Benchmarking Kinerja Enkripsi AES dan ECC untuk Keamanan Komunikasi Digital pada *Cloud System*

Benchmarking the Performance of AES and ECC Encryption for Secure Digital Communication in Cloud Systems

[1]Damas Alfiqhyanto*, [2]Eka Ardhianto
[1,2]Magister Teknologi Informasi, Teknologi Informasi dan Industri, Universitas Stikubank Semarang
[1,2]Jl. Tri Lomba Juang, Mugassari, Kecamatan Senarang Selatan
Kota Semarang, Jawa Tengah, Indonesia
*e-mail: damas..alfiqh@gmail.com

(***received*:** 23 May 2026, ***revised*:** 1 June 2026, ***accepted*:** 2 June 2026)

Abstrak

Penelitian ini membandingkan kinerja Advanced Encryption Standard (AES) dan Elliptic Curve Cryptography (ECC) dalam pengamanan komunikasi digital pada lingkungan cloud computing. Pendekatan kuantitatif eksperimental-komparatif dilakukan dengan dataset percakapan konseling sebanyak 9.036 data valid yang dikelompokkan ke dalam lima kuintil berdasarkan panjang karakter, kemudian disampel 1.805 data secara acak berstrata. Pengujian dilakukan pada Google Colab dengan Python 3.10 menggunakan metrik waktu enkripsi-dekripsi, throughput, penggunaan CPU, konsumsi memori, dan entropi ciphertext. Hasil menunjukkan bahwa AES unggul dalam kecepatan (waktu enkripsi rata-rata 0.00013 detik) dan efisiensi memori (0.83-0.86 kb), sedangkan ECC lebih sesuai untuk pertukaran kunci dengan keamanan tinggi meskipun overhead komputasi lebih besar.

Kata kunci: AES, komputasi awan, kriptografi, keamanan data, ECC

Abstract

This study compares the performance of the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) for securing digital communications in cloud computing environments. A quantitative experimental-comparative approach was employed using a counseling conversation dataset comprising 9,036 valid records. The dataset was divided into five quintiles based on text length (number of characters), from which 1,805 samples were selected through stratified random sampling. The experiments were conducted in Google Colab using Python 3.10, and the algorithms were evaluated in terms of encryption and decryption time, throughput, CPU utilization, memory consumption, and ciphertext entropy. The results indicate that AES outperformed ECC in computational efficiency, achieving an average encryption time of 0.00013 seconds while requiring only 0.83–0.86 kB of memory. In contrast, ECC demonstrated superior suitability for secure key exchange despite its higher computational overhead. These findings suggest that AES is the preferred choice for efficient data encryption in cloud-based digital communication systems, whereas ECC is more appropriate for cryptographic key exchange in applications requiring a higher level of security.

Keywords: *AES, cloud system, cryptography, data security, ECC*

1 Pendahuluan

Di era digital kontemporer, data telah menjadi aset strategis fundamental, melampaui nilai aset fisik, terutama di sektor keuangan, kesehatan, administrasi publik, dan edukasi. Infrastruktur digital berbasis internet dan cloud computing memungkinkan diseminasi data instan, namun juga meningkatkan vektor ancaman siber [1]. Ancaman seperti phishing, malware, sniffing, dan ransomware menempatkan data dalam risiko permanen, dengan dampak multidimensional termasuk kerugian finansial, reputasi, dan stabilitas infrastruktur [2]. Proyeksi global menunjukkan kerugian ekonomi akibat kejahatan siber akan terus meningkat, menuntut adopsi teknologi keamanan yang kuat dan adaptif [3].

 ISSN:2302-8149
e-ISSN:2540-9719

Kriptografi menjadi pilar utama keamanan informasi melalui prinsip CIA Triad: kerahasiaan, integritas, dan autentikasi. AES, sebagai standar industri simetris, menawarkan enkripsi bulk data efisien dengan kunci 128-256 bit, namun menghadapi masalah distribusi kunci [4][2]. ECC menyediakan solusi distribusi kunci asimetris dengan efisiensi ruang kunci tinggi dan cocok untuk lingkungan terbatas, seperti IoT [5][6].

Pendekatan AES-ECC memanfaatkan kekuatan masing-masing: AES untuk enkripsi data dan ECC untuk pertukaran kunci, mengurangi waktu komputasi hingga 40% dan meningkatkan throughput sistem cloud [7][8]. Studi pada enkripsi citra, komunikasi real-time, jaringan 5G, dan IoT menegaskan bahwa model ECC mempertahankan kecepatan, efisiensi kunci, dan keamanan tinggi [9][10].

