Design and Implementation of a Mobile-Based Export-Import Digital Document Security System Using the AES-256 Encryption Algorithm to Ensure Data Confidentiality and Integrity

Bayu Adi Prasetyo[1)*)], Rio Kurniawan[2)], Suhendro Yusuf Irianto[3)], Amnah[4)]

[1)2)3)4)]Teknik Informatika, Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya
***)Correspondence author:** Bayu Adi Prasetyo, bayuadiprasetyo2004@email.com, Bandar Lampung, Indonesia
DOI : https://doi.org/10.37012/jtik.v12i1.3420

Abstract

The increasing use of digital documents in export-import activities, especially in government agencies such as the Directorate General of Customs and Excise, has the potential to pose a threat of leaks if not supported by an adequate security system. The design of this security system aims to design and develop a web-based digital export-import document security system by implementing the Advanced Encryption Standard (AES) 256-bit encryption algorithm. The system development was carried out using the Waterfall method by utilizing PHP, HTML, CSS, JavaScript, and MySQL database technology. This system implements encryption and decryption mechanisms on export-import documents in PDF and DOCX formats. Test results indicate that encrypted documents cannot be accessed without a valid decryption process, and data integrity is maintained referring to the AES-256 validation results. This system is able to increase the level of digital document security and minimize the risk of data leaks in a web-based system environment. This research requires the addition of a multi-layer authentication mechanism, the implementation of a more comprehensive encryption key management system, and the development of applications for mobile platforms. The rapid development of information technology has changed the way individuals, organizations, and government institutions manage and distribute information. One of the main impacts is the increasing use of digital import-export documents as the primary medium for storing and exchanging critical data. These documents generally contain sensitive information, requiring security mechanisms capable of ensuring data confidentiality, integrity, and authenticity during storage and distribution.

Keywords: *Document Security, Export-Import, AES-256, Web-Based System*

Abstrak

Meningkatnya pemanfaatan dokumen digital dalam kegiatan ekspor-impor, terutama pada instansi pemerintahan seperti Direktorat Jenderal Bea dan Cukai, berpotensi menimbulkan ancaman kebocoran apabila tidak didukung oleh sistem keamanan yang memadai. Perancangan sistem keamanan ini bertujuan untuk merancang dan mengembangkan sistem keamanan dokumen digital ekspor-impor berbasis web dengan menerapkan algoritma enkripsi Advanced Encryption Standard (AES) 256-bit. Pengembangan sistem dikerjakan menggunakan metode Waterfall dengan memanfaatkan teknologi PHP, HTML, CSS, JavaScript, serta basis data MySQL. Sistem ini mengimplementasikan mekanisme enkripsi dan dekripsi pada dokumen ekspor-impor berformat PDF dan DOCX. Hasil pengujian menandakan bahwa dokumen yang dienkripsi tidak dapat diakses tanpa proses dekripsi yang valid, serta keutuhan data tetap terjaga merujuk pada hasil validasi AES-256. Sistem yang ini mampu meningkatkan tingkat keamanan dokumen digital dan meminimalkan risiko kebocoran data pada lingkungan sistem berbasis web. Penelitian ini perlu penambahan mekanisme autentikasi multi-layer, penerapan sistem pengelolaan kunci enkripsi yang lebih komprehensif, serta pengembangan

aplikasi ke platform mobile. Perkembangan teknologi informasi yang pesat telah mengubah cara individu, organisasi, dan lembaga pemerintahan dalam mengelola serta mendistribusikan informasi. Salah satu dampak utamanya adalah meningkatnya penggunaan dokumen digital ekspor-impor sebagai media utama penyimpanan dan pertukaran data penting. Dokumen tersebut umumnya memuat informasi sensitif sehingga memerlukan mekanisme keamanan yang mampu menjamin kerahasiaan, integritas, dan keaslian data selama proses penyimpanan maupun distribusi.

Kata Kunci : Keamanan Dokumen, Ekspor-Impor, AES-256, Sistem Berbasis Web.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah cara individu, organisasi, dan lembaga pemerintahan dalam mengelola serta mendistribusikan informasi. Salah satu dampak utamanya adalah meningkatnya penggunaan dokumen digital ekspor-impor sebagai media utama penyimpanan dan pertukaran data penting. Dokumen tersebut umumnya memuat informasi sensitif sehingga memerlukan mekanisme keamanan yang mampu menjamin kerahasiaan, integritas, dan keaslian data selama proses penyimpanan maupun distribusi (Irwanto, 2024).

