Jurnal Inspirasi Pembelajaran

https://ejurnals.com/ojs/index.php/jip Vol. 7, No. 1, Januari 2026

ANALISIS PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES) UNTUK MENINGKATKAN KEAMANAN DATA PENGGUNA PADA SISTEM INFORMASI

Wirda Berutu[1], Indah Sania Nasution[2], Ummi Setiani[3], Muhammad Ashraf Mubaraq[4], Tondi Alhabib Siregar[5], Jelsi Olimpia Ritonga[6]

[1,2,3,4,5,6]Universitas Labuhanbatu
Email: wyeer203@gmail.com[1], indahsanianasution@gmail.com[2], setianiumi85@gmail.com[3], rohannn2023000@gmail.com[4], tondialhabibsiregar25@gmail.com[5], jelsiolimpiaritonga@gmail.com[6]

Abstrak: Perkembangan teknologi informasi yang semakin pesat telah mendorong pemanfaatan sistem informasi secara luas dalam berbagai bidang namun di sisi lain juga meningkatkan risiko ancaman terhadap keamanan data pengguna seperti kebocoran data penyalahgunaan informasi dan akses tidak sah Oleh karena itu diperlukan mekanisme pengamanan data yang mampu melindungi informasi pengguna secara efektif Salah satu teknik pengamanan yang banyak digunakan adalah kriptografi khususnya algoritma Advanced Encryption Standard AES yang telah diakui sebagai standar internasional Penelitian ini bertujuan untuk menganalisis penerapan algoritma AES dalam sistem informasi serta mengkaji kontribusinya dalam meningkatkan keamanan data pengguna ditinjau dari aspek kerahasiaan integritas dan ketersediaan data Pendekatan penelitian yang digunakan adalah kualitatif dengan analisis konseptual melalui kajian terhadap berbagai sumber ilmiah yang relevan Hasil analisis menunjukkan bahwa algoritma AES terutama dengan penggunaan panjang kunci yang kuat mampu memberikan perlindungan yang efektif terhadap data pengguna baik pada data yang disimpan maupun data yang ditransmisikan Namun demikian tingkat keamanan yang dihasilkan sangat dipengaruhi oleh cara penerapan algoritma tersebut termasuk pemilihan mode enkripsi yang aman serta pengelolaan kunci yang tepat sehingga penerapan AES perlu didukung oleh praktik keamanan sistem informasi yang baik.

Kata Kunci: Kriptografi Advanced Encryption Standard AES Keamanan Data Sistem Informasi Enkripsi Data.

Abstract: *The rapid development of information technology has led to the widespread use of information systems across various sectors however it has also increased the risk of threats to user data security such as data breaches information misuse and unauthorized access Therefore effective data protection mechanisms are required to safeguard user information One widely adopted security technique is cryptography particularly the Advanced Encryption Standard AES algorithm which has been internationally recognized as a global standard This study aims to analyze the implementation of the AES algorithm in information systems and to examine its contribution to enhancing user data security in terms of confidentiality integrity and availability The research employs a qualitative approach with conceptual analysis based on a comprehensive review of relevant scientific sources The results indicate that the AES algorithm especially when using strong key lengths is capable of providing effective protection for user data both in storage and during transmission Nevertheless the level of security*

achieved is highly dependent on the implementation approach including the selection of secure encryption modes and proper key management Therefore the application of AES must be supported by sound information system security practices to achieve optimal protection.

Keywords: *Cryptography Advanced Encryption Standard AES Data Security Information Systems Data Encryption.*

PENDAHULUAN

Pemanfaatan sistem informasi berbasis web dan aplikasi mobile semakin meluas seiring dengan kebutuhan digitalisasi di berbagai bidang, seperti pendidikan, kesehatan, pemerintahan, dan bisnis. Sistem informasi tersebut mengelola dan menyimpan berbagai data sensitif pengguna, termasuk data pribadi, data keuangan, dan informasi penting lainnya. Kondisi ini menjadikan keamanan data pengguna sebagai aspek yang sangat krusial dalam pengembangan dan pengelolaan sistem informasi.