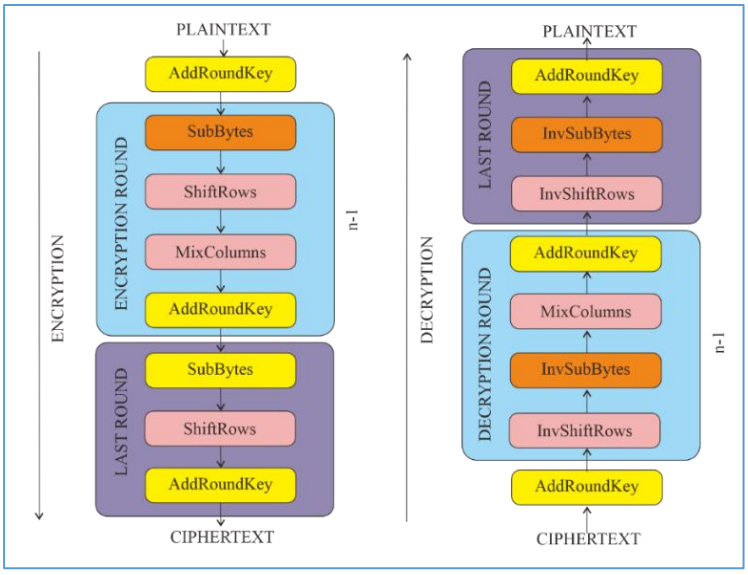
Penelitian ini bertujuan untuk mengevaluasi kinerja algoritma AES dan ECC secara empiris dalam berbagai skenario, dengan fokus pada metrik throughput, latensi, penggunaan CPU, dan konsumsi memori. Signifikansi penelitian terletak pada penyediaan benchmark objektif yang dapat menjadi acuan optimalisasi arsitektur keamanan digital, meningkatkan efisiensi enkripsi, manajemen kunci, dan perlindungan data dalam ekosistem cloud dan IoT yang kompleks.

Meskipun banyak penelitian terdahulu membahas AES dan ECC secara terpisah, sebagian besar masih terbatas pada analisis teoretis atau pengujian dengan data sintetis [11]. Studi empiris yang menggunakan dataset real-world dengan variasi ukuran input terstruktur (seperti teks percakapan alami) masih jarang dilakukan. Penelitian ini mengisi celah tersebut dengan melakukan benchmarking komparatif menggunakan dataset percakapan konseling real-world sebanyak 9.036 data yang dikelompokkan berdasarkan kuintil panjang karakter, sehingga memberikan wawasan granular tentang hubungan antara ukuran data dan performa algoritma di lingkungan cloud.

2 Tinjauan Literatur

Keamanan data pada cloud computing menjadi isu yang semakin penting seiring meningkatnya volume pertukaran informasi digital dan kompleksitas ancaman siber. Dalam konteks ini, kriptografi berperan sebagai mekanisme utama untuk menjaga kerahasiaan, integritas, dan autentikasi data selama penyimpanan maupun transmisi. AES dan ECC merupakan dua algoritma yang paling relevan dalam penelitian kriptografi modern karena keduanya menawarkan karakteristik performa yang berbeda dalam hal kecepatan, efisiensi sumber daya, dan tingkat keamanan,

Advanced Encryption Standard (AES) adalah algoritma blok simetris yang diadopsi NIST pada tahun 2001. AES memproses data dalam blok 128-bit dengan jumlah putaran 10, 12, atau 14 tergantung panjang kunci (128, 192, atau 256 bit). Keunggulan utamanya adalah kecepatan tinggi dan efisiensi enkripsi data dalam jumlah besar, sehingga sangat sesuai untuk aplikasi cloud yang membutuhkan throughput tinggi dan latensi rendah [12].

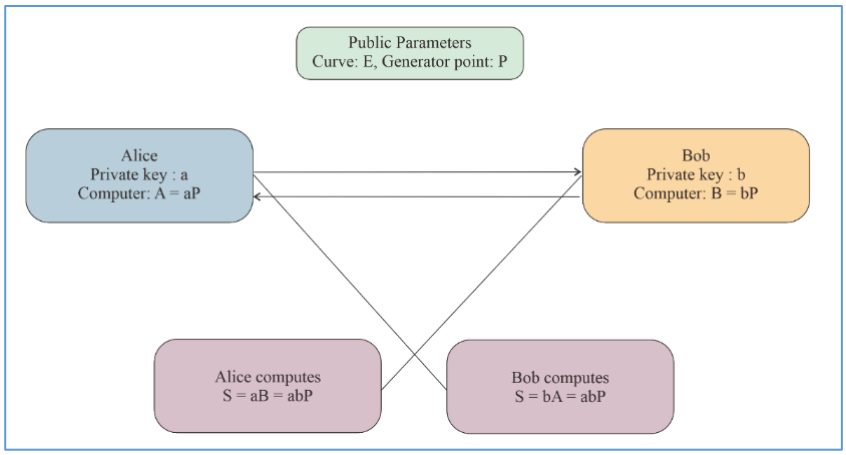


Gambar 1 Alur proses algoritma AES

 ISSN:2302-8149
e-ISSN:2540-9719

Gambar 1 menggambarkan keseluruhan proses transformasi state pada AES, memperlihatkan bagaimana setiap operasi dalam tiap putaran berkontribusi terhadap mekanisme keamanan inti berupa *confusion* dan *diffusion*. Kombinasi kedua sifat ini berfungsi untuk menyamarkan hubungan antara plaintext, ciphertext, dan kunci, sehingga meningkatkan ketahanan algoritma terhadap berbagai bentuk serangan kriptanalisis [13].

