SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 September 2025 – Jakarta, Indonesia
Volume 4, Nomor 2, September 2025 - ISSN 2962-8628 (*online*)

IMPLEMENTASI AES-128 UNTUK PENGAMANAN FILE TRANSAKSI PENJUALAN PADA CV. DNN BERBASIS WEB

Fransiskus Aldi Jebadu[1], Sejati Waluyo[2*]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1]2111500829@student.budiluhur.ac.id, [2*]Sejati.waluyo@budiluhur.ac.id
(* : corresponding author)

Abstrak – Evolusi teknologi informasi digital yang pesat menuntut perusahaan untuk memiliki sistem perlindungan data yang andal, khususnya pada sektor distribusi dan penjualan. CV. Duta Nusa Nipa menyimpan data transaksi penjualan yang bersifat strategis dan harus dijaga kerahasiaannya untuk mencegah penyalahgunaan oleh pihak tidak berwenang. Kebocoran informasi dapat mengakibatkan kerugian finansial, turunnya kepercayaan pelanggan, dan gangguan pada persaingan bisnis. Penelitian ini mengusulkan pembangunan sistem pengamanan *file* transaksi penjualan berbasis *web* dengan menerapkan algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit. Pengembangan sistem dilakukan menggunakan model *Waterfall*, yang mencakup tahap analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Aplikasi yang dibangun mampu melakukan proses enkripsi dan dekripsi pada tipe berkas *.txt, .pdf*, dan *.xlsx* dengan ukuran maksimal 8 MB, menggunakan kunci rahasia yang diinput pengguna. Proses enkripsi dilakukan secara blok untuk memastikan data tidak dapat diakses tanpa kunci yang benar. Hasil pengujian fungsional menunjukkan seluruh fitur, termasuk *login*, enkripsi, dan dekripsi, berjalan sesuai spesifikasi, sementara pengujian kinerja memperlihatkan waktu proses yang efisien, bahkan untuk *file* berukuran besar. File hasil dekripsi identik dengan *file* asli, sehingga integritas data tetap terjaga. Temuan ini membuktikan bahwa sistem yang dikembangkan efektif dalam meningkatkan keamanan *file* transaksi penjualan dan dapat diimplementasikan pada lingkungan perusahaan untuk meminimalkan risiko kebocoran data. Penelitian ini memiliki perbedaan dengan karya sebelumnya karena secara khusus menitikberatkan pada pengujian keberhasilan dekripsi *file* transaksi dengan ukuran yang lebih besar. Hasil penelitian menunjukkan bahwa tidak terdapat kegagalan pada proses dekripsi, dan *file* yang dipulihkan sepenuhnya sama dengan versi aslinya. Fokus ini jarang dibahas pada penelitian terdahulu, sehingga menambah kontribusi baru dalam bidang keamanan data

Kata Kunci: Keamanan Data, Kriptografi, Enkripsi, Dekripsi, AES-128, Sistem Berbasis Web, File Penjualan.

IMPLEMENTATION OF AES-128 FOR SECURING SALES TRANSACTION FILES AT CV. DNN WEB-BASED

Abstract *– The rapid evolution of digital information technology requires companies to implement reliable data protection systems, particularly in the distribution and sales sectors. CV. Duta Nusa Nipa stores strategic sales transaction data that must be kept confidential to prevent misuse by unauthorized parties. Information leakage can lead to financial losses, decreased customer trust, and disruption of business competition. This study proposes the development of a web-based sales transaction file security system by applying the Advanced Encryption Standard (AES) 128-bit cryptographic algorithm. The system was developed using the Waterfall model, covering the stages of requirement analysis, design, implementation, testing, and maintenance. The application is capable of performing encryption and decryption on .txt, .pdf, and .xlsx files up to 8 MB in size, using a secret key provided by the user. The encryption process is carried out in blocks to ensure that the data cannot be accessed without the correct key. Functional testing shows that all features, including login, encryption, and decryption, work according to specifications, while performance testing demonstrates efficient processing time even for large files. The decrypted files are identical to the original files, ensuring data integrity is preserved. These findings confirm that the developed system is effective in enhancing the security of sales transaction files and can be implemented in corporate environments to minimize the risk of data breaches. This study differs from previous works by specifically focusing on testing the success of decrypting larger transaction files. The results show that no decryption failures occurred, and the recovered files were completely identical to the originals. This focus, rarely addressed in earlier studies, provides a new contribution to the field of data security.*

Keywords*: data security, cryptography, encryption, decryption, AES-128, web-based system, sales file****.***

