Implementasi Algoritma AES-256 Berbasis Web untuk Pengamanan Dokumen Digital di CV. Karya Eksklusif Nusantara

Ainun Naqiyah[1*], Lilis Nur Hayati[2], Amaliah Faradibah[3]

[1,3] *Teknik Informatika, Universitas Muslim Indonesia, Jl. Urip Sumoharjo KM.05, Makassar, Indonesia*
E-mail: 13020220028@student.umi.ac.id, amaliah.faradibah@umi.ac.id

[2]*Sistem Informasi, Universitas Muslim Indonesia, Jl. Urip Sumoharjo KM.05, Makassar, Indonesia*
E-mail: lilis.nurhayati.@umi.aci.id
*Corresponding Author

***Abstrak*— Di era digital, keamanan dokumen perusahaan telah menjadi tantangan besar akibat meningkatnya risiko kebocoran data dan serangan siber. CV. Karya Eksklusif Nusantara, sebuah perusahaan yang menyediakan barang dan jasa, masih menyimpan dokumen penting dalam format digital seperti .pdf, .docx, dan .xlsx tanpa sistem perlindungan khusus, sehingga rentan terhadap akses ilegal atau kerusakan data. Penelitian ini bertujuan untuk mengimplementasikan algoritma AES-256 mode CBC pada sistem berbasis web untuk mengenkripsi dan mendekripsi dokumen digital, serta menguji kinerjanya berdasarkan ukuran *file* yang berbeda. Penelitian ini menggunakan metode Waterfall yang mencakup tahapan pengumpulan data melalui wawancara dan studi pustaka, analisis kebutuhan sistem, perancangan menggunakan UML, implementasi dengan framework Laravel, serta pengujian black-box. Hasil penelitian berupa aplikasi berbasis web yang mampu melakukan enkripsi dan dekripsi dokumen digital secara aman. Pengujian kinerja menunjukkan bahwa operasi enkripsi dan dekripsi sangat cepat, dengan rata-rata waktu enkripsi 0,2924 detik dan waktu dekripsi 0,3309 detik, sementara pengujian fungsional memastikan bahwa semua fungsi bekerja sesuai kebutuhan.**

***Kata Kunci* — AES-256; Mode CBC; Enkripsi Dokumen; Sistem Berbasis Web; Keamanan Data.**

***Abstract*— In the digital era, corporate document security has become a major challenge due to the increasing risk of data breaches and cyberattacks. CV. Karya Eksklusif Nusantara, a company that provides goods and services, still stores important documents in digital formats such as .pdf, .docx, and .xlsx without a special protection system, making them vulnerable to illegal access or data corruption. This study aims to implement the AES-256 algorithm in CBC mode on a web-based system to encrypt and decrypt digital documents, as well as to test its performance based on different file sizes. This research uses the Waterfall method, which includes stages of data collection through interviews and literature review, system requirement analysis, design using UML, implementation with the Laravel framework, and black-box testing. The result of the study is a web-based application capable of securely encrypting and decrypting digital documents. Performance testing shows that the encryption and decryption operations are very fast, with an average encryption time of 0.2924 seconds and a decryption time of 0.3309 seconds, while functional testing ensures that all functions work according to requirements.**

***Key words* — AES-256; CBC Mode; Document Encryption; Web-Based System; Data Security.**

I. PENDAHULUAN

Kemajuan teknologi informasi telah mengubah cara bisnis menangani dan menyimpan data di era digital saat ini. Untuk meningkatkan produktivitas dan aksesibilitas, dokumen seperti laporan keuangan, kontrak bisnis, dan informasi pelanggan semakin sering disimpan dalam format digital. Namun, kemajuan ini juga menghadirkan tantangan baru, terutama dalam hal keamanan data. Informasi sensitif dapat dengan mudah diakses oleh pihak yang tidak berwenang jika tidak ada sistem keamanan yang memadai, yang dapat mengakibatkan kerugian finansial dan merusak reputasi perusahaan [1], [2]. Oleh karena itu, seiring meningkatnya serangan siber di Indonesia, memahami dan menerapkan langkah-langkah keamanan data, terutama enkripsi, menjadi lebih penting dari sebelumnya [3]. Digitalisasi yang pesat juga meningkatkan volume data yang harus dilindungi dan dikelola oleh perusahaan, sehingga upaya menjaga kerahasiaan dan integritas informasi menjadi semakin kompleks [4].

https://doi.org/10.35760/ik.2025.v30i3.60

Berdasarkan data beberapa tahun terakhir, Indonesia mengalami sejumlah insiden kebocoran data yang cukup serius. Kelompok *Brain Cipher* melancarkan serangan *ransomware* terhadap Pusat Data Nasional (PDN) pada Juni 2024, mengganggu sistem publik seperti layanan imigrasi dan bandara, serta menuntut tebusan sebesar delapan juta dolar Amerika Serikat [5]. Berbagai penelitian menunjukkan bahwa lemahnya perlindungan data dan penerapan hukum serta sistem keamanan informasi yang kurang memadai terus menjadi penyebab utama meningkatnya jumlah pelanggaran data pribadi, termasuk yang terjadi di organisasi pemerintah, semakin menguatkan keadaan ini [6]. Menurut Badan Siber dan Sandi Negara (BSSN), terdapat lebih dari 330 kasus serangan siber pada tahun 2024 yang menargetkan sektor publik maupun swasta [7]. Fakta-fakta ini menunjukkan bahwa risiko terhadap keamanan digital merupakan masalah serius yang membutuhkan perhatian khusus dari berbagai pemangku kepentingan, termasuk perusahaan swasta.

CV. Karya Eksklusif Nusantara, sebuah perusahaan yang bergerak di bidang penyediaan barang dan jasa, saat ini menyimpan dokumen-dokumen penting seperti *file* dengan format .pdf, .docx, dan .xlsx di komputer tanpa pengamanan tambahan. Kondisi ini berisiko menyebabkan kehilangan data akibat kerusakan perangkat, serangan virus, atau akses ilegal, karena belum adanya sistem enkripsi yang melindungi data perusahaan dari ancaman siber [8]. Selain itu, kurangnya pengelolaan arsip digital yang efektif dapat meningkatkan kerentanannya terhadap kehilangan atau kerusakan data penting perusahaan [9].

