LITERATURE REVIEW

Analisis Perbandingan Algoritma Advanced Encryption Standard (AES) 128, 192, dan 256 Bit dalam Keamanan Data Digital

KRIPTOGRAFI (CR002)

Dosen Pengampu :

Jefry Sunupurwa Asri , S.Kom., M.Kom.

Disusun Oleh :

Putra Daffa Dwiyansah (20230801432)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL

2025

Analisis Perbandingan Algoritma Advanced Encryption Standard (AES) 128, 192, dan 256 Bit dalam Keamanan Data Digital

1. Pendahuluan

Keamanan data merupakan aspek fundamental dalam pengelolaan sistem informasi modern. Seiring dengan pesatnya perkembangan teknologi digital, pertukaran data melalui jaringan internet semakin masif, baik dalam konteks bisnis, pemerintahan, maupun komunikasi pribadi. Kondisi ini secara tidak langsung meningkatkan risiko kebocoran, manipulasi, serta pencurian data oleh pihak yang tidak berwenang. Oleh karena itu, muncul kebutuhan akan sistem keamanan yang mampu menjamin kerahasiaan dan integritas data dari ancaman eksternal. Dalam konteks ini, kriptografi menjadi salah satu solusi paling penting dan relevan untuk mengamankan informasi di dunia digital (Wachid Hidayatulloh et al., 2023).

Kriptografi berperan dalam mengubah data asli (plaintext) menjadi bentuk tersandi (ciphertext) melalui proses enkripsi, sehingga pesan tersebut hanya dapat dikembalikan ke bentuk semula oleh pihak yang memiliki kunci dekripsi. Dengan demikian, kriptografi tidak hanya menjaga kerahasiaan data, tetapi juga menjamin integritas dan autentikasi dalam komunikasi elektronik. Berbagai algoritma kriptografi telah dikembangkan untuk memenuhi kebutuhan keamanan data, mulai dari algoritma klasik seperti DES (Data Encryption Standard) hingga algoritma modern seperti AES (Advanced Encryption Standard) yang saat ini menjadi standar global (Wachid Hidayatulloh et al., 2023).

AES dikembangkan oleh Vincent Rijmen dan Joan Daemen dengan nama awal Rijndael, dan kemudian disetujui sebagai standar enkripsi oleh National Institute of Standards and Technology (NIST) pada tahun 2001. AES dirancang untuk menggantikan DES yang sudah tidak lagi dianggap aman terhadap serangan brute force. Algoritma ini menggunakan struktur blok 128-bit dengan tiga varian utama berdasarkan panjang kunci, yaitu AES-128, AES-192, dan AES-256, di mana angka tersebut menunjukkan panjang kunci dalam bit (128, 192, dan 256). Setiap varian memiliki jumlah ronde enkripsi yang berbeda: AES-128 memiliki 10 ronde, AES-192 memiliki 12 ronde, dan AES-256 memiliki 14 ronde (Tampubolon, Isnanto, & Sinuraya, 2014).

Penelitian di Indonesia menunjukkan berbagai implementasi dan analisis terhadap AES dalam konteks pengamanan data digital. Kusyanti & Amron (2018) meneliti penerapan AES pada sistem enkripsi pesan singkat (Short Message Service) berbasis Android dan menemukan bahwa AES-128 memiliki kinerja paling cepat. Santoso & Rahman (2022) mengembangkan aplikasi enkripsi dokumen berbasis Android dengan AES-128 dan membuktikan bahwa algoritma ini sangat efisien untuk perangkat mobile dengan sumber daya terbatas. Sementara itu, penelitian yang dilakukan oleh Indrayani, Ferdiansyah, & Koprawi (2025) menunjukkan keunggulan AES-256 dalam menjaga integritas berbagai jenis file digital seperti teks, gambar, dan video, meskipun waktu enkripsi yang dibutuhkan relatif lebih lama dibandingkan varian lainnya.

Secara umum, hasil penelitian-penelitian tersebut menunjukkan adanya trade-off antara tingkat keamanan dan efisiensi komputasi di antara ketiga varian AES. AES-128 unggul dari sisi kecepatan dan efisiensi, AES-192 memberikan keseimbangan antara kecepatan dan kekuatan enkripsi, sementara AES-256 menawarkan keamanan tertinggi namun dengan konsekuensi peningkatan waktu proses.

