Pengamanan Data Akademik Berbasis Web dengan Enkripsi AES-256 (Studi Kasus pada Pendataan Digital SMA XYZ)

Zahrah Hayat Arka Putri[*1], Yessy Arye Yustraini[*2], Ramdhan Ariansyah[*3], Najma Choirun Nisa[*4], Eka Dyar Wahyuni[*5] , Agung Brastama Putra[*6]

Program Studi Sistem Informasi, UPN "Veteran" Jawa Timur, Jl. Rungkut Madya No. 1, Gn. Anyar, Surabaya, Jawa Timur, Indonesia
22082010081@student.upnjatim.ac.id
22082010087@student.upnjatim.ac.id
22082010119@student.upnjatim.ac.id
22082010107@student.upnjatim.ac.id
ekawahyuni.si@upnjatim.ac.id
agungbp.si@upnjatim.ac.id

Abstract

The advancement of information technology has significantly facilitated data management, particularly in the field of education. However, this convenience also presents new challenges in ensuring data security, especially for academic information that is sensitive and vulnerable to unauthorized access. This study aims to develop a web-based academic data security system by implementing the AES-256 encryption algorithm in Cipher Block Chaining (CBC) mode. The system is built using the PHP programming language and MySQL database to manage student data such as name, NISN, class, address, gender, religion, and mother's name. The core functionality lies in encrypting and decrypting sensitive information using the openssl_encrypt and openssl_decrypt functions, integrated with a 256-bit encryption key and a randomly generated Initialization Vector (IV) to ensure confidentiality. The encrypted data is stored in base64 format to maintain compatibility with relational databases and storage systems. Testing was conducted to evaluate the accuracy of the encryption-decryption process and to assess the impact on system performance. Results show that the system effectively secures sensitive data; the encrypted entries in the database are unreadable to unauthorized users and can only be restored using the correct encryption key and IV. With a simple yet functional user interface and automated encryption handling, the system proves to enhance academic data security without compromising operational efficiency. These findings demonstrate that the implementation of AES-256-CBC encryption can be effectively applied in educational information systems, offering a practical and reliable solution for safeguarding academic data in web-based environments.

Keywords: *data encryption, AES-256-CBC, academic system.*

1. Pendahuluan

Pada era sekarang ini teknologi yang berkembang sangat pesat membuat informasi sangat mudah diperoleh dan disebarluaskan. Oleh karena itu, informasi yang beredar di internet menjadi salah satu aset yang sangat berharga bagi banyak pihak dan sangat rentan terhadap ancaman seperti pencurian data, akses di luar ijin, dan manipulasi [14]. Keamanan informasi menjadi salah satu tantangan yang harus segera ditangani. Keamanan adalah kategori yang paling penting, tetapi salah satu yang paling sulit dinilai [2]. Penilaian keamanan informasi adalah proses menentukan seberapa efektif suatu entitas yang dinilai memenuhi keamanan tertentu [3]. Kriptografi merupakan salah satu teknik untuk melindungi data dari akses pihak tidak berwenang. Salah satu metode kriptografi yang dikenal adalah AES (*Advanced Encryption Standard*) yang digunakan untuk melindungi data dengan enkripsi dan dekripsi menggunakan kunci yang sama. Untuk meningkatkan keamanannya, AES sering diimplementasikan dalam mode operasi Cipher Block Chaining (CBC), yang menambahkan dependensi antar blok data dengan menggunakan