Salah satu solusi untuk meningkatkan keamanan data adalah dengan menerapkan algoritma enkripsi yang kuat [10]. Karena keamanannya yang tinggi, *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit (AES-256) adalah teknik enkripsi simetris yang populer. Dengan menggunakan kunci 256-bit, teknik ini menghasilkan sejumlah besar kombinasi, sehingga serangan siber menjadi sulit dilakukan dengan teknologi saat ini [11]. Penggunaan mode *Cipher Block Chaining* (CBC) pada AES-256 juga memberikan tingkat keamanan yang lebih baik karena setiap blok data dienkripsi setelah dilakukan operasi XOR dengan blok *ciphertext* sebelumnya serta penggunaan *Initialization Vector* (IV) yang berbeda-beda pada setiap proses enkripsi [12]. Mode CBC dalam AES-256 adalah mode yang dipilih untuk melindungi data penting dalam bisnis dan aplikasi berbasis web karena memberikan perlindungan yang lebih besar terhadap serangan dibandingkan mode lain seperti mode ECB (*Electronic Codebook*) [13], [14].

Beberapa penelitian sebelumnya telah menerapkan algoritma AES dalam sistem pengamanan dokumen digital. Sebagian penelitian masih berfokus pada penggunaan AES-128 CBC, misalnya pada pengamanan dokumen PDF dalam sistem berbasis desktop, dengan hasil yang menunjukkan bahwa sistem mampu menjaga kerahasiaan dan integritas data dengan waktu enkripsi dan dekripsi yang relatif cepat untuk *file* berukuran sedang [15]. Penelitian lain menerapkan AES-256 CBC pada dokumen teks (.txt) dalam aplikasi desktop dan menunjukkan bahwa algoritma tersebut efektif dalam melindungi kerahasiaan data, khususnya untuk *file* berukuran kecil hingga menengah [16]. Namun demikian, penelitian yang mengkaji penerapan AES-256 CBC pada sistem berbasis web untuk pengamanan dokumen perusahaan masih terbatas. Selain itu, kajian yang secara khusus menganalisis kinerja enkripsi dan dekripsi berdasarkan variasi ukuran *file* dalam lingkungan sistem berbasis web juga masih jarang dilakukan.

Keterbatasan penelitian-penelitian sebelumnya menunjukkan adanya peluang menciptakan solusi enkripsi berbasis web yang lebih sesuai dengan kebutuhan bisnis. Untuk meningkatkan keamanan dokumen digital, penelitian ini bertujuan untuk mengimplementasikan algoritma AES-256 dalam mode CBC pada sistem berbasis web yang diimplementasikan pada lingkungan server lokal (*localhost*/intranet perusahaan) dan melakukan pengujian kinerja berdasarkan variasi ukuran *file*, agar hasilnya dapat memberikan manfaat bagi pengamanan dokumen digital.

Sistem berbasis web dipilih karena kemudahan akses serta kemudahan penggunaan, di mana sistem dapat diakses melalui *browser* tanpa perlu melakukan instalasi tambahan pada setiap perangkat pengguna [17]. Selain itu, sistem berbasis web memudahkan pemeliharaan dan pengelolaan sistem secara terpusat, sehingga lebih sesuai untuk diterapkan pada lingkungan perusahaan dibandingkan aplikasi berbasis *desktop*.

Berdasarkan hal tersebut, penelitian ini bertujuan untuk mengimplementasikan algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC) pada sistem pengamanan dokumen digital berbasis web serta mengevaluasi kinerja proses enkripsi dan dekripsi berdasarkan variasi ukuran *file*. Sistem yang dikembangkan diharapkan mampu meningkatkan keamanan dokumen digital perusahaan sekaligus

memberikan gambaran mengenai performa algoritma AES-256 CBC dalam mengamankan berbagai format dokumen digital pada lingkungan berbasis web.

II. METODE PENELITIAN

Penelitian ini menggunakan metode *Waterfall*, yang terdiri dari beberapa tahap yang dilakukan secara berurutan mulai dari pengumpulan data hingga pengujian sistem [18], [19]. Setiap tahapan dalam penelitian ini bergantung pada hasil yang diperoleh pada tahap sebelumnya, sehingga alur penelitian ini bersifat linier dan sistematis. Langkah-langkah yang digunakan dalam penelitian ini Adalah sebagai berikut:

Pengumpulan Data

Tahap pertama dalam penelitian ini adalah pengumpulan data, yang dilakukan melalui dua pendekatan utama.

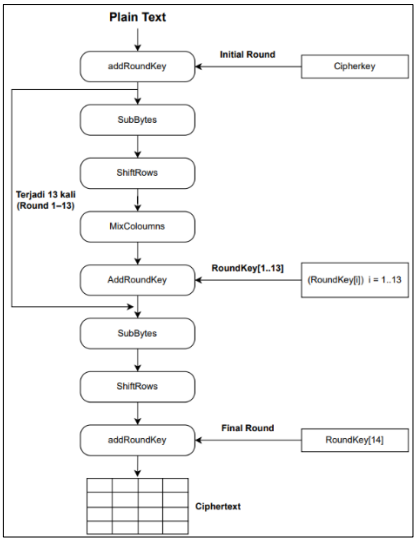
1. Wawancara

Wawancara dilakukan dengan pemilik CV. Karya Eksklusif Nusantara untuk mengetahui jenis dokumen penting yang digunakan oleh perusahaan, serta memahami tingkat kebutuhan mereka terhadap sistem keamanan data. Wawancara ini juga bertujuan untuk menggali informasi mengenai cara perusahaan selama ini mengelola dokumen digital dan tantangan yang mereka hadapi terkait perlindungan data.

2. Studi Literatur dan Analisis Algoritma

Penelitian ini dilengkapi dengan studi literatur terhadap referensi yang relevan mengenai penerapan AES-256 dan mode CBC dalam keamanan dokumen digital. Studi literatur ini digunakan untuk menetapkan metode enkripsi yang akan diimplementasikan pada sistem, meliputi pemilihan algoritma, mode operasi, serta parameter yang digunakan agar proses enkripsi dan dekripsi berjalan aman dan konsisten.