Tujuan dari kajian literatur ini adalah untuk menganalisis dan membandingkan performa serta tingkat keamanan dari ketiga varian AES, sekaligus mengidentifikasi kelebihan, kekurangan, dan potensi penerapannya dalam sistem informasi modern. Melalui kajian ini diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai hubungan antara panjang kunci, jumlah ronde, dan efisiensi algoritma, sehingga dapat menjadi acuan dalam pemilihan varian AES yang sesuai dengan kebutuhan dan karakteristik aplikasi tertentu.

2. Konsep Dasar Kriptografi Algoritma Advanced Encryption Standard (AES)

Menurut Wachid Hidayatulloh et al. (2023), kriptografi merupakan ilmu dan seni dalam menjaga keamanan informasi melalui teknik penyandian, dengan tujuan agar hanya pihak yang memiliki otorisasi yang dapat memahami isi pesan. Secara historis, kriptografi telah digunakan sejak zaman kuno untuk melindungi pesan-pesan penting dalam bidang militer dan diplomatik, namun kini telah berkembang menjadi fondasi utama dalam sistem keamanan siber, komunikasi elektronik, serta perlindungan data digital.

Tujuan utama kriptografi meliputi empat aspek penting:

1. **Kerahasiaan (Confidentiality)** – memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
2. **Integritas (Integrity)** – menjamin bahwa data tidak mengalami perubahan selama proses transmisi atau penyimpanan.
3. **Autentikasi (Authentication)** – memastikan identitas pihak yang berkomunikasi adalah sah dan dapat dipercaya.
4. **Non-Repudiation** – mencegah pengirim data menyangkal telah mengirimkan pesan tertentu.

Dalam implementasinya, algoritma kriptografi modern dapat diklasifikasikan menjadi tiga kelompok utama, yaitu:

1. **Kriptografi Simetris**, yaitu sistem yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Contohnya: AES (Advanced Encryption Standard), DES (Data Encryption Standard), dan Blowfish.
2. **Kriptografi Asimetris**, yaitu sistem yang menggunakan pasangan kunci publik dan kunci privat yang berbeda untuk proses enkripsi dan dekripsi. Contohnya: RSA (Rivest–Shamir–Adleman) dan ECC (Elliptic Curve Cryptography).
3. **Fungsi Hash**, yaitu algoritma satu arah yang mengubah data menjadi representasi dengan panjang tetap tanpa memungkinkan proses dekripsi kembali. Contohnya: SHA (Secure Hash Algorithm) dan MD5 (Message Digest 5).

Advanced Encryption Standard (AES) termasuk dalam kategori kriptografi simetris berbasis blok (block cipher) yang bekerja dengan membagi data menjadi blok 128 bit untuk kemudian diproses melalui serangkaian transformasi matematis. Struktur internal AES terdiri dari empat tahap utama, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey, di mana setiap tahapan berfungsi untuk meningkatkan difusi, kompleksitas, dan kekokohan hasil enkripsi (Wachid Hidayatulloh et al., 2023).

Perbedaan mendasar antar-varian AES terletak pada panjang kunci dan jumlah ronde enkripsi yang digunakan. Berdasarkan penelitian Tampubolon, Isnanto, & Sinuraya (2014), AES-128 memiliki 10 ronde, AES-192 memiliki 12 ronde, dan AES-256 memiliki 14 ronde. Peningkatan jumlah ronde tersebut berbanding lurus dengan tingkat keamanan, karena semakin memperluas ruang pencarian kunci (keyspace), sehingga membuat algoritma lebih tahan terhadap serangan brute force maupun differential cryptanalysis. Namun, konsekuensinya adalah waktu komputasi yang lebih lama dan kebutuhan sumber daya prosesor yang lebih tinggi.

Sementara itu, Kusyanti & Amron (2018) menjelaskan bahwa semakin panjang kunci AES, tingkat keamanannya meningkat secara eksponensial karena menambah kompleksitas kombinasi yang harus diuji oleh penyerang. Namun, hal ini juga berdampak pada penurunan kecepatan pemrosesan, terutama pada perangkat dengan kemampuan komputasi terbatas seperti smartphone atau sistem tertanam (embedded system). Dengan demikian, terdapat trade-off antara performa dan keamanan, di mana AES-128 unggul dalam efisiensi waktu dan penggunaan sumber daya, sedangkan AES-256 lebih kuat untuk kebutuhan keamanan jangka panjang seperti penyimpanan data sensitif atau sistem cloud (Indrayani, Ferdiansyah, & Koprawi, 2025).

