STUDI LITERATUR

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

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

Studi Literatur: Analisis Algoritma Advanced Encryption Standard (AES) 128, 192, dan 256 Bit dalam Pengamanan Data

1. Pendahuluan

Keamanan data digital merupakan aspek fundamental dalam pengembangan sistem informasi modern. Peningkatan aktivitas digital seperti transaksi, penyimpanan berbasis cloud, dan komunikasi daring menimbulkan risiko kebocoran serta penyalahgunaan data yang semakin kompleks. Oleh karena itu, dibutuhkan sistem perlindungan yang mampu menjamin kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication) data. Salah satu pendekatan yang paling banyak digunakan untuk memenuhi kebutuhan tersebut adalah kriptografi.

Salah satu algoritma kriptografi simetris yang menjadi standar global adalah Advanced Encryption Standard (AES). Algoritma ini disahkan oleh National Institute of Standards and Technology (NIST) pada tahun 2001 untuk menggantikan Data Encryption Standard (DES) yang telah dianggap rentan terhadap serangan kriptanalisis modern. AES memiliki struktur yang efisien, tingkat keamanan tinggi, serta dukungan tiga varian panjang kunci 128, 192, dan 256 bit sehingga banyak digunakan dalam berbagai aplikasi seperti pengamanan file digital, komunikasi jaringan, dan sistem basis data.

Pemilihan AES dalam studi literatur ini didasarkan pada relevansinya dengan kebutuhan keamanan sistem informasi masa kini dan bukti empiris dari berbagai penelitian terdahulu. Berdasarkan tinjauan pustaka, Kusyanti dan Amron (2018) meneliti performa tiga varian AES pada enkripsi pesan singkat di Android dan menemukan bahwa AES-128 unggul dalam kecepatan, sementara AES-256 lebih unggul dalam kekuatan keamanan. Widyastuti et al. (2019) membuktikan efektivitas AES dalam menjaga kerahasiaan data web, sedangkan Wachid Hidayatulloh et al. (2023) meninjau struktur internal AES secara teoretis dan menjelaskan mekanisme keamanan matematisnya. Manullang (2023) meneliti penerapan AES untuk pengamanan dokumen digital, dan Indrayani et al. (2025) menunjukkan keunggulan AES-256 dalam melindungi berbagai format file digital dari serangan brute force.

Berdasarkan berbagai temuan tersebut, studi literatur ini bertujuan untuk menganalisis dan membandingkan hasil-hasil penelitian terdahulu guna memperoleh pemahaman yang lebih mendalam mengenai performa, efisiensi, dan tingkat keamanan tiap varian AES. Hasil analisis ini juga menjadi dasar pengembangan penelitian selanjutnya yang berfokus pada implementasi algoritma AES-256 dalam framework Laravel dan Filament untuk mengamankan data catatan pribadi pengguna, sebagai langkah konkret penerapan kriptografi modern pada sistem web yang interaktif dan efisien.

2. Konsep Dasar Kriptografi dan Algoritma AES

2.1 Definisi Kriptografi

Kriptografi merupakan ilmu dan seni untuk mengamankan informasi dengan mengubah data asli (plaintext) menjadi bentuk acak yang tidak dapat dibaca (ciphertext) menggunakan algoritma dan kunci tertentu. Proses kebalikannya disebut dekripsi, yaitu mengembalikan ciphertext menjadi plaintext menggunakan kunci yang sesuai. Tujuan utama dari kriptografi adalah untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan keaslian (authenticity) data baik saat disimpan maupun dikirimkan melalui jaringan digital.

Secara umum, kriptografi terbagi menjadi dua jenis besar, yaitu kriptografi klasik dan kriptografi modern.

- Kriptografi klasik menggunakan teknik substitusi dan transposisi huruf atau simbol, di mana proses enkripsi dilakukan secara manual dengan pola tertentu. Contohnya adalah Caesar Cipher dan Vigenère Cipher. Sistem ini lebih sederhana tetapi mudah dipecahkan menggunakan analisis frekuensi atau brute force.
- Kriptografi modern, seperti Advanced Encryption Standard (AES), RSA, dan Blowfish, memanfaatkan operasi matematis yang kompleks dan pengelolaan kunci digital. Algoritma modern dirancang untuk keamanan tingkat tinggi dan efisiensi dalam pengolahan data komputer, serta mampu melindungi informasi dalam sistem besar seperti aplikasi web, jaringan, dan basis data.