Berdasarkan hasil studi literatur dan kebutuhan sistem, sistem menggunakan AES-256 sebagai algoritma enkripsi dengan panjang kunci 256-bit dan pemrosesan data per blok 128-bit. Proses AES secara umum mencakup ekspansi kunci serta transformasi berulang, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey, pada setiap blok data [20]. Alur tahapan enkripsi yang dijadikan acuan dalam implementasi sistem ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Enkripsi AES-256

AES-256 digunakan dalam mode CBC untuk meningkatkan keamanan hasil enkripsi. Setiap blok *plaintext* P_i dikombinasikan (XOR) dengan *ciphertext* blok sebelumnya C_{i-1} sebelum diproses dengan fungsi enkripsi E_k menggunakan kunci k, hal ini membuat *ciphertext* yang dihasilkan C_i saling bergantung antara blok dan membuat pola data lebih sulit dikenali [21]. Pada blok pertama digunakan *Initialization Vector* (IV) sebagai nilai awal C_0yang bersifat acak dan tidak dapat diprediksi,

https://doi.org/10.35760/ik.2025.v30i3.60

penggunaan IV memastikan dokumen yang sama tetap menghasilkan *ciphertext* berbeda meskipun memakai kunci yang sama [22]. Berdasarkan notasi tersebut, persamaan enkripsi dan dekripsi pada mode CBC [15] dirumuskan sebagai berikut :

$C_i = E_k\ (P_i \oplus C_{i-1}), C_0 = IV$ (1)

Sedangkan rumus matematis untuk dekripsi mode CBC adalah :

$P_i = D_k\ (C_i) \oplus C_{i-1}, C_0 = IV$ (2)

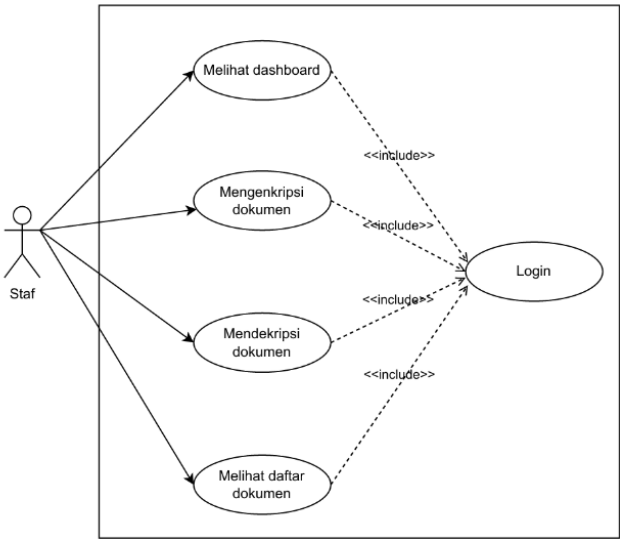
Pada persamaan (1), $P_i$merupakan blok plaintext ke-i yang dikombinasikan dengan *ciphertex*t blok sebelumnya C_{i-1}menggunakan operasi XOR sebelum diproses oleh fungsi enkripsi $E_k$dengan kunci k. Pada persamaan (2), $C_i$adalah *ciphertext* ke-i yang didekripsi menggunakan fungsi D_k dengan kunci k, kemudian dikombinasikan dengan C_{i-1}menggunakan operasi XOR untuk memperoleh kembali plaintext P_i.

Analisis Kebutuhan

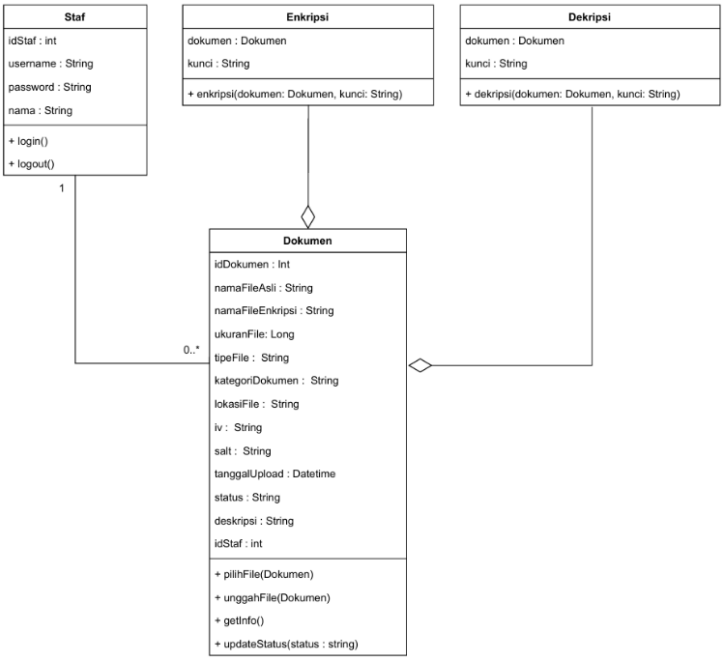
Analisis kebutuhan sistem dilakukan untuk menentukan kebutuhan fungsional dan non-fungsional yang diperlukan dalam pengembangan sistem. Informasi yang dikumpulkan dari wawancara dan studi literatur digunakan untuk menyusun analisis kebutuhan ini. Kebutuhan fungsional mencakup kemampuan sistem dalam mengunggah dokumen, mengenkripsi dan mendekripsi dokumen, serta mengelola hasil enkripsi dan dekripsi dokumen.Adapun Kebutuhan non-fungsional yang menjadi perhatian utama meliputi kemampuan sistem dalam menjaga keamanan data secara maksimal serta menjalankan proses enkripsi dan dekripsi dengan efisien, khususnya untuk dokumen berukuran besar.

Desain Sistem

Struktur dan komponen keseluruhan sistem dirancang pada tahap desain sistem [23]. Desain arsitektur sistem akan dibangun menggunakan *framework* Laravel, yang memungkinkan pengembangan aplikasi berbasis web yang aman dan efisien [18], [24], [25]. Merancang sistem dengan antarmuka pengguna yang mudah digunakan, memungkinkan pengguna untuk mengunggah dokumen, memulai proses enkripsi, dan mengunduh hasil enkripsi atau dekripsi dengan cara yang sederhana. Untuk menggambarkan interaksi pengguna dengan sistem dan struktur internal dari sistem yang sedang dikembangkan, desain sistem ini menggunakan teknik pemodelan UML (*Unified Modeling Language*) [26]. UML membantu menggambarkan komponen utama dan relasi antar bagian dalam sistem secara sistematis dan mudah dipahami.