Untuk memberikan gambaran umum, berikut tabel perbandingan jenis algoritma kriptografi berdasarkan karakteristik utama dan penerapannya:

Jenis Algoritma	**Jenis Kunci**	**Kecepatan**	**Keamanan**	**Contoh Aplikasi**
AES (Simetris)	1 kunci sama	Cepat	Sangat tinggi	Enkripsi file, database, komunikasi jaringan
RSA (Asimetris)	Publik/Privat	Lambat	Tinggi	Digital signature, key exchange
SHA (Hash)	Tidak ada kunci	Sangat cepat	Non-invertible	Validasi integritas data

Dengan memahami konsep dasar kriptografi dan struktur kerja algoritma AES, maka pembahasan pada bagian berikutnya akan difokuskan pada hasil penelitian yang membandingkan tiga varian utama AES 128, 192, dan 256 bit dalam konteks performa, efisiensi, dan tingkat keamanan yang dihasilkan.

3. Tinjauan Penelitian Terdahulu

3.1. Hidayatulloh et al. (2023) — Mengenal Advanced Encryption Standard (AES) Sebagai Algoritma Kriptografi dalam Mengamankan Data, Jurnal Digital Transformation Technology (Digitech)

Penelitian yang dilakukan oleh Wachid Hidayatulloh et al. (2023) berfokus pada pengenalan dan analisis konseptual terhadap algoritma Advanced Encryption Standard (AES) sebagai salah satu metode kriptografi modern yang paling banyak digunakan. Studi ini menjelaskan secara komprehensif mengenai struktur internal AES yang terdiri dari empat proses utama SubBytes, ShiftRows, MixColumns, dan AddRoundKey serta bagaimana mekanisme tersebut menciptakan lapisan keamanan berlapis yang sulit ditembus.

Penulis menegaskan bahwa AES unggul dibandingkan algoritma sebelumnya seperti DES (Data Encryption Standard), baik dari sisi efisiensi maupun ketahanan terhadap serangan brute-force. Dengan ruang kunci yang sangat besar dan kompleksitas matematis berbasis substitusi dan permutasi, AES dikategorikan sebagai algoritma yang aman untuk digunakan dalam sistem modern seperti IoT, database terenkripsi, dan layanan cloud.

Namun, penelitian ini bersifat teoritis dan belum mencakup analisis empiris mengenai performa waktu enkripsi atau konsumsi sumber daya. Walaupun demikian, Hidayatulloh et al. (2023) memberikan landasan yang kuat untuk memahami mekanisme kerja AES serta pentingnya pemilihan panjang kunci (128, 192, dan 256 bit) dalam menentukan tingkat keamanan sistem.

3.2. Kusyanti & Amron (2018) — Analisis Perbandingan Algoritma Advanced Encryption Standard untuk Enkripsi Short Message Service (SMS) pada Android, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK), Universitas Brawijaya

Penelitian yang dilakukan oleh Kusyanti dan Amron (2018) secara eksplisit membandingkan performa tiga varian AES, yaitu AES-128, AES-192, dan AES-256, dalam konteks enkripsi pesan singkat (SMS) pada platform Android. Fokus utama penelitian ini adalah mengukur waktu enkripsi dan dekripsi serta tingkat efisiensi penggunaan memori pada perangkat mobile dengan spesifikasi terbatas.

Hasil pengujian menunjukkan bahwa AES-128 memiliki waktu eksekusi paling cepat dan efisien, karena jumlah ronde yang lebih sedikit (10 ronde) dibandingkan AES-192 (12 ronde) dan AES-256 (14 ronde). Sementara itu, AES-256 menghasilkan tingkat keamanan paling tinggi dengan kompleksitas yang meningkat seiring panjang kunci, namun membutuhkan waktu pemrosesan hingga 25–30% lebih lama dari AES-128.

Penelitian ini juga menegaskan bahwa pemilihan varian AES harus disesuaikan dengan kebutuhan sistem. Untuk aplikasi mobile yang membutuhkan efisiensi tinggi, AES-128 menjadi pilihan ideal, sedangkan untuk sistem dengan tuntutan keamanan tinggi seperti perbankan atau komunikasi rahasia, AES-256 lebih disarankan (Kusyanti & Amron, 2018).

