5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

PENERAPAN KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA BERBASIS *WEBSITE* PADA CAHAYA BATTERY

Muhamad Rio Fauzan[1*], Pipin Farida Ariyani[2]

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

Email: [1*]2011500317@budiluhur.ac.id, [2]pipin.faridaariyani@budiluhur.ac.id
(* : corresponding author)

Abstrak- Kemajuan teknologi dalam sistem keamanan data telah meningkat pesat, memungkinkan berbagai instansi, termasuk toko-toko, untuk melakukan pencatatan berkas penting seperti penjualan secara terorganisir dan efisien. Berkas-berkas ini, yang mengandung informasi sensitif, memerlukan perlindungan khusus agar hanya individu yang berwenang yang dapat mengaksesnya. Namun, banyak toko belum memiliki sistem pengamanan yang memadai, sehingga berpotensi menimbulkan risiko penyalahgunaan data yang dapat merugikan aspek keuangan dan reputasi bisnis. Permasalahan utama dalam konteks ini adalah kurangnya sistem khusus untuk mengamankan file, terutama file penjualan yang sangat penting bagi operasional toko. Rumusan masalahnya adalah bagaimana merancang sebuah sistem yang efektif untuk melindungi file dari akses yang tidak sah. Tujuan penelitian ini adalah merancang aplikasi web yang dapat mengamankan file dengan menggunakan teknik kriptografi, khususnya algoritma Advanced Encryption Standard (AES-128), untuk enkripsi dan dekripsi dokumen. Aplikasi ini diharapkan dapat melindungi file dalam format .doc, .docx, .pdf, .xls, dan .xlsx, dengan batas ukuran unggahan file hingga 5MB. Metode penelitian yang digunakan meliputi pengembangan aplikasi berbasis web menggunakan bahasa pemrograman PHP dan database MySQL. Algoritma AES-128 dipilih karena keandalannya dalam enkripsi simetris, yang efektif untuk menjaga kerahasiaan data. Hasil penelitian menunjukkan bahwa sistem pengamanan file yang dikembangkan berhasil mencapai tingkat keberhasilan 100% dalam proses enkripsi dan dekripsi. Sistem ini berfungsi dengan baik sesuai dengan ukuran file yang diproses. Semakin besar ukuran file, semakin lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Sebagai contoh, file berukuran 14KB memerlukan waktu 0,3 detik, sedangkan file 141KB membutuhkan sekitar 3 detik. Kontribusi dari penelitian ini adalah penyediaan solusi yang efektif untuk mengamankan data penting di toko-toko, yang tidak hanya menjaga kerahasiaan informasi tetapi juga memberikan hasil yang konsisten dan dapat diandalkan.

Kata Kunci: Kriptografi,*Advanced Encryption Standard*, Keamanan Data, Dokumen

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY FOR WEB-BASED DATA SECURITY ON CAHAYA BATTERY

Abstract- *Technological advances in data security systems have increased rapidly, allowing various institutions, including shops, to keep records of important files such as sales in an organized and efficient manner. These files, which contain sensitive information, require special protection so that only authorized individuals can access them. However, many stores do not have adequate security systems in place, posing a potential risk of data misuse that could be detrimental to the financial and reputational aspects of the business. The main problem in this context is the lack of a specialized system to secure files, especially sales files that are very important for store operations. The formulation of the problem is how to design an effective system to protect files from unauthorized access. The purpose of this research is to design a web application that can secure files by using cryptographic techniques, specifically the Advanced Encryption Standard (AES-128) algorithm, for document encryption and decryption. This application is expected to protect files in .doc, .docx, .pdf, .xls, and .xlsx formats, with a file upload size limit of up to 5MB. The research methods used include web-based application development using the PHP programming language and MySQL database. The AES-128 algorithm was chosen for its reliability in symmetric encryption, which is effective for maintaining data confidentiality. The results showed that the developed file security system successfully achieved a 100% success rate in the encryption and decryption process. The system works well according to the size of the processed file. The larger the file size, the longer it takes for the encryption and decryption process. For example, a 14KB file takes 0.3 seconds, while a 141KB file takes about 3 seconds. The contribution of this research is the provision of an effective solution for securing important data in stores, which not only keeps the information confidential but also provides consistent and reliable results.*

Keywords*: Cryptography, Advanced Encryption Standard, Data Security, Documents*

1. PENDAHULUAN

Kemajuan teknologi dalam sistem keamanan data mendorong kemajuan signifikan dalam berbagai aspek kehidupan, termasuk komunikasi dan pertukaran data. Seiring dengan kemajuan ini, perlindungan data dan

kerahasiaan informasi menjadi sangat penting. Kriptografi, yang telah digunakan sejak zaman kuno, kini menggunakan algoritma dan teknologi komputer canggih untuk melindungi informasi dari akses yang tidak sah. Algoritma kriptografi modern yang ramai digunakan adalah *Advanced Encryption Standard* (AES), yang dirancang untuk mengamankan informasi dengan kunci rahasia untuk tahap enkripsi dan dekripsi. Algoritma ini diterapkan dalam berbagai aplikasi untuk melindungi informasi penting.