Elliptic Curve Cryptography (ECC) merupakan algoritma asimetris yang keamanannya didasarkan pada masalah matematis *Elliptic Curve Discrete Logarithm Problem* (ECDLP). ECC mampu memberikan tingkat keamanan setara dengan RSA menggunakan ukuran kunci yang jauh lebih kecil, sehingga sangat efisien dalam hal konsumsi bandwidth dan daya komputasi [14][15].



Gambar 2 Alur proses algoritma ECC

Terlihat pada Gambar 2 dalam protokol ini, setiap pihak, misalnya Alice dan Bob menghasilkan kunci privat berupa bilangan acak besar, kemudian mengoperasikan bilangan ini terhadap sebuah titik generator kurva elips untuk membentuk kunci publik. Proses ini menghasilkan dua pasangan kunci. Alice memiliki kunci privat a dan kunci publik $A = aP$, sedangkan Bob memiliki kunci privat b dan kunci publik $B = bP$. Setelah kedua pihak saling bertukar kunci publik, masing-masing dapat menghitung nilai rahasia bersama yang identik melalui operasi titik. Alice menghitung $S = aB = abP$ dan Bob menghitung $S = bA = abP$. Dengan demikian, *shared secret* diperoleh tanpa pernah mengirimkan kunci privat melalui jaringan. menegaskan bahwa efektivitas ECDH berasal dari kesulitan matematis *Elliptic Curve Discrete Logarithm Problem (ECDLP)*, yang membuat penyerang praktis mustahil menurunkan nilai $a$atau $b$dari kunci publik A atau B.

Penelitian terdahulu banyak membahas AES dan ECC secara terpisah, namun masih terbatas dalam hal benchmarking empiris yang menggunakan data real-world dengan variasi ukuran input yang terstruktur[11]. Sebagian studi lebih menitikberatkan pada aspek teoretis atau keamanan matematis, bukan pada evaluasi performa komputasi secara rinci[16][17]. Oleh karena itu, penelitian ini menempatkan AES dan ECC sebagai dua algoritma utama yang dibandingkan secara langsung menggunakan dataset percakapan nyata yang dikelompokkan berdasarkan kuintil panjang teks, sehingga hubungan antara ukuran data dan performa algoritma dapat dianalisis lebih mendalam.

3 Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental komparatif dengan tujuan melakukan performance benchmarking terhadap algoritma Advanced Encryption Standard (AES) dan Elliptic Curve Cryptography (ECC). Desain penelitian dirancang untuk menghasilkan data empiris yang valid, reliabel, dan dapat direproduksi dalam lingkungan cloud[18][17].

3.1 Objek dan Data Penelitian

Objek penelitian adalah kinerja komputasi algoritma kriptografi pada simulasi komunikasi digital di cloud. Dataset yang digunakan berasal dari 9.036 rekaman percakapan konseling (client-therapist) yang telah divalidasi. Data ini dipilih karena merepresentasikan teks berbahasa alami dengan variasi

 ISSN:2302-8149
e-ISSN:2540-9719

panjang yang realistis, sehingga cocok untuk menguji skalabilitas algoritma pada komunikasi digital sehari-hari.

Dataset dikelompokkan menjadi lima kuintil berdasarkan panjang karakter untuk memungkinkan analisis granular terhadap pengaruh ukuran pesan. Dari total populasi, diambil sampel sebanyak 1.805 data atau setara 20% sample acak berstrata per kuintil. Teknik sampling ini memastikan representativitas dan mengurangi bias.

3.2 Lingkungan dan Peralatan Pengujian

Pengujian dilakukan pada platform Google Colab dengan spesifikasi runtime Python 3.10, CPU Intel Xeon 2 vCPU, RAM 13 GB, dan sistem operasi Linux. Pemilihan Google Colab didasarkan pada kemampuannya menyediakan lingkungan yang konsisten, memudahkan replikasi eksperimen, serta merepresentasikan komputasi cloud yang terkontrol. Dalam pengujian ini, library utama yang digunakan meliputi *cryptography* versi stabil, yang memanfaatkan backend OpenSSL untuk enkripsi, serta *psutil* untuk memantau penggunaan sumber daya sistem. Seluruh pengujian dijalankan dalam kondisi idle untuk meminimalkan interferensi eksternal, sehingga hasil yang diperoleh mencerminkan kinerja algoritma yang objektif dan dapat direproduksi.

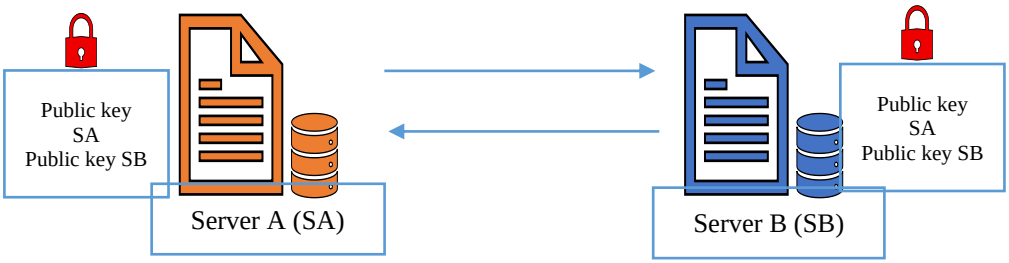
3.3 Implementasi Algoritma

AES diimplementasikan menggunakan mode operasi Cipher Block Chaining (CBC) dengan skema padding PKCS#7 untuk memastikan data yang dienkripsi memiliki panjang yang sesuai dengan ukuran blok. Pada setiap proses enkripsi, digunakan Initialization Vector (IV) yang dibangkitkan secara acak melalui fungsi os.urandom() agar setiap ciphertext yang dihasilkan memiliki tingkat keacakan yang tinggi. Pengujian dilakukan pada tiga variasi ukuran kunci, yaitu AES-128, AES-192, dan AES-256, untuk menganalisis pengaruh panjang kunci terhadap performa enkripsi dan dekripsi[19].