Urgensi keamanan semakin meningkat seiring dengan bertambahnya volume dokumen ekspor-impor yang diproses secara elektronik setiap tahun. Data internal Bea Cukai Bandar Lampung menunjukkan bahwa jumlah dokumen impor kategori BC20 dan BC23 mengalami fluktuasi namun tetap berada pada angka ribuan setiap tahun. Pada 2023 tercatat 2.265 dokumen BC20 dan 853 dokumen BC23, meningkat pada 2024 menjadi 2.330 dan 1.407 dokumen, serta pada 2025 sebesar 2.066 dan 1.085 dokumen (Bea Cukai Bandar Lampung, 2025). Tren serupa juga terlihat pada dokumen ekspor, di mana dokumen BC30 dan P3BET mencapai puluhan ribu setiap tahunnya. Kondisi ini menunjukkan tingginya potensi risiko kebocoran data apabila tidak dilindungi dengan sistem keamanan yang memadai (Bea Cukai Bandar Lampung, 2025).

Dalam konteks tersebut, penerapan kriptografi menjadi solusi penting untuk melindungi data pada kondisi data at rest, data in transit, dan data in use. Salah satu algoritma yang banyak digunakan adalah Advanced Encryption Standard (AES) dengan panjang kunci 256-bit (AES-256), yang dikenal memiliki tingkat keamanan tinggi serta direkomendasikan oleh berbagai standar internasional. Implementasi AES-256 dalam sistem berbasis web

umumnya dikombinasikan dengan pengelolaan kunci yang aman, penggunaan protokol TLS, serta kontrol akses berlapis untuk meminimalkan risiko kebocoran data (Smid, 2021).

Ancaman keamanan siber yang terus meningkat turut memperkuat kebutuhan akan sistem perlindungan dokumen digital. Berbagai laporan menunjukkan adanya peningkatan insiden kebocoran data yang berdampak pada kerugian finansial dan reputasi organisasi (Tactics, 2024). Hal ini menjadi semakin relevan bagi Direktorat Jenderal Bea dan Cukai (DJBC), yang setiap tahunnya memproses ribuan dokumen ekspor-impor berbasis web. Oleh karena itu, diperlukan mekanisme keamanan tambahan berupa fitur enkripsi dan dekripsi dokumen agar hanya pihak berwenang yang dapat mengakses informasi tersebut.

Sejumlah penelitian sebelumnya menunjukkan bahwa penerapan AES dalam sistem berbasis web mampu meningkatkan keamanan dokumen digital. Penelitian oleh (Indriyawati et al., 2021) membuktikan bahwa kombinasi AES dan digital signature dapat meningkatkan keamanan dan atribusi dokumen, sedangkan (Indrayani et al., 2025) menunjukkan bahwa AES-256 efektif dalam menjaga integritas file meskipun terdapat sedikit penambahan ukuran akibat padding. Namun, sebagian penelitian masih berfokus pada aspek penyimpanan atau enkripsi dasar, tanpa menekankan pada keamanan proses ekspor dokumen dalam sistem berbasis web (Dio Rachma Putra & Mochamad Sidqon, 2024).

Selain itu, beberapa studi juga mengungkapkan bahwa kelemahan sistem keamanan sering terletak pada manajemen kunci dan kontrol akses. Penelitian oleh (Hayat Arka Putri et al., 2025) menunjukkan bahwa meskipun data berhasil dienkripsi, pengaturan hak akses belum optimal. Sementara itu, (Jordan et al., 2022) menyoroti bahwa fitur kontrol manipulasi dokumen setelah diekspor masih belum menjadi fokus utama.

Berdasarkan kondisi tersebut, terdapat celah penelitian dalam pengembangan sistem keamanan ekspor dokumen berbasis web yang mengintegrasikan enkripsi AES-256, manajemen kunci yang aman, serta kontrol distribusi dokumen secara terpusat. Penelitian ini menawarkan pendekatan yang lebih komprehensif dengan menggabungkan seluruh aspek tersebut dalam satu sistem terpadu.

Oleh karena itu, penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan ekspor-impor dokumen berbasis web dengan menggunakan algoritma

AES-256. Sistem ini diharapkan mampu menjamin kerahasiaan, integritas, dan keaslian dokumen selama proses ekspor dan distribusi, serta dapat diintegrasikan ke dalam sistem Bea Cukai.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak (software engineering) dengan tujuan merancang dan mengembangkan sistem keamanan dokumen digital ekspor-impor berbasis web yang menerapkan algoritma kriptografi AES-256. Jenis penelitian yang digunakan adalah penelitian terapan (applied research), karena berfokus pada penyelesaian masalah nyata terkait keamanan dokumen digital pada lingkungan sistem informasi, khususnya pada proses penyimpanan dan distribusi dokumen ekspor-impor.

