ISSN : 2614-0985 (Cetak)
ISSN : 2614-0977 (Online)
KOMPUTEK
url : http://studentjournal.umpo.ac.id/index.php/komputek

Implementasi Kriptografi AES pada Sistem Enkripsi Gambar berbasis Web dengan Kunci Ephemeral yang dihasilkan API

Emir Syarif Machfudz[1], Suhardi[2]

Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara

E-mail Korespondensi : [1)]emirsyarifm@gmail.com, [2)]suhardi@uinsu.ac.id

History Artikel

Diterima : 5 Mei 2025 Disetujui : 10 September 2025 Dipublikasikan : 25 Oktober 2025

Abstract

This study implements the Advanced Encryption Standard (AES) algorithm in a web-based image encryption system utilizing an ephemeral key generated by an API. The research is motivated by the increasing threats to digital data security, such as identity theft and information manipulation, as well as the weaknesses of static key usage in AES encryption. The developed system consists of a client-side web application and a RESTful API server. The client side, built with HTML, CSS, and JavaScript, receives image input, requests the API for a key, and performs AES-256 encryption in Cipher Block Chaining (CBC) mode with a unique Initialization Vector (IV). The server side generates a random 256-bit key, stores it temporarily for approximately 30 seconds, and sends the key ID to the client. Testing was conducted on images sized 50 KB, 200 KB, and 1000 KB to measure encryption time. The results show that encryption time increases linearly with image size, with minimal overhead that does not affect performance. The ephemeral key approach enhances security by limiting the opportunity for unauthorized access to the key, while client-side encryption ensures that raw image data is never transmitted to the server. These findings demonstrate that implementing AES with ephemeral keys effectively improves the security of web-based image encryption.

Keywords: *AES-256, image encryption, ephemeral key, cryptography, data security*

Abstrak

Penelitian ini mengimplementasikan algoritma Advanced Encryption Standard (AES) pada sistem enkripsi gambar berbasis web dengan memanfaatkan kunci sementara (ephemeral key) yang dihasilkan API. Latar belakang penelitian ini adalah meningkatnya ancaman keamanan data digital, seperti pencurian identitas dan manipulasi informasi, serta kelemahan penggunaan kunci statis pada enkripsi AES. Sistem yang dikembangkan terdiri dari aplikasi web sisi klien dan API sisi server berbasis RESTful. Sisi klien dibangun dengan HTML, CSS, dan JavaScript untuk menerima gambar, memanggil API, serta melakukan enkripsi AES-256 dalam mode Cipher Block Chaining (CBC) dengan Vektor Inisialisasi (IV) unik. Sisi server bertugas membuat kunci acak 256-bit, menyimpannya sementara selama ±30 detik, lalu mengirimkan ID kunci ke klien. Pengujian dilakukan pada gambar berukuran 50 KB, 200 KB, dan 1000 KB untuk mengukur waktu enkripsi. Hasil menunjukkan waktu enkripsi meningkat secara linear sesuai ukuran gambar, dengan overhead minimal dan tanpa mengganggu kinerja. Pendekatan kunci sementara meningkatkan keamanan karena membatasi peluang akses kunci oleh pihak tidak berwenang, sementara enkripsi sisi klien memastikan data mentah tidak pernah dikirim ke server. Temuan ini membuktikan bahwa penerapan AES dengan kunci sementara efektif meningkatkan keamanan enkripsi gambar berbasis web.

Kata Kunci: *AES-256, enkripsi gambar, kunci sementara, kriptografi, keamanan data*

How to Cite: Emir Syarif Machfudz (2025). Implementasi Kriptografi AES pada Sistem Enkripsi Gambar berbasis Web dengan Kunci Ephemeral yang dihasilkan API. KOMPUTEK : Jurnal Teknik Universitas Muhammadiyah Ponorogo, Vol 9 (2): Halaman 42-47

ISSN 2614-0985 (Print)
ISSN 2614-0977 (Online)

PENDAHULUAN

Perkembangan teknologi pada sistem keamanan data, khususnya untuk melindungi data, kini telah mengalami kemajuan yang pesat (Priambudi & Mufti, 2023). Ancaman terhadap keamanan data terus meningkat seiring kemajuan teknologi informasi, seperti penyadapan, manipulasi informasi, dan pencurian identitas. Untuk melawan ancaman ini, kriptografi adalah salah satu cara paling efektif untuk melindungi informasi (Azila Tarigan et al., 2025). Steganografi dan kriptografi memiliki prinsip kerja berbeda namun saling berkaitan dalam keamanan data, di mana kriptografi menghasilkan data acak yang berbeda dari bentuk aslinya dan dapat dikembalikan melalui dekripsi, sedangkan steganografi menyamarkan informasi sehingga tampak sama secara visual dengan bentuk aslinya meski perbedaan dapat dikenali oleh perangkat digital (Putri, Kartikadewi, & Abdul Rosyid, 2020).