p-ISSN: 2986-3929
e-ISSN: 3032-1948

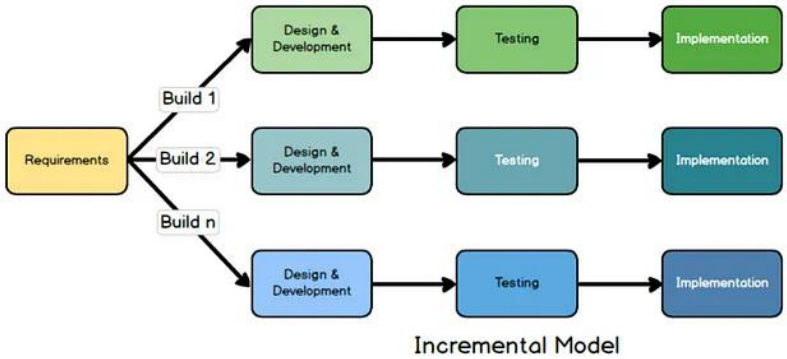
vektor inisialisasi (IV) acak [10][3]. Penerapan enkripsi AES-256 dengan mode CBC sangat relevan dalam konteks sistem berbasis web yang mengelola informasi sensitif, salah satunya adalah Learning Management System (LMS). LMS merupakan platform yang digunakan untuk mengelola proses pembelajaran secara digital, termasuk penyimpanan data akademik seperti nilai siswa, materi pelajaran, serta informasi pribadi pengguna [12][13]. Informasi-informasi ini jika tidak diamankan dengan benar berpotensi menjadi target serangan siber. Melalui studi kasus pada LMS di SMA XYZ, jurnal ini akan membahas penerapan algoritma enkripsi AES-256 dengan mode CBC untuk mengamankan data akademik. Pembahasan akan difokuskan pada proses enkripsi dan dekripsi data, manajemen kunci, serta evaluasi keamanan dan kinerja sistem setelah implementasi. Selain itu, jurnal ini juga akan meninjau dampak penggunaan enkripsi terhadap performa sistem LMS berbasis web dan bagaimana pendekatan ini dapat menjadi solusi efektif dalam menjaga kerahasiaan dan integritas data akademik.

2. Metode Penelitian

Beberapa studi sebelumnya telah mengimplementasikan algoritma AES dalam sistem informasi untuk pengamanan data sensitif. Febitri et al. (2023) menunjukkan bahwa algoritma AES-256 dengan mode OCB efektif menjaga kerahasiaan data siswa tanpa mengorbankan efisiensi sistem, sementara Azhari et al. (2022) menegaskan keberhasilan dekripsi tinggi dalam melindungi dokumen digital dari akses tidak sah. AES sendiri merupakan algoritma enkripsi kunci simetris yang banyak digunakan karena menawarkan tingkat keamanan tinggi, khususnya varian AES-256 yang sering diandalkan dalam perlindungan data penting [10]. Dalam penelitian ini, digunakan mode operasi Cipher Block Chaining (CBC), yang memiliki keunggulan menghasilkan ciphertext unik untuk input yang identik. Selain pendekatan teknis, aspek keamanan informasi juga mencakup faktor kognitif dan perilaku pengguna. Menurut G. J. Simon, keamanan informasi tidak hanya teknis, tetapi juga melibatkan pemahaman, sikap, dan perilaku pengguna terhadap ancaman digital [9]. Dalam konteks sistem pengelolaan data akademik berbasis web, platform Learning Management System (LMS) menjadi sarana utama yang membutuhkan perlindungan data, karena digunakan secara luas dalam mendukung pembelajaran daring dan pencatatan aktivitas akademik [12][13]. Oleh karena itu, penelitian ini bertujuan menguji efektivitas implementasi AES-256-CBC pada sistem akademik dari aspek keamanan dan performa menyeluruh, dengan memperhatikan elemen teknis serta perilaku pengguna.

a. Metode Pengembangan Sistem

Sistem Ini dikembangkan menggunakan pendekatan *Incremental Model,* yaitu model pengembangan yang dilakukan secara bertahap berdasarkan fitur. Setiap fitur utama seperti login, dashboard dan input data siswa dibangun satu per satu, lalu diuji sebelum ditambahkan ke sistem secara keseluruhan. Pendekatan ini memungkinkan proses pengujian dan perbaikan dilakukan lebih cepat di setiap tahap, serta mempermudah pengembangan sistem secara fleksibel sesuai kebutuhan. Model ini juga memudahkan pengelolaan perubahan tanpa harus membangun ulang seluruh sistem dari awal.