Rancangan penelitian dilakukan secara sistematis dengan mengacu pada model pengembangan perangkat lunak Waterfall. Model ini dipilih karena memiliki tahapan yang terstruktur dan berurutan, sehingga memudahkan dalam proses pengembangan sistem yang membutuhkan perencanaan matang, terutama dalam implementasi aspek keamanan data. Tahapan dalam metode Waterfall yang diterapkan meliputi analisis kebutuhan, perancangan sistem, implementasi, serta pengujian sistem.

Pada tahap analisis kebutuhan, dilakukan identifikasi terhadap kebutuhan sistem baik dari sisi fungsional maupun non-fungsional. Proses ini melibatkan studi literatur terkait keamanan informasi, kriptografi, serta analisis terhadap kebutuhan pengamanan dokumen ekspor-impor. Selain itu, dilakukan pengumpulan data melalui observasi dan studi dokumentasi terhadap proses pengelolaan dokumen digital, khususnya yang berpotensi mengalami kebocoran atau akses tidak sah. Hasil dari tahap ini berupa spesifikasi kebutuhan sistem yang akan menjadi dasar dalam proses perancangan.

Tahap selanjutnya adalah perancangan sistem (system design), yang bertujuan untuk menggambarkan arsitektur dan alur kerja sistem secara menyeluruh. Perancangan dilakukan menggunakan beberapa alat bantu pemodelan seperti use case diagram, flowchart, activity diagram, dan class diagram. Pada tahap ini juga dirancang struktur basis data yang digunakan untuk menyimpan informasi dokumen, log aktivitas, serta data pendukung lainnya. Selain

itu, dirancang pula mekanisme enkripsi dan dekripsi dokumen menggunakan algoritma AES-256, termasuk proses pengelolaan kunci enkripsi.

Tahap implementasi sistem dilakukan dengan menerjemahkan hasil perancangan ke dalam bentuk aplikasi berbasis web. Sistem dikembangkan menggunakan bahasa pemrograman PHP pada sisi backend, serta HTML, CSS, dan JavaScript pada sisi frontend. Pengelolaan data dilakukan menggunakan database MySQL, sementara lingkungan pengembangan memanfaatkan web server Apache melalui XAMPP. Pada tahap ini, fitur utama yang dikembangkan meliputi proses unggah dokumen, enkripsi dokumen sebelum penyimpanan, dekripsi dokumen saat diakses, serta fitur ekspor file yang telah diamankan.

Selanjutnya, dilakukan tahap pengujian sistem untuk memastikan bahwa sistem yang dibangun dapat berjalan sesuai dengan kebutuhan yang telah ditetapkan. Pengujian difokuskan pada aspek utama, yaitu: (1) pengujian fungsionalitas sistem untuk memastikan setiap fitur berjalan dengan baik, (2) pengujian kinerja proses enkripsi dan dekripsi untuk mengetahui waktu yang dibutuhkan dalam pengolahan dokumen, serta Selain itu, dilakukan validasi terhadap hasil dekripsi untuk memastikan integritas data tetap terjaga dan tidak mengalami perubahan dari file asli.

Subjek dalam penelitian ini adalah sistem keamanan dokumen digital yang dirancang untuk menangani file ekspor-impor dengan format umum seperti PDF dan DOCX. Sistem ini tidak hanya berfungsi sebagai media penyimpanan, tetapi juga sebagai mekanisme proteksi data melalui penerapan kriptografi. Dengan pendekatan ini, diharapkan sistem mampu memberikan perlindungan terhadap kerahasiaan, integritas, dan keamanan dokumen digital dalam lingkungan berbasis web.

Secara keseluruhan, metode penelitian yang digunakan mengintegrasikan pendekatan rekayasa sistem dengan implementasi teknik kriptografi modern, sehingga menghasilkan solusi yang tidak hanya bersifat konseptual tetapi juga aplikatif dalam meningkatkan keamanan dokumen digital.

