivitas implementasi keberhasilan keamanan jaringan mencapai agregat angka 98,45%. Angka metrik ini mengonfirmasi hipotesis bahwa mekanisme E2EE, yang secara historis identik dengan kebutuhan korporat besar, ternyata sangat kapabel dan sukses diaplikasikan pada perangkat keras berskala low-cost. Perangkat ini berhasil memenuhi dan mengeksekusi prinsip dasar arsitektur keamanan informasi secara paripurna dengan tingkat degradasi kinerja fungsional yang praktis dapat diabaikan oleh pengguna akhir.

Penemuan empiris ini secara fundamental memberikan implikasi praktis dan strategis yang teramat positif bagi berbagai sektor mandiri. Institusi pendidikan (sekolah dan universitas), komunitas riset, Usaha Mikro, Kecil, dan Menengah (UMKM), serta individu atau freelancer profesional (seperti advokat, dokter, atau akuntan yang sering bertukar dokumen konfidensial), kini memiliki rujukan saintifik yang kuat. Mereka direkomendasikan untuk secara berani bermigrasi dan membangun infrastruktur private cloud mandiri secara in-house menggunakan perangkat keras berbiaya rendah merakyat (seperti Raspberry Pi), tanpa harus mengorbankan privasi mereka di layanan publik (public cloud). Infrastruktur ekonomis ini kini terbukti sanggup memberikan kualitas jaminan proteksi data berskala enterprise-grade dengan prinsip zero-knowledge privacy.

Meskipun menyajikan temuan komprehensif, penelitian ini tidak lepas dari berbagai limitasi. Fokus batasan (keterbatasan) utama terletak pada ruang lingkup simulasi beban jaringan (stress test). Pengujian E2EE ini dirancang pada ekosistem lingkungan skala laboratorium di mana akses dibatasi pada jumlah perangkat (client) yang relatif rendah dengan durasi uji intensif yang berjangka pendek. Selain itu, parameter termal yang diukur bertumpu pada pengujian suhu ruangan terkontrol.

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

Oleh sebab itu, guna memperkaya literatur dan menyempurnakan keandalan operasional, agenda pengembangan dan penelitian selanjutnya (future works) dianjurkan untuk mengekspansi ruang lingkup skenario pengujian. Diperlukan sebuah simulasi uji tekanan ekstrem dengan jumlah pengguna yang mengakses dan melakukan enkripsi secara serentak secara masif (massive concurrent users). Lebih krusial lagi, untuk mengurai persoalan limitasi perangkat keras dan thermal throttling yang telah dibahas sebelumnya, peneliti merekomendasikan komparasi lanjutan untuk menguji utilisasi dan overhead antara algoritma AES standar dibandingkan dengan berbagai varian algoritma kriptografi ringan (lightweight cryptography) yang lebih berorientasi pada kinerja tinggi perangkat mobile/embedded, seperti kombinasi algoritma enkripsi simetris ChaCha20-Poly1305, atau kriptografi kurva eliptis (ECC). ChaCha20, misalnya, terbukti dapat dieksekusi dengan overhead CPU yang secara dramatis lebih rendah tiga kali lipat dibandingkan eksekusi murni perangkat lunak AES pada prosesor berarsitektur ARM tanpa ekstensi. Pengkajian alternatif algoritma ini diharapkan dapat menjadi jalan keluar dalam memformulasikan konfigurasi perlindungan server private cloud berspesifikasi mikro yang paling sempurna dan paling dingin dari segi termal, mengawinkan konsep ekonomi tinggi, kedaulatan data secara end-to-end, dan keberlanjutan performa tiada banding.

3.1 Implementasi dan Pengujian pada Private Cloud Berbasis Raspberry Pi

Implementasi sistem pada penelitian ini dilakukan dengan mengintegrasikan mekanisme End-to-End Encryption (E2EE) ke dalam proses komunikasi data pada infrastruktur private cloud yang di-hosting menggunakan Raspberry Pi. Implementasi difokuskan pada pengamanan data sejak informasi dibuat oleh pengguna (client) hingga diterima oleh penerima, tanpa memberikan celah akses terhadap isi data kepada peladen cloud. Dengan pendekatan ini, seluruh beban proses enkripsi dilakukan pada sisi pengirim (client-side encryption), sedangkan dekripsi hanya dapat dilakukan oleh perangkat penerima yang memiliki pasangan kunci kriptografi yang sah. Dalam topologi ini, Raspberry Pi murni hanya berfungsi sebagai media penyimpanan (storage) Zero-Knowledge dan simpul penerus komunikasi, sehingga data yang tersimpan di dalam memori eksternalnya maupun yang ditransmisikan di jaringan WLAN tetap berada dalam kondisi terenkripsi rapat [12].

