e-XXXX-XXXX

Original Article

Implementasi Enkripsi Data untuk Perlindungan Informasi Sensitif

Angel Putri Maharani[1]✉, M. Aldi Ramadana[2], Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: angelputrimaharani.241031070@mahasiswa.ith.ac.id, m.aldiramadana.241031066@mahasiswa.ith.ac.id, rakhmadi.rahman@ith.ac.id

Abstrak:

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan sistem informasi digital dalam berbagai sektor, seperti pendidikan, pemerintahan, kesehatan, dan bisnis. Sistem informasi digunakan untuk menyimpan, memproses, serta mendistribusikan data dalam jumlah besar, termasuk data yang bersifat sensitif. Informasi sensitif mencakup data pribadi, data keuangan, data kesehatan, serta dokumen penting yang memerlukan perlindungan khusus. Namun, meningkatnya ketergantungan terhadap sistem digital juga diiringi dengan meningkatnya ancaman keamanan data, seperti kebocoran data, pencurian informasi, dan akses tidak sah. Salah satu mekanisme utama dalam menjaga keamanan informasi sensitif adalah penerapan enkripsi data. Enkripsi berfungsi untuk mengubah data asli menjadi bentuk yang tidak dapat dipahami tanpa kunci tertentu. Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang telah diakui secara internasional karena memiliki tingkat keamanan tinggi serta efisiensi dalam proses enkripsi dan dekripsi. Penelitian ini bertujuan untuk mengkaji implementasi enkripsi data menggunakan algoritma AES sebagai solusi perlindungan informasi sensitif pada sistem informasi. Metode penelitian yang digunakan adalah studi literatur deskriptif dengan menganalisis tiga jurnal internasional dan dua jurnal nasional yang relevan dengan topik enkripsi data dan keamanan informasi. Analisis dilakukan dengan membandingkan pendekatan enkripsi yang digunakan serta mengevaluasi efektivitasnya berdasarkan prinsip Confidentiality, Integrity, dan Availability (CIA). Hasil kajian menunjukkan bahwa implementasi enkripsi AES mampu meningkatkan keamanan data secara signifikan dan menjadi solusi yang efektif dalam melindungi informasi sensitif.

Keywords: Enkripsi data, AES, keamanan informasi, informasi sensitif

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

Pendahuluan

Perkembangan teknologi informasi pada era digital telah membawa perubahan yang signifikan dalam pengelolaan data dan informasi. Hampir seluruh aktivitas organisasi modern bergantung pada sistem informasi berbasis komputer dan jaringan untuk menyimpan, mengolah, serta mendistribusikan data. Data yang dikelola tidak hanya berupa informasi umum, tetapi juga mencakup informasi sensitif yang memiliki nilai tinggi dan bersifat rahasia, seperti data pribadi pengguna, data keuangan, data akademik, data kesehatan, serta dokumen penting organisasi.

Seiring dengan meningkatnya pemanfaatan sistem informasi digital, ancaman terhadap keamanan data juga semakin kompleks. Berbagai kasus kebocoran data, baik di tingkat nasional maupun internasional, menunjukkan bahwa keamanan informasi masih menjadi tantangan utama. Kebocoran data dapat disebabkan oleh lemahnya mekanisme pengamanan, kesalahan konfigurasi sistem, serangan siber, maupun rendahnya kesadaran pengguna terhadap pentingnya perlindungan data. Dampak yang ditimbulkan tidak hanya merugikan individu, tetapi juga dapat menurunkan kepercayaan publik terhadap organisasi dan sistem informasi yang digunakan.

Oleh karena itu, keamanan informasi menjadi aspek yang sangat penting dalam pengelolaan sistem informasi. Keamanan informasi bertujuan untuk melindungi data dari akses tidak sah, perubahan data yang tidak diinginkan, serta gangguan terhadap ketersediaan informasi. Salah satu teknik yang banyak digunakan untuk menjaga keamanan data adalah enkripsi. Melalui enkripsi, informasi sensitif dapat disimpan dan dikirimkan dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang.