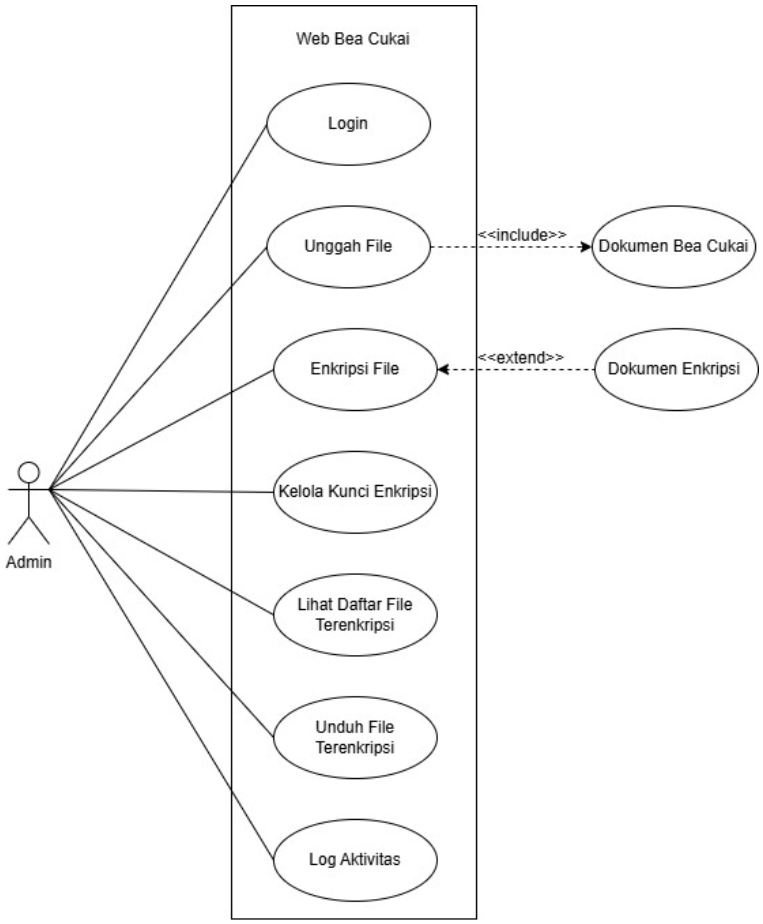
HASIL DAN PEMBAHASAN

Perancangan Sistem (System Design)

Pada segmen ini dikerjakan perancangan arsitektur sistem, Flowchart, use case diagram, Actifity Diagram, perancangan antarmuka pengguna (UI atau UX), serta implementasi algoritma AES-256 untuk mengamankan dokumen digital.

1. Use Case Diagram Admin

Use Case Diagram menggambarkan interaksi admin dengan fungsi utama sistem, meliputi unggah, enkripsi, penyimpanan, dan akses dokumen melalui aplikasi mobile. Proses ini menggunakan AES-256 untuk menjaga kerahasiaan data..



Gambar 1. Use Case Diagram Admin

Penjelasan: “

a. Aktor: Pengendalian seluruh mekanisme sistem berada pada satu pengguna khusus, ialah admin, yang bertanggung jawab atas pengaturan akses dan pengelolaan file dengan perlindungan enkripsi.
b. Use Case Utama dalam Sistem, Use case yang berada di dalam batas sistem “Web Bea Cukai” meliputi:
    - Login: Pengoperasian fitur lanjutan dikunci oleh prosedur pengenalan pengguna yang memastikan bahwa hanya admin resmi yang dapat mengakses sistem.
    - Unggah File: Admin dapat mengunggah file dokumen ke dalam sistem. Use case ini memiliki relasi (include) dengan use case Dokumen Bea Cukai, yang menandakan bahwa setiap pengunggahan file harus melibatkan spesifikasi dokumen yang ditentukan.
    - Enkripsi File: Setelah file diunggah, admin dapat melakukan proses enkripsi untuk menjaga kerahasiaan dokumen. Proses ini memiliki hubungan (extend) dengan use case Dokumen Enkripsi, yang berarti fitur tambahan dapat terjadi jika kondisi tertentu terpenuhi (misalnya pengaturan metode enkripsi tambahan).
    - Kelola Kunci Enkripsi: Admin dapat mengelola kunci enkripsi yang dipakai dalam proses pengamanan dokumen, seperti membuat, memperbarui, atau menghapus kunci.
    - Lihat Daftar File Terenkripsi: Admin dapat menampilkan daftar seluruh file yang sudah terenkripsi di dalam sistem.
    - Unduh File Terenkripsi: Admin dapat mengunduh kembali file yang telah diproses dan disimpan dalam bentuk terenkripsi.
    - Log Aktivitas: Fasilitas ini memungkinkan admin melihat riwayat aktivitas sistem, termasuk aktivitas unggah, enkripsi, maupun unduhan. Fitur ini sangat penting untuk kebutuhan audit dan keamanan.

- Include (Unggah File: Dokumen Bea Cukai) Menandakan bahwa setiap proses unggah file harus melibatkan dokumen dari Bea Cukai sebagai bagian dari prosedur standar.
- Extend (Enkripsi File: Dokumen Enkripsi) Menandakan bahwa proses enkripsi dapat diperluas dengan fungsi tambahan terkait dokumen enkripsi jika diperlukan."

c. Batas Sistem

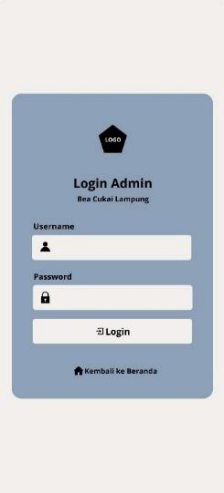
Seluruh use case berada dalam kotak bertajuk Web Bea Cukai, yang menggambarkan fungsionalitas yang berada di dalam ruang lingkup sistem yang dikembangkan.