Gambar 2. Use Case Diagram



Gambar 3. Class Diagram

Diagram *Use Case* yang menggambarkan interaksi antara pengguna (staf) dan sistem, ditampilkan pada Gambar 2. Anggota staf dapat melakukan sejumlah tugas seperti *login*, meliat *dashboard*, mengenkripsi dokumen, mendekripsi dokumen dan mengelola file. Setiap aktivitas ini menunjukkan bagaimana pengguna berinteraksi langsung dengan fitur utama sistem. Gambar 3 menampilkan *Class Diagram*, yang menunjukkan struktur kelas dalam sistem, termasuk kelas staf untuk proses autentikasi, kelas dokumen untuk menyimpan dan mengelola *file*, serta kelas enkripsi dan dekripsi untuk memproses dokumen menggunakan kunci. Diagram ini memperlihatkan bagaimana data saling berinteraksi dan diproses antar kelas dalam sistem dengan struktur yang jelas.

Implementasi

Implementasi dilakukan setelah desain sistem selesai. Sistem dibangun dengan database MySQL, framework Tailwind CSS untuk antarmuka pengguna, dan framework Laravel (PHP) untuk backend. Implementasi dimulai dengan pembuatan komponen utama, termasuk mengunggah dokumen, enkripsi dan dekripsi dokumen menggunakan AES-256 dalam mode CBC, dan melihat daftar dokumen yang sudah diproses. Untuk memastikan bahwa setiap modul beroperasi dengan benar dan aman sesuai dengan desain, masing-masing diuji secara bertahap. Implementasi juga mengutamakan efisiensi dalam pengolahan data agar sistem dapat menangani dokumen dengan berbagai ukuran tanpa mengorbankan kinerja.

Pengujian Sistem

Pengujian sistem dilakukan setelah implementasi selesai. Untuk memastikan bahwa setiap fungsi bekerja sesuai dengan kebutuhan, pengujian sistem dilakukan menggunakan pendekatan *black-box* testing, yang berfokus pada fungsi sistem berdasarkan *input* dan *output* tanpa mempertimbangkan proses internal atau kode program [27]. Tiga aspek utama yang menjadi fokus pengujian yaitu, pertama aspek fungsionalitas bahwa proses unggah, enkripsi, dan dekripsi berjalan sesuai dengan *input* pengguna (Staf). Kedua aspek keamanan dengan memverifikasi bahwa *file* yang dienkripsi tidak dapat dibuka tanpa kunci dekripsi yang tepat. Dan yang ketiga aspek kinerja yaitu mengukur waktu pemrosesan enkripsi dan dekripsi berdasarkan format *file* seperti .pdf, .xlsx, dan .docx serta berbagai ukuran *file*.

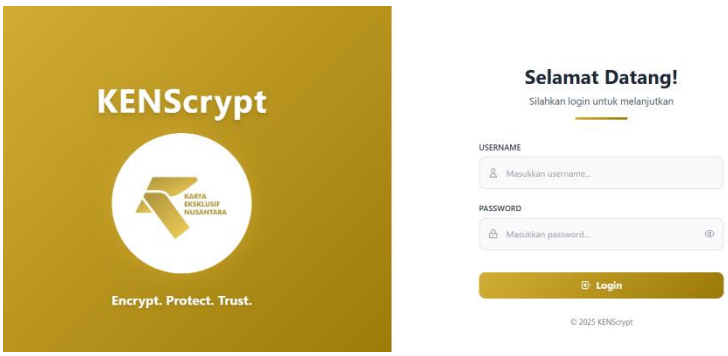
https://doi.org/10.35760/ik.2025.v30i3.60

III. HASIL DAN PEMBAHASAN

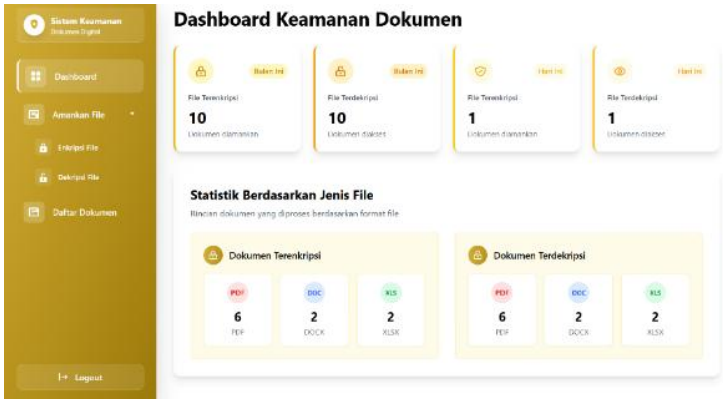
Hasil Implementasi Sistem

Hasil dari penelitian ini adalah sebuah aplikasi web yang menggunakan algoritma AES-256 dalam mode CBC untuk mengenkripsi dan mendekripsi dokumen digital. *Framework* Laravel digunakan dalam pengembangan sistem ini, yang memiliki antarmuka sederhana dan mudah digunakan oleh karyawan perusahaan. Hasil antarmuka sistem ditampilkan dalam bagian ini seperti halaman *login*, *dashboard*, *form* enkripsi, *form* dekripsi, hasil enkripsi dan dekripsi serta daftar dokumen.