Meningkatnya jumlah serangan siber, seperti pencurian data, peretasan sistem, dan penyadapan informasi, menunjukkan bahwa sistem informasi rentan terhadap berbagai bentuk ancaman keamanan. Oleh karena itu, penerapan mekanisme keamanan yang andal menjadi kebutuhan utama untuk melindungi data dari akses yang tidak sah. Salah satu mekanisme keamanan yang banyak diterapkan adalah kriptografi, yaitu teknik pengamanan data dengan mengubah informasi menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang telah ditetapkan sebagai standar internasional dan banyak digunakan dalam sistem informasi modern. Algoritma ini dikenal memiliki tingkat keamanan yang tinggi serta efisiensi komputasi yang baik. Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis penerapan algoritma AES dalam sistem informasi serta perannya dalam meningkatkan keamanan data pengguna.

TINJAUAN LITERATUR

1. Keamanan Data dalam Sistem Informasi

Keamanan data dalam sistem informasi umumnya mengacu pada tiga prinsip utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kerahasiaan bertujuan untuk memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang, integritas menjamin bahwa data tidak mengalami perubahan tanpa izin, sedangkan

ketersediaan memastikan data dapat diakses ketika dibutuhkan. Penerapan ketiga prinsip tersebut menjadi dasar dalam pengembangan sistem informasi yang aman.

2. Kriptografi sebagai Mekanisme Pengamanan Data

Kriptografi merupakan teknik yang digunakan untuk melindungi data dengan cara mengubah data asli (*plaintext*) menjadi data terenkripsi (*ciphertext*). Secara umum, algoritma kriptografi dibedakan menjadi dua jenis, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan kriptografi asimetris menggunakan pasangan kunci publik dan kunci privat. Dalam praktiknya, kriptografi simetris sering digunakan untuk enkripsi data dalam jumlah besar karena memiliki kinerja yang lebih efisien.

3. Advanced Encryption Standard (AES)

AES dikembangkan oleh National Institute of Standards and Technology (NIST) sebagai pengganti algoritma Data Encryption Standard (DES). AES merupakan algoritma *block cipher* dengan ukuran blok 128 bit dan mendukung panjang kunci 128, 192, dan 256 bit. Proses enkripsi AES terdiri dari beberapa tahap, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*, yang dilakukan secara berulang sesuai dengan panjang kunci yang digunakan. Keunggulan AES terletak pada tingkat keamanannya yang tinggi serta kemampuannya untuk diimplementasikan secara efisien pada berbagai platform sistem informasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian analisis konseptual yang bertujuan untuk mengkaji secara mendalam penerapan algoritma kriptografi Advanced Encryption Standard AES dalam sistem informasi khususnya dalam konteks peningkatan keamanan data pengguna Pendekatan ini dipilih karena penelitian berfokus pada pemahaman konsep mekanisme dan efektivitas penerapan algoritma AES berdasarkan kajian ilmiah yang relevan.

Sumber data dalam penelitian ini berupa data sekunder yang diperoleh melalui penelusuran dan seleksi literatur ilmiah yang membahas kriptografi AES keamanan data serta sistem informasi Literatur yang digunakan meliputi jurnal ilmiah nasional dan internasional buku referensi akademik serta standar keamanan informasi yang memiliki keterkaitan langsung dengan topik penelitian Proses pemilihan sumber dilakukan secara selektif dengan

mempertimbangkan kesesuaian topik kedalaman pembahasan dan kontribusi terhadap pemahaman penerapan AES dalam sistem informasi.

Teknik pengumpulan data dilakukan melalui studi pustaka dengan mengidentifikasi kata kunci yang relevan seperti Advanced Encryption Standard AES keamanan data dan sistem informasi Literatur yang diperoleh kemudian diklasifikasikan berdasarkan fokus pembahasan meliputi konsep dasar AES mekanisme enkripsi keunggulan algoritma serta penerapannya pada berbagai jenis sistem informasi Tahap ini bertujuan untuk memperoleh gambaran komprehensif mengenai pola penerapan AES dalam pengamanan data pengguna.