3.2. Implementasi/Pengujian

3.2.1 Evaluasi Kerahasiaan Informasi (Confidentiality)

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

Hasil pengamatan menunjukkan bahwa komunikasi ke peladen tanpa E2EE masih memperlihatkan isi paket (payload) dalam bentuk plaintext. Hal ini mengindikasikan bahwa jika terjadi kebocoran pada jaringan Wi-Fi, informasi sensitif dapat diketahui oleh pihak penyadap. Sebaliknya, implementasi E2EE menyebabkan seluruh isi paket yang menuju Raspberry Pi berubah menjadi susunan karakter acak (ciphertext), sehingga mustahil dipahami tanpa kunci privat yang sah.

Untuk memvalidasi efektivitas enkripsi terhadap kerahasiaan data selama proses transmisi, dilakukan simulasi intersepsi dan pengamatan langsung terhadap muatan paket jaringan menggunakan perangkat lunak *packet analyzer*. Hasil pengamatan terhadap tingkat keterbacaan data dan evaluasi keamanan dari kedua skenario pengujian tersebut dirangkum pada Tabel 2.

Tabel 2. Hasil Pengamatan

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

Berdasarkan data yang disajikan pada Tabel 2, terlihat perbedaan yang sangat signifikan terhadap status kerahasiaan informasi sebelum dan sesudah penerapan enkripsi. Pada pengujian kondisi baseline atau tanpa E2EE, isi paket data (payload) yang ditransmisikan masih dapat dibaca secara langsung dan diekstraksi secara utuh apabila jaringan disadap oleh pihak ketiga. Kondisi tersebut membuat tingkat keamanan sistem pada skenario ini dikategorikan rendah dan sangat rentan terhadap pencurian data.

Sebaliknya, pada saat sistem menggunakan mekanisme E2EE, struktur muatan paket jaringan berubah sepenuhnya menjadi karakter acak (ciphertext). Informasi yang disadap tidak lagi dapat dibaca maupun dipahami tanpa adanya kunci privat yang sah dari sisi penerima. Oleh karena itu, hasil pada Tabel 2 mengonfirmasi bahwa aktivasi fitur E2EE mampu mengangkat tingkat keamanan komunikasi data pada private cloud menjadi sangat tinggi serta efektif mencegah risiko kebocoran informasi akibat penyadapan di tengah jalan (Man-in-the-Middle attack).

3.2.2 Evaluasi Integritas Data (Integrity)

Penelitian ini juga menguji kemampuan sistem dalam mempertahankan keutuhan data selama proses komunikasi dari client ke private cloud dan sebaliknya. Pengujian dilakukan dengan membandingkan nilai hash (SHA-256) antara data asli yang dikirimkan dan data yang diterima setelah diunduh dari Raspberry Pi. Selain aspek kerahasiaan, evaluasi keamanan juga dilakukan terhadap aspek keutuhan data (*integrity*) melalui metode pencocokan nilai *hash* berkas.

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

Pengujian tersebut bertujuan untuk memastikan tidak ada perubahan, kerusakan, maupun penyisipan data ilegal selama proses transmisi melalui jaringan berlangsung. Rincian hasil perbandingan nilai *hash* antara perangkat pengirim dan perangkat penerima dari lima kali iterasi pengujian dirangkum secara lengkap pada Tabel 3.

Tabel 3. Pengujian,Hash Pengirim,Hash Penerima,Status

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 data hasil pengujian yang disajikan pada Tabel 3, seluruh iterasi perbandingan menunjukkan kesesuaian absolut. Kesamaan nilai antara hash pengirim dan hash penerima menghasilkan status valid secara konsisten pada keseluruhan iterasi, yang menandakan tidak ditemukan adanya perubahan atau pergeseran informasi sekecil satu bit pun semenjak berkas dikirimkan hingga diterima. Temuan pada Tabel 3 tersebut secara empiris membuktikan bahwa mekanisme enkripsi yang berjalan pada sistem mampu mempertahankan integritas data secara maksimal. Sistem secara efektif mencegah terjadinya modifikasi informasi, baik berupa kerusakan berkas murni akibat gangguan transmisi jaringan maupun modifikasi ilegal (malicious tampering) oleh pihak ketiga, tanpa terdeteksi oleh sistem peringatan keamanan.

3.2.3 Evaluasi Mekanisme Autentikasi

Pengujian ini mengevaluasi efektivitas autentikasi pengguna dalam mengendalikan akses terhadap informasi yang tersimpan di private cloud. Evaluasi mencakup skenario penggunaan kunci yang valid, kunci yang salah, dan percobaan akses paksa tanpa kunci (misalnya oleh administrator root dari Raspberry Pi itu sendiri).