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang telah ditetapkan sebagai standar oleh National Institute of Standards and Technology (NIST). Algoritma ini banyak diterapkan pada berbagai sistem keamanan karena memiliki tingkat keamanan yang tinggi serta efisiensi yang baik. Berdasarkan latar belakang tersebut, penelitian ini mengkaji implementasi enkripsi data menggunakan algoritma AES sebagai upaya perlindungan informasi sensitif dengan mengacu pada hasil penelitian sebelumnya dari jurnal nasional maupun internasional.

Tinjauan Pustaka

Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi informasi dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Keamanan informasi tidak hanya berkaitan dengan aspek teknis, tetapi juga mencakup kebijakan organisasi, prosedur operasional, serta perilaku pengguna dalam mengelola dan memanfaatkan informasi. Sistem keamanan yang baik harus mampu melindungi data dari ancaman internal maupun eksternal yang berpotensi menimbulkan kerugian.

Dalam konteks sistem informasi modern yang terhubung dengan jaringan global, kompleksitas ancaman keamanan semakin meningkat. Oleh karena itu, diperlukan mekanisme keamanan yang kuat, terintegrasi, dan berkelanjutan untuk melindungi data sensitif dari berbagai bentuk serangan siber.

Prinsip Confidentiality, Integrity, dan Availability (CIA)

Prinsip Confidentiality, Integrity, dan Availability (CIA) merupakan fondasi utama dalam evaluasi keamanan sistem informasi. Confidentiality memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki otorisasi. Integrity menjamin bahwa data tetap akurat, konsisten, dan tidak mengalami perubahan tanpa izin. Sementara itu,

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

Availability memastikan bahwa data dan layanan sistem dapat diakses oleh pengguna yang berwenang saat dibutuhkan. Ketiga prinsip ini saling berkaitan dan harus diterapkan secara seimbang dalam sistem informasi. Penerapan mekanisme keamanan, seperti enkripsi data, berperan penting dalam menjaga confidentiality dan integrity, serta mendukung availability dengan memastikan data tetap aman tanpa menghambat akses pengguna yang sah.

Enkripsi Data

Enkripsi data merupakan proses pengamanan informasi dengan mengubah data asli (plaintext) menjadi data terenkripsi (ciphertext) menggunakan algoritma dan kunci tertentu. Tujuan utama enkripsi adalah mencegah pihak yang tidak berwenang memahami atau memanfaatkan isi data. Enkripsi dapat diterapkan baik pada data yang disimpan (data at rest) maupun data yang ditransmisikan melalui jaringan (data in transit). Dalam sistem informasi, enkripsi menjadi salah satu mekanisme utama untuk menjaga keamanan data sensitif. Dengan menerapkan enkripsi, risiko kebocoran data dapat diminimalkan meskipun data berhasil diakses oleh pihak yang tidak berwenang.

Algoritma Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang menggunakan panjang kunci 128-bit, 192-bit, atau 256-bit. AES dikenal memiliki tingkat keamanan yang tinggi serta efisiensi yang baik dibandingkan dengan algoritma enkripsi simetris lainnya. Oleh karena itu, AES banyak digunakan dalam berbagai aplikasi keamanan, seperti sistem informasi, aplikasi web, pengamanan dokumen digital, serta perlindungan data pada perangkat penyimpanan. Penggunaan AES yang fleksibel dan aman menjadikannya salah satu standar enkripsi yang paling banyak diadopsi dalam lingkungan teknologi informasi modern.

Penelitian Terkait

Beberapa penelitian sebelumnya menunjukkan efektivitas algoritma AES dalam melindungi data sensitif. Penelitian internasional yang dipublikasikan oleh Springer membahas penerapan metode enkripsi adaptif untuk melindungi data sensitif pada basis data pusat data berbasis big data. Hasil penelitian tersebut menunjukkan bahwa penggunaan AES yang dikombinasikan dengan manajemen kunci yang baik mampu meningkatkan tingkat keamanan data secara signifikan.

Selain itu, penelitian yang diterbitkan dalam ACM Digital Library mengkaji tantangan keamanan dan privasi data pada lingkungan big data dan menegaskan bahwa enkripsi merupakan solusi utama dalam menjaga kerahasiaan informasi sensitif. Penelitian nasional yang diterbitkan dalam Jurnal BSI menunjukkan bahwa penerapan enkripsi AES-256 pada aplikasi web DNA sequencing mampu melindungi data sensitif pengguna. Sementara itu, penelitian dalam IT Science Journal membuktikan bahwa algoritma AES efektif dalam menjaga keamanan dokumen digital dari akses tidak sah.