Pada era digital ini, keamanan data sangat krusial untuk mencegah serangan terhadap sistem komputer dan jaringan. Salah satu contohnya adalah Cahaya Battery, sebuah bisnis keluarga yang berencana memperluas cabangnya dan memiliki dokumen penting seperti data penjualan bulanan yang sangat rahasia. Namun, mereka belum memiliki sistem pengamanan data yang memadai, yang membuka peluang terjadinya peretasan data oleh pihak yang tidak bertanggung jawab. Hal ini dapat mengubah data penjualan dan menimbulkan kerugian bagi bisnis. Oleh karena itu, diperlukan solusi untuk merancang sistem keamanan data menggunakan teknik kriptografi AES-128, yang dapat mengamankan file dokumen dalam format .doc, .pdf, dan .xls.

Berdasarkan latar belakang ini, penelitian ini bertujuan untuk mengembangkan program yang dapat menjaga keamanan file dokumen menggunakan algoritma AES-128 serta mengembalikan file yang telah dienkripsi ke bentuk aslinya tanpa perubahan. Dengan penerapan metode ini, diharapkan dapat meningkatkan keamanan data penting pada Cahaya Battery, mencegah kebocoran data, dan memberikan wawasan baru tentang algoritma kriptografi kepada masyarakat. Selain itu, manfaat yang diharapkan adalah meningkatkan keamanan data penting agar tidak terjadi hal-hal yang tidak diinginkan dan menambah pengetahuan masyarakat tentang keamanan informasi.

2. METODE PENELITIAN

2.1. Kriptografi

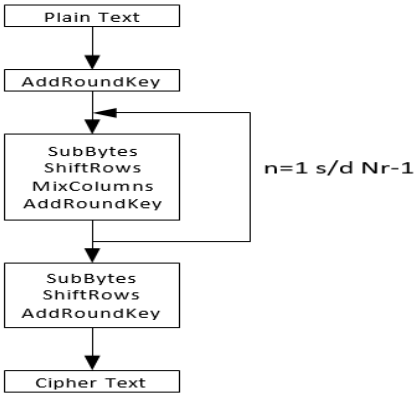
Istilah "kriptografi" berasal dari bahasa Yunani, di mana "kryptos" berarti tersembunyi dan "graphein" adalah menulis. Kriptografi adalah pengetahuan yang berfokus pada perlindungan informasi, terutama dalam hal keamanan dan kerahasiaan data. Informasi asli yang belum dienkripsi disebut plaintext, sedangkan setelah proses enkripsi, informasi tersebut dikenal sebagai ciphertext [1].

2.2. Algoritma Advanced Encryption Standard (AES)

AES adalah standar kriptografi komputer terbaru yang menggantikan Data Encryption Standard (DES) yang kini dianggap usang dan rentan terhadap serangan. Proses enkripsi dan dekripsi AES melibatkan serangkaian loop berulang yang disebut putaran, di mana jumlah putaran tergantung pada panjang kunci yang digunakan (128, 192, atau 256 bit). Setiap putaran memerlukan kunci putaran, yang dihasilkan dari kunci awal melalui proses ekspansi kunci. Karakteristik kehomogenan dari cipher block diperiksa selama proses ini untuk memastikan keamanan dan kerahasiaan data. Panjang kunci juga mempengaruhi jumlah iterasi dalam proses enkripsi. [2].