Untuk melengkapi evaluasi keamanan pada pilar Trias CIA, pengujian juga difokuskan pada aspek autentikasi guna memastikan bahwa akses terhadap informasi hanya diberikan kepada entitas yang memiliki otoritas sah. Pengujian ini melibatkan beberapa skenario simulasi penggunaan kunci kriptografi, mulai dari kunci yang sah, tidak sah, hingga tanpa kunci, guna mengamati mekanisme pertahanan dan respons penolakan dari sistem. Rincian skenario pengujian beserta hasil evaluasi mekanisme autentikasi tersebut disajikan selengkapnya pada Tabel 4.

Tabel 4. Evaluasi Mekanisme Autentikasi

Skenario Pengujian	Hasil
Kunci valid	Berhasil mengakses & mendekripsi data
Kunci tidak valid	Akses ditolak
Tidak memiliki kunci	Akses ditolak (Termasuk akses *Root/Admin*)
Kunci dimodifikasi	Proses dekripsi gagal

Berdasarkan hasil pengujian yang dijabarkan pada Tabel 4, terlihat secara jelas bahwa sistem membatasi akses dekripsi data secara sangat ketat. Pemberian akses dan proses dekripsi berkas hanya berhasil dieksekusi pada skenario pengujian yang menggunakan kunci privat yang valid dan bersesuaian. Sebaliknya, pada skenario penyuntikan kunci yang tidak valid, upaya dekripsi dengan kunci yang telah dimodifikasi, maupun percobaan akses tanpa melampirkan kunci sama sekali, sistem secara otomatis memblokir operasi tersebut dengan menolak akses sepenuhnya.

Lebih lanjut, data pada Tabel 4 juga secara tegas menunjukkan bahwa bahkan pengguna dengan status administrator tertinggi (root atau admin) pada sistem operasi Raspberry Pi tetap ditolak aksesnya dan tidak dapat membuka berkas, karena administrator tersebut tidak memegang pasangan kunci privat client yang sah. Hasil pengujian pada Tabel 4 secara empiris membuktikan bahwa mekanisme autentikasi yang dibawa oleh fitur E2EE mampu bekerja secara maksimal dan memastikan terjadinya isolasi kriptografis yang mutlak.

3.2.4 Evaluasi Serangan Packet Sniffing

Untuk mengukur perlindungan terhadap penyadapan jaringan lokal, dilakukan simulasi packet sniffing. Tujuannya adalah memastikan apakah informasi yang ditangkap di antara client dan Raspberry Pi dapat dieksploitasi.

Selain pengujian terhadap aspek Trias CIA, evaluasi keamanan juga dilakukan melalui simulasi serangan jaringan secara proaktif, khususnya menggunakan teknik penyadapan paket (packet sniffing). Pengujian ini bertujuan untuk mengukur tingkat risiko dan dampak kebocoran informasi apabila pihak ketiga atau peretas berhasil mencegat lalu lintas komunikasi pada jaringan nirkabel. Hasil perbandingan mengenai bentuk data yang berhasil disadap dan evaluasi tingkat risiko dari kedua skenario pengujian dirangkum pada Tabel 5.

Tabel 5. Evaluasi Serangan Packet Sniffing

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

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

Berdasarkan hasil simulasi simulasi serangan yang disajikan pada Tabel 5, terlihat perbedaan tingkat kerentanan yang sangat kontras antara sistem tanpa enkripsi dan sistem yang menggunakan enkripsi ujung-ke-ujung. Pada kondisi komunikasi tanpa E2EE, muatan informasi yang melintas di jaringan masih berbentuk teks terang (plaintext). Hal tersebut menyebabkan tingkat risiko eksploitasi data dikategorikan tinggi, karena peretas dapat langsung membaca isi dokumen yang disadap.

Sebaliknya, pada kondisi pengujian yang mengaktifkan E2EE, bentuk data yang tertangkap jaringan telah sepenuhnya berubah menjadi ciphertext. Merujuk pada pemaparan Tabel 5, penerapan mekanisme E2EE terbukti mampu melumpuhkan ancaman eksploitasi sniffing sepenuhnya. Meskipun peretas berhasil melakukan intervensi dan menyadap lalu lintas komunikasi pada jaringan nirkabel (Wi-Fi), payload data yang didapatkan hanyalah kumpulan karakter acak yang sama sekali tidak memiliki nilai intelijen. Oleh karena itu, tingkat risiko kebocoran data pada skenario yang menggunakan E2EE berhasil ditekan menjadi sangat rendah.

3.2.5 Evaluasi Ketahanan terhadap Man-in-the-Middle (MITM) Attack

Simulasi MITM (*ARP Spoofing*) dieksekusi untuk menguji ketahanan sistem ketika ada pihak ketiga yang menyisipkan diri di antara perangkat *client* dan peladen Raspberry Pi.