Dalam konteks penelitian ini, kriptografi modern menjadi fokus utama karena relevansinya dengan kebutuhan keamanan data digital masa kini, khususnya melalui penerapan algoritma AES pada sistem web berbasis Laravel Filament.

2.2 Tujuan Utama Kriptografi

Tujuan kriptografi mencakup empat aspek utama, yaitu:

- Kerahasiaan (Confidentiality): memastikan data tidak dapat dibaca oleh pihak yang tidak berwenang.
- Integritas (Integrity): menjamin data tidak mengalami perubahan tanpa izin.
- Autentikasi (Authentication): memastikan identitas pengirim dan penerima valid.
- Non-repudiasi: mencegah pengirim menyangkal telah melakukan pengiriman data.

Aspek-aspek ini menjadi dasar dalam setiap penerapan algoritma kriptografi, termasuk AES, terutama dalam sistem digital yang memerlukan keamanan data tinggi seperti penyimpanan dokumen dan aplikasi web.

2.3 Jenis-Jenis Kriptografi

Secara umum, kriptografi dibagi menjadi tiga jenis utama berdasarkan penggunaan kuncinya:

Jenis Kriptografi	Contoh Algoritma	Karakteristik	Catatan
Simetris	AES, DES, Blowfish	Menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi	Cepat dan efisien, cocok untuk data berukuran besar
Asimetris	RSA, ECC	Menggunakan pasangan kunci publik dan privat	Lebih aman untuk pertukaran kunci, tetapi lebih lambat
Hash	SHA, MD5	Fungsi satu arah tanpa proses dekripsi	Sangat cepat, digunakan untuk verifikasi integritas data

Dalam konteks aplikasi modern, algoritma simetris seperti AES lebih banyak digunakan karena lebih efisien dalam kecepatan proses enkripsi dan dekripsi, terutama untuk data yang sering diakses.

2.4 Prinsip dan Struktur Algoritma AES

Advanced Encryption Standard (AES) merupakan algoritma blok simetris dengan ukuran blok tetap 128 bit, serta mendukung tiga panjang kunci yang berbeda, yaitu 128, 192, dan 256 bit. Panjang kunci ini menentukan jumlah ronde atau tahap transformasi yang dilakukan selama proses enkripsi dan dekripsi:

- AES-128 terdiri dari 10 ronde,
- AES-192 terdiri dari 12 ronde,
- AES-256 terdiri dari 14 ronde.

Setiap ronde terdiri dari empat tahap utama:

1. SubBytes: melakukan substitusi non-linear pada setiap byte menggunakan tabel S-Box.
2. ShiftRows: menggeser posisi baris untuk memperluas difusi data.
3. MixColumns: mencampur kolom untuk memperkuat penyebaran bit di seluruh blok.
4. AddRoundKey: menggabungkan blok data dengan kunci ronde menggunakan operasi XOR.

Semakin panjang kunci yang digunakan, semakin besar tingkat keamanan yang diperoleh, namun waktu pemrosesan juga meningkat. Oleh karena itu, pemilihan varian AES perlu disesuaikan dengan kebutuhan sistem. Pada sistem dengan keterbatasan sumber daya, AES-128 lebih efisien, sementara AES-256 lebih ideal untuk pengamanan data sensitif dalam aplikasi berskala besar.

3. Tinjauan Penelitian Terdahulu

Lima jurnal digunakan sebagai dasar studi literatur ini karena masing-masing memberikan kontribusi terhadap pemahaman performa dan keamanan Advanced Encryption Standard (AES) dalam konteks aplikasi yang berbeda — mulai dari enkripsi pesan singkat di Android, pengamanan file digital, hingga analisis konseptual struktur AES. Kajian ini memberikan gambaran menyeluruh tentang efektivitas AES baik secara teoritis maupun praktis, serta membuka peluang penelitian lebih lanjut untuk implementasi pada sistem web modern seperti Laravel Filament.

