ANALISIS PERFORMA DAN EFISIENSI AES-256 MODE CBC UNTUK ENKRIPSI DATA NASABAH SINTETIS

Elgia Villa Yandana[1], Ivan Firdaus[2], Budi Arifitama[3]
Program Studi Teknik Informatika, Fakultas Sains, Teknik, dan Desain
Universitas Trilogi[1,2,3]
Jalan TMP Kalibata No. 1, Duren Tiga, Pancoran, Jakarta Selatan 12760
elgitheedge@gmail.com[1], ivanfirdaus2203@gmail.com[2], budi.arifitama@trilogi.ac.id[3]

Abstrak

Layanan perbankan digital yang berkembang meningkatkan volume data nasabah sekaligus risiko kebocoran data, sehingga enkripsi menjadi kebutuhan teknis sekaligus kewajiban regulatif. Penelitian ini bertujuan menganalisis performa dan efisiensi algoritma Advanced Encryption Standard 256-bit (AES-256) dengan mode Cipher Block Chaining (CBC) dalam proses enkripsi dan dekripsi data sintetis yang merepresentasikan lima field identitas nasabah, menggunakan metode kuantitatif. Pengujian dilakukan pada lima skenario ukuran data (1 KB hingga 10 MB) dengan 30 repetisi dan 5 warm-up per skenario, diimplementasikan pada Java 11 (javax.crypto/JCA), serta dievaluasi berdasarkan waktu enkripsi, waktu dekripsi, dan throughput. Validasi byte-per-byte pada seluruh pengujian menunjukkan data hasil dekripsi identik dengan data asli. Rata-rata waktu enkripsi meningkat dari 0,4351 ms (1 KB) hingga 45,9987 ms (10 MB) dan waktu dekripsi dari 0,8032 ms hingga 89,6645 ms, dengan throughput enkripsi mencapai 208,86 MB/s dan dekripsi 108,01 MB/s pada data terbesar. Dalam batas kondisi pengujian ini, AES-256 CBC menunjukkan performa dan efisiensi yang baik, terutama pada data besar. Temuan bersifat terbatas pada data sintetis, skenario, dan lingkungan uji yang digunakan serta tidak digeneralisasikan pada sistem perbankan secara umum; kekuatan kriptografis disandarkan pada NIST FIPS 197 dan SP 800-57, bukan pada kriptanalisis langsung. Validasi menggunakan dataset nyata disarankan sebagai penelitian lanjutan.

Kata Kunci: AES-256, enkripsi data, performa, throughput, data sintetis

Abstract

The growth of digital banking increases customer data volume while enlarging the risk of data breaches, making encryption both a technical necessity and a regulatory obligation. This study analyzes the performance and efficiency of the 256-bit Advanced Encryption Standard (AES-256) in Cipher Block Chaining (CBC) mode on synthetic data representing five customer-identity fields, using a quantitative method. Testing was conducted across five data-size scenarios (1 KB to 10 MB) with 30 repetitions and 5 warm-ups per scenario, implemented in Java 11 (javax.crypto/JCA), and evaluated by encryption time, decryption time, and throughput. Byte-per-byte validation showed decrypted data identical to the original. Average encryption time increased from 0.4351 ms (1 KB) to 45.9987 ms (10 MB) and decryption time from 0.8032 ms to 89.6645 ms, with encryption throughput reaching 208.86 MB/s and decryption 108.01 MB/s on the largest data. Within these test conditions, AES-256 CBC showed good performance and efficiency, particularly on large data. The findings are limited to the synthetic data, scenarios, and test environment used and are not generalized to banking systems in general; its cryptographic strength rests on NIST FIPS 197 and SP 800-57 rather than direct cryptanalysis. Validation with real datasets is recommended for future work.

Keyword: *AES-256, data encryption, performance, throughput, synthetic data*

PENDAHULUAN

Perkembangan layanan perbankan digital di Indonesia terus mengalami percepatan seiring meningkatnya pengguna internet dan layanan keuangan elektronik. Pertumbuhan transaksi digital ini menaikkan volume dan kompleksitas data nasabah yang dikelola, sehingga memperbesar konsekuensi apabila terjadi kebocoran atau penyalahgunaan data. Pada April 2025, DBS Group dan Bank of China cabang Singapura melaporkan bahwa data sekitar 8.200 nasabah DBS dan 3.000 nasabah Bank of China berpotensi terekspos setelah vendor percetakan Toppan Next Tech mengalami serangan ransomware (Finextra, 2025). Insiden serupa juga menimpa Evolve Bank and Trust di Amerika Serikat pada 2024 (Reuters, 2024). Kedua kasus menegaskan bahwa ancaman

keamanan data perbankan tidak selalu menyasar sistem inti, melainkan juga titik-titik lemah pada ekosistem pihak ketiga yang turut mengelola data nasabah.