2. Rancangan Antar Muka(Interface) Program

Tampilan web Bea cukai yang sudah ada untuk di kembangkan lagi di tambah fitur enkripsi dan dekripsi dokumen.

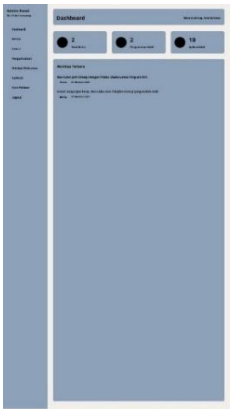
Gambar 2. Tampilan web Bea Cukai

Tampilan login admin web Bea cukai.



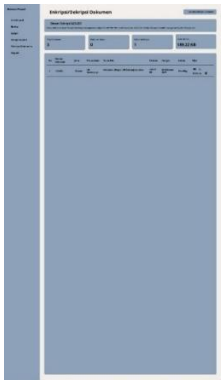
Gambar 3. Tampilan Login Admin web Bea Cukai

Tambahan untuk fitur enkripsi dan dekripsi di halaman dashboard admin.



Gambar 4. Halaman Dashboard Admin

Tampilan dari halaman Enkripsi dan dekripsi dokumen dari halaman Admin.

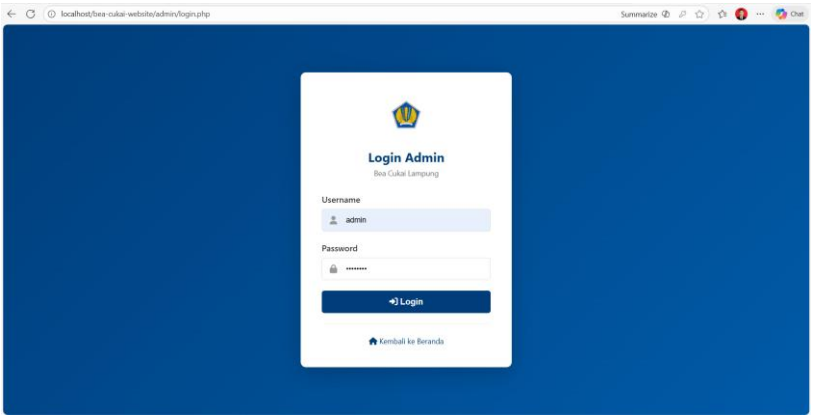


Gambar 5. Tampilan Halaman Enkripsi/Dekripsi Dokumen di Halaman Admin

Tampilan Admin

1. Halaman Login Admin

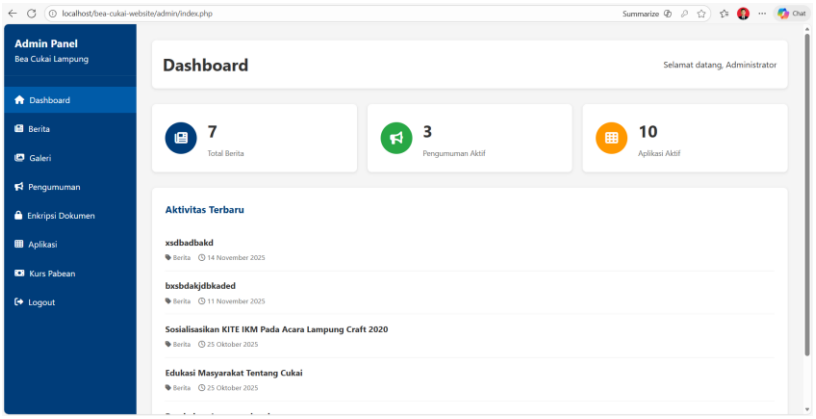
   Halaman Login Admin merupakan pintu masuk sistem yang digunakan untuk memastikan hanya pengguna berwenang yang dapat mengakses fitur pengelolaan dokumen.



