

WEB Dashboard Admin Pojok Statistik Berbasis Enkripsi AES-128 untuk Keamanan Autentikasi

WEB Dashboard Admin Statistics Corner Based on AES-128 Encryption for Authentication Security

Mochammad Darip¹

¹Fakultas Ilmu Komputer, Universitas Bina Bangsa, Kota Serang - Banten, Indonesia

*Penulis korespondensi: darif.uniba@gmail.com

Abstract

The rapid development of information technology has increased the demand for statistical data management systems that are integrated, efficient, and supported by reliable security mechanisms. In practice, however, many statistical systems are still developed in a fragmented manner and lack adequate data protection, which increases the risk of unauthorized access and information leakage. Such conditions may reduce the effectiveness of data management and weaken user trust in the implemented information systems. This study aims to design and develop a web-based admin dashboard for Pojok Statistik that implements AES-128 encryption to protect sensitive data, particularly administrator authentication credentials. The research methodology includes system requirement analysis, application architecture design, web-based dashboard development, and testing of encryption and decryption processes. The cryptographic algorithm applied is the Advanced Encryption Standard (AES) with a 128-bit key using Cipher Block Chaining (CBC) mode and PKCS7 padding. The encryption implementation focuses on the admin login process to ensure that credential data are neither stored nor transmitted in plaintext form. The results indicate that the system is capable of providing secure login authentication, centralized statistical data management, and more structured administrative access control. The encryption and decryption processes operate consistently without causing significant system performance degradation. Therefore, the developed web-based admin dashboard improves the efficiency of statistical data management while strengthening information security and has the potential to be adopted as a secure and scalable solution for institutional statistical data management.

Keywords: Web Dashboard, Statistics Corner, AES-128 Encryption, Data Security, Admin Authentication, Statistics Information System

Abstrak

Abstrak Perkembangan teknologi informasi mendorong kebutuhan akan sistem pengelolaan data statistik yang terintegrasi, efisien, dan didukung oleh mekanisme keamanan yang andal. Namun, pada praktiknya masih banyak sistem statistik yang dikembangkan secara terpisah dan belum dilengkapi perlindungan data yang memadai, sehingga meningkatkan risiko akses tidak sah dan kebocoran informasi. Kondisi tersebut berpotensi menghambat efektivitas pengelolaan data serta menurunkan tingkat kepercayaan terhadap sistem informasi yang digunakan. Penelitian ini bertujuan untuk merancang dan mengembangkan web dashboard admin Pojok Statistik yang menerapkan enkripsi AES-128 guna melindungi data sensitif, khususnya data autentikasi administrator. Metode penelitian yang digunakan meliputi analisis kebutuhan sistem, perancangan arsitektur aplikasi, pengembangan dashboard berbasis web, serta pengujian proses enkripsi dan dekripsi data. Algoritma kriptografi yang diterapkan adalah Advanced Encryption Standard (AES) dengan panjang kunci 128-bit menggunakan mode Cipher Block Chaining (CBC) dan padding PKCS7. Implementasi enkripsi difokuskan pada proses login admin agar data kredensial tidak disimpan maupun dikirimkan dalam bentuk plaintext. Hasil penelitian menunjukkan bahwa sistem mampu menyediakan autentikasi login yang aman, pengelolaan data statistik secara terpusat, serta pengaturan hak akses admin yang lebih terstruktur. Proses enkripsi dan dekripsi berjalan secara konsisten tanpa menimbulkan penurunan kinerja sistem yang signifikan. Dengan demikian, web dashboard admin Pojok Statistik yang dikembangkan dapat meningkatkan efisiensi pengelolaan data statistik sekaligus memperkuat aspek keamanan informasi dan berpotensi diterapkan sebagai solusi yang aman dan skalabel pada lingkungan institusi.