Dari sisi regulasi, Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mewajibkan penyelenggara sistem elektronik menerapkan langkah teknis dan organisasi yang memadai (Republik Indonesia, 2022). Secara lebih spesifik, Otoritas Jasa Keuangan menerbitkan POJK Nomor 11/POJK.03/2022 yang mewajibkan bank umum menerapkan tata kelola dan manajemen risiko teknologi informasi, termasuk pengendalian pengamanan data nasabah (Otoritas Jasa Keuangan, 2022). Regulasi ini memperkuat dasar hukum bahwa penerapan kontrol keamanan teknis, termasuk enkripsi, bukan sekadar praktik baik melainkan kewajiban yang melekat pada penyelenggara sistem informasi perbankan.

Advanced Encryption Standard dengan kunci 256-bit (AES-256) merupakan standar enkripsi simetris yang diakui luas karena kekuatan kriptografisnya. AES distandardisasi oleh NIST melalui FIPS 197 dan hingga kini tetap direkomendasikan untuk melindungi informasi sensitif (National Institute of Standards and Technology, 2001), sementara NIST SP 800-57 Part 1 mengklasifikasikan AES-256 pada security strength 256-bit, yaitu tingkat keamanan tertinggi pada kategori algoritma simetris yang direkomendasikan (National Institute of Standards and Technology, 2020). Dibandingkan Blowfish yang tidak memiliki status standardisasi formal, RSA yang secara inheren lebih lambat untuk data volume besar, serta AES-128 yang memiliki keyspace lebih kecil, AES-256 memberikan margin keamanan yang lebih besar sehingga sesuai dijadikan fokus analisis untuk pengamanan data tersimpan (data-at-rest).

Berdasarkan uraian tersebut, rumusan masalah penelitian ini adalah bagaimana performa dan efisiensi algoritma AES-256 mode CBC dalam proses enkripsi dan dekripsi data yang merepresentasikan data nasabah perbankan, ditinjau dari waktu enkripsi, waktu dekripsi, dan throughput. Penelitian ini bertujuan menganalisis performa dan efisiensi tersebut menggunakan metode kuantitatif. Perlu ditegaskan bahwa penelitian menggunakan data sintetis yang dibangkitkan secara terprogram, bukan data nasabah riil maupun sistem perbankan produksi; analisis difokuskan pada performa dan efisiensi implementasi, bukan pengujian efektivitas keamanan sistem perbankan secara menyeluruh, dan kekuatan kriptografis AES-256 disandarkan pada standar NIST FIPS 197 dan NIST SP 800-57 Part 1. Manfaat penelitian ini adalah menyediakan data empiris performa AES-256 pada berbagai ukuran data sebagai rujukan penerapan enkripsi data-at-rest dalam konteks pengamanan data nasabah.

PENELITIAN RELEVAN

Sejumlah penelitian terdahulu telah mengevaluasi AES-256 pada berbagai konteks. Eromosele (2025) menganalisis pengaruh AES-256 terhadap performa jaringan dan menyimpulkan keamanan tinggi tanpa penurunan performa signifikan, namun belum menyasar sistem perbankan. Alabdulrazzaq (2024) membandingkan varian AES pada beragam mode operasi, tetapi bersifat umum dan tidak spesifik pada data keuangan. Prasetya et al. (2024) mengevaluasi AES-256 pada basis data MySQL berisi 10.000 data nasabah simulasi, namun tidak membandingkan mode operasi maupun menghitung throughput per repetisi.