Teknik analisis data dilakukan secara deskriptif dan analitis dengan mengkaji setiap sumber literatur untuk mengidentifikasi temuan utama serta membandingkan pendekatan penerapan AES yang digunakan dalam berbagai konteks sistem informasi Analisis difokuskan pada aspek kerahasiaan integritas dan ketersediaan data pengguna Selain itu dilakukan pula analisis terhadap keunggulan dan keterbatasan penerapan AES untuk mengidentifikasi faktor faktor yang mempengaruhi efektivitas algoritma tersebut.

Hasil analisis kemudian disintesis untuk merumuskan kesimpulan konseptual mengenai peran dan kontribusi algoritma AES dalam meningkatkan keamanan data pengguna pada sistem informasi Sintesis ini digunakan sebagai dasar dalam penyusunan rekomendasi konseptual yang dapat menjadi acuan bagi pengembang dan pengelola sistem informasi dalam menerapkan mekanisme kriptografi yang efektif dan aman.

HASIL DAN PEMBAHASAN

1. Keunggulan Algoritma Advanced Encryption Standard (AES)

Hasil analisis konseptual terhadap berbagai penerapan kriptografi dalam sistem informasi menunjukkan bahwa algoritma Advanced Encryption Standard (AES) memiliki keunggulan signifikan dalam menjaga keamanan data pengguna. Salah satu keunggulan utama AES terletak pada kekuatan kriptografisnya yang didukung oleh panjang kunci hingga 256 bit, sehingga menjadikannya sangat resisten terhadap serangan brute force dan kriptoanalisis modern. Karakteristik ini menjadikan AES mampu memenuhi kebutuhan keamanan data pada sistem informasi yang mengelola informasi sensitif pengguna.

Selain aspek keamanan, AES juga dikenal memiliki efisiensi komputasi yang relatif tinggi. Algoritma ini dirancang agar dapat diimplementasikan secara optimal baik pada sistem berskala besar maupun pada perangkat dengan keterbatasan sumber daya, seperti sistem berbasis web dan aplikasi mobile. Efisiensi tersebut memungkinkan proses enkripsi dan

dekripsi dilakukan tanpa menimbulkan beban kinerja yang signifikan, sehingga tidak mengganggu kenyamanan pengguna dalam mengakses sistem informasi.

Keunggulan lain dari AES adalah fleksibilitas implementasinya. Algoritma ini dapat diterapkan pada berbagai lapisan sistem informasi, mulai dari pengamanan basis data, enkripsi file, hingga perlindungan data selama proses transmisi. Fleksibilitas ini menjadikan AES sebagai solusi kriptografi yang adaptif dan relevan untuk berbagai kebutuhan pengamanan data pengguna.[13]

2. Analisis Penerapan AES dalam Pengamanan Data Pengguna pada Sistem Informasi

Berdasarkan hasil sintesis dari berbagai implementasi konseptual, penerapan algoritma AES pada sistem informasi terbukti berkontribusi secara signifikan dalam meningkatkan keamanan data pengguna. Pada sistem informasi berbasis web dan aplikasi, AES banyak digunakan untuk mengenkripsi data pengguna sebelum disimpan ke dalam basis data. Pendekatan ini mampu mencegah pihak yang tidak berwenang untuk membaca atau memanipulasi data meskipun terjadi kebocoran akses ke penyimpanan data.

Dalam konteks transmisi data, AES juga berperan penting dalam menjaga kerahasiaan informasi pengguna yang dikirimkan melalui jaringan. Dengan mengenkripsi data sebelum proses pengiriman, risiko penyadapan dan pencurian data dapat diminimalkan. Penerapan ini sangat relevan bagi sistem informasi yang menangani transaksi daring, pertukaran data pribadi, serta layanan berbasis cloud.