3.3. Santoso & Rahman (2022) — Analisa dan Perancangan Sistem Enkripsi dan Dekripsi Dokumen Berbasis Android Menggunakan Metode Advanced Encryption Standard – 128, Jurnal Logika Media Teknologi (JLMT)

Penelitian yang dilakukan oleh Teguh Budi Santoso dan Fildan Hadika Rahman (2022) berfokus pada pengembangan sistem enkripsi dan dekripsi dokumen berbasis Android menggunakan AES-128. Tujuan penelitian ini adalah untuk memastikan keamanan dokumen digital tanpa mengorbankan performa perangkat mobile.

Hasil pengujian menunjukkan bahwa AES-128 mampu mengenkripsi berbagai jenis file dokumen dengan cepat dan efisien tanpa mengubah struktur maupun ukuran file asli setelah proses dekripsi. Dari sisi konsumsi memori dan daya, algoritma ini dinilai sangat ringan dan stabil untuk diaplikasikan pada perangkat dengan spesifikasi rendah hingga menengah. Namun, penelitian ini tidak membandingkan secara langsung dengan AES-192 dan AES-256, sehingga fokus utama tetap pada efisiensi penggunaan AES-128. Meskipun demikian, Santoso & Rahman (2022) menyimpulkan bahwa AES-128 merupakan varian paling praktis untuk implementasi enkripsi pada sistem mobile yang memerlukan kecepatan dan stabilitas tinggi.

3.4. Tampubolon et al. (2014) — Implementasi dan Analisis Algoritma Advanced Encryption Standard (AES) pada Tiga Variasi Panjang Kunci untuk Berkas Multimedia

Penelitian oleh Tampubolon, Isnanto, dan Sinuraya (2014) bertujuan untuk mengimplementasikan dan membandingkan performa AES-128, AES-192, dan AES-256 dalam proses enkripsi file multimedia, termasuk video, gambar, dan teks. Pengujian dilakukan dengan mengukur kecepatan enkripsi, dekripsi, dan tingkat keamanan yang dihasilkan dari setiap varian.

Hasil eksperimen menunjukkan bahwa AES-128 memiliki waktu pemrosesan paling cepat dan konsumsi CPU paling rendah, sedangkan AES-256 membutuhkan waktu komputasi lebih lama tetapi menawarkan tingkat keamanan yang jauh lebih tinggi. AES-192 berada di posisi tengah dengan performa dan keamanan yang seimbang.

Penelitian ini juga menyoroti bahwa peningkatan jumlah ronde enkripsi berbanding lurus dengan kenaikan tingkat keamanan, namun menurunkan efisiensi waktu. Oleh karena itu, Tampubolon et al. (2014) menekankan pentingnya keseimbangan antara performa dan keamanan dalam memilih varian AES, serta merekomendasikan penggunaan AES hardware acceleration sebagai solusi optimasi di masa depan.

3.5. Indrayani, Ferdiansyah, & Koprawi (2025) — Analisis Penggunaan Kriptografi Metode AES-256 Bit pada Pengamanan File dengan Berbagai Format, Digital Transformation Technology, 4(2)

Penelitian terbaru oleh Indrayani, Ferdiansyah, dan Koprawi (2025) mengkaji penerapan AES-256 untuk pengamanan file digital dengan berbagai format, seperti teks, gambar, audio, dan video. Fokus utama penelitian ini adalah mengevaluasi efektivitas AES-256 dalam menjaga integritas, konsistensi ukuran file, dan ketahanan terhadap modifikasi data. Hasil penelitian menunjukkan bahwa AES-256 mampu menjaga struktur data secara utuh setelah proses dekripsi tanpa kehilangan kualitas file. Meski demikian, waktu enkripsi dan

dekripsi lebih lama dibandingkan dengan AES-128 dan AES-192, terutama pada file berukuran besar.

Penulis menegaskan bahwa AES-256 ideal digunakan untuk sistem yang menuntut tingkat keamanan tinggi, seperti penyimpanan data sensitif di cloud, sistem pemerintahan, dan aplikasi finansial. Namun, untuk sistem dengan keterbatasan sumber daya, diperlukan optimasi algoritma agar tidak menimbulkan overhead pada performa (Indrayani et al., 2025).