Studi lain seperti Nurdin (2023), Rifqi et al. (2023), dan Tariq & Ahmed (2025) berturut-turut berfokus pada perbandingan algoritma, penyimpanan cloud, dan manajemen kunci. Berdasarkan telaah tersebut, celah yang belum banyak dibahas adalah evaluasi performa AES-256 mode CBC secara terkontrol terhadap data yang merepresentasikan field identitas nasabah, dengan pengukuran throughput yang dihitung per repetisi untuk menilai stabilitasnya. Penelitian ini mengembangkan pendekatan tersebut dengan skenario ukuran data yang bervariasi serta validasi byte-per-byte untuk memastikan kebenaran implementasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif berbasis eksperimen terkontrol. Tahapannya meliputi pembangkitan data sintetis, prapemrosesan (preprocessing), proses enkripsi dan dekripsi menggunakan AES-256, serta evaluasi performa berdasarkan waktu enkripsi, waktu dekripsi, dan throughput. Analisis dilakukan secara statistik deskriptif terhadap hasil pengukuran dari seluruh repetisi.

Dataset Sintetis

Data yang digunakan merupakan data sintetis (fully synthetic data) yang dibangkitkan secara terprogram, bukan hasil pengumpulan, modifikasi, maupun penyamaran (masking) data nasabah riil. Data disusun dalam berkas teks terstruktur berformat CSV yang merepresentasikan lima field identitas nasabah, sebagaimana ditunjukkan pada Tabel 1. Nilai setiap field, termasuk kombinasi digit NIK, dihasilkan secara acak dengan tetap mengikuti pola format yang berlaku umum, sehingga terlihat realistis dari sisi struktur namun tidak memiliki keterkaitan dengan individu nyata mana pun.

Tabel 1. Struktur Field Dataset Sintetis

No	Field	Tipe Data	Keterangan
1	Name	String	Nama lengkap nasabah, dihasilkan secara sintetis
2	Date of Birth	Date (DD-MM-YYYY)	Tanggal lahir acak dalam rentang usia nasabah dewasa
3	National Identity Number (NIK)	String, 16 digit numerik	Mengikuti format struktur NIK Indonesia; digit acak, tidak merujuk individu nyata
4	Mother's Name	String	Nama ibu kandung, dihasilkan secara sintetis
5	Phone Number	String, diawali "08"	Mengikuti format umum nomor seluler Indonesia, dihasilkan secara acak

Data disusun dalam lima ukuran berbeda, yaitu 1 KB, 10 KB, 100 KB, 1 MB, dan 10 MB, untuk melihat pengaruh ukuran data terhadap performa algoritma. Variasi ini mensimulasikan kondisi nyata pada sistem perbankan, di mana ukuran berkas dapat bervariasi bergantung pada jumlah baris nasabah, terutama pada proses pencadangan (backup) atau migrasi data.

Implementasi dan Konfigurasi Algoritma

Algoritma AES-256 diimplementasikan menggunakan bahasa Java dengan pustaka kriptografi bawaan javax.crypto (Java Cryptography Architecture/JCA). Mode operasi yang digunakan adalah Cipher Block Chaining (CBC) dengan skema padding PKCS5, melalui transformasi "AES/CBC/PKCS5Padding". Kunci sepanjang 256-bit digunakan konsisten pada seluruh skenario, sedangkan Initialization Vector (IV) dibangkitkan baru secara acak pada setiap proses enkripsi. Proses dekripsi dirancang berjalan terpisah dan mandiri: ciphertext, IV, dan kunci dibaca dari berkas Base64 hasil enkripsi, merepresentasikan kondisi nyata ketika data terenkripsi diterima sebagai berkas yang lepas dari program penghasilnya.

Skenario, Variabel, dan Lingkungan Uji

Pengujian dilakukan pada lima skenario (S1–S5) yang dibedakan hanya oleh ukuran data (1 KB, 10 KB, 100 KB, 1 MB, 10 MB) sebagai variabel independen. Variabel kontrol mencakup algoritma (AES-256), mode operasi (CBC), panjang kunci (256-bit), mekanisme pembangkitan IV, jumlah repetisi, dan lingkungan eksekusi. Variabel dependen yang diukur adalah waktu enkripsi (ms), waktu dekripsi (ms), dan throughput (MB/s). Spesifikasi lingkungan uji ditunjukkan pada Tabel 2.