Kata kunci: Web Dashboard, Pojok Statistik, Enkripsi AES-128, Keamanan Data, Autentikasi Admin, Sistem Informasi Statistik

PENDAHULUAN

Transformasi digital telah menjadi agenda strategis dalam pengelolaan organisasi, baik pada instansi pemerintah maupun institusi akademik [1],[2],[3]. Perkembangan teknologi informasi mendorong pemanfaatan sistem informasi berbasis web sebagai sarana utama dalam pengelolaan, penyimpanan, dan penyajian data secara terstruktur [4],[5]. Salah satu jenis data yang memiliki peranan krusial dalam mendukung proses pengambilan keputusan adalah data statistik [2],[6]. Data statistik berfungsi sebagai dasar perumusan kebijakan, perencanaan program, serta evaluasi kinerja institusi, sehingga keakuratan, konsistensi, dan ketersediaannya menjadi aspek yang tidak dapat diabaikan [7],[8].

Namun, pada praktiknya, pengelolaan data statistik masih sering dilakukan menggunakan sistem yang tidak terintegrasi [4],[5]. Data disimpan pada berbagai media dan format yang berbeda, seperti file spreadsheet terpisah atau basis data lokal, sehingga menyulitkan proses pengolahan dan pemantauan secara menyeluruh [2],[7]. Kondisi ini tidak hanya memperlambat proses penyajian informasi, tetapi juga meningkatkan risiko terjadinya inkonsistensi data akibat perbedaan versi atau kesalahan input [7],[9]. Selain itu, keterbatasan sistem konvensional dalam menyediakan akses data secara real-time turut menghambat efektivitas pengambilan keputusan yang berbasis data [6],[10],[11].

Permasalahan lain yang tidak kalah penting adalah aspek keamanan sistem informasi [8]. Dalam banyak kasus,

keamanan data belum menjadi prioritas utama, khususnya dalam perlindungan data sensitif seperti kredensial administrator dan informasi pengelolaan sistem [12],[13]. Penyimpanan data tanpa mekanisme pengamanan yang memadai berpotensi menimbulkan risiko kebocoran data, penyalahgunaan akses, serta serangan siber yang dapat merugikan institusi [13],[8]. Oleh karena itu, diperlukan penerapan mekanisme keamanan yang mampu menjamin kerahasiaan dan integritas data dalam sistem informasi [12],[14],[9].

Dashboard interaktif berbasis web telah terbukti efektif dalam menyajikan data statistik secara visual dan mudah dipahami oleh pengambil Keputusan [6],[15],[10]. Implementasi dashboard memungkinkan akses data secara real-time, meningkatkan transparansi, dan mempercepat proses analisis data [10],[11]. Penelitian menunjukkan bahwa penggunaan dashboard visualisasi dapat meningkatkan akurasi pengambilan keputusan hingga 40% dan mengurangi waktu analisis data secara signifikan [15],[11].

Kriptografi merupakan salah satu pendekatan yang efektif dalam meningkatkan keamanan sistem informasi [12],[13],[14]. Advanced Encryption Standard (AES) dengan panjang kunci 128 bit merupakan algoritma kriptografi simetris yang telah banyak digunakan karena memiliki tingkat keamanan yang tinggi serta efisiensi komputasi yang baik [12],[13], khususnya untuk aplikasi berbasis web [16]. AES-128 menggunakan 10 putaran transformasi (rounds) untuk mengenkripsi data dalam blok 128-bit, dengan tingkat keamanan yang memadai untuk melindungi informasi rahasia tingkat SECRET menurut standar NIST [14]. Implementasi algoritma AES-128 dapat digunakan untuk melindungi data sensitif, seperti informasi autentikasi admin, sehingga hanya pihak yang berwenang yang dapat mengakses sistem [12],[16].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan perancangan dan implementasi web dashboard admin Pojok Statistik yang terintegrasi dan dilengkapi dengan mekanisme enkripsi AES-128 [1],[6],[12]. Sistem ini diharapkan mampu menyediakan pengelolaan data statistik secara terpusat, aman, dan mudah diakses [4],[15],[16]. Dashboard yang dirancang dilengkapi dengan visualisasi data interaktif yang mendukung pengambilan keputusan berbasis data real-time [6],[10],[11]. Selain itu, dashboard admin yang dirancang juga memiliki fleksibilitas untuk dikembangkan di masa mendatang sesuai dengan kebutuhan institusi [2],[17], sehingga dapat mendukung pengelolaan data statistik secara berkelanjutan dan adaptif terhadap perkembangan teknologi [3],[5].