Kusyanti dan Amron (2018) meneliti perbandingan algoritma AES-128, AES-192, dan AES-256 untuk enkripsi pesan singkat (SMS) pada perangkat Android. Hasil menunjukkan bahwa AES-128 memiliki waktu enkripsi tercepat, sedangkan AES-256 memberikan tingkat keamanan tertinggi, meskipun membutuhkan waktu proses lebih lama. Penelitian ini menegaskan bahwa pemilihan varian AES harus disesuaikan dengan kebutuhan antara performa dan keamanan, namun masih terbatas pada data teks dan belum melibatkan pengujian pada sistem berskala besar.

Widyastuti, Ariandi, dan Sulistiono (2019) melakukan studi tentang penerapan AES untuk melindungi informasi dalam sistem berbasis web. Hasil penelitian menunjukkan bahwa AES mampu menjaga kerahasiaan dan integritas data pengguna melalui mekanisme enkripsi simetris yang efisien. Meskipun demikian, penelitian ini tidak menguraikan secara rinci varian panjang kunci yang digunakan dan belum membahas analisis komparatif antarvarian AES.

Wachid Hidayatulloh, Tahir, dan Amalia (2023) mengulas konsep dan implementasi algoritma AES dalam konteks pengamanan data digital. Penelitian ini menyoroti struktur internal AES, termasuk proses SubBytes, ShiftRows, MixColumns, dan AddRoundKey, serta keunggulannya dalam melindungi data dari serangan kriptanalisis linear dan diferensial. Kajian ini bersifat konseptual dan memberikan landasan teoretis yang kuat, namun belum diikuti dengan implementasi pada sistem nyata.

Manullang (2023) meneliti penerapan AES dalam konteks pengamanan dokumen digital. Hasilnya menunjukkan bahwa algoritma ini mampu mempertahankan kerahasiaan dan konsistensi data, serta memberikan tingkat keamanan tinggi terhadap modifikasi tidak sah. Akan tetapi, penelitian belum membahas dampak ukuran file dan panjang kunci terhadap performa waktu enkripsi dan dekripsi.

Indrayani, Ferdiansyah, dan Koprawi (2025) fokus pada implementasi AES-256 untuk pengamanan file dengan berbagai format digital. Penelitian ini menegaskan bahwa AES-256 menawarkan perlindungan data yang sangat kuat terhadap brute-force attack dan cocok digunakan pada aplikasi yang memerlukan keamanan tinggi. Namun, kompleksitas komputasi AES-256 menyebabkan waktu enkripsi lebih lama, terutama untuk file berukuran besar.

Secara keseluruhan, kelima penelitian tersebut menunjukkan bahwa AES tetap menjadi algoritma unggulan dalam keamanan data digital berkat kombinasi efisiensi dan kekuatannya. Meski demikian, masih terdapat ruang penelitian dalam pengujian performa pada framework web modern seperti Laravel dan integrasinya dengan antarmuka manajemen data seperti Filament.

Ringkasan Penelitian Terdahulu Terkait Algoritma AES

Peneliti & Tahun	Metode / Algoritma	Tujuan Penelitian	Hasil & Temuan	Kelemahan / Keterbatasan
Kusyanti & Amron (2018)	AES-128, AES-192, AES-256	Membandingkan performa enkripsi SMS di Android	AES-128 tercepat, AES-256 paling aman	Pengujian terbatas pada teks SMS
Widyastuti et al. (2019)	AES (umum)	Pengamanan data web pengguna	AES efektif menjaga kerahasiaan data	Tidak membahas varian dan performa
Wachid Hidayatulloh et al. (2023)	AES (kajian teoretis)	Analisis struktur dan mekanisme AES	Analisis mendalam terhadap kekuatan AES	Tidak ada implementasi nyata
Manullang (2023)	AES (file-level encryption)	Pengamanan dokumen digital	AES efektif menjaga integritas data	Tidak menganalisis waktu enkripsi
Indrayani et al. (2025)	AES-256	Pengamanan berbagai format file	AES-256 sangat kuat terhadap brute-force	Waktu enkripsi meningkat untuk file besar

4. Analisis dan Sintesis

4.1 Perbandingan Performa dan Keamanan

Algoritma AES memiliki tiga varian utama, yaitu AES-128, AES-192, dan AES-256, yang dibedakan berdasarkan panjang kunci dan jumlah ronde enkripsi. Varian dengan kunci lebih pendek memiliki kecepatan lebih tinggi, sedangkan varian dengan kunci lebih panjang memberikan tingkat keamanan lebih kuat.