2.3. Proses Enkripsi Advanced Encryption Standard (AES)

AES adalah penerapan yang memanfaatkan enkripsi simetris untuk mengamankan dan membuka informasi. Dalam proses enkripsi, data diubah menjadi ciphertext yang tidak dapat dibaca, sedangkan tahap dekripsi mengembalikan *ciphertext* menjadi *plaintext* yang bisa dibaca Kembali [3].
Ilustrasi dapat dilihat dalam gambar 1:

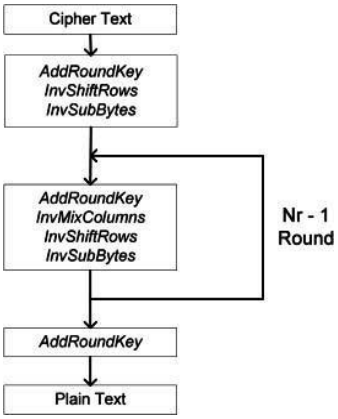


Gambar 1. Proses Enkripsi AES-128

Keterangan:
a. *AddRoundKey* adalah menggabungkan *ciphertext* yang ada dengan kunci *cipher* yang sesuai menggunakan operasi XOR
b. *SubBytes* adalah mengganti isi tabel yang ada dengan tabel lain yang dikenal Rijndael S-Box.
c. *ShiftRows* adalah proses yang menggeser elemen-elemen dalam tabel pada setiap baris, dimana bit paling kiri akan dipindahkan ke posisi paling kanan (Rotasi Bit)
d. *MixColumns* adalah mengacak data dalam setiap kolom pada array state manggunakanpersamaan tertentu.
e. Final Round adalah tahap terakhir dari proses enkripsi yang mencangkup langkah-langkah *SubBytes*,*Shiftrows*, dan *AddRoundKey*.

2.4. Proses Dekripsi Advanced Encryption Standard (AES)

Modifikasi *cipher* diterapkan dalam urutan terbalik untuk membentuk inverse cipher yang sesuai dengan algoritma AES. Modifikasi *byte* yang dipakai dalam *inverse cipher* mencakup *InvShiftRows, InvSubBytes, InMixColumns, dan AddRoundKey*[4].



Gambar 2. Proses Dekripsi AES-128

Keterangan:
a. *InvShiftRows* adalah pada bagian transformasi *InvShiftRows*, bit-bit digeser ke kanan.
b. *InvSubBytes* adalah setiap tahap dalam state disekat menggunakan kotak *Inverse S-Box.* Proses ini dilakukan sebanyak *Nr-1* kali.
c. *InvMixColumns* adalah setiap kolom didalam state dikalikan dengan operasi perkalian dalam AES.

2.5. Penerapan Metode

Dalam metode yang digunakan adalah algoritma kriptografi *Advanced Encryption Standard* (AES-128) [5].
a. Menentukan kunci Advanced Encryption Standard (AES) yang bisa digunakan dalam tahap enkripsi dan dekripsi file.
b. Tahap enkripsi dilakukan dengan memakai kunci Advanced Encryption Standard (AES), yaitu dengan mengubah file yang akan dienkripsi menjadi ciphertext menggunakan kunci AES yang telah ditentukan.
c. Proses dekripsi file ciphertext dilakukan dengan menggunakan kunci Advanced Encryption Standard (AES), yaitu mengubah ciphertext kembali menjadi file asli yang dapat dibaca (PlainText).

Sebagai contoh penggunaan algoritma *Advanced Encryption Standard* (AES-128) diterapkan pada kalimat. Misalkan, kata *plaintext* 'budiluhurkerennn' dengan kunci 'qwertyuiopasdfgh' yang akan dienkripsi menggunakan algoritma *Advanced Encryption Standard* (AES-128) [6].

Key

q	w	e	r
t	y	u	i
o	p	a	s
d	f	g	h

Plaintext

b	u	d	i
l	u	h	u
r	k	e	r
e	n	n	n

Gambar 3. Contoh Key Dan Plaintext
Ubah Menjadi hexadesimal

Key

71	77	65	72
74	79	75	69
6F	70	61	73
64	66	67	68

Plaintext

62	75	64	69
6C	75	68	75
72	6B	65	72
65	6E	6E	6E

Gambar 4. Hasil Hexadesimal

Ubah menjadi biner

Key

01110001	01110111	01110111	01110010
01110100	01111001	01110101	01101001
01101111	01110000	00011011	01110011
01100100	01100110	01100111	01101000

PlainText

01100010	01110101	01100100	01101001
01101100	01110101	01101000	01110101
01110010	01101011	01100101	01110010
01100101	01101110	01101110	01101110

Gambar 5 . Hasil Binner

a. Proses *AddRoundKey* dimana proses ini terjadi XOR antara masing-masing *Key* dan *Plaintext.*

00010011	00000010	00010011	00011011
00011000	00001100	00011101	00011100
00011101	00011011	01111110	00000001
00000001	00001000	00001001	00000110