METODE PENELITIAN

Penelitian ini merupakan penelitian rekayasa perangkat lunak (software engineering) dengan pendekatan pengembangan sistem. Metode ini dipilih karena penelitian berfokus pada perancangan, implementasi, dan pengujian suatu sistem informasi berbasis web yang dilengkapi dengan mekanisme kriptografi.

A. ANALISIS KEBUTUHAN SISTEM

Tahap analisis kebutuhan bertujuan untuk mengidentifikasi permasalahan dan kebutuhan utama dalam pengelolaan data statistik. Pada tahap ini dilakukan identifikasi terhadap proses bisnis yang berjalan, keterbatasan sistem yang ada, serta risiko keamanan yang mungkin timbul akibat penyimpanan dan transmisi data yang belum terenkripsi.

Hasil analisis menunjukkan bahwa pengelolaan data statistik masih dilakukan secara terpisah dan belum terintegrasi dalam satu sistem terpusat. Selain itu, mekanisme autentikasi belum dilengkapi dengan perlindungan data sensitif, sehingga berpotensi menimbulkan risiko kebocoran data. Berdasarkan kondisi tersebut, ditetapkan kebutuhan fungsional sistem meliputi autentikasi login admin, pengelolaan konten statistik, pengaturan hak akses pengguna, serta penyimpanan data pada basis database. Kebutuhan nonfungsional sistem mencakup aspek keamanan, keandalan, dan kemudahan pengembangan sistem.

B. PERANCANGAN SISTEM

Tahap perancangan sistem difokuskan pada penyusunan arsitektur sistem dan alur kerja aplikasi. Sistem dirancang sebagai aplikasi berbasis web yang terdiri atas antarmuka dashboard admin, server aplikasi, dan basis data. Antarmuka dashboard admin berfungsi sebagai media interaksi pengguna dalam mengelola data statistik.

Pada tahap ini juga dirancang mekanisme keamanan sistem dengan menerapkan algoritma kriptografi simetris Advanced Encryption Standard (AES) 128-bit. Algoritma ini dipilih karena memiliki tingkat keamanan yang tinggi dan efisiensi komputasi yang baik untuk aplikasi berbasis web.[1] Mode operasi yang digunakan adalah Cipher Block Chaining (CBC) dengan skema padding PKCS7, yang bertujuan memastikan kesesuaian ukuran data dengan blok enkripsi AES.

C. IMPLEMENTASI ALGORITMA ENKRIPSI

Tahap implementasi dilakukan dengan mengembangkan sistem sesuai rancangan yang telah ditetapkan. Implementasi algoritma AES-128 dimulai dengan proses penyiapan plaintext berupa data kredensial admin. Plaintext contoh yang digunakan adalah admin:admin123 dengan panjang 14 byte. Karena AES-128 bekerja pada blok berukuran 16 byte, maka dilakukan proses padding menggunakan skema PKCS7 dengan menambahkan dua byte bernilai 02.

Secara matematis, proses penyesuaian panjang data dapat dituliskan sebagai berikut:

(1)

dengan adalah panjang plaintext setelah padding, adalah panjang data awal, dan adalah panjang padding yang ditambahkan.