Metode

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif kualitatif dengan pendekatan studi literatur. Pendekatan ini dipilih karena penelitian bertujuan untuk mengkaji dan menganalisis konsep, metode, serta hasil penelitian terdahulu yang berkaitan dengan implementasi enkripsi data untuk perlindungan informasi sensitif.

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

Studi literatur memungkinkan peneliti memperoleh pemahaman yang komprehensif mengenai penerapan algoritma enkripsi, khususnya Advanced Encryption Standard (AES), tanpa melakukan eksperimen atau implementasi sistem secara langsung.

Pendekatan deskriptif digunakan untuk menggambarkan secara sistematis bagaimana enkripsi data diterapkan pada berbagai sistem informasi berdasarkan hasil penelitian yang telah dipublikasikan. Dengan demikian, penelitian ini berfokus pada analisis konsep, temuan, serta kesimpulan dari penelitian sebelumnya yang relevan dengan topik keamanan informasi dan enkripsi data.

Sumber dan Jenis Data

Sumber data dalam penelitian ini berasal dari data sekunder, yaitu publikasi ilmiah berupa jurnal nasional dan jurnal internasional. Literatur yang digunakan terdiri dari tiga jurnal internasional dan dua jurnal nasional yang membahas topik enkripsi data, keamanan informasi, dan perlindungan data sensitif.

Jurnal internasional yang digunakan mencakup penelitian yang dipublikasikan oleh Springer, ResearchGate, dan ACM Digital Library yang membahas penerapan enkripsi AES pada lingkungan big data, pusat data, serta praktik terbaik keamanan informasi. Sementara itu, jurnal nasional yang digunakan berasal dari Jurnal BSI dan IT Science Journal yang membahas implementasi enkripsi AES-256 pada aplikasi web dan pengamanan dokumen digital. Pemilihan sumber data dilakukan dengan mempertimbangkan relevansi topik, kredibilitas sumber, serta keterkaitan dengan tujuan penelitian.

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui studi dokumentasi, yaitu dengan mengumpulkan dan menelaah berbagai literatur ilmiah yang berkaitan dengan enkripsi data dan keamanan informasi. Proses pengumpulan data meliputi pencarian jurnal melalui basis data ilmiah, seleksi literatur berdasarkan kesesuaian judul dan abstrak, serta pembacaan mendalam terhadap isi jurnal yang terpilih. Setiap jurnal yang digunakan kemudian dicatat poin-poin pentingnya, seperti tujuan penelitian, metode yang digunakan, algoritma enkripsi yang diterapkan, serta hasil dan kesimpulan penelitian. Data yang diperoleh dari literatur tersebut selanjutnya disusun secara sistematis untuk memudahkan proses analisis.

Teknik Analisis Data

Teknik analisis data dalam penelitian ini dilakukan secara deskriptif-analitis. Analisis dimulai dengan mengelompokkan hasil penelitian berdasarkan topik utama, yaitu implementasi enkripsi data, algoritma AES, serta perlindungan informasi sensitif. Selanjutnya, dilakukan perbandingan antara hasil penelitian internasional dan nasional untuk mengidentifikasi persamaan dan perbedaan dalam penerapan enkripsi data.

Analisis juga dilakukan berdasarkan prinsip Confidentiality, Integrity, dan Availability (CIA) sebagai kerangka evaluasi keamanan informasi. Setiap penelitian dianalisis untuk mengetahui sejauh mana penerapan enkripsi AES mampu memenuhi ketiga prinsip tersebut. Hasil analisis kemudian diinterpretasikan untuk memberikan gambaran mengenai efektivitas enkripsi data dalam melindungi informasi sensitif.

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

Kerangka Penelitian

Kerangka penelitian dalam studi ini dimulai dari identifikasi permasalahan keamanan informasi, khususnya terkait perlindungan data sensitif. Selanjutnya dilakukan pengumpulan literatur yang relevan, analisis terhadap penerapan enkripsi data menggunakan algoritma AES, serta evaluasi hasil penelitian berdasarkan prinsip CIA. Tahapan akhir dari penelitian ini adalah penarikan kesimpulan dan pemberian saran berdasarkan hasil analisis literatur.