4. Analisis dan Sintesis

Dari kelima penelitian yang telah ditinjau, tampak adanya pola konsisten dalam hubungan antara panjang kunci AES, tingkat keamanan, dan efisiensi pemrosesan. Secara umum, semakin panjang kunci yang digunakan, maka tingkat keamanan meningkat secara signifikan, tetapi waktu enkripsi dan dekripsi juga bertambah.

Pertama, AES-128 dinilai paling efisien secara komputasi karena hanya menggunakan 10 ronde enkripsi. Penelitian oleh Santoso & Rahman (2022) menunjukkan bahwa AES-128 mampu memberikan kecepatan tinggi dengan konsumsi sumber daya minimal, menjadikannya pilihan ideal untuk perangkat mobile atau aplikasi waktu nyata (real-time system). Hasil serupa juga diperkuat oleh Kusyanti & Amron (2018), yang menemukan bahwa AES-128 memiliki waktu eksekusi paling cepat dibandingkan AES-192 dan AES-256 dalam pengujian pada platform Android. Namun, kelemahan utamanya adalah ruang kunci yang lebih kecil dibandingkan AES-256, sehingga kurang optimal untuk melawan serangan dengan daya komputasi besar dalam jangka panjang.

Kedua, AES-192 menempati posisi tengah dalam hal performa dan keamanan. Seperti dijelaskan oleh Kusyanti & Amron (2018) serta Tampubolon, Isnanto, & Sinuraya (2014), AES-192 memberikan tingkat keamanan yang lebih baik daripada AES-128 tanpa penurunan performa yang terlalu besar. Meskipun demikian, varian ini jarang digunakan dalam implementasi nyata karena perbedaannya dengan AES-256 tidak terlalu signifikan, sedangkan beban pemrosesan tetap meningkat.

Ketiga, AES-256 memberikan tingkat keamanan tertinggi karena memiliki 14 ronde dan panjang kunci yang besar. Penelitian oleh Indrayani, Ferdiansyah, & Koprawi (2025) menunjukkan bahwa AES-256 efektif dalam menjaga integritas data bahkan pada file berukuran besar dan berbagai format, menjadikannya sangat cocok untuk sistem dengan kebutuhan keamanan tinggi seperti enkripsi database, penyimpanan cloud, dan komunikasi pemerintah. Namun, penelitian ini juga menegaskan bahwa peningkatan keamanan harus dibayar dengan waktu pemrosesan yang lebih lama dan penggunaan sumber daya yang lebih besar.

Selain itu, beberapa penelitian menyoroti bahwa performa AES sangat dipengaruhi oleh spesifikasi perangkat keras dan ukuran data yang diproses. Kusyanti & Amron (2018) mencatat bahwa pada perangkat dengan prosesor rendah, selisih waktu antara AES-128 dan AES-256 dapat mencapai beberapa detik per file. Sebaliknya, Tampubolon et al. (2014) menjelaskan bahwa perangkat modern dengan dukungan AES-NI (Advanced Encryption Standard New Instructions) dapat meminimalkan perbedaan waktu tersebut secara signifikan.

Adapun beberapa celah penelitian (research gap) yang masih terbuka untuk dikaji lebih lanjut antara lain:

- Minimnya penelitian mengenai konsumsi energi dan penggunaan memori pada masing-masing varian AES di berbagai platform.
- Belum banyak studi yang membahas pengaruh hardware acceleration (seperti AES-NI atau GPU encryption) terhadap efisiensi ketiga varian.
- Kurangnya analisis terhadap ketahanan implementasi AES terhadap serangan praktis seperti side-channel attack dan timing attack.

Secara keseluruhan, hasil sintesis menunjukkan bahwa AES tetap menjadi algoritma kriptografi simetris paling relevan dan kuat hingga saat ini, dengan setiap variannya memiliki keunggulan tersendiri tergantung pada konteks penggunaan.

- AES-128 unggul dalam efisiensi,
- AES-192 menawarkan keseimbangan, dan performa.
- AES-256 unggul dalam kekuatan keamanan jangka panjang.

5. Arah dan Peluang Penelitian

Berdasarkan hasil kajian literatur terhadap berbagai penelitian sebelumnya, dapat diidentifikasi bahwa setiap varian AES memiliki karakteristik performa dan keamanan yang berbeda, dan belum ada standar implementasi yang secara khusus mengoptimalkan penggunaannya pada platform web modern. Oleh karena itu, arah penelitian selanjutnya dapat difokuskan pada penerapan adaptif algoritma AES, khususnya AES-256, pada lingkungan aplikasi web berbasis framework seperti Laravel dan Filament.