AES (Advanced Encryption Standard) merupakan algoritma enkripsi dengan kunci simetris yang diperkenalkan oleh National Institute of Standards and Technology (NIST) pada tahun 2001 (Nafis & Sidqon, 2024). Namun, kekuatan kriptografi AES sangat bergantung pada keamanan kuncinya. Penggunaan kunci statis atau yang dikelola secara tidak aman dapat menjadi kelemahan dalam sistem enkripsi.

Artikel ini mengusulkan solusi untuk masalah ini dengan menerapkan sistem enkripsi gambar berbasis web yang menggunakan kunci sementara. Kunci-kunci ini, yang hanya berlaku untuk satu sesi enkripsi, dibuat dan dikelola oleh API terpisah. Pendekatan ini secara signifikan mengurangi risiko serangan yang menargetkan kunci enkripsi, karena kunci-kunci ini tidak disimpan dalam jangka panjang dan hanya diakses sekali 9 (ephemeral). Ephemeral berarti sesuatu yang bersifat sementara atau hanya digunakan dalam waktu singkat (Khasanah & Sutabri, 2023).

Selain itu, penelitian ini bertujuan mengimplementasikan teknik tersebut pada antarmuka situs web, menguji tingkat efektivitas keamanannya, serta memberikan sumbangan pada pengembangan bidang keamanan informasi (Sidiq, Erwin, Rahayu, & Supriatna, 2023).

METODE PENELITIAN

Metode penelitian ini disusun berdasarkan kajian literatur dari berbagai sumber jurnal ilmiah yang relevan, sehingga perancangan sistem memiliki landasan teori yang kuat.

Data penelitian berupa file foto yang diambil langsung dari galeri pribadi peneliti, sehingga mencerminkan skenario penggunaan nyata. Sistem yang diusulkan terdiri dari dua komponen utama, yaitu aplikasi web sisi klien dan API sisi server.

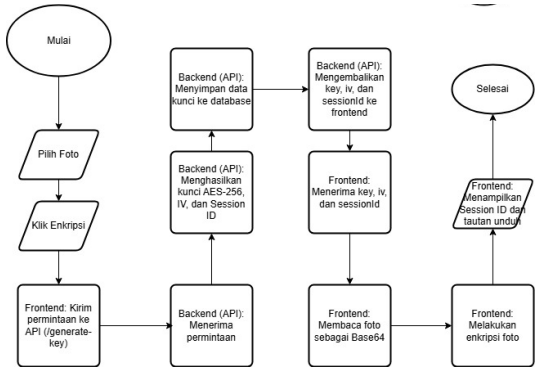
Application Programming Interface (API) adalah layanan yang menyediakan seperangkat aturan untuk memungkinkan suatu aplikasi berinteraksi dan bertukar informasi dengan aplikasi lainnya (Permana, Maulindar, & Hartanti, 2022).

Antarmuka pengguna dibangun menggunakan HTML, CSS, dan JavaScript untuk menerima masukan gambar dari pengguna, memanggil API untuk mendapatkan kunci sementara, serta menjalankan proses enkripsi AES. REST adalah standar arsitektur komunikasi

berbasis web yang umumnya menggunakan protokol HTTP untuk pertukaran data, dan sistem yang menerapkan prinsip-prinsipnya disebut "RESTful" (Gustiegan & Painem, 2022).

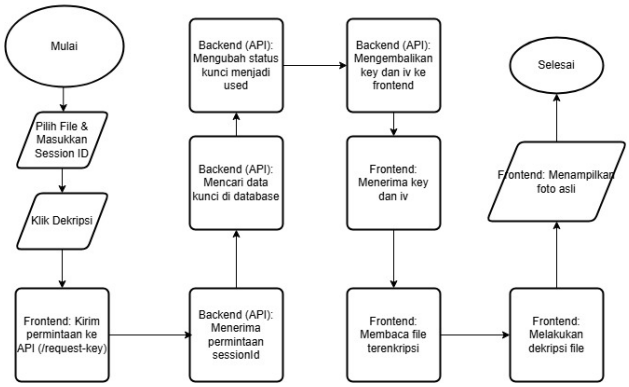
API berbasis RESTful bertugas menghasilkan kunci AES 256-bit yang unik dan acak, menyimpannya sementara (misalnya 30 detik), dan mengirimkan ID kunci ke klien. Untuk API sendiri dijalankan melalui Nodejs. Node.js adalah salah satu teknologi JavaScript yang populer, merupakan lingkungan runtime lintas platform yang memudahkan pembuatan aplikasi web cepat dan skalabel, dibangun di atas runtime JavaScript milik Chrome (Challapalli et al., 2021).