Hasil pembahasan juga menunjukkan bahwa AES sering dikombinasikan dengan mekanisme keamanan lain, seperti fungsi hash untuk menjaga integritas data atau kriptografi asimetris untuk distribusi kunci. Kombinasi tersebut membentuk sistem keamanan berlapis yang mampu meningkatkan perlindungan data pengguna secara menyeluruh. Dengan demikian, AES tidak hanya berperan sebagai algoritma enkripsi tunggal, tetapi juga sebagai bagian integral dari arsitektur keamanan sistem informasi.

3. Dampak Penerapan AES terhadap Aspek Keamanan Data (CIA Triad)

Penerapan algoritma AES dalam sistem informasi memberikan dampak positif terhadap tiga aspek utama keamanan data, yaitu kerahasiaan, integritas, dan ketersediaan. Dari aspek kerahasiaan, AES memastikan bahwa data pengguna hanya dapat diakses oleh pihak yang

memiliki kunci enkripsi yang sah. Hal ini secara langsung mengurangi risiko penyalahgunaan data oleh pihak yang tidak berwenang.

Dari sisi integritas, meskipun AES berfokus pada enkripsi, penerapannya dalam sistem informasi sering dikombinasikan dengan mekanisme verifikasi tambahan untuk mendeteksi perubahan data yang tidak sah. Dengan demikian, sistem mampu menjaga keutuhan data pengguna selama proses penyimpanan maupun transmisi. Sementara itu, dari aspek ketersediaan, efisiensi AES memungkinkan sistem informasi tetap memberikan layanan yang stabil tanpa penurunan performa akibat proses pengamanan data.

Ketiga aspek tersebut menunjukkan bahwa penerapan AES berkontribusi secara holistik terhadap peningkatan keamanan data pengguna, sehingga mendukung keandalan dan kepercayaan terhadap sistem informasi.

4. Tantangan dan Faktor Penentu Keberhasilan Implementasi AES

Meskipun AES memiliki tingkat keamanan yang tinggi, hasil analisis menunjukkan bahwa efektivitas penerapannya sangat bergantung pada strategi implementasi. Tantangan utama yang sering muncul adalah manajemen kunci yang kurang optimal. Pengelolaan kunci enkripsi yang tidak aman dapat menurunkan tingkat perlindungan data, meskipun algoritma yang digunakan memiliki kekuatan kriptografis yang tinggi.

Selain itu, pemilihan mode enkripsi yang tidak sesuai juga dapat membuka celah keamanan. Mode enkripsi yang lemah atau tidak dilengkapi mekanisme autentikasi berpotensi dimanfaatkan oleh penyerang. Oleh karena itu, pemilihan mode enkripsi yang aman serta penerapan kebijakan rotasi dan penyimpanan kunci yang baik menjadi faktor penentu keberhasilan penerapan AES.

Evaluasi dan pembaruan sistem keamanan secara berkala juga menjadi aspek penting dalam menjaga efektivitas AES. Sistem informasi yang tidak melakukan pembaruan berisiko tertinggal dalam menghadapi perkembangan teknik serangan siber. Dengan demikian, penerapan AES harus dipandang sebagai bagian dari strategi keamanan berkelanjutan, bukan sebagai solusi statis.

5. Implikasi Penerapan AES bagi Pengembangan Sistem Informasi

Hasil pembahasan menunjukkan bahwa penerapan algoritma AES memiliki implikasi strategis bagi pengembangan sistem informasi yang berorientasi pada keamanan data pengguna. Integrasi AES sejak tahap perancangan sistem memungkinkan pengembang untuk

membangun arsitektur keamanan yang lebih kuat dan terstruktur. Pendekatan ini dapat meningkatkan kepercayaan pengguna terhadap sistem serta mendukung kepatuhan terhadap standar keamanan informasi yang berlaku.

Dengan mempertimbangkan keunggulan dan tantangan implementasinya, AES dapat dijadikan sebagai komponen utama dalam kebijakan keamanan data pada sistem informasi. Penerapan yang tepat dan terintegrasi akan memberikan perlindungan optimal terhadap data pengguna serta memperkuat ketahanan sistem informasi terhadap ancaman keamanan siber.