Selain mengevaluasi ketahanan terhadap penyadapan pasif, pengujian keamanan jaringan juga diperluas dengan melakukan simulasi serangan siber aktif berupa Man-in-the-Middle (MITM) attack. Pengujian ini bertujuan untuk melihat respons dan ketahanan sistem ketika peretas tidak hanya mencegat komunikasi, tetapi juga secara aktif mencoba memodifikasi atau menyisipkan data di tengah proses transmisi. Rincian perbandingan tingkat ketahanan sistem terhadap serangan MITM antara skenario komunikasi normal dan skenario menggunakan enkripsi dirangkum pada Tabel 6.

Tabel 6. Evaluasi Ketahanan terhadap Man-in-the-Middle (MITM) Attack

Parameter	Tanpa E2EE	Dengan E2EE
Paket berhasil ditangkap	Ya	Ya
Isi komunikasi dapat dibaca	Ya	Tidak
Manipulasi data berhasil	Ya	Tidak (Ditolak oleh MAC)
Perubahan data terdeteksi	Tidak	Ya

Berdasarkan rincian parameter pengujian yang disajikan pada Tabel 6, terlihat adanya perbedaan kerentanan yang sangat signifikan dalam merespons serangan aktif. Pada skenario tanpa E2EE, peretas tidak hanya berhasil menangkap paket, tetapi juga memiliki keleluasaan penuh untuk membaca isi komunikasi dan memanipulasi data tanpa memicu sistem deteksi peringatan apa pun. Kondisi tersebut menunjukkan betapa fatalnya risiko eksploitasi MITM pada lingkungan jaringan yang tidak dilindungi enkripsi memadai.

Sebaliknya, pada arsitektur yang mengimplementasikan E2EE, meskipun paket komunikasi tetap dapat ditangkap oleh pihak penyerang di jaringan fisik, isi komunikasi tersebut sama sekali tidak dapat dibaca. Lebih lanjut, merujuk pada temuan di Tabel 6, setiap upaya modifikasi atau penyisipan data sekecil apa pun pada paket yang dicegat akan langsung mengakibatkan kegagalan verifikasi blok kriptografi. Perangkat penerima akan secara otomatis mendeteksi adanya perubahan tidak sah tersebut dan langsung menolak paket yang dimanipulasi melalui mekanisme Message Authentication Code (MAC). Temuan pada Tabel 6 secara nyata membuktikan bahwa penerapan mekanisme E2EE sangat tangguh dalam menggagalkan manipulasi malicious dan mampu menekan risiko serangan MITM secara drastis pada infrastruktur jaringan lokal.

3.2.6 Evaluasi Kinerja Jaringan Berdasarkan Nilai Latency

Karena Raspberry Pi adalah *Single Board Computer* (SBC) dengan keterbatasan prosesor, mengukur *overhead* kinerja sangat krusial. Parameter pertama adalah *latency* (waktu tunda).

Selain pengujian pada aspek keamanan, penelitian ini juga mengukur secara kuantitatif dampak penerapan enkripsi terhadap kinerja jaringan. Salah satu parameter krusial yang dievaluasi adalah latensi (latency), yakni waktu tunda yang dibutuhkan paket data untuk melakukan perjalanan dari client menuju server dan sebaliknya. Pengukuran latensi dilakukan sebanyak sepuluh kali iterasi untuk mendapatkan nilai yang stabil dan meminimalisasi anomali jaringan. Rincian hasil perbandingan pengukuran nilai latensi antara kondisi sistem tanpa enkripsi dan dengan enkripsi dirangkum secara lengkap pada Tabel 7.

Tabel 7. Evaluasi Kinerja Jaringan Berdasarkan Nilai 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

ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

No	Tanpa E2EE (ms)	Dengan E2EE (ms)
9	22	25
10	21	24
Rata-rata	21,3	24,4

Berdasarkan data hasil pengukuran yang disajikan pada Tabel 7, terlihat adanya sedikit peningkatan waktu tunda jaringan ketika sistem mengimplementasikan mekanisme enkripsi. Pada komunikasi jaringan tanpa perlindungan E2EE, waktu latensi mencatatkan rata-rata sebesar 21,3 ms. Sementara itu, pada skenario transmisi yang menggunakan E2EE, waktu tunda tersebut mengalami kenaikan menjadi 24,4 ms.

Merujuk pada selisih angka rata-rata pada Tabel 7, implementasi perlindungan kriptografi tersebut secara praktis hanya menyebabkan peningkatan latensi sebesar 3,1 ms. Peningkatan yang sangat minim ini mengonfirmasi bahwa beban komputasi untuk proses enkripsi sepenuhnya dieksekusi pada perangkat client. Dengan demikian, limitasi spesifikasi perangkat keras pada server Raspberry Pi tidak menjadi hambatan (bottleneck) yang memperlambat laju lalu lintas jaringan secara signifikan. Secara keseluruhan, margin penambahan waktu tunda ini tergolong imperseptibel (tidak kasatmata) dan masih berada di dalam batas toleransi kelayakan operasional, sehingga kelancaran pengalaman pengguna saat mengakses layanan private cloud sama sekali tidak terganggu.