1. PENDAHULUAN

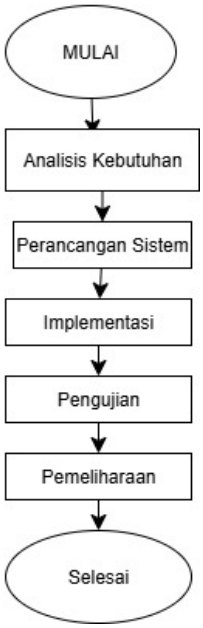
Kemajuan teknologi dan informasi di era digital menuntut adanya perlindungan data yang andal, karena informasi kini menjadi aset strategis yang memengaruhi proses bisnis dan pengambilan keputusan. Salah satu data vital bagi perusahaan adalah data penjualan yang dikelola secara berkala. Kebocoran data ini dapat dimanfaatkan pesaing untuk memperoleh keuntungan tidak wajar, memicu persaingan tidak sehat, dan menurunkan kepercayaan pelanggan. CV. Duta Nusa Nipa, yang bergerak di bidang distribusi dan penjualan produk, memiliki arsip *file* penting yang wajib dijaga kerahasiaan dan integritasnya untuk menghindari risiko penyalahgunaan informasi.

Diantara berbagai metode,terdapat pendekatan efektif untuk mengantisipasi ancaman tersebut yakni penerapan algoritma kriptografi. *Advanced Encryption Standard* (AES) dijadikan pilihan lantaran tingkat proteksinya yang unggul dan telah terbukti melindungi data sensitif pada berbagai penelitian sebelumnya. AES-128 mampu mengenkripsi berbagai format *file* seperti *Word, Excel*, dan *PDF* menjadi data yang tidak dapat dibaca tanpa kunci yang tepat, sehingga mencegah akses ilegal. Berdasarkan hal tersebut, penelitian ini bertujuan mengimplementasikan AES-128 terhadap sistem dengan dukungan web untuk mengoptimalkan proteksi arsip dan dokumen digital transaksi penjualan di CV. Duta Nusa Nipa. Penelitian sebelumnya umumnya berfokus pada pengamanan teks ataupun basis data. Sementara itu, penelitian ini secara khusus diarahkan pada perlindungan *file* transaksi penjualan dengan berbagai format *(.txt, .pdf, .xlsx*) serta ukuran hingga 8 MB. Selain itu, penelitian ini menambahkan aspek evaluasi integritas hasil dekripsi sehingga *file* yang dipulihkan benar-benar identik dengan *file* asli. Perbedaan inilah yang menjadi gap penelitian yang ingin diisi oleh studi ini.

Pemilihan algoritma AES-128 didasarkan pada kajian sejumlah penelitian yang menyatakan bahwa varian ini mampu memberikan keseimbangan optimal antara kecepatan pemrosesan dan tingkat keamanan. Dibandingkan dengan AES-192 dan AES-256 yang memiliki tingkat proteksi lebih tinggi tetapi memerlukan waktu komputasi lebih lama, AES-128 lebih sesuai untuk aplikasi berbasis web dengan kebutuhan pemrosesan *file* berukuran menengah hingga besar. AES-128 dipilih karena memberikan keseimbangan optimal antara tingkat keamanan dan efisiensi pemrosesan dibanding varian lain, sehingga cocok untuk sistem berbasis web dengan *file* ukuran sedang hingga besar.

2. METODE PENELITIAN

Gambar di atas menunjukkan tahapan pengembangan sistem menggunakan model *Waterfall* yang dimulai dari analisis kebutuhan untuk mengidentifikasi spesifikasi sistem, dilanjutkan dengan perancangan sistem mencakup desain arsitektur, *database*, dan antarmuka, kemudian tahap implementasi untuk mengembangkan aplikasi sesuai desain, tahap pengujian untuk memastikan fungsi berjalan sesuai spesifikasi, tahap pemeliharaan untuk memperbaiki atau mengoptimalkan sistem, dan diakhiri dengan tahap selesai saat sistem siap digunakan[1].



Gambar 1. Tahap Penelitian

2.1 Analisis Kebutuhan

Tahap awal tahap ini diarahkan untuk mendeteksi spesifikasi arsitektur sistem yang hendak direalisasikan, mencakup persyaratan fungsional maupun non-fungsional. Data dikumpulkan melalui observasi di CV. Duta Nusa Nipa, wawancara dengan pihak terkait, serta telaah literatur mengenai keamanan data dan penerapan algoritma AES-128[2]. Informasi yang diperoleh menjadi dasar perancangan sistem agar mampu menjawab kebutuhan pengguna dan tujuan penelitian..

2.2 Perancangan Sistem

Pada tahap perancangan, dibuat gambaran menyeluruh mengenai sistem berbasis *web* yang memanfaatkan algoritma AES-128 untuk proses enkripsi dan dekripsi[3]. Perancangan meliputi penyusunan flowchart, diagram UML (*use case, sequence*, dan *activity diagram*), rancangan database, serta desain antarmuka pengguna. Hasil dari tahap ini berfungsi sebagai acuan dalam proses implementasi[4].