KESIMPULAN DAN SARAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa algoritma kriptografi Advanced Encryption Standard (AES) merupakan salah satu mekanisme pengamanan data yang sangat efektif untuk diterapkan pada sistem informasi. AES mampu memberikan perlindungan yang kuat terhadap data pengguna, khususnya dalam menjaga aspek kerahasiaan dan integritas data, baik pada data yang disimpan dalam basis data maupun data yang ditransmisikan melalui jaringan. Tingkat keamanan yang ditawarkan oleh AES, terutama dengan penggunaan panjang kunci yang kuat, menjadikannya tetap relevan dalam menghadapi berbagai ancaman keamanan siber yang terus berkembang.

Selain tingkat keamanannya yang tinggi, AES juga memiliki keunggulan dari sisi efisiensi komputasi dan fleksibilitas implementasi. Algoritma ini dapat diterapkan pada berbagai jenis sistem informasi, mulai dari sistem berbasis web, aplikasi mobile, hingga sistem pengelolaan basis data, tanpa memberikan beban kinerja yang signifikan. Hal tersebut menjadikan AES sebagai solusi yang praktis dan efisien dalam mendukung keamanan data pengguna pada lingkungan sistem informasi modern.

Namun demikian, hasil analisis juga menunjukkan bahwa efektivitas penerapan AES tidak hanya ditentukan oleh kekuatan algoritma itu sendiri, tetapi sangat dipengaruhi oleh cara implementasinya. Aspek seperti manajemen kunci yang aman, pemilihan mode enkripsi yang tepat, serta integrasi dengan kebijakan keamanan sistem informasi yang komprehensif menjadi faktor penentu keberhasilan perlindungan data. Implementasi AES yang tidak disertai dengan pengelolaan kunci dan konfigurasi keamanan yang baik berpotensi menurunkan tingkat keamanan yang diharapkan.

Oleh karena itu, penerapan algoritma AES dalam sistem informasi perlu dilakukan secara menyeluruh dan terintegrasi dengan praktik keamanan informasi yang baik. Pengembang dan pengelola sistem informasi disarankan untuk tidak hanya mengandalkan algoritma enkripsi,

tetapi juga menerapkan kebijakan keamanan yang mencakup pengelolaan kunci, pemilihan mode enkripsi yang aman, serta evaluasi dan pembaruan sistem keamanan secara berkala. Dengan pendekatan tersebut, algoritma AES dapat memberikan kontribusi yang optimal dalam meningkatkan keamanan data pengguna pada sistem informasi.

DAFTAR PUSTAKA

R. Ganesh, B. U. I. Khan, A. R. Khan, and A. Bin Kamsin, *A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges*, vol. 24, no. 5. 2025. doi: 10.1007/s10207-025-01116-x.

T. W. Lingga, O. K. Sulaiman, and K. Nasution, "Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data pada Aplikasi E-Pariwisata," *sudo J. Tek. Inform.*, vol. 3, no. 4, pp. 201–216, 2025, doi: 10.56211/sudo.v3i4.923.

S. P. Ananda and S. Lukman, "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital," *J. Ilm. Komputasi*, vol. 21, no. 3, pp. 333–344, 2022, doi: 10.32409/jikstik.21.3.2973.

S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

A. R. Hakim and K. F. Margolang, "Analisis Keamanan Data Rekam Medis Digital Menggunakan Algoritma Kriptografi AES Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD," *J. Teknol. Sist. Inf. dan Sist. Komput. TGD*, vol. 8, pp. 108–114, 2025.

M. Mulyadi, "Aplikasi Kriptografi Pesan Teks Menggunakan Algoritma Advanced Encryption Standard 256 Bit (Aes-256) Dan Diffie Hellman," *Sisfo J. Ilm. Sist. Inf.*, vol. 3, no. 2, pp. 23–38, 2019, doi: 10.29103/sisfo.v3i2.6330.