Tabel 2. Spesifikasi Lingkungan Uji

Komponen	Spesifikasi
Bahasa pemrograman	Java
Library kriptografi	javax.crypto/JCA bawaan JDK
Versi JDK	Java 11
Sistem operasi	Windows 10
RAM	16 GB
Prosesor	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz (8 CPUs)

Prosedur, Parameter Evaluasi, dan Validasi

Setiap proses enkripsi dan dekripsi pada tiap skenario dijalankan sebanyak 30 kali pengukuran yang didahului 5 kali warm-up yang tidak dicatat, guna mengurangi kesalahan pengukuran (measurement error) akibat inisialisasi Just-In-Time (JIT) compilation pada Java Virtual Machine (JVM). Waktu enkripsi dan dekripsi diperoleh dari selisih waktu mulai dan selesai proses, lalu dirata-ratakan dari ke-30 pengukuran. Throughput dihitung sebagai rasio ukuran data (MB) terhadap waktu proses (detik). Berbeda dengan pendekatan yang menghitung satu nilai throughput dari rata-rata waktu, penelitian ini menghitung throughput pada setiap repetisi kemudian menghitung statistik deskriptifnya, sehingga stabilitas throughput dapat dinilai secara kuantitatif. Untuk memastikan kebenaran implementasi (correctness), hasil dekripsi pada repetisi terakhir divalidasi secara byte-per-byte terhadap data asli sebelum dienkripsi.

HASIL DAN PEMBAHASAN

Waktu Enkripsi

Hasil pengukuran waktu enkripsi untuk kelima skenario disajikan pada Tabel 3. Rata-rata waktu enkripsi meningkat konsisten seiring bertambahnya ukuran data, dari 0,4351 ms (S1) hingga 45,9987 ms (S5). Peningkatan ini tidak berbanding lurus secara sederhana; dari S4 (1 MB) ke S5 (10 MB), ukuran data naik sepuluh kali lipat namun rata-rata waktu enkripsi hanya naik sekitar 8,6 kali. Standar deviasi relatif terhadap rata-rata cukup besar pada S1–S2 (mencapai ±62% pada S1), tetapi menyusut menjadi ±9–16% pada S3–S5, mengindikasikan bahwa waktu enkripsi pada ukuran data kecil lebih rentan terhadap variasi antar-repetisi akibat inisialisasi JIT compilation pada JVM, sedangkan pada ukuran data besar komputasi AES menjadi dominan sehingga pengukuran lebih stabil.

Tabel 3. Statistik Waktu Enkripsi (ms)

Skenario	Ukuran Data	Rata-rata	Std. Deviasi	Minimum	Maksimum
S1	1 KB	0,4351	0,6103	0,2519	3,7033
S2	10 KB	0,7153	0,4455	0,3789	1,8948
S3	100 KB	0,8215	0,1341	0,6512	1,1120
S4	1 MB	5,3698	0,7255	4,3692	7,3368
S5	10 MB	45,9987	4,0759	40,0007	59,6074

Waktu Dekripsi dan Validasi

Statistik waktu dekripsi disajikan pada Tabel 4. Polanya tidak sepenuhnya seragam: S2 justru mencatat rata-rata (0,5938 ms) lebih rendah dari S1 (0,8032 ms) meskipun ukurannya sepuluh kali lebih besar, disebabkan oleh ketidakstabilan pengukuran pada repetisi awal S1 yang nilai maksimumnya (5,5025 ms) lebih dari sepuluh kali mediannya. Mulai S3, waktu dekripsi kembali meningkat seiring ukuran data. Dibandingkan dengan waktu enkripsi, waktu dekripsi pada data besar tercatat lebih tinggi—pada S5, rata-rata dekripsi (89,6645 ms) hampir dua kali rata-rata enkripsi (45,9987 ms). Selisih ini melampaui yang diperkirakan dari teori dasar AES sehingga kemungkinan besar disebabkan faktor non-algoritmik pada testbed seperti Garbage Collection (GC) pada JVM atau beban proses lain pada sistem operasi, bukan kelemahan algoritma.