2.3 Implementasi

Tahap ini merealisasikan rancangan yang telah dibuat menjadi aplikasi yang dapat dijalankan. Sistem dikembangkan menggunakan bahasa pemrograman PHP dengan basis data *MySQL*, kemudian diintegrasikan dengan algoritma AES-128 untuk menyandikan serta memulihkan data berkas bertipe *.txt, .pdf*, dan *.xlsx* dengan kapasitas maksimum 8 MB. Proses implementasi juga memperhatikan keamanan kunci enkripsi untuk memastikan data tetap terlindungi[5].

2.4 Pengujian

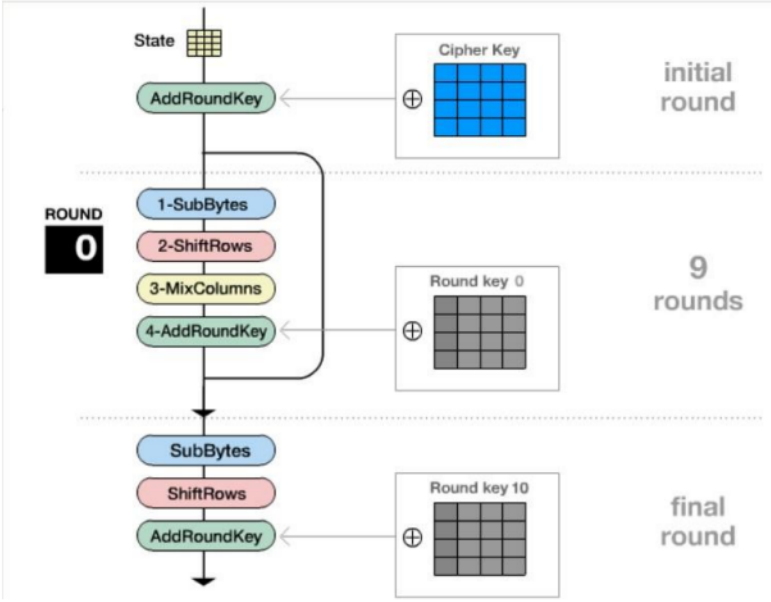
Usai tahap implementasi,dilakukan pengujian guna menjamin setiap fitur beroprasi sebagaimana direncanakan spesifikasi. Evaluasi dilakukan dengan metode *black box testing* yang berfokus pada fungsi-fungsi utama seperti *login*, unggah *file*, enkripsi, dan dekripsi. Selain itu, dilakukan pengujian kinerja untuk menilai kecepatan proses enkripsi dan dekripsi pada *file* dengan ukuran yang bervariasi[6].

2.5 Pemeliharaan

Tahap pemeliharaan dilakukan setelah sistem digunakan untuk memastikan kinerja dan keamanannya tetap optimal. Kegiatan pada tahap ini meliputi perbaikan kesalahan, penambahan fitur, serta peningkatan proses enkripsi dan dekripsi sesuai kebutuhan. Dengan pemeliharaan yang tepat, sistem diharapkan dapat beroperasi stabil dan terus menyesuaikan dengan perkembangan kebutuhan perusahaan[7].

2.6 Kriptografi AES 128

Kriptografi merupakan teknik pengamanan data dengan mengubah informasi asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*) menggunakan algoritma tertentu. Tujuannya adalah menjaga kerahasiaan, integritas, serta autentikasi data dengan demikian,hanya pemilik kunci sah yang bisa mengembalikannya ke bentuk semula (dekripsi). Dalam penelitian ini digunakan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 128-bit, yang dikenal memiliki tingkat keamanan tinggi dan efisiensi dalam pengolahan data[8].



Gambar 2. Enkripsi Dekripsi AES

Proses kerja AES terdiri dari dua tahap utama, yaitu enkripsi dan dekripsi. Pada proses enkripsi, data dibagi ke dalam blok-blok berukuran tetap, lalu diproses melalui serangkaian operasi *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey*. Jika pada proses tahap pemulihan data, langkah-langkah tersebut dibalik untuk mendapatkan kembali data asli[9].

Implementasi AES-128 pada sistem ini digunakan untuk mengamankan *file* transaksi penjualan berformat **.**txt, **.**pdf, dan **.**xlsx dengan ukuran maksimum 8 MB. Proses enkripsi dilakukan di sisi server aplikasi berbasis *web*, sementara kunci enkripsi ditentukan langsung oleh pengguna. Hal ini memastikan hanya pemilik kunci yang dapat membuka *file* terenkripsi, sehingga risiko kebocoran data dapat diminimalkan[10].