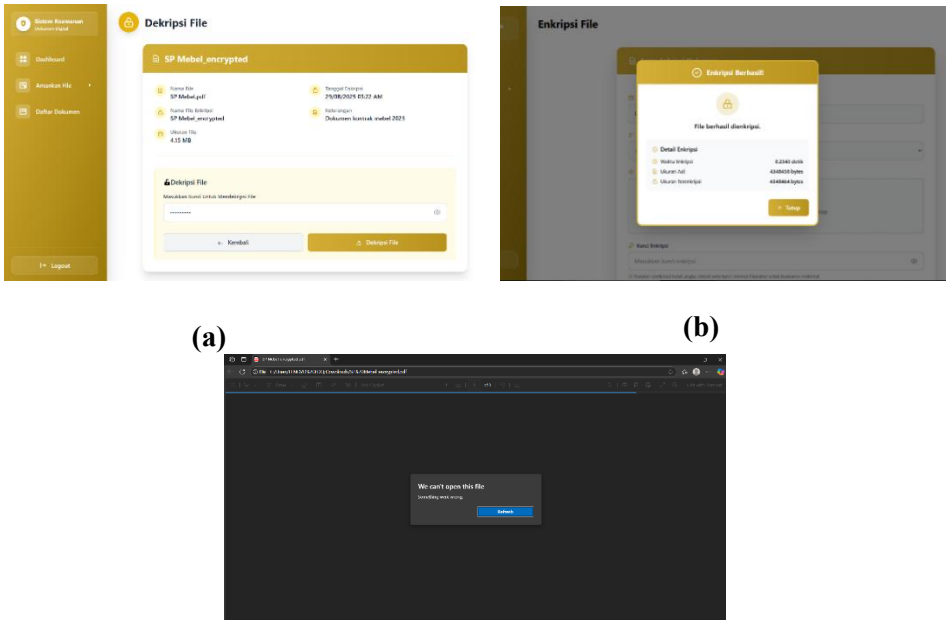
1. Halaman *Login*, adalah halaman awal yang muncul di sistem. Seperti yang ditunjukkan pada Gambar 4, pengguna harus melakukan autentikasi dengan memasukkan nama pengguna dan kata sandi sebelum dapat mengakses fungsi utama sistem. Untuk memastikan hanya pengguna yang berwenang yang dapat mengenkripsi atau mendekripsi dokumen, halaman ini berfungsi sebagai lapisan keamanan awal.
2. *Dashboard* Sistem, setelah berhasil melakukan *login* pengguna diarahkan menuju halaman *dashboard* seperti ditunjukkan pada Gambar 5. *Dashboard* berfungsi sebagai pusat informasi yang menampilkan ringkasan aktivitas dalam sistem, seperti jumlah dokumen yang telah dienkripsi maupun didekripsi, serta jumlah dokumen yang telah diproses atau yang tersimpan berdasarkan jenis *file*.
3. Enkripsi *File*. Pada Gambar 6(a) *form* enkripsi ditampilkan untuk melakukan proses enkripsi terhadap dokumen digital perusahaan dengan beberapa bagian penting di dalamnya, seperti pilihan kategori dokumen, proses memilih dan mengunggah *file*, mengisi kunci enkripsi, serta menambahkan keterangan *file*. Pada Gambar 6(b) Setelah pengguna menekan tombol Enkripsi *File*, sistem akan menampilkan notifikasi bahwa *file* berhasil dienkripsi serta menampilkan detail hasil enkripsi, seperti waktu enkripsi, ukuran *file* asli, dan ukuran *file* setelah terenkripsi. Selanjutnya pada Gambar 6(c). mencoba membuka *file* hasil enkripsi tanpa melalui proses dekripsi, isi *file* akan ditampilkan dalam kondisi tidak dapat terbaca. Hal ini menunjukkan bahwa sistem telah berhasil mengamankan dokumen melalui algoritma AES-256 CBC sehingga *file* tidak dapat diakses tanpa kunci dekripsi yang sesuai.



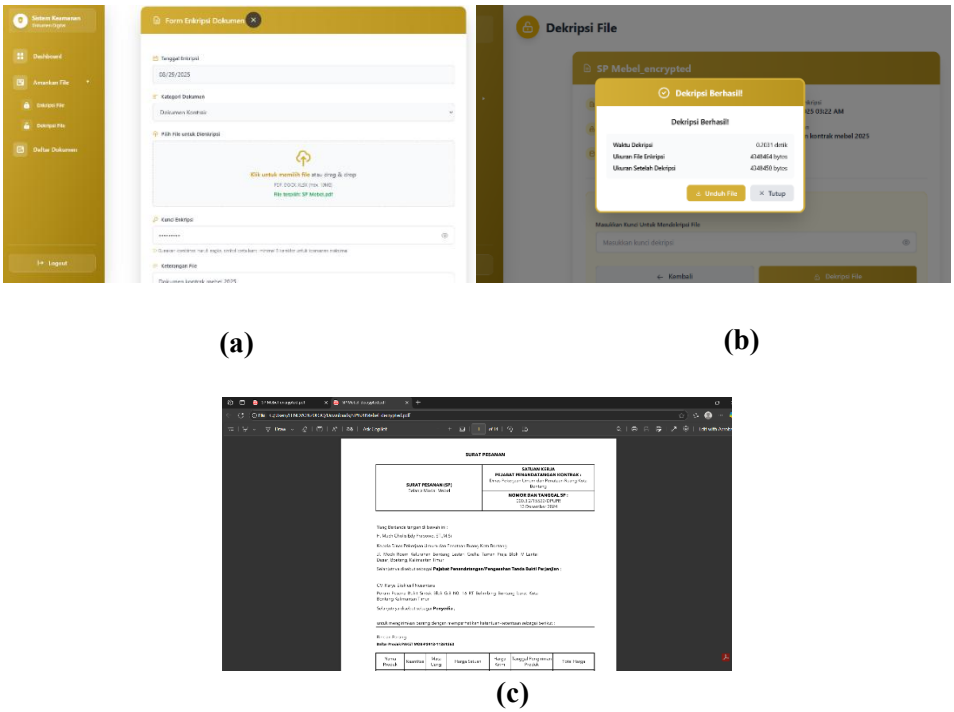
Gambar 4. Halaman Login



Gambar 5. Halaman Dashboard



Gambar 6. (a) *Form* Enkripsi, (b) Notifikasi Enkripsi, (c) Hasil Enkripsi



Gambar 7. (a) Tampilan Dekripsi, (b) Notifikasi Dekripsi, (c) Hasil Dekripsi

4. Dekripsi *File*, setelah dokumen berhasil dienkripsi, pengguna dapat melakukan dekripsi untuk mengembalikan dokumen ke bentuk semula. Pada Gambar 7(a) setelah pengguna memilih dokumen yang ingin didekripsi, dan memasukkan kunci enkripsi yang sesuai. Pada Gambar 7(b) sistem akan menampilkan notifikasi bahwa proses dekripsi berhasil. Selanjutnya pada Gambar 7(c), dokumen dapat diunduh kembali dalam bentuk aslinya dan dapat dibaca seperti semula. Dengan demikian, fitur dekripsi ini memastikan bahwa hanya pihak yang memiliki kunci yang tepat yang dapat mengakses dokumen, sehingga kerahasiaan dan keamanan tetap terjaga.