A. Z. Ifani, R. N. J. S.Intam, A. I. Syair, and H. Husnawati, "Application of Advanced Encryption Standard (AES) Algorithm in E-Commerce Login System for User Data Security," *J. Syst. Comput. Eng.*, vol. 6, no. 1, pp. 1–9, 2025, doi: 10.61628/jsce.v6i1.1511.

Satria Gunawan Zain, Abdul Wahid, and Iin Rahmawati, "Data Confidentiality Pada Kontrol Smart PDAM Menggunakan AES Algorithm," *J. Embed. Syst. Secur. Intell. Syst.*, vol. 04, no. May, pp. 39–47, 2023, doi: 10.59562/jessi.v4i1.472.

M. Muslih, L. B. Handoko, and A. Rizqy, "File Cryptography Optimization Based on Vigenere Cipher and Advanced Encryption Standard (AES)," *J. Appl. Intell. Syst.*, vol. 8, no. 2, pp. 152–161, 2023, doi: 10.33633/jais.v8i2.7899.

Tarisa Auliya Ramadhani, A. Fajaryanto Cobantoro, and S. Sugianti, "Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem Registrasi Pasien," *J. Inform. Polinema*, vol. 10, no. 4, pp. 521–526, 2024, doi: 10.33795/jip.v10i4.5619.

M. L. Assidiq, F. Mahardika, and D. Santika, "Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi," *Simpatik J. Sist. Inf. dan Inform.*, vol. 4, no. 1, pp. 44–52, 2024, doi: 10.31294/simpatik.v4i1.3386.

A. Alvian Winata, M. Syafrullah, and I. Irawan, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-128) untuk Pengamanan Data Berbasis Web pada McDonald's Cabang T.B. Simatupang," *J. Ticom Technol. Inf. Commun.*, vol. 12, no. 3, pp. 91–96, 2024, doi: 10.70309/ticom.v12i3.124.

M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

F. A. Naimnule *et al.*, "Implementation of AES Encryption for Data Security on Web-Based Information Systems in Fafinesu A Village," *Sist. Kendali Jaringan) E-ISSN*, vol. 4, no. 3, pp. 2808–3520, 2025, [Online]. Available: https://doi.org/10.58982/krisnadana.v4i3.836https://ejournal.sidyanusa.org/index.php/jkdn/index

D. N. Simbolon, N. B. Nugroho, and R. Mahyuni, "Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Pengamanan Data Pengiriman Barang Di J & T Cargo Menggunakan Metode Rivest Shamir Adleman (RSA) Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD," vol. 8, pp. 73–82, 2025.

Z. Hayat Arka Putri, Y. Arye Yustraini, R. Ariansyah, N. Choirun Nisa, E. Dyar Wahyuni, and A. Brastama Putra, "Pengamanan Data Akademik Berbasis Web dengan Enkripsi AES-256 (Studi Kasus pada Pendataan Digital SMA XYZ)," *Jnatia*, vol. 3, no. 3, p. 2025, 2025.

I. G. Indra, “Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force,” *J. Media Inform.*, vol. 4, no. 2, pp. 102–109, 2023, doi: 10.55338/jumin.v4i2.496.

A. H. Nasrullah, “Secure Web-Based File Encryption Using AES-128,” *J. Embed. Syst. Secur. Intell. Syst.*, vol. 6, no. 2, pp. 146–155, 2025, doi: 10.59562/jessi.v6i2.8436.

G. S. Yudha and R. H. Laluma, “Sistem Keamanan Jaringan Dalam Ujian Online Sma/Smk Menggunakan Metode Algoritma Advanced Encryption Standard (Aes),” *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 4, no. 2, p. 71, 2019, doi: 10.32897/infotronik.2019.4.2.261.

N. Cristy and F. Riandari, “Implementasi Metode Advanced Encryption Standard (AES 128 Bit) UnCristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI), 4(2), ,” *J. Ilmu Komput. dan Sist. Inf.*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181.