Proses enkripsi dimulai saat pengguna mengunggah gambar. JavaScript di sisi klien mengirim permintaan ke API untuk memperoleh kunci enkripsi. API membuat kunci AES baru, menyimpannya sementara di cache server, lalu mengirim ID kunci ke klien. Data gambar kemudian dikonversi menjadi array byte dan dienkripsi menggunakan AES dalam mode Cipher Block Chaining (CBC) dengan Vektor Inisialisasi (IV) unik. CBC digunakan berdasarkan kebutuhan spesifik aplikasi untuk mencapai efisiensi yang diinginkan (Ugwunna et al., 2024). Hasil enkripsi berisi data gambar terenkripsi, IV, dan metadata yang digabungkan menjadi satu berkas untuk diunduh.



Gambar 1. Flowchart Enkripsi Foto

Proses dekripsi menggunakan kunci yang sama dengan yang digunakan saat enkripsi. Untuk menjaga keamanan, mekanisme pertukaran kunci yang aman seperti Diffie-Hellman atau API terenkripsi diperlukan.

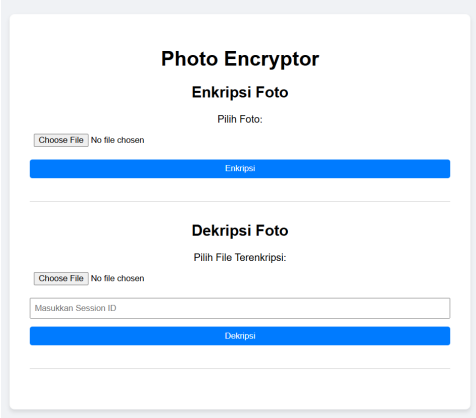


Gambar 2. Flowchart Dekripsi Foto

HASIL DAN PEMBAHASAN

A. Tampilan Website

Berikut ini adalah tampilan dari website untuk mengenkripsi dan mendekripsi foto. Untuk mengenkripsi data, user harus mengupload foto dari file explorer mereka.



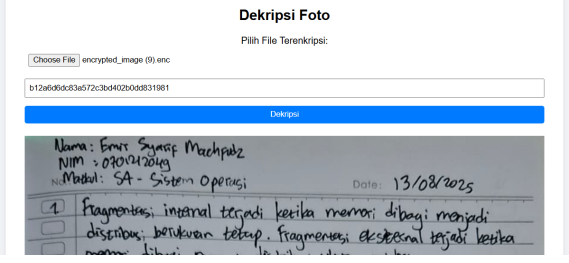
Gambar 3. Tampilan Website

B. Proses Enkripsi

Gambar 4. Proses Enkripsi

Saat user menekan tombol enkripsi, website menampilkan sessionid atau key yang digunakan nantinya untuk penerima file untuk mendekripsikan file enkripsi foto.

C. Proses Dekripsi



Gambar 5. Proses Dekripsi

Sistem yang dikembangkan berhasil menerapkan enkripsi gambar berbasis web menggunakan AES-256 dan kunci sementara. Pengujian kinerja dilakukan dengan mengenkripsi gambar dengan berbagai ukuran.

Tabel 1. Kinerja Website

Ukuran Gambar (KB)	Waktu Enkripsi (ms)
50	120
200	450
1000	2500

Hasil pengujian menunjukkan bahwa waktu enkripsi meningkat secara linear seiring dengan ukuran gambar. Overhead yang dihasilkan oleh proses enkripsi, termasuk permintaan API untuk kunci, minimal dan tidak mengganggu pengalaman pengguna.

Pendekatan kunci sementara ini secara signifikan meningkatkan keamanan dibandingkan dengan metode kunci statis. Meskipun API dapat menjadi target serangan, kunci yang dihasilkan memiliki masa pakai yang sangat singkat, sehingga secara signifikan membatasi peluang penyerang untuk menyalahgunakannya. Lebih lanjut, enkripsi sisi klien memastikan bahwa data gambar mentah tidak pernah dikirimkan ke server.