https://doi.org/10.35760/ik.2025.v30i3.60

5. Daftar Dokumen, halaman ini digunakan untuk menampilkan seluruh dokumen yang telah diproses, baik itu dokumen yang telah terenkripsi maupun terdekripsi. Pada Gambar 8 menampilkan setiap *file* yang simpan dalam bentuk tabel yang berisi kategori dokumen, nama *file*, tanggal upload, status dokumen,

Pengujian Sistem

Metode pengujian *black-box* digunakan dalam penelitian ini untuk memastikan bahwa fitur utama sistem berfungsi sesuai dengan kebutuhan pengguna. Pengujian dilakukan dengan memberikan *input* tertentu pada sistem dan kemudian membandingkan hasilnya dengan *output* yang diharapkan. Selain memastikan ukuran *file* dan penggunaan kunci dekripsi yang salah, pengujian juga difokuskan pada fungsi login, enkripsi, dan dekripsi dokumen. Hasil pengujian fungsional ditampilkan pada Tabel 1. Hasil Pengujian Black-Box.

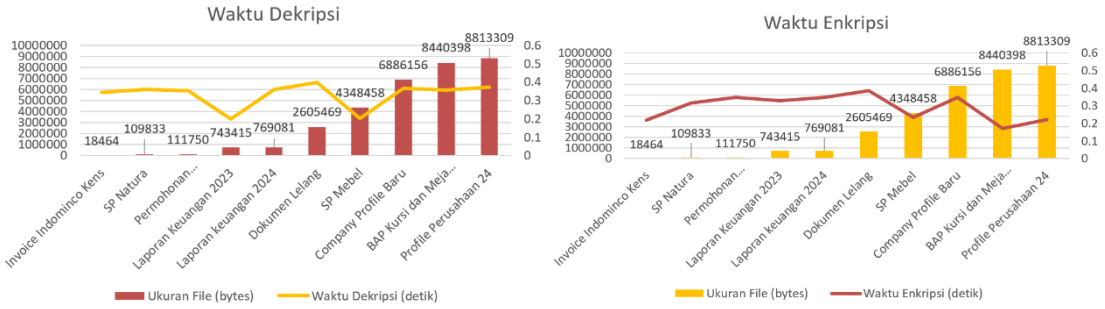
Gambar 8. Halaman Daftar Dokumen

Tabel 1. Hasil Pengujian Black-Box.

No	Skenario Uji	Input	Output yang Diharapkan	Hasil	Dekripsi
1	Login berhasil	Username dan password valid	Sistem mengarahkan ke halaman dashboard	Berhasil	Menguji autentikasi awal agar hanya pengguna yang berwenang dapat mengakses sistem
2	Login gagal	Username/password salah	Sistem gagal melakukan autentikasi dan menampilkan pesan error "Login gagal, username atau password salah"	Berhasil	Memastikan keamanan login dengan menolak akses yang tidak sah
3	Enkripsi dokumen	Pilihan *file* dan kunci enkripsi	Sistem menghasilkan *file* terenkripsi, yang tidak dapat dibuka atau dibaca seperti semula	Berhasil	Memastikan proses enkripsi berjalan sesuai algoritma AES-256 CBC
4	Enkripsi dokumen yang lebih dari batas ukuran maximum (10 MB)	Dokumen dengan ukuran 15 MB	Tampil pesan error "Ukuran *file* tidak boleh lebih dari 10120 KB."	Berhasil	Memastikan sistem membatasi ukuran *file* yang dapat dienkripsi sesuai dengan ukuran maksimum *file*
5	Dekripsi dokumen	*File* terenkripsi dan kunci enkripsi yang sesuai	Dokumen kembali ke bentuk asli dan dapat dibaca	Berhasil	Memastikan dekripsi hanya berhasil jika menggunakan kunci yang benar
6	Dekripsi dengan kunci salah	*File* terenkripsi dan kunci tidak sesuai	Tampil pesan error "Dekripsi gagal, kunci yang dimasukkan salah"	Berhasil	Menguji keamanan sistem agar data tidak bisa diakses tanpa kunci yang benar

Tabel 2. Hasil Pengujian Kinerja Sistem

No	Nama *File*	Format *File*	Ukuran *File* (bytes)	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	Invoice Indominco Kens	.xlsx	18464	0.2197	0.344
2	SP Natura	.docx	109833	0.3172	0.3586
3	Permohonan Pembayaran Penyedia	.docx	111750	0.3485	0.3533
4	Laporan Keuangan 2023	.xlsx	743415	0.3297	0.1984
5	Laporan keuangan 2024	.pdf	769081	0.3468	0.3595
6	Dokumen Lelang	.pdf	2605469	0.3847	0.3995
7	SP Mebel	.pdf	4348458	0.2343	0.2031
8	Company Pro*file* Baru	.pdf	6886156	0.3492	0.3663
9	BAP Kursi dan Meja Rapat	.pdf	8440398	0.1719	0.356
10	Pro*file* Perusahaan 24	.pdf	8813309	0.2226	0.3712



(a) **(b)**

Gambar 9. Grafik Hasil Pengujian Kinerja Sistem (a) Waktu Enkripsi, (b) Waktu Dekripsi

Menurut hasil pada Tabel 1, setiap skenario pengujian memberikan hasil yang sesuai dan konsisten dengan output yang diharapkan. Ini menunjukkan bahwa sistem telah mampu melakukan tugas *login*, enkripsi, dan dekripsi dengan benar. Ini juga memungkinkan sistem untuk mengatasi kesalahan seperti *login* gagal, ukuran *file* yang lebih besar, atau penggunaan kunci dekripsi yang salah. Oleh karena itu, dapat disimpulkan bahwa bahwa sistem telah memenuhi segi fungsionalitas utama serta kebutuhan pengguna.

Setelah pengujian fungsional, sistem juga diuji dari segi kinerja (*performance testing*). Tujuan pengujian ini adalah untuk mengukur kecepatan proses enkripsi dan dekripsi dokumen dengan format seperti.pdf,.docx, dan.xlsx serta dengan ukuran dokumen yang berbeda-beda. Dengan cara ini, tingkat kemampuan sistem untuk menangani dokumen dari berbagai jenis dan ukuran dapat diukur. Hasil pengujian kinerja ditampilkan pada Tabel 2. hasil pengujian kinerja sistem.