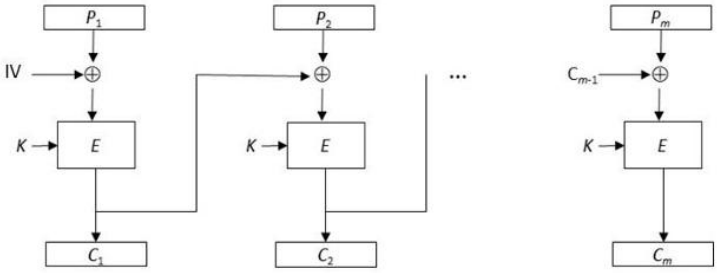
Gambar 1. Proses Enkripsi dan Dekripsi mode CBC

b. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang menjadi standar global untuk pengamanan data. Varian AES-256 menggunakan kunci 256-bit yang memberikan tingkat keamanan sangat tinggi terhadap serangan *brute-force*, sebagaimana dinyatakan dalam standar NIST FIPS 197 (2001). Proses enkripsi dilakukan dengan membagi data menjadi blok 128-bit, kemudian melalui 14 putaran transformasi yang meliputi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* [2]. Setiap putaran menggunakan kunci turunan yang dihasilkan melalui proses ekspansi kunci. Mekanisme ini menghasilkan *ciphertext* yang sangat sulit dipecahkan tanpa kunci yang sesuai, sementara proses dekripsi dilakukan dengan membalikkan langkah-langkah enkripsi tersebut.

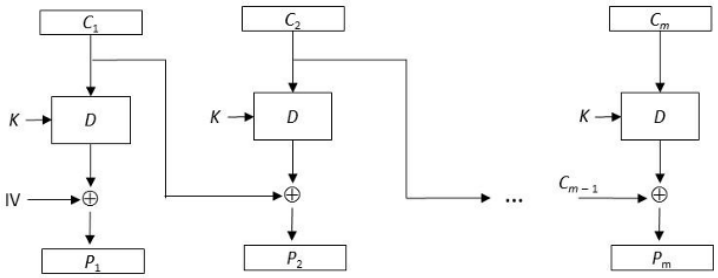
c. Cipher Block Chaining (CBC)

Mode operasi CBC meningkatkan keamanan AES dengan memperkenalkan ketergantungan antar blok data [3]. Setiap blok *plaintext* di-XOR terlebih dahulu dengan *ciphertext blok* sebelumnya sebelum dienkripsi. Untuk blok pertama, digunakan *Initialization Vector* (IV) acak yang bersifat unik. Evaluasi mode operasi *block cipher*, pendekatan ini memastikan bahwa meskipun terdapat blok *plaintext* yang identik, *ciphertext* yang dihasilkan akan berbeda [4]. Namun, CBC memiliki kerentanan terhadap serangan *padding oracle* jika implementasinya tidak dilakukan dengan benar [5].Secara matematis, proses enkripsi dapat dirumuskan dengan C_i = AES-EncK ($P_i \oplus C_{i-1}$) dengan C_0 = IV [3].



Gambar 2. Proses Enkripsi dan Dekripsi mode CBC

Dekripsi dilakukan dengan membalikkan proses enkripsi. Setiap blok *ciphertext* di dekripsi menggunakan AES standar, kemudian di-XOR dengan *ciphertext* blok sebelumnya (atau IV untuk blok pertama) untuk mendapatkan *plaintext* asli adalah P_i = AES-Dec(K, C_i) $\oplus$ C_{i-1} [3]. IV harus disimpan atau dikirim bersama ciphertext karena merupakan komponen kritis untuk dekripsi blok pertama. Proses ini bersifat deterministik - dengan kunci dan IV yang benar, *plaintext* asli dapat dipulihkan secara sempurna.