Tabel 1. Jenis Algoritma AES

Varian AES	Panjang Kunci	Ukuran Blok	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Tabel 1 menampilkan perbedaan spesifikasi tiga varian algoritma AES, yaitu AES-128, AES-192, dan AES-256, yang dibedakan berdasarkan panjang kunci, ukuran blok, serta jumlah putaran pada proses enkripsi maupun dekripsi. AES-128 menggunakan panjang kunci 4 kata (128-bit) dengan ukuran blok tetap 4 kata (128-bit) dan 10 putaran. Sementara itu, AES-192 memiliki panjang kunci 6 kata (192-bit) dengan jumlah putaran 12, dan AES-256 memanfaatkan kunci berukuran 8 kata (256-bit) melalui 14 siklus proses.

Secara prinsip, peningkatan panjang kunci dan jumlah putaran akan memperkuat tingkat keamanan algoritma, karena mempersulit upaya pembobolan melalui *brute force*. Namun, konsekuensinya adalah waktu pemrosesan yang lebih lama. Pada penelitian ini, AES-128 dipilih karena dinilai memiliki keseimbangan antara keamanan dan kecepatan pemrosesan, sehingga dapat mengamankan *file* transaksi penjualan berukuran hingga 8 MB secara efektif di sistem berbasis *web[11]*.

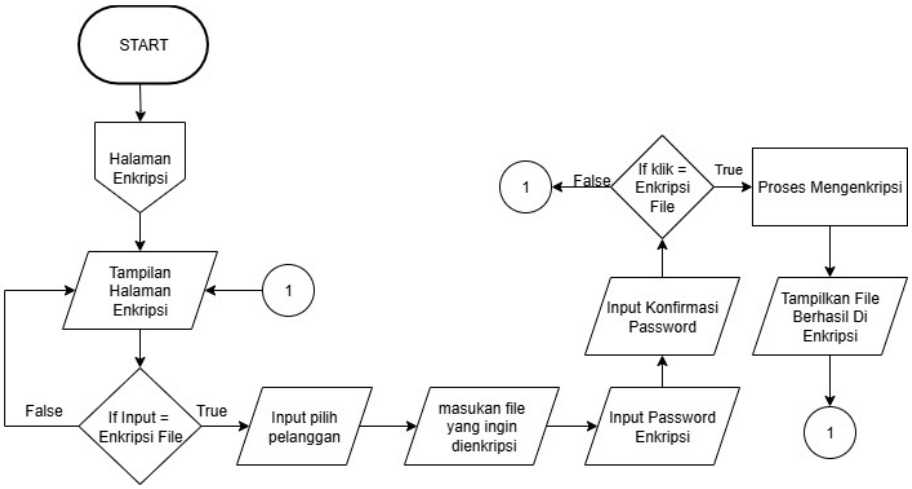
3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi sistem enkripsi dan dekripsi *file* transaksi penjualan berbasis *web* yang dikembangkan menggunakan algoritma AES-128. Hasil penelitian mencakup tampilan antarmuka sistem, hasil pengujian fungsional, serta pembahasan performa sistem dalam mengamankan data. Pengujian dilakukan untuk memastikan bahwa setiap fitur bekerja sesuai rancangan dan mampu memberikan perlindungan data yang optimal.

3.1 Flowchart

Flowchart merupakan representasi visual dari rangkaian proses yang terjadi dalam sistem. Diagram ini digunakan untuk mempermudah pemahaman alur kerja aplikasi, mulai dari interaksi pengguna hingga pemrosesan data di dalam sistem. Pada penelitian ini, *flowchart* dibuat untuk menggambarkan urutan langkah dalam aplikasi pengamanan *file* transaksi penjualan berbasis *web*, mulai dari proses login, pemilihan *file*, penentuan kunci enkripsi, hingga proses enkripsi atau dekripsi, dan berakhir pada penyimpanan atau pengunduhan *file* hasil.