Sementara itu, ECC diimplementasikan kurva eliptik standar NIST, yaitu SECP256R1 dan SECP521R1. Implementasi mencakup pembangkitan pasangan kunci (private-public key pair) dan operasi titik pada kurva eliptik untuk enkripsi/dekripsi serta pertukaran kunci melalui ECDH. Penggunaan dua kurva tersebut dimaksudkan untuk membandingkan kinerja ECC pada tingkat keamanan dan kompleksitas komputasi yang berbeda[20].

3.4 Skenario Pengujian

Skenario pengujian dirancang untuk mengevaluasi kinerja dan efisiensi algoritma enkripsi secara menyeluruh. Pada pengujian enkripsi-dekripsi teks, setiap sampel data diproses menggunakan seluruh algoritma dan variasi ukuran kunci yang telah ditentukan, sehingga memungkinkan perbandingan performa yang komprehensif. Selain itu, dilakukan simulasi komunikasi *server-to-server* dengan membangun dua entitas virtual, yaitu Server A dan Server B, dalam satu notebook Google Colab untuk merepresentasikan interaksi end-to-end yang realistis dalam lingkungan cloud. Untuk meningkatkan keandalan data, setiap pengujian diulang minimal sepuluh kali, sehingga diperoleh nilai rata-rata yang lebih stabil dan meminimalkan efek noise pada pengukuran kinerja.



Gambar 3 Simulasi Server-to-Server

3.5 Matrik Kinerja

Metrik yang akan diukur dan dianalisis adalah variabel terikat dalam penelitian ini, yang mencerminkan efektivitas dan efisiensi algoritma.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 1 Matrik kinerja

Performa	Fokus Algoritma	Keterangan
Waktu Komputasi	Waktu yang dibutuhkan untuk menyelesaikan proses enkripsi/dekripsi data atau pertukaran kunci	AES (Enkripsi & Dekripsi), ECC (Enkripsi & Dekripsi atau Pertukaran Kunci)
Penggunaan Memori (*Memory Usage*)	Jumlah memori yang dialokasikan selama proses kriptograf	AES dan ECC
Ukuran Kunci (*Key Size)*	Digunakan sebagai variabel untuk mengukur efisiensi algoritma dalam mencapai tingkat keamanan tertentu	AES (128, 192, 256 bit), ECC (256, 521 bit)
Nilai *Entropy*	Mengukur tingkat keacakan kunci, yang berhubungan dengan keamanan	AES dan ECC

3.6 Teknik Analisa Data

Analisis dilakukan secara komparatif antar algoritma, variasi ukuran kunci, dan antar kuintil menggunakan statistik deskriptif. Visualisasi grafik digunakan untuk mengidentifikasi pola dan tren performa.

4 Hasil dan Pembahasan

Pada Tabel 2 dibawah ini menyajikan rangkuman rata-rata metrik performa, penggunaan sumber daya, dan kualitas keluaran untuk setiap metode enkripsi yang dianalisis, dibagi berdasarkan kelompok kuintil (Kuintil) dari dataset yang digunakan. Kolom Metode menunjukkan jenis algoritma enkripsi yang diterapkan. Kolom Waktu Enkripsi dan Waktu Dekripsi mencatat durasi proses enkripsi dan dekripsi dalam satuan detik dengan presisi hingga enam angka di belakang koma, memberikan gambaran mengenai performa waktu dari setiap metode untuk setiap kuintil. Kolom Memory Enkripsi dan Memory Dekripsi menunjukkan jumlah memori yang digunakan selama proses enkripsi dan dekripsi dalam satuan kilobyte, juga dengan presisi enam angka di belakang koma, sehingga memungkinkan pemantauan konsumsi sumber daya untuk setiap kuintil.