Plaintext yang telah dipadding kemudian dilakukan operasi XOR dengan initialization vector (IV) sebelum dienkripsi menggunakan AES-128. Proses enkripsi ini menghasilkan ciphertext dalam bentuk biner yang selanjutnya dikodekan menggunakan Base64 untuk memudahkan peny-

Tabel 1. Kebutuhan fungsional system

No	Kebutuhan Fungsional	Deskripsi
1	Autentikasi Admin	Sistem menyediakan login admin menggunakan username dan password terenkripsi
2	Enkripsi Kredensial	Data login admin dienkripsi menggunakan algoritma AES-128
3	Manajemen Data Statistik	Admin dapat menambah, mengubah, dan menghapus data
4	Manajemen Konten	Admin mengelola infografis, berita, dan dokumentasi
5	Hak Akses Admin	Sistem membatasi akses berdasarkan peran admin

Tabel 2. Kebutuhan non fungsional system

No	Kebutuhan Fungsional	Deskripsi
1	Keamanan	Data sensitif tidak disimpan dalam bentuk plaintext
2	Kinerja	Proses enkripsi tidak menurunkan performa sistem
3	Usability	Antarmuka mudah dipahami oleh admin.
4	Scalability	Sistem mudah dikembangkan di masa depan
5	Realibility	Sistem berjalan stabil dan konsisten

impanan dan transmisi data.

D. Pengujian Sistem

Pengujian sistem dilakukan untuk memverifikasi bahwa seluruh fungsi aplikasi berjalan sesuai dengan kebutuhan yang telah ditetapkan serta memastikan mekanisme enkripsi AES-128 diterapkan dengan benar. Metode pengujian yang digunakan meliputi pengujian fungsional dan pengujian keamanan sistem.

Pengujian fungsional difokuskan pada proses autentikasi admin, navigasi dashboard, serta pengelolaan data statistik. Setiap fungsi diuji dengan skenario input yang sesuai untuk memastikan sistem dapat merespons dengan benar.

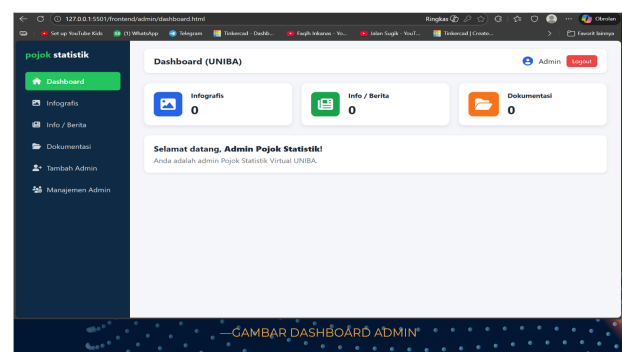
Pengujian keamanan dilakukan dengan mengevaluasi proses enkripsi dan dekripsi data kredensial admin menggunakan algoritma AES-128 dengan mode Cipher Block Chaining (CBC) dan padding PKCS7. Pengujian ini bertujuan memastikan bahwa data sensitif tidak diproses maupun disimpan dalam bentuk plaintext.

Selain itu, dilakukan pengujian kinerja untuk mengamati dampak penerapan algoritma enkripsi terhadap waktu respons sistem, khususnya pada proses login admin dan pengelolaan data statistik.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil perancangan, implementasi, serta pengujian sistem web dashboard admin Pojok Statistik yang dikembangkan berdasarkan metode penelitian pada Bab II. Pembahasan difokuskan pada perancangan antarmuka sistem, penerapan mekanisme autentikasi admin menggunakan algoritma enkripsi AES-128, serta pengujian sistem untuk memastikan keamanan dan kinerja sistem berjalan sesuai dengan kebutuhan.

Selain menyajikan hasil implementasi sistem, bagian ini juga membahas keterkaitan antara rancangan sistem dan kebutuhan operasional pengelolaan data statistik di lingkungan institusi. Evaluasi dilakukan untuk memastikan bahwa sistem yang dikembangkan tidak hanya berfungsi secara teknis, tetapi juga mampu mendukung proses kerja admin secara efektif dan aman.