Untuk memperjelas hasil pengujian, analisis selanjutnya ditampilkan dalam bentuk grafik yang menggambarkan perbandingan waktu enkripsi dan dekripsi terhadap ukuran *file*, seperti yang ditampilkan pada Gambar 9(a) dan Gambar 9(b).

Berdasarkan hasil pengujian kinerja sistem yang di tunjukkan pada Tabel 2, didapatkan rata-rata waktu yang dibutuhkan untuk proses enkripsi sebesar 0,2924 detik dan proses dekripsi sebesar 0,3309 detik, yang menunjukkan bahwa proses enkripsi dan dekripsi berlangsung dalam waktu kurang dari satu detik. Selanjutnya, Gambar 9(a) dan Gambar 9(b) memperlihatkan bahwa ukuran *file* tidak selalu berbanding lurus dengan waktu proses. Dokumen berukuran lebih besar pada beberapa kasus dapat diproses lebih cepat dibandingkan dokumen berukuran lebih kecil. Hal ini menandakan bahwa waktu enkripsi dan dekripsi tidak hanya dipengaruhi oleh ukuran *file*, tetapi juga oleh kompleksitas isi dokumen, seperti tingkat kompresi internal dan jumlah elemen di dalam *file*.

https://doi.org/10.35760/ik.2025.v30i3.60

Sistem berfungsi dengan baik, sesuai dengan hasil pengujian. Terdapat beberapa keterbatasan yang ditemukan, antara lain sistem belum diuji untuk penggunaan secara bersamaan oleh banyak pengguna dan hanya mendukung pemrosesan satu *file* dalam satu waktu. Selain itu, sistem belum mendukung pengelolaan *file* dengan ukuran yang sangat besar. Meskipun demikian, sistem ini telah memenuhi kebutuhan dasar pengamanan dokumen perusahaan dan memiliki potensi untuk dikembangkan lebih lanjut serta diintegrasikan dengan sistem manajemen dokumen pada CV. Karya Eksklusif Nusantara.

Keberhasilan implementasi sistem ini tidak terlepas dari penggunaan metode *Waterfall* dalam proses pengembangannya. Setiap langkah dilakukan secara berurutan dan sistematis sehingga hasil dari satu langkah membentuk fondasi yang kuat untuk langkah berikutnya. Misalnya, fase pengumpulan data memberikan dasar teoritis untuk algoritma AES-256 dan mode CBC. Analisis kebutuhan dan perancangan sistem kemudian didukung oleh fase ini. Implementasi dilakukan sesuai dengan rancangan, dan tahap pengujian digunakan untuk memvalidasi secara menyeluruh kinerja dan keamanan sistem. Salah satu keunggulan utama metode *Waterfall* adalah alur kerja yang teratur, validasi yang konsisten, dan dokumentasi yang jelas untuk tiap langkah. Oleh karena itu, metode linear ini dinilai sesuai untuk membangun sistem keamanan yang membutuhkan verifikasi ketat pada setiap tahap proses agar kualitas dan keandalan sistem dapat dipertahankan sebelum melanjutkan ke tahap berikutnya.

IV. KESIMPULAN

Penelitian ini menggunakan metode Waterfall yang terbukti efektif digunakan untuk membangun sistem keamanan dokumen digital. Secara berurutan dan sistematis, setiap tahap penelitian dapat dilakukan, mulai dari pengumpulan data, analisis kebutuhan, perancangan, implementasi, dan pengujian. Metode ini memastikan bahwa sistem memiliki fondasi teori yang kuat dan dapat divalidasi di setiap tahap sebelum lanjut ke tahap berikutnya.

Hasil penelitian menunjukkan bahwa tujuan utama yaitu membangun sistem untuk enkripsi dan dekripsi dokumen digital di CV. Karya Eksklusif Nusantara berhasil dicapai dengan menerapkan algoritma AES-256 mode CBC pada sistem berbasis web. Sistem ini, yang dibuat menggunakan framework Laravel, dapat mengamankan dokumen dengan format seperti .pdf, .docx, dan .xlsx, serta memiliki tingkat keamanan yang tinggi.

Semua fitur penting seperti autentikasi, enkripsi, dan dekripsi, berjalan dengan baik dalam pengujian *Black-box Testing*. Selain itu, telah ditunjukkan bahwa sistem dapat melindungi dari akses yang tidak diinginkan dan menjamin bahwa hanya kunci yang tepat yang dapat digunakan untuk dekripsi. Dalam pengujian kinerja, proses enkripsi dan dekripsi berlangsung sangat cepat untuk berbagai ukuran *file*, dengan rata-rata waktu enkripsi 0,2924 detik dan dekripsi 0,3309 detik, atau kurang dari satu detik. Menariknya, tidak hanya ukuran *file* yang memengaruhi kecepatan pemrosesan, tetapi juga kompleksitas dalam dokumen, seperti tingkat kompresi dan jumlah elemen. Selain itu, *Initialization Vector* (IV) digunakan pada setiap sesi enkripsi untuk menjamin bahwa hasil enkripsi selalu berbeda meskipun dokumen yang sama diproses. Ini meningkatkan pertahanan terhadap serangan pemecahan sandi.

Meskipun sistem ini bekerja dengan baik, masih ada keterbatasan. Sistem belum diuji pada penggunaan bersamaan dengan banyak pengguna, hanya mendukung pemrosesan satu dokumen dalam satu proses. Untuk penelitian lebih lanjut, pengembangan dapat difokuskan pada dukungan *multi-user*, optimasi kinerja untuk *file* besar, dan pengujian keamanan yang lebih mendalam, termasuk simulasi serangan terhadap algoritma. Dengan pengembangan lebih lanjut, sistem ini memiliki potensi besar untuk diintegrasikan ke dalam sistem manajemen dokumen CV. Karya Eksklusif Nusantara.

DAFTAR PUSTAKA

[1] A. M. Alenezi, “Cloud Security Assurance: Strategies For Encryption In Digital Forensic Readiness A Preprint,” 2024. doi: https://doi.org/10.48550/arXiv.2403.04794.

[2] M. A. Al Hilmi and R. K. Yunan, “Pengujian Keamanan Fitur Upload File Pada Sistem Aplikasi Web,” *Jurnal Informatika: Jurnal pengembangan IT (JPIT)*, vol. 7, no. 1, Jan. 2022, doi: https://doi.org/10.30591/jpit.v7i1.3336.