Tabel 2 Rata-rata matrik per metode

Metode	Kuintil	Waktu Enkripsi	Waktu Dekripsi	Memory Enkripsi	Memory Dekripsi	CPU Enkripsi byte/detik	CPU Dekripsi byte/detik	Entropy
AES-128	0	0,000129	0,000122	0,832644	0,835699	793397,16	775295,27	5,363804
AES-128	1	0,000129	0,000116	0,832737	0,835277	796341,60	779106,12	5,43128
AES-128	2	0,000132	0,000123	0,838444	0,844008	849795,03	830329,76	5,536174
AES-128	3	0,000126	0,000121	0,845470	0,852098	927193,94	910339,44	5,665278
AES-128	4	0,000132	0,000120	0,864967	0,888205	1052064,42	1032292,17	5,721453
AES-192	0	0,000125	0,000118	0,832655	0,835615	802559,24	776254,41	5,371878
AES-192	1	0,000127	0,000118	0,832755	0,835259	799955,19	777711,50	5,437372
AES-192	2	0,000133	0,000121	0,838530	0,843987	854193,95	826661,33	5,544694
AES-192	3	0,000128	0,000118	0,845495	0,852086	931746,59	905821,56	5,669843
AES-192	4	0,000124	0,000118	0,864953	0,888141	1063117,17	1023237,25	5,727386
AES-256	0	0,000127	0,000126	0,832548	0,835538	790356,46	778195,36	5,368020
AES-256	1	0,000126	0,000123	0,832737	0,835237	801320,41	779476,73	5,433438
AES-256	2	0,000127	0,000128	0,838444	0,843960	850350,62	831416,32	5,540960
AES-256	3	0,000127	0,000123	0,845470	0,852070	938000,69	911261,88	5,665219
AES-256	4	0,000125	0,000128	0,864873	0,888088	1061550,35	1031815,49	5,723716
ECC-256	0	0,000785	0,000517	1,256429	0,851574	115734,06	183777,27	5,364847
ECC-256	1	0,000780	0,000516	1,241496	0,849840	116497,99	185456,74	5,431681
ECC-256	2	0,000805	0,000538	1,311555	0,853862	123814,93	196629,36	5,538669

 ISSN:2302-8149
e-ISSN:2540-9719

ECC-256	3	0,000775	0,000508	1,197347	0,855037	136321,26	218073,38	5,664386
ECC-256	4	0,000784	0,000511	1,406938	0,885314	154887,15	246279,55	5,721528
ECC-521	0	0,001699	0,001046	1,404432	0,886216	55194,14	90709,81	5,368073
ECC-521	1	0,001687	0,001031	1,395900	0,884803	55634,41	91901,43	5,435010
ECC-521	2	0,001758	0,001080	1,446480	0,887969	58788,54	96672,60	5,540357
ECC-521	3	0,001670	0,001021	1,666857	0,889329	65089,82	107232,1	5,667483
ECC-521	4	0,001697	0,001045	1,456910	0,919967	73493,76	120908,44	5,724105

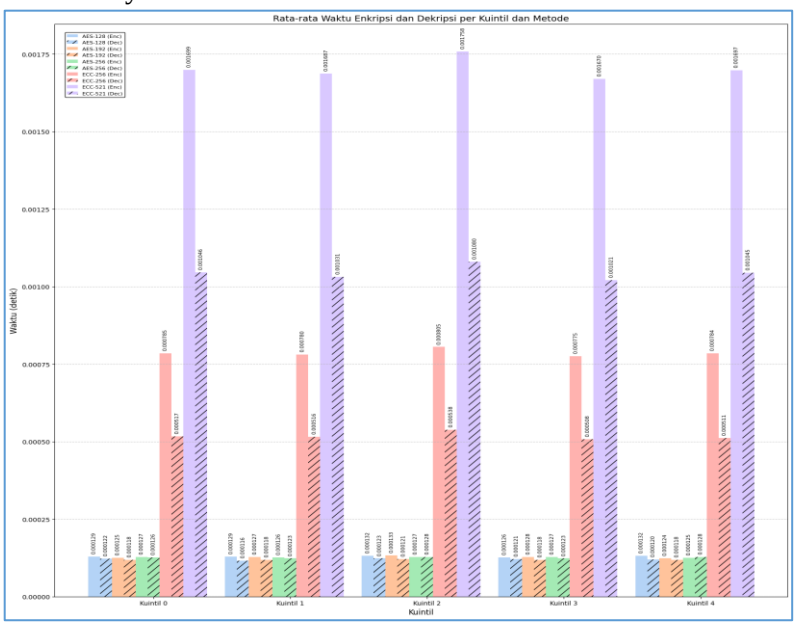
Hasil pengujian menunjukkan bahwa AES secara konsisten lebih cepat dibanding ECC pada seluruh skenario yang terlihat pada Gambar 4. Waktu enkripsi dan dekripsi AES berada pada orde mikrodetik, sedangkan ECC memerlukan waktu yang lebih besar karena operasi matematika pada kurva eliptik jauh lebih kompleks daripada transformasi blok pada AES. Pada data yang lebih panjang, perbedaan ini semakin terasa karena ECC mengalami peningkatan overhead komputasi yang lebih signifikan.

Penggunaan memori AES jauh lebih efisien dan stabil dibanding ECC. ECC membutuhkan memori tambahan untuk menangani operasi titik pada kurva eliptik dan representasi bilangan besar, sehingga konsumsi memorinya cenderung lebih tinggi, dimana hal itu tersaji pada Gambar 5. Dalam lingkungan cloud dengan banyak sesi paralel, perbedaan ini dapat berdampak signifikan terhadap skalabilitas sistem.

Penggunaan CPU juga memperlihatkan pola yang menarik. AES cenderung menggunakan CPU secara konsisten karena prosesnya sederhana dan repetitif, sementara ECC menunjukkan konsumsi CPU yang lebih rendah pada beberapa kondisi enkripsi, tetapi meningkat pada proses dekripsi dan kurva yang lebih besar. Ini memperlihatkan bahwa ECC bukan algoritma yang ideal untuk bulk encryption, tetapi tetap sangat berguna untuk key exchange yang aman.