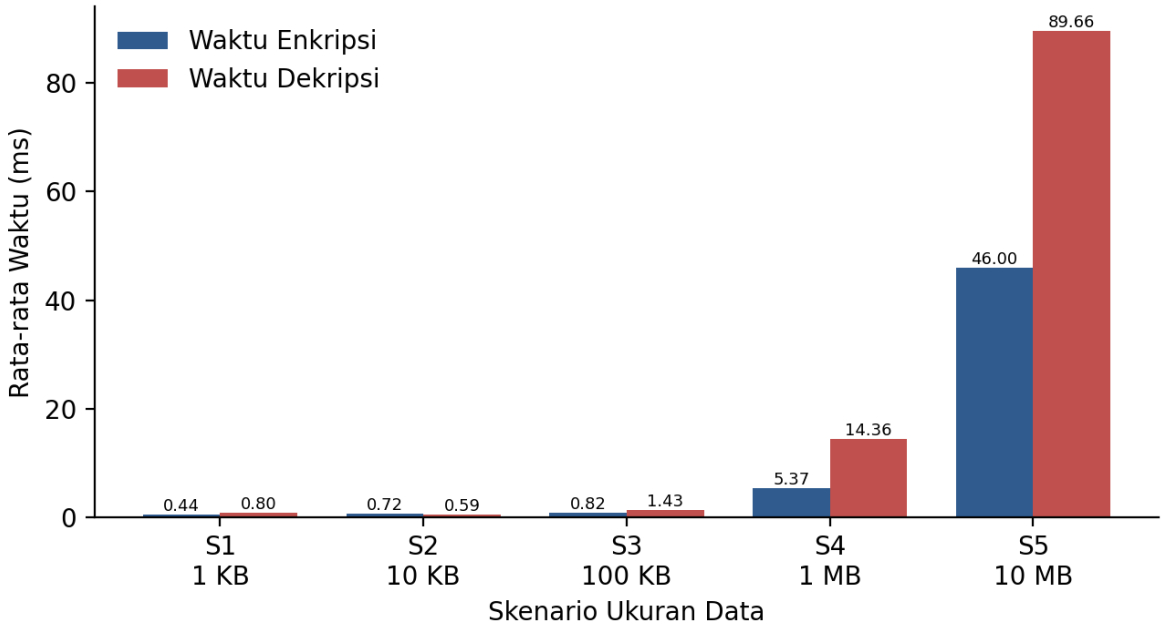
Tabel 4. Statistik Waktu Dekripsi (ms)

Skenario	Ukuran Data	Rata-rata	Std. Deviasi	Minimum	Maksimum
S1	1 KB	0,8032	0,9152	0,4180	5,5025
S2	10 KB	0,5938	0,1821	0,4433	1,2539
S3	100 KB	1,4290	0,3604	1,1823	2,5960
S4	1 MB	14,3639	4,6663	10,3048	31,6690
S5	10 MB	89,6645	11,3823	72,7259	114,3387

Validasi byte-per-byte pada seluruh skenario menunjukkan hasil dekripsi identik dengan data asli (Tabel 5). Ukuran hasil dekripsi kembali tepat ke ukuran plaintext, dengan selisih terhadap ciphertext sesuai jumlah padding PKCS5 yang dihapus, sehingga implementasi AES-256 mode CBC terbukti bekerja secara benar (*correct*) sesuai spesifikasi algoritma.

Tabel 5. Hasil Validasi Dekripsi

Skenario	Ukuran Data	Ukuran Ciphertext (byte)	Ukuran Hasil Dekripsi (byte)	Validasi terhadap Data Asli
S1	1 KB	1.024	1.010	Identik (Berhasil)
S2	10 KB	10.064	10.056	Identik (Berhasil)
S3	100 KB	100.064	100.056	Identik (Berhasil)
S4	1 MB	1.000.032	1.000.031	Identik (Berhasil)
S5	10 MB	10.000.048	10.000.038	Identik (Berhasil)