**Gambar 1.** Tampilan dashboard admin Pojok Statistik

PERANCANGAN DAN IMPLEMENTASI

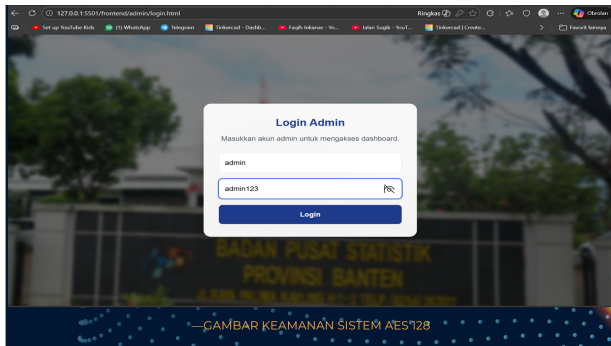
Perancangan difokuskan pada penyusunan tata letak antarmuka yang sederhana, informatif, dan mudah digunakan agar admin dapat mengakses serta mengelola data secara terpusat dan efisien.

Perancangan sistem mencakup penyusunan struktur menu utama, penempatan elemen informasi, serta pengelompokan fitur pengelolaan data statistik. Menu utama dirancang untuk memberikan akses langsung ke fitur-fitur penting seperti pengelolaan infografis, informasi atau berita, dokumentasi, serta manajemen admin. Pendekatan ini bertujuan untuk meminimalkan kompleksitas navigasi dan meningkatkan efisiensi penggunaan sistem.

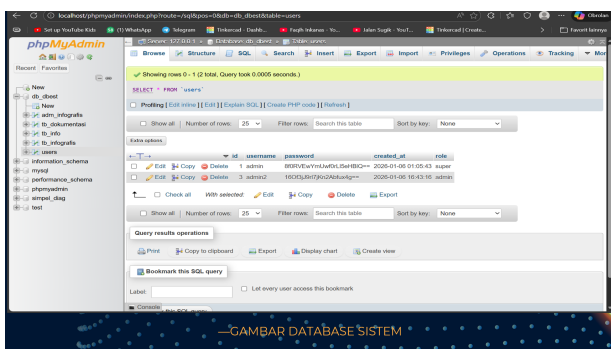
Tampilan hasil perancangan dashboard admin Pojok Statistik ditunjukkan pada gambar 1.

Tata letak yang sederhana dan konsisten memudahkan admin dalam melakukan pemantauan serta pengolahan data statistik tanpa memerlukan proses navigasi yang rumit.

Selain itu, perancangan antarmuka juga mempertimbangkan aspek usability dan user experience (UX), sehingga sistem dapat digunakan oleh admin dengan berbagai tingkat pengalaman. Dengan rancangan yang fleksibel dan terstruktur, sistem diharapkan dapat dikembangkan lebih lanjut apabila diperlukan penambahan fitur di masa mendatang.



Gambar 2. Tampilan proses autentikasi login dengan penerapan enkripsi AES-128



Gambar 3. Penyimpanan password admin dalam basis data dalam bentuk terenkripsi.

IMPLEMENTASI SISTEM

Hasil Berdasarkan hasil perancangan yang telah dijelaskan pada subbab sebelumnya, tahap selanjutnya adalah implementasi sistem web dashboard admin Pojok Statistik. Pada tahap ini, seluruh rancangan antarmuka dan arsitektur sistem direalisasikan ke dalam bentuk aplikasi berbasis web yang dapat dioperasikan oleh administrator.

Implementasi sistem diawali dengan penerapan mekanisme autentikasi login admin sebagai lapisan keamanan awal sistem. Pada halaman login, admin diwajibkan memasukkan username dan password untuk dapat mengakses dashboard. Data kredensial yang dimasukkan tidak diproses secara langsung, melainkan terlebih dahulu dienkripsi menggunakan algoritma AES-128 sebelum dilakukan proses verifikasi oleh sistem. Tampilan proses autentikasi login dengan penerapan enkripsi AES-128 ditunjukkan pada gambar 2.

Halaman login pada Gambar 2 menunjukkan implementasi mekanisme autentikasi admin sebagai lapisan keamanan awal sistem. Penerapan enkripsi pada tahap ini bertujuan untuk melindungi data sensitif dari potensi penyadapan maupun akses tidak sah selama proses autentikasi berlangsung.