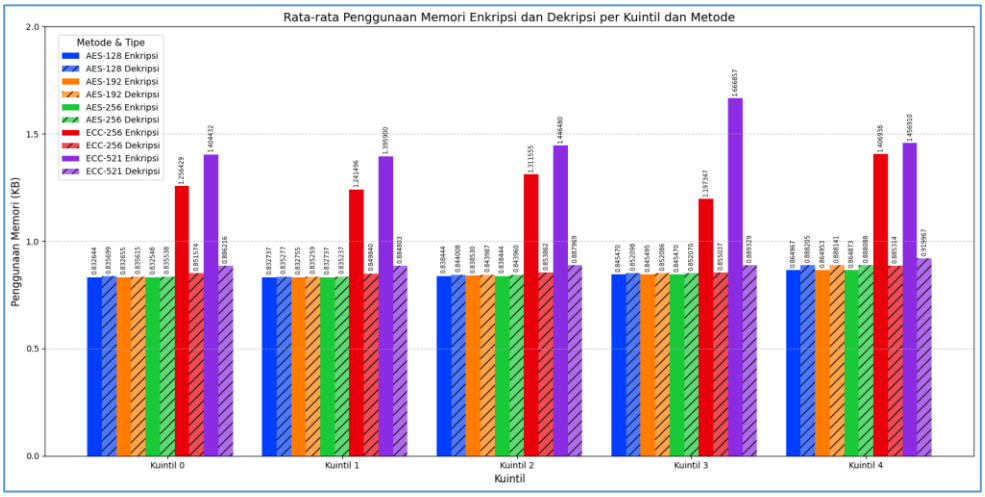
Analisis lebih lanjut terhadap variasi ukuran kunci semakin menegaskan temuan tersebut. Pada AES, peningkatan panjang kunci dari 128-bit ke 256-bit tidak menimbulkan penurunan kinerja yang signifikan dan bahkan cenderung meningkatkan throughput, yang mengindikasikan skalabilitas yang baik. Sebaliknya, ECC lebih sensitif terhadap perubahan ukuran kunci, di mana penggunaan kurva eliptik dengan parameter lebih besar menyebabkan peningkatan waktu enkripsi yang substansial.

Nilai entropi di Tabel 2 (5.36-5.72) dihitung berdasarkan distribusi karakter, sedangkan visualisasi Gambar 6 (7-7.7) menunjukkan entropi per byte pada ciphertext (skala maksimum 8). Meskipun demikian nilai entropi ciphertext pada seluruh metode berada pada kisaran tinggi dan relatif seragam. Artinya, semua algoritma berhasil menghasilkan ciphertext yang acak dan sulit diprediksi. Perbedaan performa utama bukan terletak pada kualitas keamanan output, melainkan pada efisiensi eksekusi dan kebutuhan sumber daya sistem.



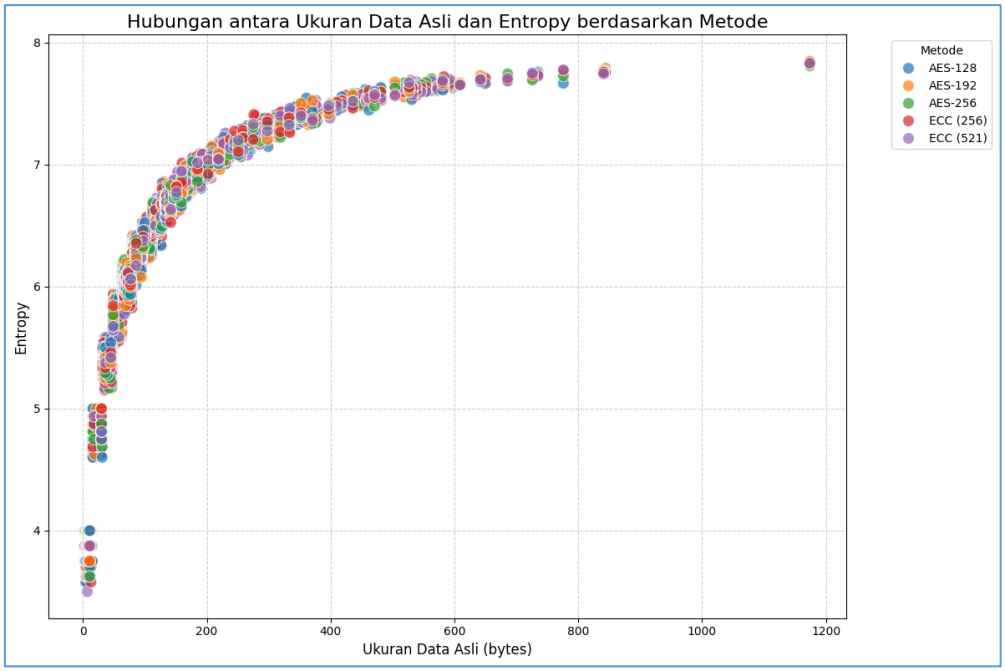
Gambar 4 Rata-rata waktu enkripsi dan dekripsi

