LITERATURE REVIEW:
PERBANDINGAN KEAMANAN DAN PERFORMA ALGORITMA AES-128, AES-192, DAN AES-256

1. PENDAHULUAN

Seiring pesatnya perkembangan teknologi informasi, ketergantungan pada data digital menuntut jaminan keamanan yang semakin kuat. Algoritma kriptografi adalah fondasi utama dalam melindungi kerahasiaan dan integritas informasi tersebut. *Advanced Encryption Standard* (AES) telah diakui secara global sebagai standar emas (*gold standard*) untuk enkripsi simetris, yang distandarisasi oleh *National Institute of Standards and Technology* (NIST) (Information & Standards, 2023). Namun, AES bukanlah satu algoritma tunggal yang bersifat "satu ukuran untuk semua". Standar resmi dari NIST dalam publikasi FIPS 197 (Information & Standards, 2023) secara spesifik mendefinisikan tiga varian yang berbeda, yang dibedakan berdasarkan panjang kuncinya: AES-128, AES-192, dan AES-256. Ketiga varian ini, meskipun berasal dari keluarga algoritma Rijndael yang sama dan menggunakan ukuran blok 128-bit (Karki, 2018), memiliki perbedaan fundamental dalam arsitektur internalnya. Perbedaan itu terletak pada *key schedule* (proses pembentukan kunci) dan, yang paling penting, pada jumlah putaran (rounds) enkripsi AES-128 menggunakan 10 putaran, AES-192 menggunakan 12 putaran, dan AES-256 menggunakan 14 putaran (Information & Standards, 2023). Di sinilah letak inti permasalahannya. Perbedaan jumlah putaran ini secara langsung menciptakan sebuah *trade-off* (pertukaran) yang krusial, varian dengan kunci lebih panjang dan putaran lebih banyak (seperti AES-256) menawarkan tingkat keamanan teoretis yang lebih tinggi, namun harus "membayarnya" dengan kinerja komputasi yang lebih lambat (Andriani et al., 2018; Bi Irie guy-cedric, 2018). Oleh karena itu, tinjauan literatur ini bertujuan untuk menyelami dan menganalisis secara kritis *trade-off* algoritmik tersebut. Tinjauan ini akan menyintesis penelitian-penelitian sebelumnya untuk membandingkan secara langsung dua aspek utama dari ketiga varian AES, keamanan (termasuk seberapa besar *security margin* mereka dan resistensinya terhadap ancaman masa depan (Smith-tone, n.d.)) dan performa (seperti kecepatan *throughput*, latensi, dan konsumsi sumber daya (Alenezi et al., 2024; Andriani et al., 2018)). Manfaat dari studi ini adalah untuk memberikan gambaran yang jelas dan komprehensif bagi akademisi, pengembang, atau praktisi keamanan, sebagai panduan untuk menjawab pertanyaan praktis: "Kapan sebaiknya kita menggunakan AES-128 yang cepat?" dan "Dalam kondisi apa kita benar-benar membutuhkan keamanan ekstra dari AES-256?" Studi ini berupaya mengidentifikasi kasus penggunaan yang ideal untuk masing-masing varian berdasarkan analisis *trade-off* fundamental tersebut.

2. KONSEP DASAR ALGORITMA AES

Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris (*symmetric-key*) yang dipilih oleh NIST pada tahun 2001 untuk menggantikan standar DES yang sudah

usang (Information & Standards, 2023). AES didasarkan pada algoritma Rijndael dan secara teknis diakui karena kombinasi keamanan, performa, dan kemudahan implementasinya.

Sebagai *block cipher*, AES beroperasi pada blok data berukuran tetap, yaitu 128 bit (Information & Standards, 2023; Karki, 2018). Proses enkripsi dan dekripsi terdiri dari beberapa putaran (*rounds*) yang identik. Setiap putaran (kecuali putaran terakhir) menjalankan empat operasi matematis (Karki, 2018):

1. SubBytes: Substitusi non-linear untuk mengacak data.
2. ShiftRows: Transposisi untuk menggeser baris-baris data.
3. MixColumns: Operasi pencampuran (mixing) untuk difusi data.
4. AddRoundKey: Operasi XOR dengan kunci putaran (*round key*).