Dengan adanya kerangka penelitian yang sistematis, penelitian ini diharapkan dapat memberikan pemahaman yang jelas mengenai implementasi enkripsi data sebagai solusi perlindungan informasi sensitif pada sistem informasi.

Hasil dan Pembahasan

Berdasarkan kajian literatur terhadap tiga jurnal internasional dan dua jurnal nasional, penerapan enkripsi data menggunakan algoritma Advanced Encryption Standard (AES) terbukti memiliki peranan penting dalam melindungi informasi sensitif pada sistem informasi. Enkripsi AES efektif dalam meningkatkan keamanan data baik pada proses penyimpanan (data at rest) maupun transmisi data melalui jaringan (data in transit).

Analisis Berdasarkan Jurnal Internasional

1. Springer – *Adaptive Encryption Method of Sensitive Data in Data Center Database Based on Big Data Cross-Mapping Fusion Algorithm*

   Penelitian ini menekankan pentingnya penerapan enkripsi adaptif pada pusat data dan lingkungan big data. Hasil kajian menunjukkan bahwa kombinasi AES dengan teknik adaptif dan manajemen kunci yang baik dapat meningkatkan tingkat keamanan data secara signifikan, meskipun sistem menangani volume data yang besar dan kompleks.

2. ResearchGate – Best Practices for Implementing Data Encryption and Anonymization

   Penelitian ini menyoroti praktik terbaik dalam penerapan enkripsi dan anonimisasi data. AES direkomendasikan sebagai algoritma andal karena telah teruji secara luas. Keberhasilan enkripsi tidak hanya bergantung pada algoritma, tetapi juga pada pengelolaan kunci, kebijakan keamanan, dan integrasi enkripsi dalam sistem informasi. AES terbukti melindungi informasi sensitif dari akses tidak sah jika diterapkan secara konsisten.

3. ACM Digital Library – Privacy Protection and Data Security for Big Data Encryption

   Penelitian ini mengkaji tantangan keamanan dan privasi pada pengolahan big data. AES dipilih karena menawarkan keseimbangan antara keamanan tinggi dan efisiensi komputasi, sehingga tidak mengganggu kinerja sistem. Hasil penelitian menegaskan relevansi AES untuk sistem informasi modern yang memproses data dalam skala besar.

Analisis Berdasarkan Jurnal Nasional

1. Jurnal BSI – Peningkatan Keamanan dan Privasi Aplikasi Website DNA Sequencing Menggunakan Enkripsi AES-256

   Penerapan AES-256 pada aplikasi web terbukti meningkatkan keamanan dan privasi data pengguna, khususnya data DNA yang sangat sensitif. Data dienkripsi sebelum disimpan dan ditransmisikan sehingga tidak dapat diakses oleh pihak tidak berwenang. Enkripsi ini dapat diintegrasikan dengan sistem autentikasi pengguna untuk

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

perlindungan tambahan.

2. IT Science Journal – Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi AES

AES digunakan untuk mengamankan dokumen digital. Dokumen yang telah dienkripsi hanya dapat diakses dengan kunci sah, sehingga menjaga kerahasiaan dan integritas data. Proses enkripsi dan dekripsi AES juga relatif cepat, sehingga tidak menghambat akses dokumen oleh pengguna yang berwenang.

Analisis Berdasarkan Prinsip CIA

Berdasarkan prinsip Confidentiality, Integrity, dan Availability (CIA), penerapan AES memberikan kontribusi positif pada ketiga aspek:

1. Confidentiality: Data sensitif hanya dapat diakses oleh pihak yang memiliki kunci sah.
2. Integrity: Modifikasi data tanpa izin dapat terdeteksi, sehingga mencegah perubahan data yang tidak sah.
3. Availability: Efisiensi AES memastikan proses enkripsi dan dekripsi tidak menghambat ketersediaan data bagi pengguna yang berwenang.

Pembahasan Keseluruhan

Secara keseluruhan, kajian literatur menunjukkan bahwa AES merupakan solusi efektif dan relevan untuk melindungi informasi sensitif pada era digital. Hasil penelitian internasional maupun nasional konsisten menunjukkan bahwa AES mampu memberikan perlindungan yang kuat terhadap data. Keberhasilan implementasi AES juga dipengaruhi oleh manajemen kunci yang baik, kebijakan keamanan, dan integrasi sistem. Oleh karena itu, AES dapat dijadikan metode utama dalam strategi keamanan informasi untuk melindungi data sensitif dari ancaman akses tidak sah dan kebocoran data.