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 5 Rata-rata Penggunaan Memory

Kemudian Gambar 6 menunjukkan hubungan antara ukuran data asli dan entropi pada setiap metode enkripsi. Seluruh metode yang diuji, yaitu AES-128, AES-192, AES-256, serta ECC-256 dan ECC-521, menghasilkan nilai entropi tinggi pada kisaran 7-7,7 dari maksimum 8, yang menunjukkan ciphertext memiliki tingkat keacakan yang baik. Nilai entropi juga relatif stabil terhadap variasi ukuran data, sehingga dapat disimpulkan bahwa kualitas randomisasi output tidak dipengaruhi secara signifikan oleh panjang plaintext. Selain itu, tidak terdapat perbedaan mencolok antar metode dalam pola entropi, sehingga dari aspek keacakan, seluruh algoritma sama-sama efektif dalam menyamarkan pola data asli. Temuan ini menegaskan bahwa perbedaan utama antar metode lebih mungkin muncul pada metrik lain, seperti waktu komputasi dan penggunaan sumber daya.



Gambar 6 Korelasi jumlah karakter awal dan nilai entropy

Secara umum, temuan penelitian ini konsisten dengan literatur yang menyatakan bahwa AES unggul dalam throughput dan efisiensi pemrosesan data besar. Studi sebelumnya juga menunjukkan bahwa algoritma simetris seperti AES lebih cocok untuk bulk encryption karena lebih ringan secara operasional dibanding algoritma asimetris. Sementara itu, hasil bahwa ECC lebih efisien untuk pertukaran kunci dan penggunaan ukuran kunci yang lebih kecil juga sejalan dengan penelitian terdahulu yang menempatkan ECC sebagai solusi efektif untuk komunikasi aman dengan overhead kunci rendah.

 ISSN:2302-8149
e-ISSN:2540-9719

Namun, penelitian ini memiliki posisi yang lebih kuat karena tidak hanya membandingkan algoritma secara umum, tetapi juga menguji performa berdasarkan variasi ukuran data nyata yang dibagi dalam lima kuintil. Pendekatan ini memberi gambaran yang lebih granular tentang bagaimana performa algoritma berubah terhadap panjang plaintext, sesuatu yang masih jarang dibahas secara rinci dalam studi sebelumnya. Selain itu, penggunaan dataset percakapan konseling real-world membuat hasil penelitian lebih relevan dengan kondisi komunikasi digital yang sesungguhnya, bukan sekadar data sintetis.

5 Kesimpulan

Berdasarkan hasil pengujian yang dilakukan, algoritma Advanced Encryption Standard (AES) menunjukkan performa yang lebih unggul dibandingkan Elliptic Curve Cryptography (ECC) dalam hal efisiensi komputasi. AES berhasil mencapai waktu enkripsi dan dekripsi yang sangat cepat dengan rata-rata 0,00013 detik serta konsumsi memori yang rendah dan stabil sekitar 0,83-0,86 KB di seluruh kuintil data. Sementara itu, ECC memerlukan waktu komputasi yang lebih tinggi, yaitu berkisar antara 0,00078 hingga 0,00175 detik, disertai konsumsi memori yang lebih besar, meskipun menawarkan tingkat keamanan kunci yang lebih kuat dengan ukuran kunci yang lebih efisien. Meskipun demikian, kedua algoritma menghasilkan nilai entropi ciphertext yang tinggi dan relatif seragam, berkisar antara 5,36 hingga 5,72, yang menandakan kualitas keacakan data yang baik dan tingkat keamanan yang memadai terhadap serangan statistik. Secara keseluruhan, penelitian ini menyimpulkan bahwa pemilihan algoritma kriptografi harus disesuaikan dengan prioritas aplikasi, di mana AES lebih sesuai untuk proses enkripsi data berukuran besar yang membutuhkan kecepatan tinggi, sedangkan ECC lebih ideal untuk mekanisme pertukaran kunci yang memerlukan keamanan asimetris yang kuat. Penelitian ini memiliki beberapa keterbatasan, antara lain pengujian yang dilakukan pada lingkungan Google Colab dengan spesifikasi hardware terbatas serta hanya menggunakan dataset teks percakapan konseling. Oleh karena itu, hasil penelitian ini dapat bervariasi ketika diimplementasikan pada infrastruktur cloud produksi atau jenis data yang berbeda. Untuk penelitian lanjutan, disarankan melakukan pengujian pada skala yang lebih besar, integrasi dengan algoritma post-quantum cryptography, serta evaluasi performa pada berbagai platform cloud dan jenis data multimedia.

Referensi

[1] C. Risky, R. Pawestri, O. S. Putro, and V. A. Mardani, "Analisis Algoritma Enkripsi AES untuk Pengamanan Data dalam Media Komunikasi Digital," *Semin. Nas. Teknol. Inf. dan Bisnis*, pp. 421–426, 2024.

[2] V. V. N. Akwukwuma, F. O. Chete, M. N. Oshioluamhe, and A. E. Okpako, "*Text Encryption using Advanced Encryption Standard (AES) Algorithm*," *NIPES - J. SCI. Technol. Res.*, Vol. 6, No. 2, pp. 214–228, 2024, DOI: 10.5281/zenodo.12558923.