Gambar 3. Proses Dekripsi mode CBC

d. Manajemen Kunci dan Integritas Data pada LMS Berbasis Web

Aspek kritis dalam implementasi AES-256-CBC adalah manajemen kunci yang aman. Dalam implementasi sistem enkripsi modern, khususnya pada pengamanan data sensitif seperti informasi akademik dalam LMS, penting untuk memperhatikan cara penyimpanan kunci enkripsi agar tetap aman dan terisolasi. Salah satu pendekatan yang direkomendasikan secara luas adalah dengan memanfaatkan modul perangkat keras khusus seperti *Hardware Security Module* (HSM), yang dirancang untuk melindungi dan mengelola kunci kriptografi secara fisik terpisah dari sistem utama [6]. Selain itu, praktik keamanan yang baik juga mengharuskan adanya rotasi kunci secara berkala, baik berdasarkan waktu tertentu maupun setelah sejumlah operasi enkripsi dilakukan, guna mengurangi risiko kompromi terhadap kunci yang digunakan. Di sisi lain, menjaga integritas data yang dienkripsi menjadi hal yang tak kalah penting, salah satunya dengan menerapkan teknik verifikasi seperti HMAC (*Hash-based Message Authentication Code*) serta mencatat setiap aktivitas akses terhadap kunci melalui audit log yang lengkap dan dapat ditelusuri [1]. Untuk mencegah kerentanan dalam proses enkripsi itu sendiri, validasi terhadap nilai inisialisasi (*Initialization Vector*/IV) juga wajib dilakukan, dengan memastikan bahwa setiap operasi enkripsi menggunakan IV yang unik dan tidak dapat ditebak ulang [7]. Kombinasi dari praktik-praktik ini membentuk fondasi penting dalam penerapan enkripsi yang tidak hanya kuat secara algoritmik, tetapi juga aman secara operasional [1].

e. Evaluasi Keamanan dan Kinerja

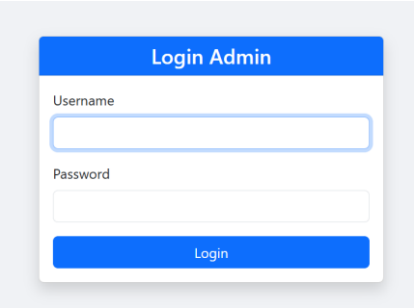
Evaluasi terhadap sistem pengamanan data, khususnya yang menggunakan algoritma enkripsi seperti AES-256, mencakup dua aspek utama: keamanan dan kinerja. Dari sisi keamanan, pengujian terhadap sistem kriptografi perlu dilakukan secara menyeluruh untuk menilai seberapa baik sistem mampu bertahan terhadap berbagai jenis serangan, baik yang bersifat pasif seperti penyadapan, maupun yang aktif seperti modifikasi data atau serangan *brute force* [8]. Proses evaluasi ini biasanya mencakup teknik seperti *penetration testing*, analisis struktur kunci, dan simulasi serangan untuk menguji tingkat resistensi sistem. Sementara itu, dari sisi kinerja, penggunaan algoritma enkripsi seperti AES-256 dengan mode operasi tertentu—misalnya CBC (*Cipher Block Chaining*)—diketahui dapat memberikan beban tambahan pada sistem, terutama dalam konteks transmisi data secara *real-time*. *Overhead* ini bisa berkisar antara 10 hingga 15 persen tergantung pada spesifikasi perangkat dan efisiensi implementasi sistem [7]. Dalam berbagai studi perbandingan, performa antar mode operasi AES pun menunjukkan perbedaan yang cukup signifikan, baik dalam hal kecepatan enkripsi maupun efisiensi sumber daya, sehingga pemilihan mode operasi yang tepat menjadi bagian penting dari proses optimasi sistem. Evaluasi yang menyeluruh terhadap kedua aspek ini sangat penting untuk memastikan bahwa sistem tidak hanya aman secara teoritis, tetapi juga dapat diimplementasikan secara praktis tanpa mengorbankan performa layanan [5].

3. Hasil dan Pembahasan

Aplikasi pengamanan data akademik dengan enkripsi AES-256 telah berhasil dikembangkan menggunakan bahasa pemrograman PHP dan basis data MySQL. Sistem ini terdiri dari beberapa halaman antarmuka seperti, Halaman LogIn, Dashboard Admin, Tambah Siswa.