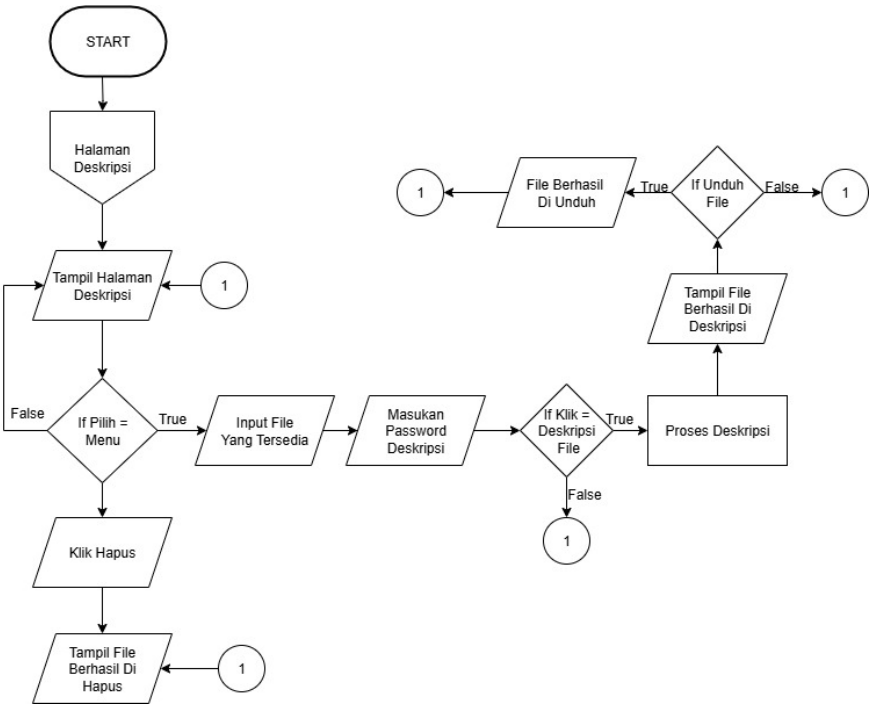
3.1.1 Flowchart Enkripsi



Gambar 3. Proses Enkripsi

Flowchart sebagai terlihat pada ilustrasi 4 menjelaskan langkah-langkah yang dilakukan sistem dalam proses enkripsi. Setelah *file* diunggah dan kunci dimasukkan, sistem membagi data menjadi blok 128-bit. Selanjutnya, data melewati 10 putaran transformasi AES-128 yang meliputi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Keluaran yang dihasilkan dari tahapan ini yakni *file* berkas tersandikan (*ciphertext*) yang disimpan di *server* serta bisa diunduh pengguna

3.1.2 Flowchart Dekrispsi



Gambar 4. Proses Dekripsi

Flowchart pada Gambar 4 memperlihatkan proses dekripsi *file*. Dimulai dengan pemilihan *file* terenkripsi dan input kunci dekripsi, sistem memeriksa kecocokan kunci. Jika valid, data dibagi menjadi blok 128-bit lalu diproses melalui tahapan kebalikan enkripsi, yaitu *Inverse ShiftRows, Inverse SubBytes, AddRoundKey*, dan *Inverse MixColumns*. Hasilnya adalah *file* asli yang identik dengan versi awal sebelum dienkripsi.

3.2 Algoritma

Bagian berikut menguraikan algoritma yang digunakan didalam konteks sistem sesuai alur pada flowchart yang telah dijelaskan terdahulu. Pemaparan algoritma diberikan dalam wujud potongan kode (kode program) dengan tujuan mempermudah dibaca serta dipahami. Penjelasan algoritma dibagi menjadi dua, yaitu proses enkripsi dan proses dekripsi, yang keduanya menggunakan metode *Advanced Encryption Standard* (AES) dengan panjang kunci 128-bit.

3.2.1 Algoritma Enkripsi

Hal berikut adalah prosedur yang digunakan dalam proses enkripsi arsip digital

```
        START
      DISPLAY "Form Enkripsi File"
      DISPLAY "Pilih Client"
      READ client
      DISPLAY "Pilih File"
      READ file

      IF client == "" OR file == "" THEN
        DISPLAY "Client dan File harus dipilih"
        KEMBALI ke form
      ELSE
        LAKUKAN proses enkripsi file
        SIMPAN file terenkripsi ke database
        DISPLAY "File berhasil dienkripsi dan disimpan"
      ENDIF
END
```

Sistem menampilkan form, membaca input client dan *file*, lalu memvalidasi. Jika input kosong → kembali ke form. Jika valid → *file* dienkripsi dengan AES-128, disimpan, dan ditampilkan pesan sukses.