AES-128 menunjukkan kinerja enkripsi paling cepat karena hanya memerlukan 10 ronde proses, sehingga cocok diterapkan pada sistem dengan kebutuhan performa tinggi dan data berukuran kecil. AES-192 memberikan keseimbangan antara kecepatan dan keamanan, namun belum banyak diuji dalam konteks sistem informasi dinamis. AES-256 memiliki ketahanan paling tinggi terhadap serangan brute force dan analisis kriptografi karena ruang kunci yang sangat besar, tetapi waktu pemrosesan yang dibutuhkan lebih lama.

Secara umum, AES memberikan kombinasi antara efisiensi dan keamanan yang dapat disesuaikan dengan kebutuhan sistem. Pada aplikasi berbasis web atau perangkat mobile, AES-128 lebih efisien digunakan, sedangkan untuk perlindungan data jangka panjang atau file besar, AES-256 menjadi pilihan yang lebih aman.

4.2 Analisis Sintesis Kontekstual

Implementasi AES banyak digunakan untuk melindungi data dalam berbagai bentuk seperti pesan teks, file digital, maupun basis data. Pada konteks sistem web, algoritma ini berfungsi menjaga kerahasiaan data pengguna selama proses penyimpanan dan pertukaran informasi. Penggunaan AES juga dapat diterapkan pada pengamanan data pribadi, misalnya catatan aktivitas pengguna atau catatan pribadi dalam aplikasi manajemen harian.

Sebagian besar penelitian sebelumnya menekankan pengamanan pada data statis seperti file dokumen atau arsip digital. Namun, potensi penggunaan AES dalam sistem web dinamis yang melibatkan interaksi CRUD masih belum dieksplorasi secara mendalam. Integrasi AES dalam framework PHP modern seperti Filament dapat menjadi pendekatan baru untuk mengamankan data pengguna secara langsung di tingkat aplikasi, tanpa perlu sistem eksternal tambahan.

4.3 Research Gap

Hasil analisis menunjukkan adanya peluang penelitian baru dalam penerapan algoritma AES, yaitu:

1. Implementasi langsung AES pada framework PHP modern seperti Filament untuk mengamankan data pengguna secara terintegrasi.
2. Evaluasi performa tiga varian AES (128, 192, dan 256 bit) dalam konteks sistem web dinamis dengan aktivitas CRUD.
3. Pengujian pengaruh mode operasi AES (CBC, ECB, dan GCM) terhadap kecepatan enkripsi dan tingkat keamanan pada aplikasi web.

Celah ini membuka arah penelitian lanjutan untuk mengembangkan sistem informasi berbasis web yang tidak hanya efisien, tetapi juga memiliki lapisan keamanan yang kuat menggunakan algoritma kriptografi AES.

5. Arah dan Peluang Penelitian

Arah penelitian yang diusulkan berfokus pada penerapan algoritma AES-256 untuk mengamankan data pada aplikasi web berbasis Laravel dan Filament. Penelitian ini bertujuan untuk membangun sistem sederhana yang dapat menjaga kerahasiaan catatan pribadi pengguna melalui proses enkripsi sebelum data disimpan ke database, serta dekripsi otomatis saat data ditampilkan kembali.

Penerapan ini dapat dimulai dengan membangun fitur CRUD (Create, Read, Update, Delete) untuk catatan pengguna, di mana setiap proses penyimpanan dan pembaruan data akan dienkripsi menggunakan AES-256. Dengan demikian, meskipun data diakses langsung melalui database, isinya tetap tidak dapat dibaca tanpa kunci enkripsi yang tepat.

Selain itu, penelitian dapat diarahkan untuk mengukur efisiensi proses enkripsi dan dekripsi pada data berukuran kecil hingga sedang, yang umum digunakan pada aplikasi web personal. Evaluasi performa meliputi waktu pemrosesan dan penggunaan sumber daya server.