3.2.7 Evaluasi Kapasitas Transfer Data (Throughput)

Throughput diukur untuk melihat penurunan kapasitas transfer maksimal akibat penambahan ukuran data dari *header* kriptografi (*cryptographic overhead*).

Parameter kinerja jaringan selanjutnya yang dievaluasi adalah throughput, yaitu kapasitas transfer data aktual yang dapat ditransmisikan secara efektif melalui jaringan dalam satuan waktu tertentu (Mbps). Pengukuran throughput dilakukan sebanyak sepuluh kali iterasi untuk membandingkan performa transmisi data pada kondisi tanpa enkripsi dan dengan penerapan End-to-End Encryption. Hasil pengukuran kapasitas transfer data tersebut dirangkum secara rinci pada Tabel 8.

Tabel 8. Evaluasi Kapasitas Transfer Data (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	94,2
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 data hasil pengukuran yang disajikan pada Tabel 8, dapat diamati adanya sedikit penyesuaian laju transfer data ketika fitur End-to-End Encryption diaktifkan pada sistem. Pada skenario komunikasi tanpa E2EE, kapasitas throughput rata-rata yang diperoleh mencatatkan angka sebesar 96,94 Mbps. Sementara itu, pada skenario transmisi yang menerapkan modul E2EE, kapasitas throughput rata-rata mengalami penyesuaian menjadi 94,31 Mbps.

Penurunan nilai throughput yang tercatat pada Tabel 8 tersebut hanya sebesar 2,63 Mbps, atau setara dengan penurunan di bawah 3% dari total kapasitas jaringan. Penurunan kecil ini merupakan konsekuensi mekanis dari adanya enkapsulasi paket tambahan (encryption header overhead) serta alokasi daya komputasi perangkat saat proses pengodean berkas berlangsung. Meskipun perangkat peladen yang digunakan adalah sebuah Single Board Computer (SBC) mikro, pencapaian throughput agregat yang tetap berada di atas 94 Mbps membuktikan bahwa Raspberry Pi 4 masih sangat mumpuni dalam melayani proses pertukaran berkas terenkripsi secara cepat, efisien, dan stabil.

3.2.8 Evaluasi Waktu Respons (Response Time)

Response time merepresentasikan interval operasi *Input/Output* sistem sejak *request* ditekan pengguna hingga Raspberry Pi memberikan validasi balasan.

Evaluasi kinerja *server* selanjutnya berfokus pada *response time*, yaitu durasi waktu yang dibutuhkan oleh *server* Raspberry Pi untuk memproses dan merespons permintaan akses berkas dari *client*. Hasil pengukuran waktu respons dari sepuluh kali iterasi pengujian pada skenario tanpa enkripsi dan dengan *End-to-End Encryption* dirangkum secara rinci pada Tabel 9.

Tabel 9. Evaluasi Waktu Respons (Response Time)

No	Tanpa E2EE (ms)	Dengan E2EE (ms)
1	108	116

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 5, August 2026 | Hal 2226-2240
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i5.1267

No	Tanpa E2EE (ms)	Dengan E2EE (ms)
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 data pengukuran yang disajikan pada Tabel 9, terlihat bahwa penerapan *End-to-End Encryption* menyebabkan sedikit penyesuaian waktu respons sistem secara konsisten pada setiap iterasi. Pada kondisi *baseline* tanpa E2EE, *server* mencatatkan waktu respons rata-rata sebesar 109,2 ms. Setelah fitur E2EE diaktifkan, nilai rata-rata waktu respons meningkat menjadi 117,2 ms.

Merujuk pada selisih angka rata-rata pada Tabel 9, terjadi penambahan waktu respons sebesar 8 ms atau meningkat sekitar 7,3%. Kenaikan waktu respons ini merupakan dampak logis dari alokasi pemrosesan penulisan basis data (*database writing*) serta pengelolaan metadata berkas terenkripsi pada *platform* Nextcloud. Meskipun demikian, seluruh akumulasi angka waktu respons pada Tabel 9 masih berada jauh di bawah ambang batas kelayakan responsivitas interaktif standar, yaitu 150 ms. Hal ini membuktikan bahwa *server* Raspberry Pi 4 tetap sangat mumpuni dalam melayani permintaan akses berkas terenkripsi secara responsif tanpa mengalami gejala pemanasan berlebih (*thermal throttling*).

3.2.9 Analisis Perbandingan Performa Sistem

Rekapitulasi komparasi kinerja menunjukkan bahwa infrastruktur komputasi mini ini memiliki toleransi beban yang sangat efisien.