Gambar 6. Halaman Login

2. Halaman Dashboard

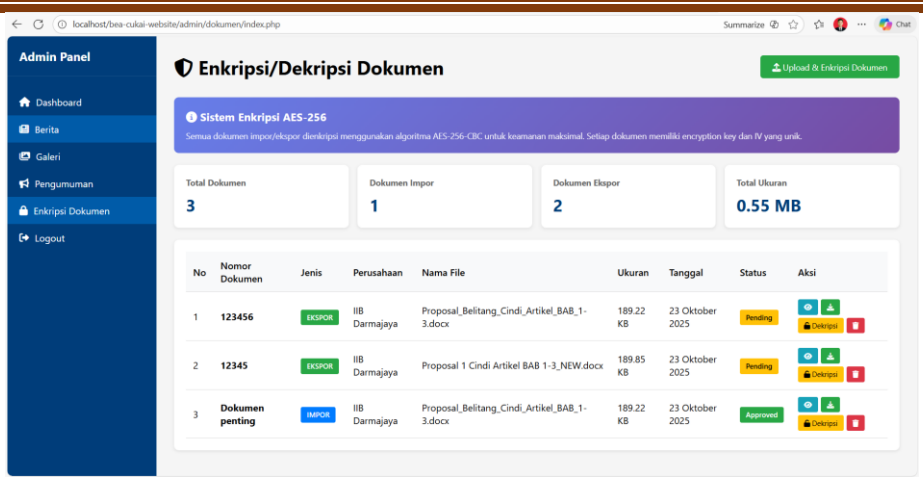
   Halaman Dashboard merupakan tampilan utama setelah login yang berfungsi sebagai pusat kontrol admin dalam mengelola keamanan dokumen dan aktivitas sistem.



Gambar 7. Halaman Dashboard

3. Halaman Enkripsi Dekripsi Dokumen

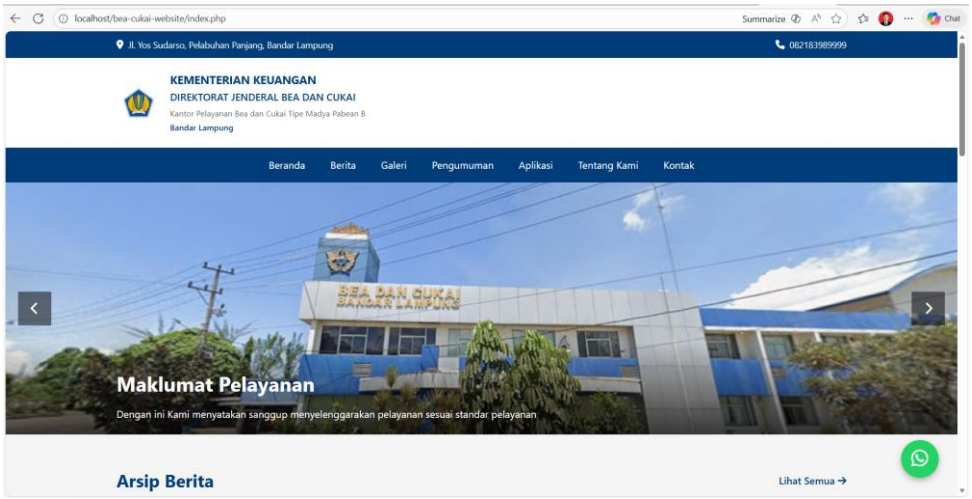
   Halaman Enkripsi dan Dekripsi merupakan fitur inti yang memungkinkan admin mengamankan dokumen menggunakan algoritma AES-256.



Gambar 8. Halaman Enkripsi Dekripsi Dokumen

Tampilan Homepage

Halaman Beranda yakni halaman utama yang pertama kali ditampilkan kepada pengguna setelah masuk ke web mobile. Halaman ini berguna sebagai pusat informasi umum dan navigasi awal bagi pengguna non-admin, seperti eksportir atau importir, yang memerlukan akses cepat terhadap informasi penting tanpa harus masuk ke fungsi-fungsi khusus admin.



Gambar 9. Halaman Beranda

Pengujian Fungsi Sistem

1. Pengujian Waktu Enkripsi dan Dekripsi

Pengujian waktu dikerjakan dengan mengenkripsi dan mendekripsi file dengan ukuran yang berbeda mulai dari 1 MB hingga 10 MB. Tujuan pengujian ini ialah mengetahui seberapa cepat algoritma AES-256 memproses data merujuk pada besarnya ukuran file. Tabel pengujian waktu enkripsi dan dekripsi ditunjukkan berikut ini:

Tabel 1. Waktu Enkripsi dan Dekripsi File

No	Ukuran File	Waktu Enkripsi(ms)	Waktu Dekripsi(ms)
1	1 MB	2.41 ms	3.16 ms
2	2 MB	7.43 ms	2.45 ms
3	3 MB	13.67 ms	2.23 ms
4	4 MB	10.99 ms	4.01 ms
5	5 MB	12.42 ms	3.04 ms
6	6 MB	26.02 ms	5.04 ms
7	7 MB	19.60 ms	8.88 ms
8	8 MB	29.89 ms	7.05 ms
9	9 MB	27.50 ms	5.29 ms
10	10 MB	36.35 ms	9.19 ms

Analisis:

a. Waktu enkripsi meningkat seiring bertambahnya ukuran file, sesuai karakteristik algoritma blok AES-256.
b. Waktu dekripsi cenderung lebih kecil dibandingkan enkripsi.
c. Tidak ditemukan error atau kegagalan proses pada setiap ukuran file.