Setelah proses autentikasi berhasil, sistem akan mengarahkan admin ke halaman dashboard utama. Tampilan dashboard admin setelah login ditunjukkan pada gambar 3.

Gambar 3 memperlihatkan bahwa dashboard hanya dapat diakses setelah kredensial admin berhasil diverifikasi oleh sistem. Dashboard menampilkan informasi ringkas serta

menu pengelolaan data statistik yang siap digunakan oleh admin.

Selain pada proses autentikasi, implementasi sistem juga mencakup pengamanan penyimpanan data kredensial. Password admin disimpan dalam basis data dalam bentuk ciphertext hasil enkripsi AES-128 yang telah melalui proses encoding Base64. Dengan mekanisme ini, informasi password tidak dapat dibaca secara langsung meskipun basis data diakses secara manual, sehingga meningkatkan keamanan data sistem secara keseluruhan.

PENGUJIAN SISTEM

Pada tahap ini dilakukan pengujian terhadap sistem web dashboard admin Pojok Statistik untuk memastikan bahwa seluruh fungsi yang telah diimplementasikan dapat berjalan sesuai dengan kebutuhan dan rancangan sistem. Pengujian sistem bertujuan untuk mengevaluasi keandalan mekanisme autentikasi admin, efektivitas penerapan algoritma enkripsi AES-128, serta kinerja sistem dalam mendukung aktivitas pengelolaan data statistik.

Pengujian sistem difokuskan pada beberapa aspek utama, yaitu pengujian fungsional autentikasi admin, pengujian keamanan data kredensial, dan pengujian kinerja sistem setelah penerapan mekanisme enkripsi. Dengan pengujian ini, diharapkan dapat diketahui apakah sistem telah memenuhi kebutuhan fungsional sekaligus memberikan tingkat keamanan yang memadai tanpa mengganggu performa sistem. Pengujian sistem diawali dengan pengujian proses enkripsi data kredensial admin menggunakan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 128-bit. Pengujian ini bertujuan untuk memastikan bahwa setiap tahapan enkripsi, mulai dari proses padding data, penggunaan initialization vector (IV), hingga pembentukan ciphertext, telah diimplementasikan sesuai dengan spesifikasi algoritma AES-128 yang digunakan. Melalui pengujian ini, sistem dievaluasi untuk memastikan bahwa data kredensial tidak diproses maupun disimpan dalam bentuk plaintext, serta menghasilkan output terenkripsi yang konsisten dan aman sebelum digunakan pada proses autentikasi admin. Berdasarkan hasil pengujian proses enkripsi AES-128 pada sistem, tahapan enkripsi data kredensial admin dapat dijelaskan sebagaimana ditunjukkan pada Tabel 3.

Pengujian autentikasi dilakukan dengan memasukkan data username dan password melalui halaman login admin. Berdasarkan hasil pengujian, setiap data kredensial yang dimasukkan terlebih dahulu diproses menggunakan algoritma enkripsi AES-128 dengan mode Cipher Block Chaining (CBC) dan padding PKCS7 sebelum dilakukan proses verifikasi oleh sistem. Hasil pengujian menunjukkan bahwa sistem tidak memproses data kredensial dalam bentuk plaintext, baik pada saat proses autentikasi maupun pada tahap penyimpanan data.

Selain pengujian proses autentikasi, dilakukan pula pengujian terhadap mekanisme penyimpanan data kredensial pada basis data. Hasil pengujian menunjukkan bahwa password admin tersimpan dalam bentuk ciphertext hasil

Tabel 3. Proses enkripsi AES-128

No	Tahapan	Deskripsi Proses
1	Plaintext	Admin: admin123
2	Padding PKCS7	Penambahan 02 02 untuk memenuhi ukuran blok
3	XOR dengan IV	Proses pengacakan awal menggunakan initialization vector.
4	Enkripsi AES-128	Pembentukan ciphertext biner
5	Encoding Base64	j0LizBWgf1iXJwXenn5IA

enkripsi AES-128 yang telah melalui proses encoding Base64. Dengan demikian, meskipun basis data diakses secara langsung, informasi password tidak dapat dibaca atau dikenali secara langsung. Hal ini menunjukkan bahwa sistem mampu melindungi data sensitif dari potensi kebocoran data akibat akses tidak sah.