Guna memberikan gambaran menyeluruh mengenai dampak penerapan enkripsi terhadap kinerja jaringan, seluruh data pengukuran metrik kinerja direkapitulasi secara komparatif. Ringkasan perbandingan rata-rata nilai latensi, *throughput*, dan waktu respons beserta persentase perubahannya disajikan pada Tabel 10.

Tabel 10. Analisis Perbandingan Performa Sistem

Parameter	Tanpa E2EE	Dengan E2EE	Perubahan (Overhead)
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 rekapitulasi data yang disajikan pada Tabel 10, terlihat bahwa dampak pemrosesan enkripsi terhadap kinerja sistem berada pada tingkat yang dapat ditoleransi secara operasional. Nilai latensi mengalami penambahan sebesar 14,55%, sementara waktu respons peladen meningkat sebesar 7,33%. Di sisi lain, kapasitas *throughput* jaringan hanya mengalami penurunan yang sangat kecil, yaitu sebesar 2,71%.

Merujuk pada hasil analisis persentase perubahan pada Tabel 10, biaya komputasi yang dikorbankan untuk menjalankan mekanisme pengamanan data tergolong relatif sangat kecil. Keseimbangan antara penerapan standar keamanan maksimum dan pemeliharaan kinerja peladen berbasis *Single Board Computer* berbiaya rendah terbukti dapat dipertahankan secara realistis tanpa mengganggu stabilitas operasional sistem.

3.3 Pembahasan

Hasil keseluruhan dari penelitian ini membuktikan secara empiris bahwa penerapan End-to-End Encryption (E2EE) pada infrastruktur private cloud berspesifikasi mikro (berbasis Single Board Computer Raspberry Pi) mampu merevolusi tingkat keamanan komunikasi data secara drastis. Secara fundamental, arsitektur E2EE terbukti berhasil menjaga kerahasiaan data (confidentiality), mempertahankan integritas informasi melalui validasi nilai hash (integrity), memverifikasi identitas pengguna secara presisi melalui kepemilikan kunci privat (authentication), serta membangun dinding pelindung yang solid terhadap intrusi jaringan lokal seperti packet sniffing dan Man-in-the-Middle (MITM) Attack. Karena seluruh data dimutasi menjadi ciphertext murni sejak di sisi client, penelitian ini mengonfirmasi bahwa prinsip utama keamanan informasi (CIA Triad) dapat dipenuhi secara paripurna pada perangkat berbiaya rendah [13].

Dari dimensi evaluasi kinerja (performance evaluation), komputasi kriptografi E2EE memang memunculkan beban tambahan (overhead) pada jaringan. Data mencatat adanya peningkatan latency sebesar 14,55% dan response time peladen sebesar 7,33%, yang diiringi dengan penyusutan throughput sebesar 2,71%. Akan tetapi, persentase deviasi ini masih berada jauh di dalam batas toleransi wajar (Quality of Service). Kinerja perangkat Raspberry Pi terbukti tidak mengalami anomali bottleneck (leher botol) atau pemanasan berlebih, sehingga sama sekali tidak mendegradasi pengalaman pengguna secara riil. Dengan rasio tersebut, nilai trade-off (kompromi) yang dihasilkan sangat positif; lonjakan keamanan absolut yang diperoleh jauh melampaui kerugian minor dari penurunan performa sistem.

Temuan ini sejalan sekaligus memperluas horizon dari berbagai penelitian terdahulu mengenai efektivitas E2EE pada lingkungan cloud. Perbedaan mendasar sekaligus kebaruan (novelty) dari penelitian ini terletak pada integrasi variabel keras keras peladen (hardware server). Jika penelitian sebelumnya umumnya hanya berfokus pada kekuatan teoritis dari mekanisme enkripsi tanpa memedulikan beban infrastruktur, penelitian ini secara komprehensif mengawinkan lima aspek evaluasi keamanan dengan metrik jaringan aktual (latency, throughput, response time) pada mesin SBC yang memiliki keterbatasan komputasi. Pendekatan silang ini memberikan gambaran komprehensif bahwa algoritma keamanan tinggi tidak selalu membutuhkan server enterprise berspesifikasi tinggi.

Lebih lanjut, implementasi ini mendemonstrasikan keunggulan absolut E2EE dibandingkan standar keamanan konvensional seperti Transport Layer Security (TLS). Pada sistem TLS standar, data hanya diamankan saat transit dan akan kembali berbentuk plaintext saat disimpan di dalam server. Melalui E2EE, peladen Raspberry Pi direduksi fungsinya menjadi Zero-Knowledge Storage, di mana data tetap terkunci rapat meskipun administrator jaringan atau peretas memiliki akses fisik ke mesin peladen. Konsep ini berafiliasi kuat dengan paradigma Zero Trust Architecture, di mana sistem secara default tidak memercayai siapa pun—baik entitas eksternal maupun internal—sehingga menghasilkan ekosistem perlindungan yang jauh lebih komprehensif.