[3] N. Kshetri, M. M. Rahman, M. M. Rana, O. F. Osama, and J. Hutson, "*algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography – A Comparative Analysis in AI Era*," *Int. J. Adv. Comput. SCI. Appl.*, Vol. 15, No. 12, pp. 1–14, 2024, DOI: 10.14569/IJACSA.2024.0151201.

[4] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "*Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing †*," *Eng. Proc.*, Vol. 20, No. 1, 2022, DOI: 10.3390/engproc2022020014.

[5] J. Jebrane, A. Chhaybi, S. Lazaar, and A. Nitaj, "*Elliptic Curve Cryptography with Machine Learning*," *Cryptography*, Vol. 9, No. 1, pp. 1–21, 2025, DOI: 10.3390/cryptography9010003.

[6] S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "*Hybrid AES-ECC Model for the Security of Data Over Cloud Storage*," *Electron.*, Vol. 10, No. 21, pp. 1–20, 2021, DOI: 10.3390/electronics10212673.

[7] M. Manimozhi and R. K. Mugelan, "*Post-Quantum AES Encryption using ECC Points Derived from BB84 Sifted Keys*," *EPJ Quantum Technol.*, Vol. 12, No. 1, 2025, DOI: 10.1140/epjqt/s40507-025-00411-9.

[8] E. Ahialey, R. E. Turkson, A.-L. Yussif, E. A. Frimpong, E. Attipoe, and E. D. Tetteh,

 ISSN:2302-8149
e-ISSN:2540-9719

"*Hybrid Encryption Models for Optimal Balance of Security, Scalability, and Computational Efficiency in Cloud Computing*," *Cureus J. Comput. SCI.*, 2025, DOI: 10.7759/s44389-025-05146-3.

[9] F. T. A. Hussien and T. W. A. Khairi, "*Performance Evaluation of AES, ECC and Logistic Chaotic Map Algorithms in Image Encryption*," *Int. J. Interact. Mob. Technol.*, Vol. 17, No. 10, pp. 193–211, 2023, DOI: 10.3991/ijim.v17i10.38787.

[10] H. Verma and N. M. Dubba, "*Enhancing AES and ECC Cryptographic Protocols for Real-Time Data Security*," Vol. 31, pp. 37–46, 2025, DOI: 10.63278/mme.vi.1555.

[11] M. Karanam, S. Reddy S, A. Chakilam, and S. Banothu, "*Performance Evaluation of Cryptographic Security Algorithms on Cloud*," *E3S Web Conf.*, Vol. 391, pp. 1–9, 2023, DOI: 10.1051/e3sconf/202339101015.

[12] A. Nik and A. Koupaei, "*Hybrid Encryption Scheme Combining AES and ECC for Enhanced Data Security*," pp. 1–8, [Online]. Available: https://www.researchgate.net/publication/384241551

[13] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Informatics*, Vol. 1, No. 2, pp. 54–60, 2020.

[14] Y. M. A. Abualkas and D. L. Bhaskari, "*Hybrid Approach to Cloud Storage Security using ECC-AES Encryption and Key Management Techniques*," *Int. J. Eng. Trends Technol.*, Vol. 72, No. 4, pp. 92–100, 2024, DOI: 10.14445/22315381/IJETT-V72I4P110.

[15] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "*Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices*," *Sensors*, Vol. 24, No. 12, 2024, DOI: 10.3390/s24124008.

[16] S. SR, U. N, C. R, and A. CM, "*Comparison between Encryption Algorithms: A Performance and Security Perspective*," *Int. J. SCI. Technol.*, Vol. 16, No. 3, pp. 1–7, 2025, DOI: 10.71097/ijsat.v16.i3.7986.

[17] F. Sherali, "*A New Approach for Enhancing AES-based Data Encryption using ECC*," *Int. J. Math. Comput. SCI.*, Vol. 19, No. 1, pp. 229–235, 2024, [Online]. Available: http://ijmcs.future-in-tech.net

[18] R. Ganesh, B. U. I. Khan, A. R. Khan, and A. Bin Kamsin, *A Panoramic Survey of the Advanced Encryption Standard: From Architecture to Security Analysis, Key Management, Real-World Applications, and Post-Quantum Challenges*, Vol. 24, No. 5. 2025. DOI: 10.1007/s10207-025-01116-x.

[19] R. Priambudi, J. Jayanta, and C. Nugrahaeni, "Penerapan Algoritma Kriptografi AES (*Advanced Encryption Standard*) dan *Algoritma Kompresi RLE* (*Run Length Encoding*) untuk Pengamanan File Dokumen," *Format J. Ilm. Tek. Inform.*, Vol. 11, No. 1, p. 11, 2022, DOI: 10.22441/10.22441/format.2022.v11.i1.002.

[20] T. Fadia and L. Toufik, "*Elliptic Curves Cryptography for Lightweight Devices in IoT System*," *Brazilian J. Technol.*, Vol. 7, No. 4, p. e73725, 2024, DOI: 10.38152/bjtv7n4-003.