Perbedaan fundamental antara tiga varian AES yang disetujui NIST tidak terletak pada ukuran blok, melainkan pada panjang kunci (key length) dan jumlah putaran yang dieksekusi (Information & Standards, 2023):

- AES-128: Menggunakan kunci 128-bit dan menjalankan 10 putaran.
- AES-192: Menggunakan kunci 192-bit dan menjalankan 12 putaran.
- AES-256: Menggunakan kunci 256-bit dan menjalankan 14 putaran.

Perbedaan jumlah putaran inilah yang menjadi inti dari *trade-off* algoritma ini. Lebih banyak putaran (seperti pada AES-256) meningkatkan proses difusi dan konfusi, yang secara teoretis memperkuat algoritma terhadap serangan kriptanalisis. Namun, lebih banyak putaran juga berarti lebih banyak operasi komputasi yang harus dilakukan, yang secara langsung berdampak pada kinerja (kecepatan) algoritma (Andriani et al., 2018; Bi Irie guy-cedric, 2018).

3. TINJAUAN PENELITIAN TERDAHULU

Tinjauan literatur ini didasarkan pada analisis dan sintesis dari penelitian-penelitian kunci yang relevan. Studi-studi terdahulu yang digunakan sebagai landasan perbandingan keamanan dan performa varian AES dirangkum dalam tabel berikut:

No.	Penulis & Tahun	Judul Penelitian	Fokus Penelitian	Temuan Kunci / Hasil Utama	Kaitan dengan Topik Ini
[1]	National Institute of Standards and Technology	*Advanced Encryption Standard (AES)*	Standarisasi teknis algoritma AES.	Secara resmi menetapkan 3 varian AES: 128-bit (10 putaran), 192-bit (12	Landasan Teoretis Utama: Menjadi sumber primer yang mendefinisikan

	(NIST) (2023)	- *FIPS 197 Update 1*		putaran), dan 256-bit (14 putaran).	perbedaan jumlah putaran, yang merupakan dasar dari *trade-off* performa dan keamanan.
[2]	Karki, A. (2018)	*A Review on Advanced Encryption Standard (AES)*	Tinjauan umum (review) arsitektur dan langkah-langkah internal AES.	Menjelaskan 4 operasi internal (SubBytes, ShiftRows, MixColumns, AddRoundKey) yang diulang pada setiap putaran.	Landasan Konseptual: Menjelaskan *apa* operasi komputasi yang diulang-ulang, yang menyebabkan varian dengan putaran lebih banyak (AES-256) menjadi lebih lambat.
[3]	Andriani, R., dkk. (2018)	*Comparision Of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File*	*Benchmark* performa empiris dari ketiga varian AES (128, 192, 256) untuk enkripsi/dekripsi file.	Menemukan perbedaan waktu yang signifikan. Urutan performa (kecepatan) adalah: AES-128 (Tercepat) > AES-192 (Sedang) > AES-256 (Terlambat).	Bukti Performa Utama: Memberikan data empiris langsung yang mendukung argumen bahwa AES-128 unggul dalam performa.
[4]	Guy-Cedric, T. B. I., & Sup-Masa, A. (2018)	*A Comparative Study on AES 128 BIT AND AES 256 BIT*	Perbandingan performa (waktu) dan analisis keamanan teoretis antara AES-128 dan AES-256.	Mengonfirmasi bahwa AES-256 "membutuhkan lebih banyak waktu" karena arsitektur putarannya. Menyatakan bahwa keduanya (128 & 256) sangat aman dari serangan klasik (*brute-force*).	Bukti Trade-Off Ganda: Mendukung argumen Performa (128 > 256) sekaligus argumen Keamanan (128 & 256 sama-sama aman dari serangan klasik).
[5]	Alenezi, M., dkk. (2024)	*On the performance of AES algorithm variants*	Analisis performa modern dari ketiga varian AES, termasuk dalam konteks platform spesifik seperti IoT.	Mengonfirmasi temuan (Andriani et al., 2018), urutan performa 128 > 192 > 256. Menyoroti bahwa *trade-off* ini sangat penting di perangkat berdaya rendah (IoT) di mana performa (AES-128) lebih diutamakan.	Bukti Performa Modern: Memberikan validasi terbaru dan relevansi kasus penggunaan (IoT) untuk *trade-off* performa.