3.2.2 Algoritma Dekripsi

berikut adalah algoritma untuk tahapan pemulihan berkas

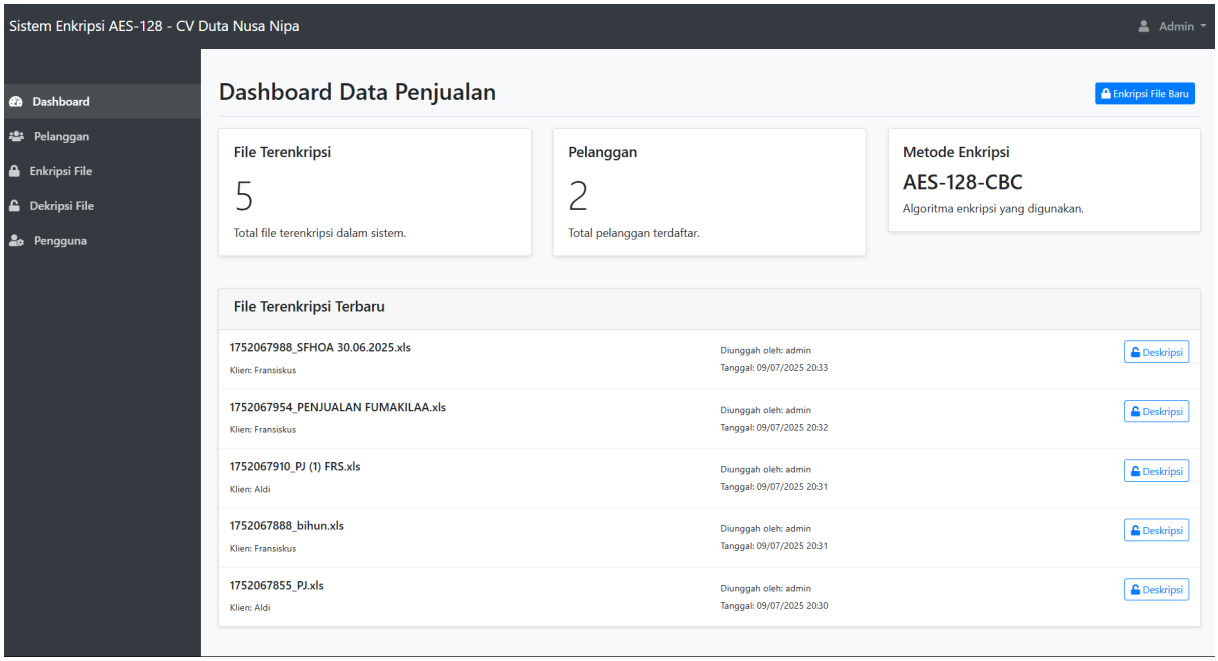
```
      START
      DISPLAY "Form Deskripsi File"
      DISPLAY "Pilih File"
      READ file

      IF file == "" THEN
        DISPLAY "File harus dipilih"
        KEMBALI ke form
      ELSE
        LAKUKAN proses dekripsi file
        TAMPILKAN hasil dekripsi
      ENDIF
END
```

Sistem menampilkan form dekripsi, membaca *file* yang dipilih, lalu memvalidasi. Jika kosong → kembali ke form. Jika valid → *file* diproses dengan AES-128 dan hasil dekripsi ditampilkan.