Gambar 1. Rata-rata Waktu Enkripsi dan Dekripsi per Skenario

Throughput

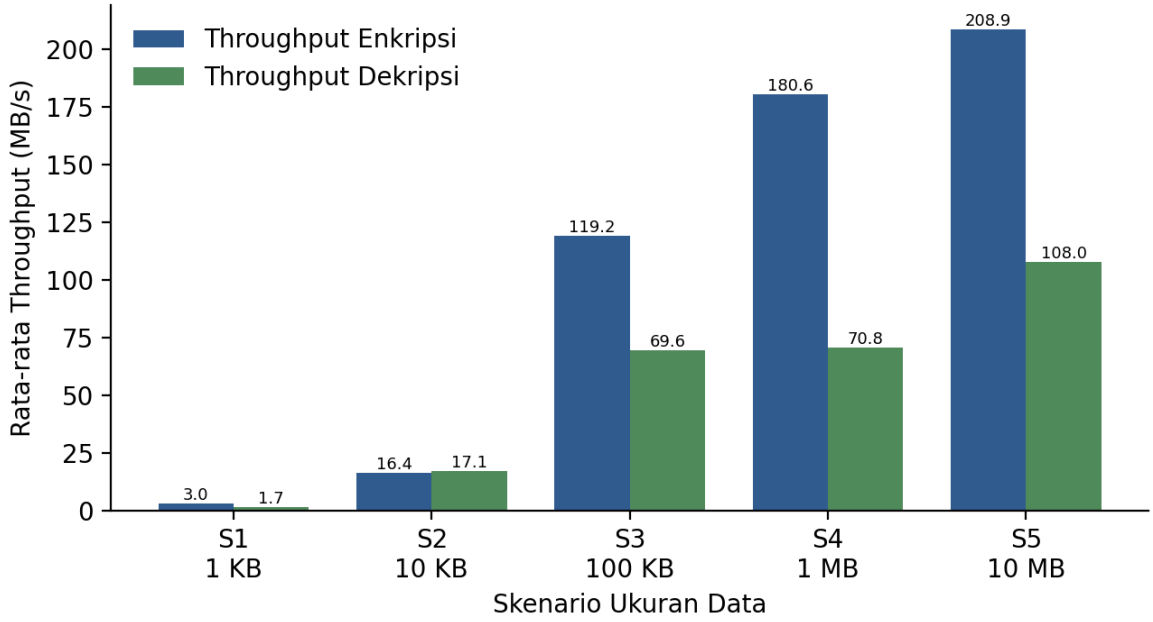
Statistik throughput enkripsi dan dekripsi disajikan pada Tabel 6 dan Tabel 7. Rata-rata throughput pada kedua arah meningkat konsisten seiring bertambahnya ukuran data—throughput enkripsi dari 2,9874 MB/s (S1) hingga 208,8561 MB/s (S5), dan throughput dekripsi dari 1,6696 MB/s hingga 108,0093 MB/s. Peningkatan ini sejalan dengan argumen bahwa pada ukuran data kecil, overhead non-algoritmik (inisialisasi objek Cipher pada JVM) masih dominan terhadap waktu total, sehingga throughput terukur belum merepresentasikan kapasitas pemrosesan AES-256 yang sesungguhnya.

Tabel 6. Statistik Throughput Enkripsi (MB/s)

Skenario	Ukuran Data	Rata-rata	Std. Deviasi	Minimum	Maksimum
S1	1 KB	2,9874	0,6917	0,2601	3,8238
S2	10 KB	16,3878	5,0685	5,0613	25,3105
S3	100 KB	119,1762	18,6679	85,8101	146,5308
S4	1 MB	180,6042	22,3939	129,9891	218,2788
S5	10 MB	208,8561	17,4115	159,9932	238,4153

Tabel 7. Statistik Throughput Dekripsi (MB/s)

Skenario	Ukuran Data	Rata-rata	Std. Deviasi	Minimum	Maksimum
S1	1 KB	1,6696	0,5804	0,1750	2,3043
S2	10 KB	17,1478	3,4163	7,6483	21,6335
S3	100 KB	69,5881	11,3320	36,7569	80,7078
S4	1 MB	70,8036	14,2283	30,1147	92,5495
S5	10 MB	108,0093	13,0685	83,4081	131,1332



Gambar 2. Rata-rata Throughput Enkripsi dan Dekripsi per Skenario

Koefisien variasi throughput enkripsi menurun secara umum seiring bertambahnya ukuran data, dari ±23% (S1) menjadi ±8% (S5), meskipun tidak sepenuhnya monoton. Pola serupa teramati pada throughput dekripsi dengan koefisien variasi ±12–35% tanpa penurunan monoton. Dengan demikian, throughput belum sepenuhnya stabil pada seluruh rentang ukuran, khususnya S1–S3, dan baru menunjukkan kestabilan lebih baik pada data besar (S5). Throughput enkripsi juga secara umum lebih tinggi daripada dekripsi—pada S5 hampir dua kali lipat—yang, mengingat kompleksitas komputasi AES-256-CBC secara teoretis setara pada kedua arah, kembali mengindikasikan pengaruh faktor non-algoritmik pada testbed.

Secara keseluruhan, pola peningkatan waktu dan throughput seiring bertambahnya ukuran data konsisten dengan karakteristik AES sebagai block cipher yang memproses data per blok 128-bit. Temuan ini selaras dengan Eromosele (2025) dan Prasetya et al. (2024) yang melaporkan performa AES-256 tetap baik tanpa penurunan signifikan. Namun, kriteria stabilitas throughput tidak terpenuhi seragam pada seluruh skenario, dan terdapat selisih waktu/throughput enkripsi–dekripsi yang melampaui prediksi teoretis sederhana, sehingga performa AES-256 yang terukur turut dipengaruhi faktor non-algoritmik pada lingkungan eksekusi seperti karakteristik JVM dan kondisi sistem operasi saat pengujian.