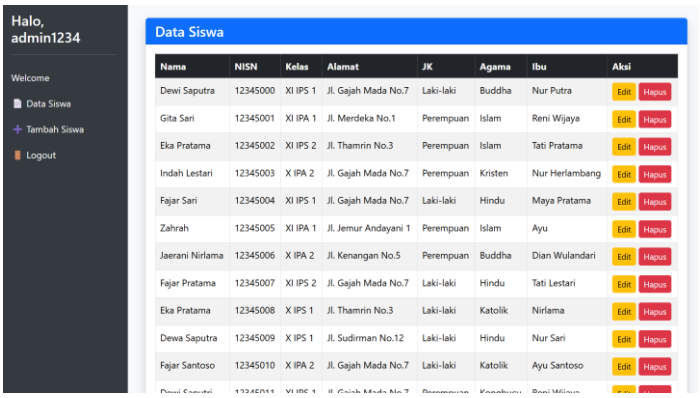
p-ISSN: 2986-3929
e-ISSN: 3032-1948

a. Tampilan Aplikasi



Gambar 4. Halaman Login Admin

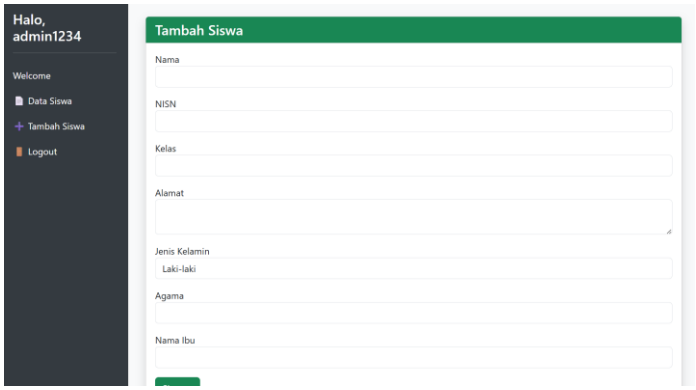
Halaman login admin merupakan pintu masuk utama bagi pengguna yang memiliki hak akses ke sistem pengelolaan data akademik berbasis web. Tampilan antarmuka dirancang secara sederhana namun tetap fungsional, terdiri atas dua kolom input untuk username dan password, serta sebuah tombol aksi untuk melakukan proses login. Bagian atas form ditandai dengan header berwarna biru cerah bertuliskan "Login Admin" yang memberikan identifikasi jelas terhadap peran pengguna yang dapat mengakses sistem. Seluruh elemen disusun secara simetris untuk menjaga keterbacaan dan kemudahan penggunaan. Pengisian form login ini menjadi langkah awal dalam proses autentikasi, di mana data yang dimasukkan akan diverifikasi terhadap database dan melalui proses enkripsi untuk menjaga keamanan informasi. Dengan desain yang responsif dan ringkas, halaman ini mendukung efisiensi interaksi pengguna tanpa mengesampingkan aspek keamanan.



Gambar 5. Halaman Dashboard Admin

Halaman dashboard admin berfungsi sebagai pusat kendali utama dalam sistem pengelolaan data akademik. Pada tampilan ini, pengguna yang telah berhasil login akan disambut dengan panel navigasi di sisi kiri yang memuat menu seperti “Data Siswa”, “Tambah Siswa”, dan “Logout”. Di bagian utama halaman, terdapat tabel yang menyajikan data siswa secara terstruktur dan informatif, meliputi nama, NISN, kelas, alamat, jenis kelamin, agama, serta nama ibu. Setiap baris data dilengkapi dengan dua tombol aksi, yaitu “Edit” dan “Hapus”, yang memudahkan admin dalam memperbarui maupun menghapus informasi siswa secara langsung. Warna-warna kontras digunakan untuk membedakan antara fungsi, seperti tombol “Edit” berwarna oranye dan “Hapus” berwarna merah, guna meminimalkan kesalahan saat pengguna berinteraksi. Dengan rancangan antarmuka yang ringkas dan intuitif, halaman ini mendukung efisiensi kerja admin dalam mengelola data akademik secara cepat, aman, dan terorganisir.