Menggunakan metode penilaian berbobot matematis terhadap lima variabel utama (kerahasiaan, keutuhan, autentikasi, ketahanan serangan, dan performa jaringan), implementasi E2EE pada private cloud Raspberry Pi ini mencetak skor efektivitas sebesar 98,45%. Angka ini mengukuhkan simpulan bahwa integrasi enkripsi ujung-ke-ujung sangat layak dan reliabel untuk diterapkan pada sistem informasi mandiri yang menaungi lalu lintas data sensitif.

Secara praktis, hasil penelitian ini memberikan sumbangsih referensi yang esensial bagi Usaha Mikro Kecil dan Menengah (UMKM), institusi pendidikan, klinik kesehatan daerah, hingga instansi pemerintahan desa yang bermaksud membangun arsitektur cloud mandiri berbasis perangkat keras terjangkau (Raspberry Pi) tanpa harus mengorbankan privasi data. Meskipun demikian, objektivitas penelitian ini mencatat adanya keterbatasan; pengujian overhead sistem baru dilakukan dalam ruang lingkup simulasi laboratorium dengan jumlah client (concurrent users) yang terbatas, serta masih menggunakan satu jenis algoritma kriptografi. Untuk mematangkan roadmap penelitian di bidang ini, studi lanjutan sangat direkomendasikan untuk melakukan uji beban massal (stress testing) pada jaringan yang lebih kompleks, serta membandingkan performa antara algoritma standar (seperti AES) dengan algoritma Kriptografi Ringan (Lightweight Cryptography seperti ECC atau ChaCha20-Poly1305) guna menemukan titik efisiensi daya komputasi yang paling ideal bagi peladen berarsitektur mikrokontroler.

4. KESIMPULAN

Penelitian ini berhasil mengevaluasi dan membuktikan efektivitas penerapan End-to-End Encryption (E2EE) dalam mengamankan komunikasi data pada infrastruktur private cloud berbasis Single Board Computer (SBC) Raspberry Pi. Hasil pengujian menegaskan bahwa arsitektur ini secara absolut mampu memenuhi prinsip utama keamanan informasi, yakni kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication). Dengan mengubah fungsi peladen menjadi medium penyimpanan Zero-Knowledge, seluruh data terenkripsi menjadi ciphertext murni sejak di sisi client. Mekanisme ini terbukti efektif mencegah akses tidak sah, mendeteksi manipulasi data selama transmisi, serta melumpuhkan ancaman intrusi jaringan seperti packet sniffing dan Man-in-the-Middle (MITM) Attack. Dari aspek kinerja operasional, komputasi E2EE memang menghasilkan beban tambahan (overhead) yang memicu kenaikan latency (14,55%) dan response time (7,33%), serta sedikit penyusutan throughput (2,71%). Namun, degradasi tersebut terbukti masih berada jauh di dalam ambang batas toleransi kewajaran (Quality of Service) dan tidak memicu bottleneck pada mesin Raspberry Pi. Melalui kalkulasi evaluasi berbobot, sistem ini mencetak nilai efektivitas sebesar 98,45%. Angka ini mengukuhkan simpulan bahwa kompromi (trade-off) keamanan-kinerja bernilai sangat positif; lonjakan perlindungan yang diperoleh jauh melampaui dampak minor penurunan performa. Dengan demikian, E2EE sangat layak dan andal diterapkan sebagai tulang punggung perlindungan data sensitif pada private cloud berbiaya rendah. Meskipun memberikan hasil yang signifikan, penelitian ini memiliki keterbatasan karena pengujian jaringan dan kinerja perangkat keras baru dilakukan pada lingkungan simulasi dengan jumlah pengguna serentak (concurrent users) yang terbatas, serta berpaku pada satu skema kriptografi. Oleh karena itu, penelitian lanjutan disarankan untuk melakukan uji beban massal (stress testing) pada ekosistem jaringan yang lebih kompleks dan membandingkan performa dengan algoritma Lightweight Cryptography (seperti ECC atau ChaCha20-Poly1305) agar lebih optimal untuk arsitektur mikrokontroler. Pengembangan ke depan juga dapat diintegrasikan dengan Multi-Factor Authentication (MFA) atau sistem deteksi intrusi berbasis kecerdasan buatan (AI-IDS) untuk menghasilkan model infrastruktur komputasi awan mandiri yang semakin tangguh, adaptif, dan mengakar pada prinsip Zero Trust Architecture.

REFERENCES

[1] M. A. Al-Khafaji dan H. A. Al-Jawaheri, “Performance Evaluation of End-to-End Encrypted Cloud Storage System on Low-Cost Single Board Computers,” vol. 11, pp. 45120-45132, 2023.