3.3 Tampilan Layar

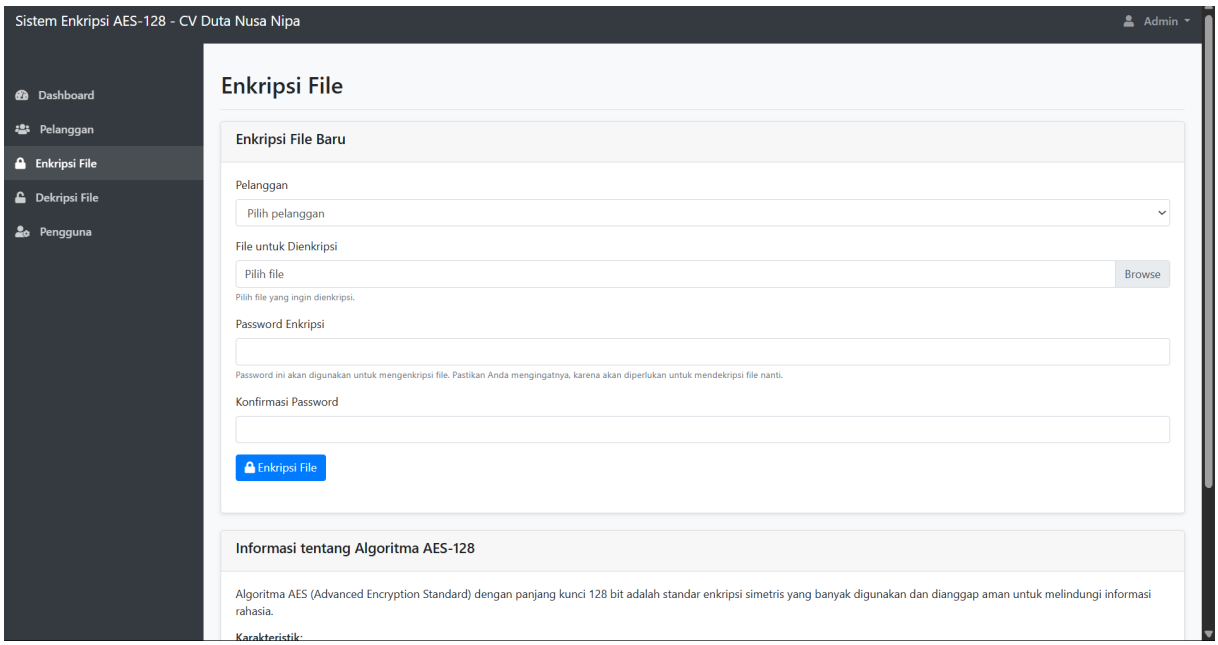
3.3.1 Menu Dashboard



Gambar 5. Menu *Dashboard*

Halaman *dashboard* berfungsi sebagai pusat navigasi sistem, menampilkan ringkasan menu utama yang dapat diakses pengguna. Dari sini, pengguna dapat memilih untuk melakukan proses enkripsi, dekripsi, atau melihat riwayat aktivitas. Desainnya dibuat sederhana agar memudahkan interaksi pengguna.

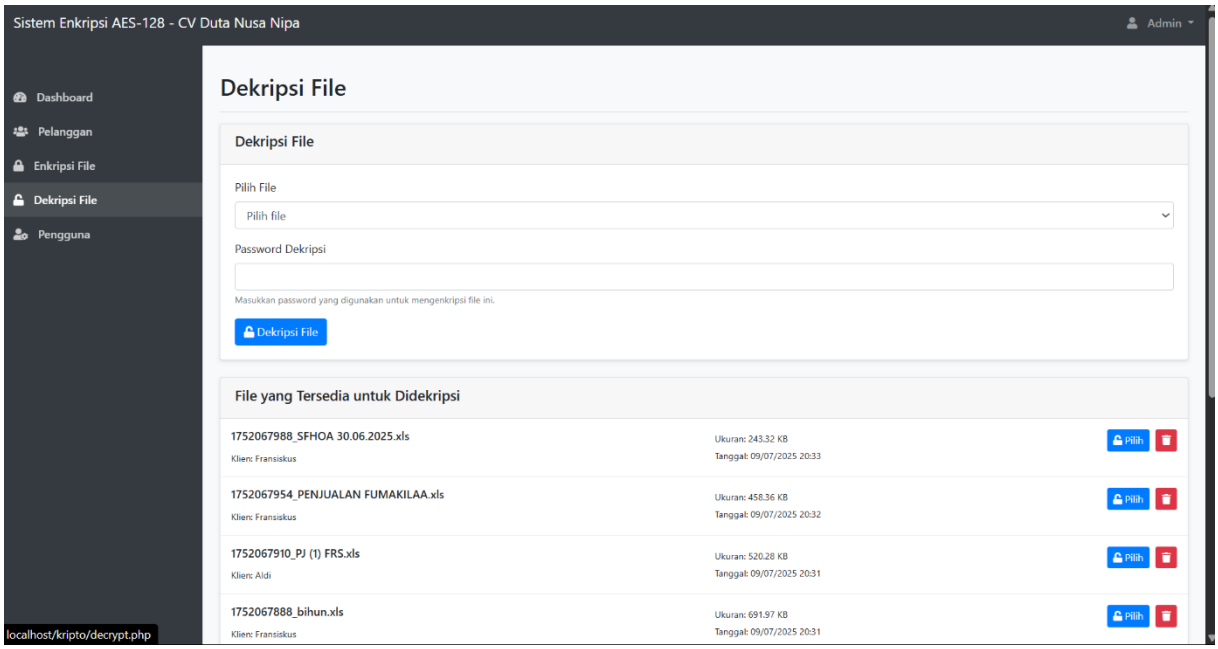
3.3.2 Menu Enkripsi



Gambar 6. Menu Enkripsi

Menu ini digunakan untuk mengamankan *file* transaksi penjualan. Pengguna mengunggah *file* berformat *.txt, .pdf,* atau *.xlsx*, lalu memasukkan kunci enkripsi. Sistem akan memproses *file* menggunakan algoritma AES-128 dan menghasilkan *file* terenkripsi yang siap diunduh.

3.3.3 Menu Dekripsi



Gambar 7. Menu Dekripsi

Menu ini digunakan untuk memulihkan *file* terenkripsi menjadi *file* asli. Pengguna mengunggah *file* hasil enkripsi dan memasukkan kunci yang sesuai. Jika kunci valid, sistem akan mengembalikan *file* ke bentuk semula tanpa perubahan isi dan format

3.4 Pengujian Program

Tabel 2. Pengujian Kinerja

No	Ukuran File	Waktu Enkripsi	Waktu Dekripsi
1	146.92 kb	98.84 ms	43.38 ms
2	1.35 mb	103.86 ms	51.65 ms
3	5.25 mb	137.41 ms	59.27 ms
4	761.65 kb	101.81 ms	49.6 ms
5	991.49 kb	89.81 ms	46.51 ms
6	743.68 kb	72.36 ms	49.49 ms
7	691.97 kb	107.73 ms	49.6 ms
8	1 mb	109.88 ms	52.67 ms
9	1.01 mb	144.63 ms	49.49 ms
10	2.14 mb	125.36 ms	55.49 ms

Pada tabel 2 Hasil pengujian memperlihatkan bahwa seluruh *file* yang dienkripsi dapat didekripsi kembali tanpa hambatan. Tidak ditemukan adanya kegagalan proses dekripsi, sehingga *file* hasil pemulihan tetap sama dengan *file* asli baik dari sisi isi maupun format. Hal ini membuktikan bahwa sistem yang dikembangkan mampu menjaga integritas data dengan baik.