Gambar 6. Hasil XOR

Ubah menjadi hexadesimal

13	02	13	1B
18	0C	1D	1C
1D	1B	7E	01
01	08	09	06

Gambar 7. Hasil Hexadesimal

b. Proses Sub-Bytes, di mana setiap byte dalam matriks state digantikan oleh byte yang sesuai dari S-Box (Substitution Box). S-Box adalah tabel substitusi yang berisi 256 nilai (dari 0x00 hingga 0xFF), yang digunakan untuk melakukan substitusi non-linear. [7]

7D	77	7D	9C
96	78	9D	82
9D	9C	3C	7C
7C	30	01	6B

Gambar 8. Hasil Proses Sub-Bytes

c. Proses *ShiftRows*, dimana baris-baris dalam *matriks state* diubah posisi berdasarkan aturan tertentu [8]. Berikut adalah aturan untuk proses *ShiftRows*
Baris Pertama : Tidak ada pergeseran
Baris Kedua : Pergeseran satu posisi ke kiri
Baris Ketiga : Pergeseran dua posisi ke kiri
Baris Keempat : Pergeseran tiga posisi ke kiri

7D	77	7D	9C
78	9D	82	96
3C	7C	9D	9C
6B	7C	30	01

Gambar 9. Hasil Proses Sub-Bytes

d. Proses *MixColumns*, dimana melibatkan pengolahan setiap kolom dari *matriks state* menggunakan operasi aritmatika. Ini dilakukan dengan mengalihkan setiap kolom dengan *matriks* tetap[9].

2.6. Spesifikasi Database

Berikut ini adalah struktur basis data yang akan digunakan. Table ini menyimpan *record* yang telah diteruskan oleh program sesuai dengan dekripsinya [10].akan

a. Tabel User

Nama Tabel : users
Primary Key : username
Foreign Key : -

Tabel 1 . Tabel Database User

Nama Field	Type	Ukuran	Keterangan
username	Varchar	15	Username
password	Varchar	100	Kata Sandi
fullname	Varchar	50	Nama Pengguna
job_title	Varchar	50	Pengguna
join_date	Timestamp	-	Tanggal Login
last_activity	Timestamp	-	Aktivitas Terakhir
Status	Enum	‘1’,’2’	Status

b. Tabel Berkas

Nama Tabel : file
Primary Key : id_file
Foreign Key : username

Tabel 2. Tabel Database File

Nama Field	Type	Ukuran	Keterangan
id_file	int	11	Id file
username	varchar	15	Username
file_name_source	varchar	255	File nama awal
file_name_finish	varchar	255	File nama akhir
file_url	varchar	255	Url file
file_size	float	-	Size file
password	varchar	16	Password
random_key	varchar	16	Random kunci file
tgl_upload	timestamp	-	Tanggal upload
status	enum	1’,’2’	Status
keterangan	varchar	255	Keterangan

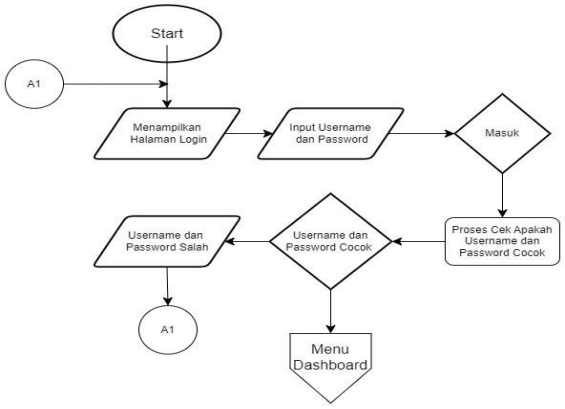
3. HASIL DAN PEMBAHASAN

3.2. *Flowchart*

Diagram alur atau flowchart sistem yang mengenggunakan algoritma *Advanced Encryption Standard* (AES-128).

a. *Flowchart* Proses Login

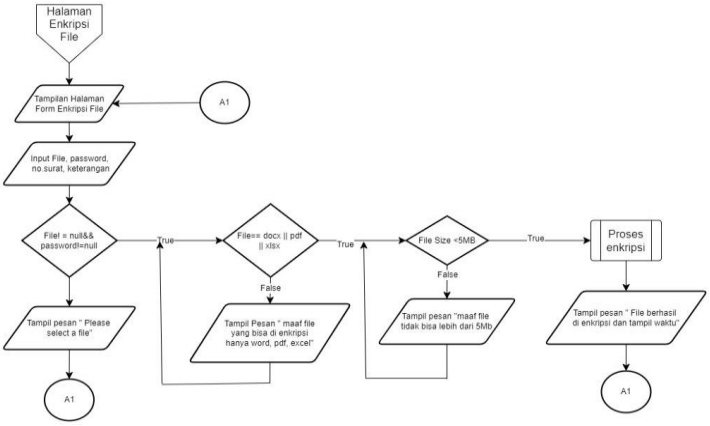
Flowchart dari halaman login menjelaskan validasi *username* dan *password* untuk bisa mengakses *website* pengamanan data ini. Yang dapat dilihat pada gambar 10.