Pengujian keamanan sistem juga dilakukan untuk memastikan bahwa penerapan enkripsi dapat memberikan perlindungan terhadap data selama proses penggunaan sistem. Berdasarkan hasil pengujian, mekanisme enkripsi yang diterapkan mampu menjaga kerahasiaan data kredensial admin dan mencegah penyalahgunaan data pada proses autentikasi. Hasil ini menunjukkan bahwa sistem telah memenuhi prinsip dasar keamanan informasi, khususnya terkait aspek kerahasiaan data (confidentiality).

Selain aspek keamanan, dilakukan pula pengujian kinerja sistem untuk mengetahui dampak penerapan algoritma enkripsi terhadap performa sistem secara keseluruhan. Pengujian kinerja dilakukan dengan mengamati waktu respons sistem pada saat proses login dan pengelolaan data statistik. Berdasarkan hasil pengujian, proses enkripsi dan dekripsi dapat dijalankan dengan waktu eksekusi yang relatif singkat dan tidak menimbulkan keterlambatan yang signifikan dalam penggunaan sistem.

Hasil pengujian kinerja menunjukkan bahwa sistem tetap responsif dan stabil saat digunakan oleh admin. Proses login dapat dilakukan dengan lancar, dan fitur pengelolaan data statistik dapat diakses tanpa mengalami penurunan performa yang berarti. Hal ini menunjukkan bahwa penerapan enkripsi AES-128 tidak memberikan dampak negatif yang signifikan terhadap kinerja sistem.

Berdasarkan keseluruhan hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa sistem web dashboard admin Pojok Statistik telah berfungsi dengan baik sesuai dengan rancangan yang ditetapkan. Penerapan algoritma enkripsi AES-128 terbukti mampu meningkatkan keamanan autentikasi admin dan perlindungan data kredensial tanpa mengorbankan kinerja sistem. Dengan demikian, sistem yang dikembangkan layak digunakan sebagai media pengelolaan data statistik yang aman, efisien, dan andal.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem yang telah dilakukan, dapat disimpulkan bahwa sistem web dashboard admin Pojok Statistik berhasil dikembangkan sesuai dengan kebutuhan pengelolaan data statistik pada lingkungan institusi. Sistem ini mampu menyediakan antarmuka yang sederhana, terstruktur, dan mudah digu-

nakan, sehingga memudahkan admin dalam melakukan pemantauan serta pengolahan data statistik secara terpusat.

Penerapan mekanisme autentikasi admin dengan algoritma enkripsi AES-128 menggunakan mode Cipher Block Chaining (CBC) dan padding PKCS7 terbukti mampu meningkatkan keamanan sistem. Data kredensial admin tidak diproses maupun disimpan dalam bentuk plaintext, melainkan dalam bentuk ciphertext hasil proses enkripsi dan encoding Base64. Dengan demikian, sistem mampu menjaga kerahasiaan data kredensial dan meminimalkan risiko kebocoran data akibat akses tidak sah.

Hasil pengujian sistem menunjukkan bahwa mekanisme enkripsi yang diterapkan dapat berjalan secara konsisten dan tidak menimbulkan kesalahan pada proses autentikasi. Selain itu, penerapan enkripsi AES-128 tidak memberikan dampak signifikan terhadap kinerja sistem. Proses login dan pengelolaan data statistik tetap berjalan dengan responsif dan stabil, sehingga sistem dapat digunakan secara optimal dalam mendukung aktivitas admin.