2. Pengujian Validasi AES-256 File Asli dan File Setelah Dekripsi

Pengujian validasi AES-256 dilakukan untuk memastikan proses enkripsi dan dekripsi tidak mengubah isi dokumen. Pengujian ini berfokus pada integritas data dengan membandingkan nilai hash antara file asli dan hasil dekripsi. Hasil menunjukkan bahwa kedua nilai identik, sehingga membuktikan data tetap utuh tanpa perubahan. Algoritma AES-256 akan menghasilkan nilai yang berbeda total apabila terjadi perubahan sekecil apa pun pada konten file. Didapatkan hasil pengujian :

Tabel 2. Validasi AES-256 File Asli dan File Setelah Dekripsi

No	Ukuran File	AES-256(file asli)	AES-256(file setelah dekripsi)	Validasi Kesesuaian
1	1 MB	881A52E5C33DB29FFD8213A1E7399F387CAEC37A1CCD9D44D867AB1C8AF4D5E0	881A52E5C33DB29FFD8213A1E7399F387CAEC37A1CCD9D44D867AB1C8AF4D5E0	Sesuai
2	2 MB	73A9A95DAD992C005AF968BFECAA618CE83BF6D8453256304F8134639DE516B4	73A9A95DAD992C005AF968BFECAA618CE83BF6D8453256304F8134639DE516B4	Sesuai
3	3 MB	AFCB9C9EFB6960B4CC73365FC6E9B201B1DD23787423E3EC46C01D15A6733C48	AFCB9C9EFB6960B4CC73365FC6E9B201B1DD23787423E3EC46C01D15A6733C48	Sesuai
4	4 MB	89BB3130293DA57DA7450E0BC5F89AABC127D9A5FA04B24174BDB914A4FBE593	89BB3130293DA57DA7450E0BC5F89AABC127D9A5FA04B24174BDB914A4FBE593	Sesuai
5	5 MB	030154C5F026128350360E56362316C29E1A43AC874684867BE6B5B4E76B3C95	030154C5F026128350360E56362316C29E1A43AC874684867BE6B5B4E76B3C95	Sesuai
6	6 MB	90F9E045A7AB1ED3A71BCFD267B98DAAD96184392B7C6D1EE9306840535E6770	90F9E045A7AB1ED3A71BCFD267B98DAAD961843 92B7C6D1EE9306840535E6770	Sesuai
7	7 MB	962FEA51ABF936CF60E5A7A5C14442568BB52A5C2A4AC9E41B243A2F1402FBB4	962FEA51ABF936CF60E5A7A5C14442568BB52A5C2A4AC9E41B243A2F1402FBB4	Sesuai
8	8 MB	BFB34BF0CF02CD28B311716F0935E1BEE037C221A68A6D3991E11D33F56492B7	BFB34BF0CF02CD28B311716F0935E1BEE037C221A68A6D3991E11D33F56492B7	Sesuai
9	9 MB	A82BFC4FED163E4BAB20E3A81587BDDEF096E2A947DBE6E3979E1EA9A69725AD	A82BFC4FED163E4BAB20E3A81587BDDEF096E2A947DBE6E3979E1EA9A69725AD	Sesuai
10	10 MB	1AF3E69E0C23CD2B9FA6A1D39071A4E794E5F68536D3A93076DEE240F57D45A9	1AF3E69E0C23CD2B9FA6A1D39071A4E794E5F68536D3A93076DEE240F57D45A9	Sesuai

Analisis:

a. Seluruh nilai AES-256 file asli dan hasil dekripsi identik.

b. Ini membuktikan tidak ada perubahan bit atau kerusakan data selama proses enkripsi-dekripsi.

c. Integritas data terjamin dan algoritma AES-256 bekerja sesuai standar keamanan.

3. Kesimpulan Pengujian Enkripsi dan Dekripsi

Merujuk pada seluruh rangkaian pengujian, dapat disimpulkan bahwa:

a. Sistem berhasil melakukan enkripsi dan dekripsi file dengan waktu pemrosesan yang sesuai dengan ukuran file.
b. Nilai AES-256 file asli dan file hasil dekripsi identik, membuktikan integritas file terjaga.
c. Seluruh fungsi utama sistem-enkripsi, dekripsi, validasi ukuran, dan validasi integritas berjalan berhasil 100%.