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 6. Halaman Tambah Siswa

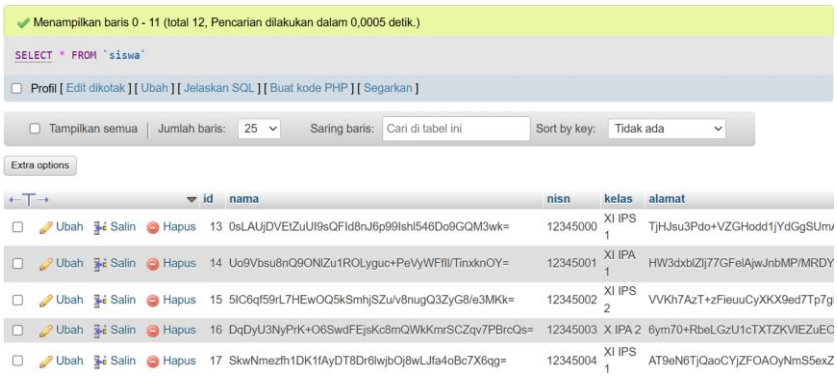
Halaman Tambah Siswa merupakan fitur yang disediakan untuk memungkinkan admin memasukkan data siswa baru ke dalam sistem. Antarmuka halaman ini disusun secara vertikal dengan kolom-kolom input yang telah diberi label, meliputi Nama, NISN, Kelas, Alamat, Jenis Kelamin, Agama, dan Nama Ibu. Setiap isian dirancang agar mudah diakses dan diisi, dengan field yang cukup luas untuk mendukung keterbacaan dan kenyamanan dalam penginputan data. Penggunaan warna hijau pada bagian header form menandakan fungsi penambahan atau pendaftaran baru, dan membantu membedakannya dari halaman lain seperti dashboard. Pada sisi kiri layar, panel navigasi tetap tersedia, memberikan akses cepat ke fitur Data Siswa, Tambah Siswa, dan Logout tanpa harus meninggalkan konteks halaman. Setelah form diisi, data yang dimasukkan akan diproses melalui sistem enkripsi AES-256 sebelum disimpan ke dalam database, sebagai bagian dari upaya pengamanan informasi akademik.

b. Tampilan Database

Gambar 7. Database table users

Tabel users pada database login_app digunakan untuk menyimpan data login admin yang memiliki akses ke sistem. Tabel ini terdiri dari tiga kolom, yaitu id sebagai identitas unik yang bersifat auto-increment, kode_login untuk menyimpan username, serta password yang berisi kata sandi yang telah dienkripsi guna menjaga keamanan akses. Data dalam tabel ini akan digunakan saat proses autentikasi login, di mana sistem akan mencocokkan input pengguna dengan data terenkripsi di database. Dengan struktur ini, sistem memastikan bahwa hanya pengguna terdaftar dan sah yang dapat mengakses fitur manajemen data siswa.

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 8. Proses Enkripsi Dekripsi Pada Data Sensitif di Database

Gambar tersebut menampilkan isi kolom jenis_kelamin, agama, dan nama_ibu dari tabel siswa dalam database, di mana dua kolom terakhir telah melalui proses enkripsi menggunakan algoritma AES-256-CBC. Berdasarkan file encryption.php, setiap data yang dimasukkan akan dienkripsi dengan encryption key sepanjang 32 karakter, lalu digabung dengan Initialization Vector (IV) sepanjang 16 byte, dan disimpan dalam bentuk string yang telah di-encode menggunakan base64. Tujuan dari penerapan enkripsi ini adalah untuk menjaga kerahasiaan data sensitif siswa, khususnya yang berkaitan dengan identitas pribadi dan keyakinan. Meskipun tampilan data di database tidak dapat dibaca langsung, data tersebut tetap dapat dikembalikan ke bentuk aslinya melalui proses dekripsi jika dilakukan oleh sistem yang memiliki akses terhadap kunci enkripsi yang sesuai. Ini membuktikan bahwa sistem telah menerapkan praktik keamanan data yang baik, khususnya dalam konteks pengelolaan data akademik berbasis web.

Gambar 9. Hasil Proses Enkripsi Dekripsi pada Database

Gambar tersebut menunjukkan isi tabel siswa pada kolom jenis_kelamin, agama, dan nama_ibu. Data pada kolom agama dan nama_ibu telah dienkripsi menggunakan algoritma AES-256-CBC, sebagaimana didefinisikan dalam file encryption.php. Setiap nilai terenkripsi ditampilkan dalam format base64 yang tidak dapat dibaca langsung oleh manusia. Proses ini bertujuan untuk menjaga kerahasiaan data sensitif siswa dan memastikan bahwa informasi pribadi tidak dapat diakses tanpa proses dekripsi yang sah melalui sistem.