[6]	Chen, L., dkk. (NIST) (2016)	*Report on Post-Quantum Cryptography (NISTIR 8105)*	Analisis ancaman komputasi kuantum terhadap standar kriptografi saat ini.	Algoritma Grover (kuantum) memberikan *quadratic speedup* pada serangan *brute-force*. Ini melemahkan AES-128 (menjadi 2^{64}, rentan), tetapi AES-256 tetap aman (menjadi 2^{128}).	Bukti Keamanan Utama: Menjadi justifikasi ilmiah *mengapa* AES-256 (yang lebih lambat) ada dan diperlukan untuk keamanan jangka panjang (*future-proof*).

Tabel 3.1: Matriks Tinjauan Pustaka Varian AES

4. ANALISIS DAN SINTESIS

Sintesis dari literatur yang ada mengungkapkan *trade-off* yang jelas dan konsisten. Analisis ini dibagi menjadi tiga bagian: perbandingan performa, perbandingan keamanan, dan sintesis *trade-off* untuk kasus penggunaan.

4.1. Analisis Performa (Fokus: Kecepatan)

Hampir seluruh literatur *benchmark* menunjukkan korelasi langsung antara jumlah putaran dan kinerja.

- AES-128 adalah yang Tercepat karena hanya mengeksekusi 10 putaran, studi seperti yang dilakukan (Andriani et al., 2018) dan (Alenezi et al., 2024) secara konsisten menunjukkan bahwa AES-128 memiliki waktu enkripsi/dekripsi tercepat dan *throughput* (kecepatan transfer data) tertinggi.
- AES-256 adalah yang Terlambat dengan 14 putaran (40% lebih banyak dari AES-128), AES-256 secara konsisten menunjukkan performa paling lambat. Studi oleh Guy-Cedric & Sup-Masa (Bi Irie guy-cedric, 2018) menyoroti bahwa AES-256 "membutuhkan lebih banyak waktu" karena arsitektur putarannya yang lebih banyak.
- AES-192 Selalu di Tengah seperti yang diduga, kinerja AES-192 (12 putaran) selalu berada di antara AES-128 dan AES-256 (Alenezi et al., 2024; Andriani et al., 2018).

Perlu dicatat bahwa kesenjangan performa ini dapat mengecil pada CPU modern yang memiliki instruksi *hardware acceleration* (AES-NI). Namun, pada perangkat berdaya rendah (seperti *Internet of Things* atau *smartphone*) yang tidak memiliki AES-NI, perbedaan performa ini sangat signifikan dan menjadi faktor penentu utama.

4.2. Analisis Keamanan (Fokus: Kekuatan)

Pada aspek keamanan, perbandingannya lebih bernuansa:

- **Keamanan Saat Ini (Klasikal):** Terhadap komputer klasik yang ada saat ini, semua varian AES (termasuk AES-128) dianggap sangat aman. Jumlah 2^{128} kemungkinan kunci pada AES-128 secara praktis tidak mungkin di-*brute-force*. Studi seperti (Bi Irie guy-cedric, 2018) juga mengonfirmasi bahwa ketiganya memiliki *security margin* yang lebih dari cukup terhadap serangan kriptanalisis yang dikenal.
- **Keamanan Masa Depan (Kuantum):** Di sinilah letak perbedaan krusial dan justifikasi utama untuk AES-256. Laporan resmi dari NIST tentang Kriptografi Pasca-Kuantum (Smith-tone, n.d.) menyoroti ancaman dari Algoritma Grover pada komputer kuantum. Algoritma ini memberikan "percepatan kuadrat" (*quadratic speedup*) pada serangan *brute-force*.

Dampaknya adalah sebagai berikut (Smith-tone, n.d.):

- Keamanan efektif AES-128 (2^{128}) jatuh menjadi 2^{64}. Angka ini dianggap rentan dan tidak lagi aman untuk jangka panjang.
- Keamanan efektif AES-256 (2^{256}) jatuh menjadi 2^{128}. Angka ini (setara dengan AES-128 saat ini) dianggap masih sangat aman terhadap serangan kuantum.

Oleh karena itu, AES-256 adalah satu-satunya varian yang dianggap "quantum-resistant" atau *future-proof* (tahan masa depan).

4.3. Sintesis dan Rekomendasi (Analisis Trade-Off)

Analisis di atas menunjukkan bahwa tidak ada satu varian yang "terbaik". Pilihan di antara ketiganya adalah *trade-off* strategis:

- Pilih AES-128 jika prioritas Anda adalah performa, kecepatan, dan efisiensi energi. Ini adalah pilihan ideal untuk aplikasi *real-time* seperti *streaming*, game, koneksi web (HTTPS), dan terutama perangkat IoT (Alenezi et al., 2024) di mana keamanannya sudah lebih dari cukup untuk ancaman saat ini.
- Pilih AES-256 jika prioritas Anda adalah keamanan jangka panjang (future-proof). Ini adalah keharusan untuk data yang sangat sensitif (misal, "Top Secret" pemerintah), data arsip (perbankan, medis) yang harus tetap aman selama 50 tahun ke depan, dan untuk sistem yang ingin memitigasi risiko ancaman komputer kuantum (Smith-tone, n.d.).
- AES-192 secara praktis jarang digunakan. Studi (Alenezi et al., 2024; Andriani et al., 2018) menunjukkannya sebagai "jalan tengah" yang canggung. Pengembang biasanya memiliki kebutuhan yang jelas: "tercepat yang aman" (AES-128) atau "paling aman" (AES-256).

5. ARAH DAN PELUANG PENELITIAN

Tinjauan literatur ini telah memetakan *trade-off* fundamental antara AES-128, 192, dan 256: AES-128 unggul dalam performa (Alenezi et al., 2024; Andriani et al., 2018), sementara AES-256 unggul dalam jaminan keamanan jangka panjang terhadap ancaman kuantum (Smith-tone, n.d.).

Meskipun kesimpulan dasar ini sudah mapan, sebagian besar literatur (Alenezi et al., 2024; Andriani et al., 2018; Bi Irie guy-cedric, 2018) berfokus pada *apakah* ada perbedaan, bukan *bagaimana* perbedaan tersebut berdampak pada platform komputasi modern dan spesifik. Hal ini membuka beberapa celah penelitian (*research gaps*) yang jelas untuk studi di masa depan:

1. **Benchmark pada Arsitektur Modern (Non-x86):**

   Studi (Alenezi et al., 2024; Andriani et al., 2018) sudah valid, namun platform komputasi telah bergeser. Terdapat kebutuhan mendesak untuk penelitian baru yang mengukur trade-off performa (termasuk konsumsi energi/daya) dari ketiga varian pada arsitektur yang kini dominan, seperti:

   - **CPU berbasis ARM:** (Misalnya, di *smartphone*, Apple M-series, atau server AWS Graviton).
   - **GPU (Komputasi Paralel):** Untuk mengukur efisiensi enkripsi data skala besar (Big Data) secara paralel.

2. **Analisis di Luar Throughput Standar:**

   Performa bukan hanya soal throughput (MB/detik). Peluang penelitian ada pada analisis metrik yang lebih spesifik:

   - **Analisis Latensi (Penundaan):** Mengukur *penundaan* (latency) spesifik dari 10 vs 14 putaran. Ini sangat kritis untuk sistem *real-time* (misalnya, di industri otomotif atau avionik) di mana penundaan *milisecond* sangat berpengaruh.
   - **Resistensi *Side-Channel Attack* (SCA):** Menganalisis apakah *key schedule* AES-256 yang lebih kompleks (dan memakan lebih banyak waktu) membuatnya lebih rentan (atau justru lebih kuat) terhadap serangan fisik praktis seperti *Differential Power Analysis* (DPA) dibandingkan AES-128.

3. **Analisis Biaya Praktis vs Teoretis Kuantum:**

   Laporan NIST (Smith-tone, n.d.) menjelaskan ancaman Algoritma Grover secara teoretis. Namun, penelitian di masa depan diperlukan untuk menganalisis biaya komputasi praktis (resource cost) yang dibutuhkan untuk menjalankan serangan tersebut. Studi ini akan membantu industri memutuskan kapan (misal, dalam 10, 20, atau 30 tahun) ancaman teoretis terhadap AES-128 ini menjadi sebuah risiko praktis yang nyata.

6. KESIMPULAN DAN SARAN

Kesimpulan

Tinjauan literatur ini menyimpulkan bahwa pilihan antara AES-128, AES-192, dan AES-256 bukanlah pilihan antara "aman" dan "tidak aman", melainkan sebuah trade-off strategis antara kinerja (performa) dan jaminan keamanan jangka panjang. Literatur (Alenezi et al., 2024; Andriani et al., 2018) secara konsisten membuktikan bahwa AES-128 adalah standar untuk kinerja tinggi dengan tingkat keamanan yang sangat memadai untuk hampir semua ancaman komputasi klasik saat ini (Bi Irie guy-cedric, 2018). Sebaliknya, AES-256 meskipun lebih lambat (Andriani et al., 2018; Bi Irie guy-cedric, 2018) adalah standar untuk keamanan maksimum, yang menawarkan security margin tertinggi dan merupakan satu-satunya varian yang memberikan perlindungan memadai terhadap ancaman komputasi kuantum di masa depan (Smith-tone, n.d.).

Saran

Meskipun perbandingan performa dasar sudah banyak diteliti, celah penelitian (research gap) masih ada. Penelitian di masa depan dapat berfokus pada analisis trade-off ini pada arsitektur komputasi yang lebih baru, seperti perbandingan performa dan konsumsi energi pada CPU berbasis ARM (misal, di smartphone atau server modern) versus x86. Selain itu, studi yang menganalisis efisiensi ketiga varian ini dalam lingkungan komputasi paralel masif (menggunakan GPU/CUDA) untuk enkripsi data skala besar (Big Data) akan sangat berharga.

DAFTAR PUSTAKA

Alenezi, M., Alabdulrazzaq, H., Alhatlani, H., & Alobaid, F. (2024). On the performance of AES algorithm variants. *International Journal of Information and Computer Security*, *23*, 322–337. https://doi.org/10.1504/IJICS.2024.138494

Andriani, R., Wijayanti, S. E., & Wibowo, F. W. (2018). Comparision Of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File. *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, 120–124. https://doi.org/10.1109/ICITISEE.2018.8720983

Bi Irie guy-cedric, T. (2018). A Comparative Study on AES 128 BIT AND AES 256 BIT. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, *volume 6*, 30–33. https://doi.org/10.26438/ijsrcse/v6i4.3033

Information, F., & Standards, P. (2023). *Advanced Encryption Standard (AES)*.

Karki, A. (2018). A Review on Advanced Encryption Standard (AES). *International Journal of Computer Sciences and Engineering*, *6*, 551–556. https://doi.org/10.26438/ijcse/v6i8.551556

Smith-tone, D. (n.d.). *Report on Post-Quantum Cryptography Report on Post-Quantum Cryptography*.