Secara keseluruhan, sistem web dashboard admin Pojok Statistik yang dikembangkan telah memenuhi aspek fungsionalitas, keamanan, dan kinerja sistem. Dengan karakteristik tersebut, sistem ini layak diterapkan sebagai solusi pengelolaan data statistik yang aman dan efisien. Pengembangan lebih lanjut dapat dilakukan dengan menambahkan fitur pengelolaan data yang lebih kompleks serta penerapan mekanisme keamanan tambahan guna meningkatkan tingkat perlindungan sistem di masa mendatang.

DAFTAR PUSTAKA

- [1] 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.
- [2] A. N. Oghenekevwe, O. A. Daniel, A. B. Elohor, A. M. Ifioko, O. A. Micheal, and A. O. Regha, "Strengthening Web3 Data Confidentiality Through Blockchain-Enabled Multifactor Authentication : A Comparative Security Evaluation," vol. 10, no. 10, 2025.
- [3] J. Simarmata, T. Limbong, M. B. R. Ginting, R. Damanik, and M. I. Padli, "Implementation of AES Algorithm for Information Security of Web-Based Application," vol. 7, pp. 318–320, 2018.
- [4] E. Bertino and R. Sandhu, "Database Security — Concepts , Approaches , and Challenges," vol. 2, no. 1, pp. 2–19, 2005.
- [5] R. Ganesh, B. Ul, I. Khan, A. Raouf, K. Amirrudin,

- and B. Kamsin, A panoramic survey of the advanced encryption standard : from architecture to security analysis , key management , real-world applications , and post-quantum challenges. 2025.
- [6] C. A. License, K. Shen, R. Hu, Y. Yang, and R. Deng, “Retracted: Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things,” vol. 2022, 2023, doi: 10.1155/2022/8424100.
- [7] J. M. A. Baluro and G. Kumar, “A Systematic Study of E-Governance Infrastructure for Smart Campus Development in CBSUA,” vol. 0, pp. 337–345, 2025.
- [8] C. E. O. Skilloxy, “The Integration of Information Systems in Strategic Decision-Making : A Management Perspective,” vol. 10, no. 2, 2025.
- [9] B. Szedmák, L. Varga, and R. Z. Szabó, “Digital Transformation of Public Services : The Case of the Document Management Application Digital Transformation of Public Services : The Case of the Document,” *Int. J. Public Adm.*, vol. 00, no. 00, pp. 1–18, 2025, doi: 10.1080/01900692.2025.2520522.
- [10] G. Stahlman, I. Yanovitzky, and M. Kim, “Design , Application , and Actionability of US Public Health Data Dashboards : Scoping Review Corresponding Author :,” vol. 27, pp. 1–20, 2025, doi: 10.2196/65283.
- [11] G. Neri, S. Marshall, H. K. Chan, A. Yaghi, D. Tabor, and R. Sinha, “Data visualization in AI-assisted decision-making : a systematic review,” no. 2016, 2022.
- [12] M. Yang, Y. Hou, L. Li, R. Chang, and W. Zeng, “Dashboard Vision : Using Eye-Tracking to Understand and Predict Dashboard Viewing Behaviors,” *IEEE Trans. Vis. Comput. Graph.*, vol. 31, no. 10, pp. 6930–6945, 2025, doi: 10.1109/TVCG.2025.3532497.
- [13] S. An and D. Han, “Information Management System of University Education Based on Big Data Analysis,” 2023, doi: 10.4108/eai.23-12-2022.2329181.
- [14] H. S. Mamede and F. Branco, “The relationship between digital transformation and digital literacy - an explanatory model : Systematic literature José Arnaud,” 2025.
- [15] D. Frempong et al., “Real-Time Analytics Dashboards for Decision-Making Using Tableau in Public Sector and Business Intelligence Applications Received : 03-09-2022 Accepted : 05-10-2022 Page No : 65-80,” pp. 65–80, 2022.
- [16] “Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- 19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ’ s public news and information website . Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories , such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source . These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active .,” no. January, 2020.
- [17] H. A. Mahmoud and H. M. Yasin, “Data Integrity and Consistency Challenges in Distributed Database Systems,” vol. 10, no. 05, pp. 5077–5086, 2025, doi: 10.47191/etj/v10i05.36.