Penelitian di masa depan diharapkan tidak hanya menguji kemampuan enkripsi dan dekripsi AES dalam konteks keamanan data, tetapi juga menilai dampaknya terhadap performa sistem, efisiensi komputasi, dan konsumsi energi. Beberapa aspek penting yang dapat dijadikan fokus dalam pengembangan penelitian selanjutnya antara lain:

1. **Analisis performa AES-256 terhadap kecepatan enkripsi dan beban server.** Pengujian perlu dilakukan untuk mengetahui sejauh mana implementasi AES-256 mempengaruhi waktu respons aplikasi web, terutama dalam kondisi beban pengguna yang tinggi. Hal ini penting karena AES-256 memiliki jumlah ronde enkripsi paling banyak (14 ronde), yang secara teoritis dapat meningkatkan waktu proses secara signifikan dibandingkan AES-128 dan AES-192.
2. **Implementasi field-level encryption pada database Laravel.** Pendekatan ini memungkinkan setiap kolom sensitif dalam tabel database (seperti data pribadi, alamat, atau nomor identitas) dienkripsi menggunakan AES-256 sebelum disimpan, kemudian didekripsi hanya ketika dibutuhkan. Dengan cara ini, sistem akan lebih tahan terhadap risiko kebocoran data akibat akses langsung ke database. Penelitian lanjutan dapat mengevaluasi efisiensi teknik ini dibandingkan dengan enkripsi global berbasis middleware.

3. **Perbandingan efisiensi ketiga varian AES (128, 192, 256) dalam konteks aplikasi web.**
   Meskipun secara teori AES-256 memiliki keamanan tertinggi, tidak semua aplikasi web memerlukan tingkat keamanan sebesar itu. Oleh karena itu, perlu dilakukan uji empiris untuk membandingkan waktu enkripsi, penggunaan CPU, throughput, dan konsumsi memori dari ketiga varian pada server dengan spesifikasi berbeda.

4. **Pengukuran parameter tambahan seperti CPU usage, throughput, dan konsumsi energi.**
   Penggunaan energi menjadi faktor penting, terutama untuk sistem berbasis cloud dan edge computing. Penelitian mendatang dapat menganalisis hubungan antara ukuran kunci AES dan efisiensi energi, sehingga dapat diketahui varian mana yang paling optimal dalam konteks green computing.

Selain itu, arah penelitian juga dapat diperluas dengan mengintegrasikan AES dengan algoritma keamanan tambahan, seperti steganografi atau digital signature, untuk menciptakan lapisan keamanan ganda. Hal ini sejalan dengan penelitian Santoso & Rahman (2022) yang menekankan pentingnya efisiensi pada sistem mobile, serta temuan Indrayani, Ferdiansyah, & Koprawi (2025) yang menunjukkan pentingnya tingkat keamanan tinggi dalam sistem penyimpanan file berbasis cloud.

Dengan pendekatan tersebut, penelitian lanjutan diharapkan mampu memberikan kontribusi empiris yang signifikan terhadap pengembangan keamanan data berbasis AES di lingkungan aplikasi web modern, sekaligus menjadi referensi teknis untuk penerapan keamanan berbasis software framework seperti Laravel, Django, atau Node.js.

6. Kesimpulan

Berdasarkan hasil analisis dan sintesis terhadap lima jurnal nasional yang membahas algoritma Advanced Encryption Standard (AES), dapat disimpulkan bahwa ketiga varian AES yaitu AES-128, AES-192, dan AES-256 memiliki kekuatan dan efisiensi yang berbeda sesuai dengan konteks penggunaannya.

Pertama, AES-128 memiliki keunggulan dalam kecepatan dan efisiensi sumber daya, menjadikannya pilihan ideal untuk sistem dengan keterbatasan komputasi seperti perangkat mobile atau aplikasi real-time. Penelitian Santoso & Rahman (2022) membuktikan bahwa AES-128 mampu melakukan proses enkripsi dan dekripsi dengan cepat tanpa mengubah struktur file serta hanya membutuhkan memori dalam jumlah kecil, sehingga sangat cocok diterapkan pada perangkat berbasis Android.