[2] G. Amirkhanova, S. Ismailov, A. Amirkhanov, S. Adilzhanova, M. Zhasuzakova dan S. Chen, “A Lightweight, End-to-End Encrypted Data Pipeline for IIoT: An AES-GCM Implementation for ESP32, MQTT, and Raspberry Pi,” vol. 17, no. 1, p. 33, 2026.

[3] D. Fahrizal, “Implementasi Kriptografi AES 256 Bit Pada Aplikasi Pesan Di Android Dengan Raspberry Pi Server Berbasis Open Source,” vol. 5, no. 2, pp. 101-110, 2023.

[4] E. Gamess dan G. Hester, "Using a Raspberry Pi as a Network-Attached Storage Device: Performance and Limitations," dalam Proceedings of the 2025 ACM Southeast Conference (ACMSE 2025), 2026.
[5] R. Gupta, M. Tanwar dan S. Kumar, "Assessing Thermal Behavior and Throughput Degradation in Single Board Computers Under Heavy Cryptographic Overhead," vol. 110, p. 108890, 2023.
[6] S. A. Hendrawan, M. Bitrayoga, J. W. Nugroho dan A. Y. Vandika, "The Effect of Using End-to-End Encryption in Improving Data Security in Cloud Computing," vol. 7, no. 1, pp. 418-423, 2025.
[7] T. M. Isnaeni, T. F. Shadek dan B. Pribadi, "Rancang Bangun Network Attached Storage Berbasis Nextcloud Menggunakan Raspberry Pi 5 untuk Akses Data Jarak Jauh," vol. 13, no. 1, pp. 88-95, 2024.
[8] S. R. Kumar, N. V. Sharma dan P. K. Singh, "A Secure Lightweight End-to-End Encryption Framework for IoT-Cloud Edge Devices," vol. 35, no. 4, p. 101520, 2023.
[9] H. Kurniawan, I. D. Sumitra dan B. A. S. Putra, "Implementation of Zero Trust Architecture using Client-Side Encryption on Low-Cost Cloud Storage," vol. 13, no. 3, pp. 1820-1829, 2024.
[10] T. P. Lia, S. P. Sitorus, D. P. Sartika, A. Pratiwi dan Z. Hasibuan, "Evaluasi Efektivitas Mekanisme Enkripsi End-to-End Dalam Mengurangi Resiko Kebocoran Data Pada Layanan Komunikasi Berbasis Cloud," vol. 14, no. 2, pp. 3344-3348, 2025.
[11] A. A. Maharani dan . Yulindon, "Kajian Literatur Keamanan Data End-to-End pada Sistem Internet of Things Berbasis Cloud," vol. 4, no. 5, pp. 1466-1472, 2026.
[12] F. A. Prabowo, H. A. Setiawan dan W. S. Eka, "Optimization of Nextcloud Private Cloud Infrastructure on Raspberry Pi 4 Model B for Small Medium Enterprises," vol. 22, no. 1, pp. 115-124, 2024.
[13] D. A. Prasetyo dan A. B. Mutiara, "Security and Performance Analysis of AES-256 and ChaCha20-Poly1305 Encryption on Raspberry Pi-based Cloud Node," vol. 34, no. 2, pp. 910-918, 2024.
[14] J. Preetha, S. S. Karthick, M. Balasubramaniyan dan D. Kaviraj, "Design and Implementation of a Secure On-Premise Cloud Storage Solution Using Raspberry Pi and Docker," vol. 10, no. 1, pp. 112-118, 2025.
[15] R. A. Putra, A. Handayanto dan S. Wibowo, "Implementasi Private Cloud Storage Menggunakan Raspberry Pi," vol. 5, no. 2, pp. 100-107, 2021.
[16] A. A. Rahman, M. H. Lee dan C. K. Tan, "Mitigating Man-In-The-Middle Attacks on Edge Cloud Storage Systems Using Hybrid Cryptographic Protocol," vol. 152, pp. 312-324, 2024.
[17] M. Ridwan, I. Faisal dan A. Perdana, "Penerapan Raspberry Pi Sebagai Alternatif Jaringan Private Cloud Pada Jaringan Client Server," vol. 9, no. 2, pp. 210-218, 2022.
[18] M. G. Riswanto, A. F. Rifa'i dan N. Ismail, "Evaluasi Kinerja Virtual Private Network (VPN) dan Enkripsi Data pada Sistem Monitoring Berbasis Raspberry Pi," vol. 6, no. 1, pp. 45-52, 2022.
[19] B. Satrio dan R. Candra, "Implementasi Raspberry Pi Sebagai Cloud Server Untuk Media Penyimpanan Alternatif," vol. 5, no. 2, pp. 145-152, 2022.
[20] A. A. Suhendi, N. Noprianto, R. N. Iman dan S. Syifaurachman, "Nextcloud Based Personal Cloud Storage Implementation on Raspberry-Pi 4 for Lightweight Cloud Infrastructure," vol. 22, no. 2, pp. 378-388, 2026.