SIMPULAN

Algoritma AES-256 mode CBC berhasil diimplementasikan pada sistem pengujian berbasis Java (javax.crypto/JCA) untuk memproses data nasabah sintetis yang mencakup lima field identitas. Validasi byte-per-byte pada seluruh 150 pengujian (5 skenario × 30 repetisi) menunjukkan data hasil dekripsi identik dengan data asli tanpa kehilangan maupun kerusakan, sehingga implementasi terbukti bekerja secara benar sesuai spesifikasi algoritma. Analisis performa menunjukkan rata-rata waktu enkripsi meningkat dari 0,4351 ms (1 KB) hingga 45,9987 ms (10 MB) dan waktu dekripsi dari 0,8032 ms hingga 89,6645 ms, sedangkan rata-rata throughput enkripsi meningkat hingga 208,8561 MB/s dan dekripsi hingga 108,0093 MB/s pada data terbesar. Throughput pada data besar (S4–S5) menunjukkan koefisien variasi lebih kecil, mengindikasikan kestabilan performa yang lebih baik pada ukuran data yang lebih besar dalam rentang yang diuji.

Berdasarkan hasil tersebut, dalam batas kondisi pengujian ini AES-256 mode CBC menunjukkan performa dan efisiensi yang baik untuk enkripsi data saat penyimpanan (data-at-rest) pada rentang ukuran yang diuji. Seluruh temuan bersifat terbatas pada data sintetis, skenario, dan lingkungan uji yang digunakan, sehingga tidak dapat digeneralisasikan pada sistem perbankan secara umum yang mencakup basis data, transaksi, API, maupun sistem produksi dengan beban dan konfigurasi yang berbeda. Kekuatan kriptografis AES-256 disandarkan pada standar NIST FIPS 197 dan NIST SP 800-57 Part 1, bukan pada pengujian kriptanalisis langsung; dengan demikian, penelitian ini menyimpulkan efisiensi performa implementasi AES-256 pada kondisi uji tertentu, bukan efektivitas keamanan pada sistem perbankan secara menyeluruh. Penelitian selanjutnya disarankan untuk melengkapi pengujian kekuatan kriptografis (misalnya avalanche effect dan NIST Statistical Test Suite), mengisolasi faktor non-algoritmik pada testbed, serta memvalidasi hasil menggunakan dataset nyata dari sistem perbankan dengan tetap mematuhi etika dan regulasi perlindungan data pribadi.

DAFTAR PUSTAKA

Alabdulrazzaq, H. (2024). On the performance of AES algorithm variants. *International Journal of Cryptography Engineering, 12*(1), 33–47.

Eromosele, C. C. (2025). Evaluating the impact of AES-256 encryption on network performance: An analysis of transfer time, latency, and throughput. *International Journal of Network Security Systems, 20*(1), 14–29.

Finextra. (2025). DBS and Bank of China customers hit by Toppan Next Tech ransomware breach. *Finextra Research*.

National Institute of Standards and Technology. (2001). *FIPS PUB 197: Advanced Encryption Standard (AES)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). *NIST SP 800-57 Part 1 Rev. 5: Recommendation for key management*. U.S. Department of Commerce.

Nurdin, N. (2023). Comparative analysis between AES and Fully Homomorphic Encryption (FHE) in financial technology. *Journal of Fintech Security, 4*(1), 25–39.

Otoritas Jasa Keuangan. (2022). *Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*.

Prasetya, D., Harianto, L., & Widodo, H. (2024). Performance evaluation of cryptographic security in banking database systems. *Indonesian Journal of Information Security, 13*(2), 89–102.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Reuters. (2024). Evolve Bank & Trust discloses data breach affecting customer information. *Reuters*.

Rifqi, M., Andika, R., & Setiawan, T. (2023). Cloud data protection using AES-256 for banking storage systems. *Cloud Computing and Security Journal, 11*(3), 55–71.

Tariq, S., & Ahmed, K. (2025). Key management optimization for AES-256 in financial systems. *Journal of Information Security Strategies, 10*(1), 40–58.