Seluruh pengujian menunjukkan *file* yang didekripsi identik dengan *file* asli. Tidak ditemukan kasus kegagalan dekripsi.

3.5 Manajemen Kunci

Sistem memakai kunci yang dimasukkan langsung oleh pengguna sehingga lebih aman, namun jika kunci hilang *file* tidak bisa dipulihkan. Penelitian masih terbatas pada tiga format *file* kecil dengan AES-128. Ke depan dapat ditingkatkan dengan AES-192/256, dukungan format lebih luas, dan integrasi protokol keamanan. Antarmuka dibuat sederhana agar mudah digunakan dan tetap aman.

4. KESIMPULAN

Penelitian ini berhasil menghasilkan sistem pengamanan *file* transaksi penjualan berbasis web dengan menerapkan algoritma AES-128. Sistem mampu melakukan penyandian serta pemulihan berkas berekstensi .txt, .pdf, juga .xlsx hingga ukuran 8 MB dengan hasil dekripsi yang identik dengan *file* asli. Pengujian menunjukkan bahwa seluruh fitur berjalan sesuai perancangan dan proses enkripsi–dekripsi berlangsung efisien. Implementasi sistem ini dinilai efektif dalam meningkatkan keamanan data dan dapat diterapkan pada lingkungan perusahaan untuk melindungi informasi penting dari akses tidak sah.

DAFTAR PUSTAKA

[1] A. Abdul Wahid Sekolah Tinggi Manajemen Informatika Dan Komputer Sumedang, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi 2020." [Online]. Available: Https://Www.Researchgate.Net/Publication/346397070

[2] I. Priambudi, "Implementasi Kriptografi Dengan Metode Aes-128 Untuk Pengamanan File Berbasis Web Pada Smp Yapipa," *Skanika: Sistem Komputer Dan Teknik Informatika*, Vol. 6, No. 1, P. 22, 2023.

[3] A. H. Dartasanjaya, D. Virgian, And S. Y. Sakti, "3 Rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (Senafti) 30 Agustus 2023-Jakarta," 2023.

[4] A. J. Jehanu, "Sistem Informasi Pengelolaan Data Buku Perpustakaan Pada Politeknik Negeri Bali Berbasis Web Program Studi Diii Manajemen Informatika Jurusan Teknik Elektro Politeknik Negeri Bali 2023."

[5] D. Widyawan And I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, Vol. 4, No. 1, Pp. 15–22, Jan. 2021, Doi: 10.36080/Skanika.V4i1.2216.

[6] A. Permana And E. Jaelani, "Implementasi Algoritma Aes 128 Bit Sebagai Pengaman Teks Di Aplikasi Note Berbasis Android," *Jurnal Teknologi Dan Manajemen Informatika*, Vol. 5, No. 2, 2020, [Online]. Available: Https://Journal.Uniku.Ac.Id/Index.Php/Jejaring

[7] M. Pemeliharaan Peralatan Berbasis Web, "Asraf, Rasyidah 163," 2023.

[8] T. Auliya Ramadhani And A. Fajaryanto Cobantoro, "Jip (Jurnal Informatika Polinema) Implementasi Algoritma Advanced Encryption Standard 128 Untuk Pengamanan Database Sistem Registrasi Pasien".

[9] M. Azhari, J. Perwitosari, And F. Ali, "Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (Aes)," *Jurnal Pendidikan Sains Dan Komputer*, Vol. 2, No. 1, Pp. 2809–476, 2022, Doi: 10.47709/Jpsk.V2i1.1390.

[10] F. Ahmad Sitorus, N. Budi Nugroho, U. Fatimah Sari Sitorus Pane, P. Studi Mahasiswa, S. Triguna Dharma, And P. Studi Dosen Pembimbing, "Implementasi Algoritma Advanced Encryption Standard (Aes) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada Pt. Mitsubishi Electric Indonesia," 2020. [Online]. Available: Https://Ojs.Trigunadharma.Ac.Id/

[11] N. Benino Tampubolon, R. R. Isnanto, And E. W. Sinuraya, "Implementasi Dan Analisis Algoritma Advanced Encryption Standard (Aes) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia."