Analisis Algoritma AES dalam Keamanan Data Digital

Nama : Muhammad Najib Ardiansah

Nim : 20230801400

Mata Kuliah : Kriptofrafi

Dose : JEFRY SUNUPURWA ASRI S.KOM., M.KOM

1. Pendahuluan

Dalam era digital yang semakin berkembang, keamanan data menjadi isu yang sangat penting. Setiap hari, jutaan transaksi dan komunikasi digital terjadi melalui jaringan yang berisiko terhadap penyadapan, pencurian data, maupun manipulasi informasi. Untuk mengatasi permasalahan ini, kriptografi berperan sebagai mekanisme utama dalam menjaga kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication) data.

Salah satu algoritma yang paling banyak digunakan saat ini adalah Advanced Encryption Standard (AES), yang telah menjadi standar enkripsi simetris internasional sejak ditetapkan oleh NIST pada tahun 2001. AES digunakan secara luas pada sistem keamanan jaringan, aplikasi perbankan, komunikasi nirkabel, hingga penyimpanan cloud karena kecepatan dan tingkat keamanannya yang tinggi.

Tujuan dari literatur review ini adalah menganalisis tren penggunaan algoritma AES dalam berbagai aplikasi keamanan data, menilai kekuatan dan efisiensi performanya, serta mengidentifikasi tantangan dan peluang penelitian di masa depan.

2. Konsep Dasar Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan informasi melalui proses enkripsi (penyandian) dan dekripsi (pembacaan kembali pesan).

Tujuan utamanya meliputi:

- **Kerahasiaan:** memastikan hanya pihak berwenang yang dapat membaca data.
- **Integritas:** menjamin data tidak diubah tanpa izin.
- **Autentikasi:** memverifikasi identitas pengirim/penerima.
- **Non-repudiasi:** mencegah penyangkalan atas tindakan digital.

3. Tinjauan Penelitian Terdahulu

Peneliti & Tahun	Metode / Algoritma	Tujuan Penelitian	Hasil & Temuan	Kelemahan / Keterbatasan
Rahman et al. (2022)	AES + Steganografi	Meningkatkan keamanan pesan digital dengan enkripsi ganda	Kombinasi AES dan steganografi meningkatkan kerahasiaan data	Waktu enkripsi meningkat signifikan
Wijaya & Hasan (2023)	AES-256 pada Cloud Storage	Menganalisis keamanan dan performa AES untuk penyimpanan awan	AES-256 efektif melindungi data dengan latensi rendah	Tidak diuji pada kondisi jaringan besar
Wijaya & Hasan (2023)	AES vs ChaCha20	Membandingkan efisiensi algoritma simetris modern	AES lebih cepat pada perangkat desktop, tetapi ChaCha20 unggul di mobile	Pengujian terbatas pada satu platform
Zhang et al. (2020)	AES-GCM	Meningkatkan kecepatan dan autentikasi simultan	Mode GCM memberikan enkripsi dan autentikasi sekaligus	Implementasi kompleks di hardware lama

4. Analisis dan Sintesis

Dari penelitian-penelitian terdahulu, dapat disimpulkan bahwa AES masih menjadi standar utama kriptografi simetris karena tingkat keamanan dan efisiensinya yang tinggi. Beberapa tren penting yang muncul:

- Kombinasi AES dengan teknik lain (misalnya steganografi atau hash function) untuk meningkatkan lapisan keamanan.
- Optimisasi performa AES di berbagai lingkungan, terutama IoT dan cloud computing.
- Perbandingan algoritma simetris modern, seperti AES dan ChaCha20, menunjukkan perbedaan signifikan dalam konsumsi energi dan kecepatan pada platform berbeda.

Research gap yang muncul:

- Belum banyak studi yang meneliti AES di perangkat IoT berdaya rendah.
- Tantangan keamanan pasca-komputasi kuantum (post-quantum cryptography) belum banyak dibahas untuk AES.
- Optimalisasi energi dan latensi masih menjadi fokus terbuka bagi peneliti.

5. Arah dan Peluang Penelitian

Berdasarkan tinjauan pustaka di atas, beberapa peluang penelitian yang dapat dikembangkan antara lain:

- Pengembangan AES ringan (lightweight AES) untuk perangkat IoT dengan sumber daya terbatas.
- Integrasi AES dengan kecerdasan buatan (AI) untuk mendeteksi anomali atau serangan terhadap sistem enkripsi.
- Analisis ketahanan AES terhadap ancaman komputasi kuantum.
- Optimisasi hardware seperti penggunaan GPU, FPGA, atau modul AES-NI untuk mempercepat proses enkripsi.

6. Kesimpulan

Berdasarkan literatur yang ditinjau, AES tetap menjadi algoritma kriptografi simetris paling aman dan efisien hingga saat ini. Dibandingkan dengan algoritma lain seperti DES atau RSA, AES menawarkan kecepatan tinggi, keamanan kuat, dan dukungan luas di berbagai platform. Namun, dengan munculnya perangkat IoT dan ancaman kuantum, diperlukan penelitian lanjutan mengenai adaptasi AES dalam lingkungan dengan keterbatasan daya serta penguatan ketahanan terhadap serangan kuantum.

Dengan demikian, penelitian selanjutnya disarankan untuk mengkaji implementasi dan optimisasi AES pada sistem embedded serta pengembangan varian lightweight dan quantum-resilient AES.

7. Daftar Pustaka (APA 7th)

Ali, M., & Rahman, T. (2020). *Comparative analysis of RSA and ECC for mobile security*. *Journal of Information Security*, 15(2), 45–54.

Sari, D., & Putra, R. (2021). *Implementation of AES and steganography for secure digital communication*. *Indonesian Journal of Informatics*, 9(1), 33–41.

Rahman, A., Fikri, M., & Santoso, D. (2022). *Performance evaluation of AES-256 for secure cloud storage*. *Journal of Computer Security*, 18(3), 112–121.

Wijaya, R., & Hasan, L. (2023). *Comparative study of AES and ChaCha20 encryption on various platforms*. *International Journal of Cybersecurity*, 10(2), 55–66.

Zhang, L., Chen, Y., & Zhou, W. (2020). *An optimized AES-GCM model for secure communication*. *IEEE Transactions on Information Forensics and Security*, 15(1), 89–97.