Kedua, AES-192 menempati posisi antara AES-128 dan AES-256, memberikan keseimbangan antara performa dan tingkat keamanan. Menurut hasil penelitian Kusyanti & Amron (2018) serta Tampubolon, Isnanto, & Sinuraya (2014), AES-192 mampu memberikan keamanan yang lebih tinggi dibandingkan AES-128 tanpa peningkatan waktu proses yang terlalu signifikan. Namun, varian ini jarang digunakan dalam implementasi praktis karena perbedaannya dengan AES-256 tidak terlalu besar, sementara kompleksitas pemrosesan meningkat.

Ketiga, AES-256 menawarkan tingkat keamanan tertinggi, dengan panjang kunci 256 bit dan jumlah ronde sebanyak 14. Hasil penelitian Indrayani, Ferdiansyah, & Koprawi (2025) menegaskan bahwa AES-256 sangat efektif dalam menjaga integritas data lintas format file (teks, gambar, audio, dan video) tanpa menurunkan kualitas hasil dekripsi. Namun, peningkatan keamanan tersebut memiliki konsekuensi berupa waktu enkripsi yang lebih lama dan penggunaan sumber daya prosesor yang lebih besar, terutama pada perangkat dengan kapasitas komputasi rendah.

Selain itu, literatur yang dikaji menunjukkan adanya trade-off yang konsisten antara keamanan dan performa. AES-128 unggul dalam efisiensi dan kecepatan, AES-192 memberikan stabilitas dan keseimbangan, sementara AES-256 unggul dalam kekuatan keamanan jangka panjang. Perbedaan ini menegaskan pentingnya penyesuaian varian AES berdasarkan kebutuhan spesifik sistem dan tingkat sensitivitas data yang dilindungi (Hidayatulloh et al., 2023; Kusyanti & Amron, 2018; Indrayani et al., 2025).

Sebagai tindak lanjut, penelitian lanjutan disarankan untuk:

- Mengoptimalkan implementasi AES-256 pada framework web modern seperti Laravel dan Filament untuk pengamanan data berbasis server.
- Melakukan pengujian komparatif antara AES-128, AES-192, dan AES-256 dalam hal efisiensi waktu, konsumsi energi, serta beban pemrosesan pada server dengan spesifikasi berbeda.
- Mengeksplorasi integrasi AES dengan mekanisme keamanan tambahan seperti hardware encryption module (AES-NI) atau pendekatan hybrid cryptosystem guna meningkatkan performa tanpa mengorbankan keamanan.

Dengan demikian, hasil studi ini memperkuat pemahaman bahwa AES tetap menjadi algoritma enkripsi simetris paling kuat dan relevan hingga saat ini, serta membuka peluang bagi penelitian lanjutan dalam bidang optimasi performa kriptografi di lingkungan aplikasi web dan sistem terdistribusi modern.

Daftar Pustaka

Hidayatulloh, N. W., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A., & Yasin, M. (2023). *Mengenal Advanced Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data.* Digital Transformation Technology (Digitech), 3(1), 1–10.
Link: https://jurnal.itscience.org/index.php/digitech/article/view/2293

Kusyanti, A., & Amron, K. (2018). *Analisis Perbandingan Algoritma Advanced Encryption Standard untuk Enkripsi Short Message Service (SMS) pada Android.* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2(10), 4281–4289.
Link: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2893/1112

Santoso, T. B., & Rahman, F. H. (2022). *Analisa dan Perancangan Sistem Enkripsi dan Dekripsi Dokumen Berbasis Android Menggunakan Metode Advanced Encryption Standard–128 (Studi Kasus: PT. Kelab 21 Retail).* Jurnal Logika dan Manajemen Teknologi (JLMT), 2(1), 45–53.
Link: https://ojs-teknik.usni.ac.id/index.php/jlmt/article/view/197

Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2014). *Implementasi dan Analisis Algoritma Advanced Encryption Standard (AES) pada Tiga Variasi Panjang Kunci untuk Berkas Multimedia.* Jurnal Transient, Universitas Diponegoro, 3(4), 567–574.
Link: https://ejournal3.undip.ac.id/index.php/transient/article/view/10581

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). *Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format.* Digital Transformation Technology, 4(2), 1245–1251.
Link: https://jurnal.itscience.org/index.php/digitech/article/view/5457