[3] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/s23156666.
[4] S. Liu, "Digital Transformation and Data Privacy and Security: Challenges and Strategies for Enterprises," *Law and Economy*, vol. 4, no. 5, pp. 65–70, Jul. 2025, doi: 10.63593/le.2788-7049.2025.06.007.
[5] R. D. Anggaini Puspita, P. Dahlian Persadha, and Mulyadi, "Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional," *Syntax Literate*, vol. 10, no. 5, May 2025, doi: https://doi.org/10.36418/syntax-literate.v10i5.59084.
[6] Tanti Kirana Utami, Kayla Andini Putri, Salsa Octaviani Suryanto, and Fina Asriani, "Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law," *Journal Customary Law*, vol. 2, no. 2, p. 21, Feb. 2025, doi: https://doi.org/10.47134/jcl.v2i2.3742.
[7] Y. W. Ghalib *et al.*, "Analisis Perkembangan Keamanan Siber Dampak Dari Kebocoran Data Pusat Data Nasional Sementara 2 Surabaya," *JISCO(Journal of Informaton System and Computng)*, vol. 2, 2024, doi: https://doi.org/10.30631/jisco.v2i1.100.
[8] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, no. 27, p. 12, 2022, doi: 10.34010/jati.v12i2.
[9] T. Kurahmadan, "Analisa Dan Perancangan Sistem Informasi Kearsipan Berbasis Digital," *Jurnal Teknologi Informasi*, vol. 10, Dec. 2024, doi: https://doi.org/10.52643/jti.v10i2.5705.
[10] E. Sutanty, M. B. Siregar, and E. Setiyaningsih, "Implementasi Feistel Block Cipher Dalam Enkripsi File Berbentuk Teks," *Jurnal Ilmiah Informatika Komputer*, vol. 26, no. 2, pp. 136–148, 2021, doi: 10.35760/ik.2021.v26i2.4238.
[11] "Advanced Encryption Standard (AES)," May 2023. doi: 10.6028/NIST.FIPS.197-upd1.
[12] B. Schneier, *Applied cryptography : protocols, algorithms, and source code in C*. Wiley, 2015.
[13] W. Prabowo and N. Anwar, "Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC," Mar. 2025, doi: 10.37817/ikraith-informatika.v9i1.
[14] A. Ridho and Moh. A. Romli, "Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256)," *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, Nov. 2024, doi: 10.51401/jinteks.v6i4.4887.
[15] S. Manullang, Allwine, and Jakaria Sembiring, "Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining," *Antivirus : Jurnal Ilmiah Teknik Informatika*, vol. 17, no. 1, pp. 53–67, Jun. 2023, doi: 10.35457/antivirus.v17i1.2811.
[16] F. Baso and N. Anriani, "Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File," *INTEC Journal: Information Technology Education Journal*, vol. 3, no. 3, 2024, doi: https://doi.org/10.59562/intec.v3i3.5525.
[17] M. S. Affandi, R. Setiyanto, and M. Za, "Analisis Perbandingan Sistem Bengkel Berbasis Dekstop dan Web Menggunakan Metode User Acceptance Testing," *JSAI : Journal Scientific and Applied Informatics*, vol. 08, no. 2, 2025, doi: 10.36085.
[18] S. A. Syafrudin, I. Wahyuni, and Oktaviani, "Penerapan Metode Waterfall Pada Sistem Otomatisasi Website Pembelajaran Smp Kelas 9," *Jurnal Ilmiah Informatika Komputer*, vol. 28, no. 2, pp. 88–99, 2023, doi: 10.35760/ik.2023.v28i2.8030.
[19] S. Supiyandi, M. Zen, C. Rizal, and M. Eka, "Perancangan Sistem Informasi Desa Tomuan Holbung Menggunakan Metode Waterfall," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 2, p. 274, Apr. 2022, doi: 10.30865/jurikom.v9i2.3986.
[20] D. S. Purwanti, M. Fadli, M. Surono, and E. R. Susanto, "Perancangan Penerapan Algoritma Kriptografi Aes 256 Untuk Keamanan Database Aplikasi Manajemen Siswa," *STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 4, no. 2, pp. 111–119, May 2025, doi: https://doi.org/10.55123/storage.v4i2.5237.
[21] M. J. Dworkin, "Recommendation for Block Cipher Modes of Operation," Gaithersburg, MD, 2001. doi: 10.6028/NIST.SP.800-38a.

[22] B. Dos, S. Rocha, J. A. M. Xexéo, and R. H. Torres, “Artificial Intelligence Applied to the Identification of Block Ciphers under CBC Mode,” 2023. doi: 10.5120/ijca2023923114.
[23] L. N. Hayati *et al.*, “JPM (Jurnal Pemberdayaan Masyarakat) Pemberdayaan Pengrajin Kana Tojeng Melalui Pemasaran E-Commerce Produk Anyaman Serat Lontara Songko Guru Desa Bontokassi,” 2025, doi: 10.21067/jpm.v10i2.12742.
[24] G. V. Dewaji, D. R. Arifatno, S. E. Pratiwi, and Rogayah, “Penerapan Framework Laravel Pada Pembuatan Aplikasi Sewa Properti ‘Rentify’ Dengan Metode Ux System Usability Scale (SUS),” *Jurnal Ilmiah Informatika Komputer*, vol. 29, no. 2, pp. 197–211, 2024, doi: 10.35760/ik.2024.v29i2.12075.
[25] A. Khaliq, S. Batubara, M. Syaula, and Y. E. Lubis, “Perancangan Sistem Karir Berbasis Web Menggunakan Framework Laravel,” Dec. 2022. doi: 10.30645/brahmana.v4i1A.144.
[26] M. A. Syaifullah, L. N. Hayati, and L. B. Ilmawan, “Application of the First Come First Served Method in the Mobile-Application System,” *bit-Tech*, vol. 8, no. 2, pp. 2653–2662, Dec. 2025, doi: 10.32877/bt.v8i2.3331.
[27] F. Kawakib Kartono *et al.*, “Pengujian Black Box Testing Pada Sistem Website Osha Snack: Pendekatan Teknik Boundary Value Analysis,” Dec. 2024. doi: https://doi.org/10.53863/kst.v6i02.1407.