Kesimpulan

Berdasarkan kajian literatur terhadap tiga jurnal internasional dan dua jurnal nasional, implementasi enkripsi data menggunakan algoritma Advanced Encryption Standard (AES) terbukti efektif dalam melindungi informasi sensitif pada sistem informasi. Enkripsi AES berperan penting dalam menghadapi berbagai ancaman, seperti kebocoran data, pencurian informasi, dan akses tidak sah. Penerapan AES menjaga kerahasiaan (confidentiality) dengan mengubah data menjadi bentuk terenkripsi yang hanya dapat diakses dengan kunci sah. Penelitian internasional menunjukkan efektivitas AES dalam lingkungan big data dan pusat data, sementara penelitian nasional membuktikan keberhasilan AES-256 dalam melindungi data pada aplikasi web dan dokumen digital.

Selain itu, AES mendukung integritas (integrity) dengan mencegah perubahan data tanpa izin, menjaga keakuratan dan konsistensi informasi. Dari sisi ketersediaan (availability), AES memiliki efisiensi komputasi yang baik, sehingga proses enkripsi dan dekripsi tidak menghambat akses pengguna yang berwenang. Secara keseluruhan, literatur menunjukkan bahwa AES merupakan komponen penting dalam strategi keamanan informasi modern. Keberhasilan implementasinya tidak hanya bergantung pada algoritma, tetapi juga pada pengelolaan kunci, kebijakan keamanan, dan integrasi enkripsi secara menyeluruh dalam sistem informasi.

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026

Saran

Berdasarkan hasil kajian literatur mengenai implementasi enkripsi AES untuk perlindungan informasi sensitif, penelitian selanjutnya dapat mengembangkan studi lebih lanjut dengan beberapa arah. Pertama, disarankan untuk melakukan uji implementasi enkripsi AES secara langsung pada sistem informasi nyata, baik dalam skala institusi maupun industri, untuk mengukur performa dan efektivitasnya dalam kondisi operasional yang dinamis. Kedua, penelitian mendatang dapat mengeksplorasi kombinasi algoritma enkripsi AES dengan teknik keamanan tambahan, seperti manajemen kunci adaptif atau integrasi dengan sistem deteksi intrusi, untuk meningkatkan tingkat keamanan secara menyeluruh. Ketiga, penelitian dapat diperluas pada berbagai jenis data sensitif, termasuk data kesehatan dan keuangan, untuk memperoleh hasil yang lebih representatif terhadap berbagai skenario ancaman. Terakhir, evaluasi efektivitas enkripsi dapat dikaitkan secara lebih mendalam dengan prinsip Confidentiality, Integrity, dan Availability (CIA) serta dampaknya terhadap kinerja sistem, sehingga memberikan panduan implementasi yang lebih praktis dan komprehensif bagi pengelola sistem informasi.

Daftar Pustaka

ACM Digital Library. (2019). Privacy protection and data security for big data encryption.

Alotaibi, F., & Alshammari, R. (2021). Detection of rogue access point attacks in wireless networks: A survey. International Journal of Computer Networks & Communications, 13(2), 1–16.

Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security and what to do about it. Oxford University Press.

IT Science Journal. (2022). Implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi AES.

Jurnal BSI. (2023). Peningkatan keamanan dan privasi aplikasi website DNA sequencing menggunakan enkripsi AES-256.

ResearchGate. (2020). Best practices for implementing data encryption and anonymization.

Scarfone, K., & Mell, P. (2012). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology.

Springer. (2021). Adaptive encryption method of sensitive data in data center database based on big data cross-mapping fusion algorithm.

Stallings, W. (2018). Network security essentials: Applications and standards (6th ed.). Pearson Education.

Wofford, P. (2020). Rogue access points: The threat to public wireless networks (Capstone Project). Utica College, New York.

Received: November 14, 2025 – Revised: November 26, 2025 - Accepted: Desember 15, 2025 - Published online: January 10, 2026