KESIMPULAN DAN REKOMENDASI

Merujuk pada hasil penelitian, perancangan, implementasi, dan pengujian terhadap Sistem Keamanan Dokumen Digital Ekspor-Impor Berbasis Mobile Menggunakan Enkripsi AES-256, Dari keseluruhan pembahasan dan temuan yang dikaji, dapat ditarik beberapa pokok kesimpulan:

1. Sistem keamanan dokumen digital ekspor-impor berbasis mobile berhasil dirancang dan diimplementasikan dengan fitur unggah, enkripsi, penyimpanan, dekripsi, dan pengunduhan yang terintegrasi, sehingga mampu melindungi dokumen penting dari akses tidak sah.
2. Penerapan algoritma AES-256 terbukti efektif dalam menjaga kerahasiaan dan integritas dokumen, karena file hanya dapat diakses dengan kunci yang benar dan dapat dikembalikan tanpa perubahan.
3. Proses enkripsi dan dekripsi berjalan stabil dan efisien berdasarkan hasil pengujian, tanpa error atau kerusakan data.
4. Sistem memberikan lapisan keamanan tambahan melalui mekanisme autentikasi dan pengelolaan kunci, sehingga meminimalkan risiko kebocoran data.

5. Penelitian ini berkontribusi sebagai solusi keamanan dokumen digital yang dapat diterapkan pada sistem kepabeanan untuk melindungi dokumen ekspor-impor.

REFERENSI

Arianty, K. P. (2025). Analysis of Information Security Management System Implementation at BSN. Jurnal Informatika: Jurnal Pengembangan IT, 10(1), 119–129. https://doi.org/10.30591/jpit.v10i1.8211

Dio Rachma Putra, & Mochamad Sidqon. (2024). Rancang Bangun Sistem Informasi E-Arsip Berbasis Website Untuk Pengamanan Dokumen Menggunakan Metode Advance Encryption Standard (Aes) Dkpp Kota Surabaya. Jurnal Rekayasa Sistem Informasi Dan Teknologi, 2(1), 445–454. https://doi.org/10.59407/jrsit.v2i1.972

Guy-Cedric, T. B. I., & R., S. (2018). A Comparative Study on AES 128 BIT AND AES 256 BIT. International Journal of Scientific Research in Computer Science and Engineering, 6(4), 30–33. https://doi.org/10.26438/ijsrcse/v6i4.3033

Hayat Arka Putri, Z., Arye Yustraini, Y., Ariansyah, R., Choirun Nisa, N., Dyar Wahyuni, E., & Brastama Putra, A. (2025). Pengamanan Data Akademik Berbasis Web dengan Enkripsi AES-256 (Studi Kasus pada Pendataan Digital SMA XYZ). Jnatia, 3(3), 2025.

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format. Digital Transformation Technology, 4(2), 1245–1251. https://doi.org/10.47709/digitech.v4i2.5457

Indriyawati, H., Winarti, T., & Vydia, V. (2021). Web-based document certification system with advanced encryption standard digital signature. Indonesian Journal of Electrical Engineering and Computer Science, 22(1), 516–521. https://doi.org/10.11591/ijeecs.v22.i1.pp516-521

Irwanto, D. (2024). File Encryption and Decryption Using Algorithm Aes-128 Bit Based Website. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4(2), 670–677. https://doi.org/10.57152/malcom.v4i2.1305

Jordan, Y., Anwar, E. L., Habibi, R., & Riza, N. (2022). Untuk Mengamankan File Dokumen. 16(2).

Maria, M. (2024). Usable Privacy and Security Features in Smartwatches. June. https://trepo.tuni.fi/bitstream/handle/10024/158852/MakelaMaria.pdf

NIST. (2001). FIPS 197 Advanced encryption standard. Federal Information Processing Standards Publication Advanced, 91–126.

Paar, C., & Pelzl, J. (2009). Chapter 4 – The Advanced Encryption Standard (AES). Understanding Cryptography.

Rainer, R. K., Prince, B., Sánchez-Rodríguez, C., Ebrahimi, S., & Splettstoesser, I. (2023). Introduction to Information Systems. John Wiley & Sons Canada, Limited.

Sharma, S., Verma, Y., & Nadda, A. (2019). Information Security Cyber Security Challenges. International Journal of Scientific Research in Computer Science and Engineering, 7(1), 10–15. https://doi.org/10.26438/ijsrcse/v7i1.1015

Smid, M. E. (2021). Development of the advanced encryption standard. Journal of Research of the National Institute of Standards and Technology, 126(126024), 1–18. https://doi.org/10.6028/JRES.126.024

Spyridon Samonas, & David Coss. (2017). The CIA strikes back: Redefining confidentiality, integrity, and availability in security. Journal of Information System Security, 10(3), 21–45.

Stallings, W. (2020). Cryptography and Network Security Chapter 11 Fifth Edition. Network Security, 2–13.

Sychev, Y. (2023). Fundamentals of information security. Fundamentals of Information Security. https://doi.org/10.12737/1932260

Tactics, C. C. (2024). Data Leakage 2024 + : Current Cyberthreat Tactics and Beyond .