c. Hasil Proses Enkripsi dan Dekripsi

Pada tahap ini dilakukan pengujian untuk memastikan bahwa proses enkripsi dan dekripsi data berjalan sesuai fungsinya. Data yang dimasukkan ke dalam sistem, seperti informasi agama dan nama ibu siswa, secara otomatis dienkripsi menggunakan algoritma AES-256 dalam mode CBC. Proses ini menghasilkan ciphertext berupa deretan karakter acak yang

tidak dapat dibaca secara langsung, sebagaimana terlihat pada isi tabel siswa dalam database. Setiap data terenkripsi disimpan dalam format base64, yang memungkinkan penyimpanan aman di dalam basis data tanpa mengubah struktur atau kompatibilitasnya. Untuk mengakses data asli, sistem akan melakukan proses dekripsi secara otomatis menggunakan kunci enkripsi dan Initialization Vector (IV) yang sesuai. Hasil dekripsi menunjukkan bahwa data dapat dikembalikan ke bentuk aslinya secara utuh dan akurat, sehingga validitas informasi tetap terjaga. Hasil ini sejalan dengan penelitian Febitri et al. (2023) dan Azhari et al. (2022) yang membuktikan efektivitas AES. Namun, pendekatan ini lebih fokus pada integrasi otomatis enkripsi-dekripsi dalam sistem web akademik secara real-time, dengan penyimpanan base64 yang kompatibel. Hal ini menunjukkan bahwa AES-256-CBC dapat diterapkan secara praktis dan efisien di lingkungan pendidikan.

4. Kesimpulan

Penelitian ini menunjukkan bahwa penerapan algoritma enkripsi AES-256 dengan mode operasi CBC pada sistem pengelolaan data akademik berbasis web mampu memberikan perlindungan yang efektif terhadap data sensitif siswa. Sistem yang dikembangkan mampu melakukan proses enkripsi dan dekripsi secara otomatis, menjaga kerahasiaan informasi seperti agama dan nama ibu dari akses yang tidak sah. Selain itu, penerapan enkripsi tidak mengganggu performa sistem secara signifikan, sehingga tetap efisien digunakan dalam lingkungan pendidikan. Dengan struktur antarmuka yang sederhana dan manajemen data yang terintegrasi, sistem ini dapat menjadi solusi praktis bagi institusi pendidikan dalam meningkatkan keamanan informasi akademik. Hasil ini juga membuktikan bahwa pendekatan enkripsi berbasis AES-256-CBC dapat diterapkan secara langsung dan relevan pada sistem informasi berbasis web.

Daftar Pustaka

[1] *Advanced Encryption Standard (AES)*, FIPS PUB 197, National Institute of Standards and Technology, 2001. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197
[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard,* 2nd ed. Berlin, Germany: Springer, 2013.
[3] *Recommendation for Block Cipher Modes of Operation*, SP 800-38A, National Institute of Standards and Technology, 2001. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-38A
[4] P. Rogaway, *"Evaluation of Some Blockcipher Modes of Operation,"* Univ. California, Davis, CA, USA, Tech. Rep., 2011.
[5] *"Cryptographic Storage Cheat Sheet,"* Open Web Application Security Project, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
[6] *Payment Card Industry Data Security Standard: Requirements and Testing Procedures*, v4.0, PCI Security Standards Council, 2022.
[7] *Benchmarking Encryption Performance in Cloud Environments,* Cloud Security Alliance, 2021. [Online]. Available: https://cloudsecurityalliance.org
[8] *Technical Guide to Information Security Testing*, SP 800-115, National Institute of Standards and Technology, 2008.
[9] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564-573.
[10] Febitri, N., Witriyono, H., Muntahanah, M., & Marhalim, M. (2023). Application of AES 256 Cryptography Algorithm OCB Mode on Student Data. Jurnal Komputer, Informasi dan Teknologi, 3(2), 423-432.
[11] Rogaway, P., Bellare, M., & Black, J. (2003). OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security, 6(3), 365–403. https://doi.org/10.1145/937527.937529
[12] Rumahweb Indonesia. (2023). Apa Itu Learning Management System (LMS) Beserta Contohnya. Diakses dari https://blog.rumahweb.com/lms-adalah/
[13] SEVIMA. (2023). Pengertian Learning Management System (LMS). Diakses dari

https://sevima.com/pengertian-learning-management-system/
[14] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains dan Komputer, 2(01), 163-171.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Halaman ini sengaja dibiarkan kosong