KESIMPULAN

Penelitian ini berhasil mengimplementasikan algoritma AES-256 pada sistem enkripsi gambar berbasis web dengan memanfaatkan kunci sementara (*ephemeral key*) yang dihasilkan API. Hasil pengujian menunjukkan bahwa waktu enkripsi meningkat secara linear seiring dengan ukuran gambar, dengan overhead minimal yang tidak mengganggu kinerja sistem. Pendekatan penggunaan kunci sementara terbukti

meningkatkan keamanan karena membatasi masa pakai kunci dan mengurangi risiko penyalahgunaan oleh pihak tidak berwenang. Selain itu, penerapan enkripsi di sisi klien memastikan bahwa data mentah tidak pernah dikirim ke server, sehingga privasi pengguna tetap terjaga. Dengan demikian, metode ini efektif untuk meningkatkan keamanan data pada aplikasi web yang memproses file gambar.

DAFTAR PUSTAKA

Azila Tarigan, N., Cut Nabila Anggreni, A., Balqis, A., Nurfadilah, I., Setia Bakti, E., Mahyudin, F., & Malikussaleh, U. (2025). Pengembangan Aplikasi Kriptografi RSA dan SHA-256 Berbasis Web Menggunakan Flask. *Journal.Dcircle.Org*, *1*(2). https://doi.org/10.62671/jikum.v1i2.40

Challapalli, S. S. N., Kaushik, P., Suman, S., Shivahare, B. D., Bibhu, V., & Gupta, A. D. (2021). Web Development and performance comparison of Web Development Technologies in Node.js and Python. *Proceedings of International Conference on Technological Advancements and Innovations, ICTAI 2021*, 303–307. https://doi.org/10.1109/ICTAI53825.2021.9673464

Gustiegan, G. Y., & Painem, P. (2022). Implementation of a RESTful Web Service with JSON Web Token Authentication and AES-256 Cryptographic Algorithm for Mobile-Based Laboratory Loan Applications at Budi Luhur University. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, *19*(1), 9–16. https://doi.org/10.36080/BIT.V19I1.1835

Khasanah, S., & Sutabri, T. (2023). ANALISIS PENCEGAHAN PENCURIAN DATA MELALUI APLIKASI WHATSAPP MENGGUNAKAN METODE KRIPTOGRAFI. *Sainteks: Jurnal Sain Dan Teknik*, *5*(2), 145–153. Retrieved from https://journals.penerbitjurnal.com/index.php/teknik/article/view/14

Nafis, R. O., & Sidqon, M. (2024). RANCANG BANGUN SISTEM E-ARSIP BERBASIS WEBSITE MENGGUNAKAN METODE ENKRIPSI AES (Advanced Encryption Standard) STUDI KASUS KPU SIDOARJO. *Jurnal Rekayasa Sistem Informasi Dan Teknologi*, *2*(1), 488–497. https://doi.org/10.59407/JRSIT.V2I1.963

Permana, A. A., Maulindar, J., & Hartanti, D. (2022). Implementasi Sistem Kriptografi Algoritma AES (256-bit) Berbasis Web API untuk Mengamankan Data Pribadi di CV. Elang Cahaya Sukses Surakarta | Prosiding Seminar Nasional Teknologi Informasi dan Bisnis. Retrieved from https://ojs.udb.ac.id/Senatib/article/view/1994

Priambudi, I., & Mufti, M. (2023). IMPLEMENTASI KRIPTOGRAFI DENGAN METODE AES-128 UNTUK PENGAMANAN FILE BERBASIS WEB PADA SMP YAPIPA. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *6*(1), 22–31. https://doi.org/10.36080/SKANIKA.V6I1.2997

Putri, A. E. (Anggraeni), Kartikadewi, A. (Aghistina), & Abdul Rosyid, L. A. (2020). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information Systems and Management*, *3*(2), 69–78. https://doi.org/10.15408/AISM.V3I2.14722

Sidiq, R. F., Erwin, R., Rahayu, G., & Supriatna, A. D. (2023). Implementasi Kriptografi Advanced Encryption Standard dan Least Significant Bit untuk Keamanan Pesan Email dalam Gambar. *Jurnal Algoritma*, *20*(2), 305–315. https://doi.org/10.33364/ALGORITMA/V.20-2.1407

Ugwunna, C. O., Okimba, P. E., Alabi, O. A., Orji, E. E., Olowofeso, E. O., & Ayomide, S. O. (2024). ADVANCED ENCRYPTION STANDARD (AES) IMPLEMENTATION EFFICIENCY USING JAVA AND NODE.JS PLATFORMS. *FUDMA JOURNAL OF SCIENCES*, *8*(6), 42–49. https://doi.org/10.33003/fjs-2024-0806-2832