Pemilihan AES-256 didasarkan pada tingkat keamanan yang lebih tinggi dibandingkan varian lainnya (AES-128 dan AES-192), karena memiliki panjang kunci yang lebih besar dan ketahanan yang kuat terhadap serangan brute force. Meskipun membutuhkan sedikit lebih banyak waktu proses, selisihnya tidak signifikan untuk aplikasi skala kecil seperti sistem catatan pribadi.

Peluang pengembangan lanjutan dapat mencakup integrasi enkripsi AES-256 dengan fitur keamanan Laravel lainnya, seperti middleware autentikasi atau enkripsi otomatis pada kolom sensitif di model Eloquent. Selain itu, tampilan berbasis Filament dapat dimanfaatkan untuk memberikan pengalaman pengguna yang lebih interaktif sekaligus aman, tanpa mengurangi efisiensi sistem.

6. Kesimpulan

Berdasarkan hasil kajian terhadap lima jurnal yang dianalisis, dapat disimpulkan bahwa Advanced Encryption Standard (AES) masih menjadi algoritma yang paling relevan dan kuat dalam pengamanan data digital modern. AES memiliki kombinasi optimal antara kecepatan pemrosesan, efisiensi sumber daya, dan kekuatan kriptografi yang tinggi, menjadikannya algoritma yang secara luas diadopsi dalam berbagai sistem mulai dari aplikasi mobile, pengamanan basis data web, hingga proteksi file digital.

Hasil tinjauan menunjukkan bahwa:

- AES-128 memiliki keunggulan dalam kecepatan enkripsi dan dekripsi, sehingga cocok untuk aplikasi dengan kebutuhan performa tinggi dan data ringan, seperti yang dibuktikan pada penelitian Kusyanti dan Amron (2018).
- AES-192 memberikan keseimbangan antara efisiensi dan keamanan, namun masih memerlukan lebih banyak penelitian empiris untuk menilai performanya pada konteks aplikasi nyata, sebagaimana dijelaskan oleh Widyastuti, Ariandi, dan Sulistiono (2019).
- AES-256 memberikan tingkat keamanan tertinggi berkat panjang kunci yang lebih besar, seperti yang diuraikan oleh Indrayani, Ferdiansyah, dan Koprawi (2025), meskipun membutuhkan waktu proses yang sedikit lebih lama.

Dari keseluruhan literatur, terlihat bahwa penerapan AES dalam konteks aplikasi web modern masih jarang dieksplorasi, terutama dalam framework berbasis Laravel dan Filament. Oleh karena itu, penelitian lanjutan diarahkan untuk mengimplementasikan AES-256 dalam sistem catatan pribadi berbasis Laravel Filament, dengan tujuan mengamankan data pengguna dari potensi akses tidak sah, sekaligus menguji sejauh mana efisiensi dan keamanan AES-256 dapat dioptimalkan dalam konteks aplikasi web interaktif.

Dengan demikian, studi ini memberikan landasan teoretis dan arah praktis bagi pengembangan sistem keamanan data berbasis kriptografi modern di lingkungan web, khususnya bagi pengembang yang ingin memadukan keamanan tingkat tinggi (AES-256) dengan kemudahan pengelolaan data melalui Filament.

7. Daftar Pustaka

[1] A. Kusyanti and K. Amron, “Analisis Perbandingan Algoritma Advanced Encryption Standard Untuk Enkripsi Short Message Service (SMS) Pada Android,” *J. Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 10, pp. 4281–4289, 2018.

[2] S. Widyastuti, W. Ariandi, and V. Sulistiono, “Implementasi Kriptografi AES Dalam Pengamanan Data Seleksi Peserta JAMKESMAS,” *J. Ilmiah Intech: Information Technology Journal of UMUS*, vol. 1, no. 02, pp. 13–22, Nov. 2019.

[3] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, “Mengenal Advance Encryption Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data,” *Digital Transformation Technology (Digitech)*, vol. 3, no. 1, pp. 1–10, 2023.

[4] S. F. Manullang, “Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Cipher Block Chaining,” *J. Ilmiah Teknik Informatika*, vol. 17, no. 1, pp. 53–67, 2023.

[5] R. Indrayani, P. Ferdiansyah, and M. Koprawi, “Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format,” *Digital Transformation Technology*, vol. 4, no. 2, pp. 1245–1251, 2025, doi:10.47709/digitech.v4i2.5457.