Gambar 10. *Flowchart* Proses Login

b. *Flowchart* Proses Enkripsi

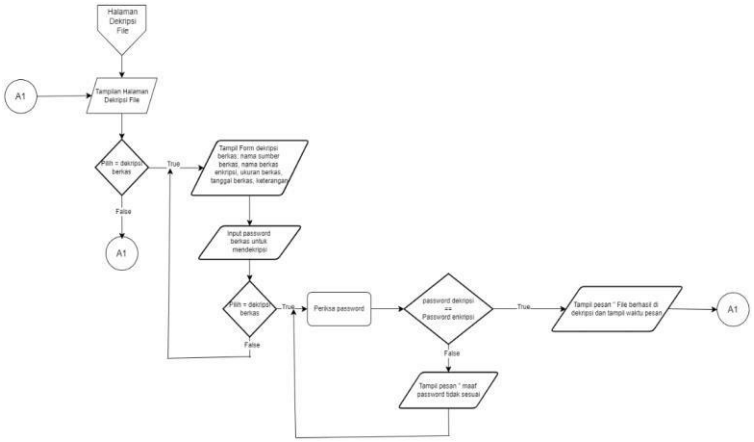
Flowchart enkripsi ini menjelaskan tahapan–tahapan dalam memproses enkripsi file yang bisa pengguna jalankan. File yang dapat dienkripsi beberapa file dengan format .doc, .xlsx, dan .pdf.



Gambar 11. *Flowchart* Proses Enkripsi

c. *Flowchart* Proses Dekripsi

Setelah tahapan enkripsi selesai, kemudian akan ditemukan untuk melakukan proses dekripsi file dengan tahapan. Sebagaimana dapat dilihat digambar 12.



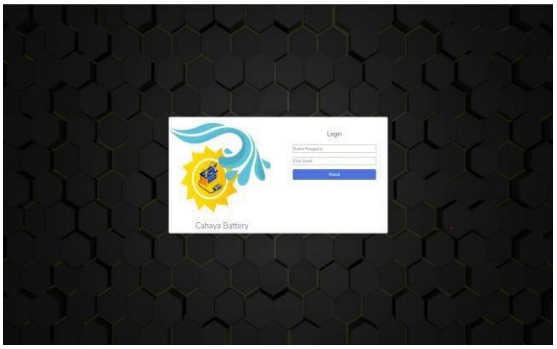
Gambar 12. *Flowchart* Proses Dekripsi

3.3. Tampilan Layar Aplikasi

Pada tahap ini dijelaskan antarmuka pengguna dalam aplikasi pengamanan file di Cahaya Battery. Yang dimana sistem yang dibuat untuk memenuhi kebutuhan pengamanan data.

a. Tampilan Layar Halaman Login

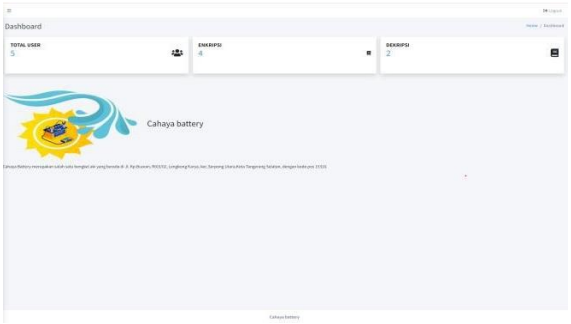
Pada halaman login disini akan diperlihatkan kepada pengguna tersedia kotak *username* dan *password* yang wajib diinput oleh pengguna agar bisa masuk ke dalam *dashboard.* Sebagaimana dapat dilihat pada gambar 13.



Gambar 13. Tampilan Halaman Login

b. Tampilan Layar *Dashboard*

Pada halaman ini pengguna akan diperlihatkan menu utama pada *website* ini. Yang memperlihatkan jumlah dari file yang sudah di enkripsi dan dekripsi pada *website* ini, juga memperlihatkan jumlah pengguna yang sudah terdaftar pada *website.* Seperti pada gambar 14.



Gambar 14. Tampilan Layar *Dashboard*

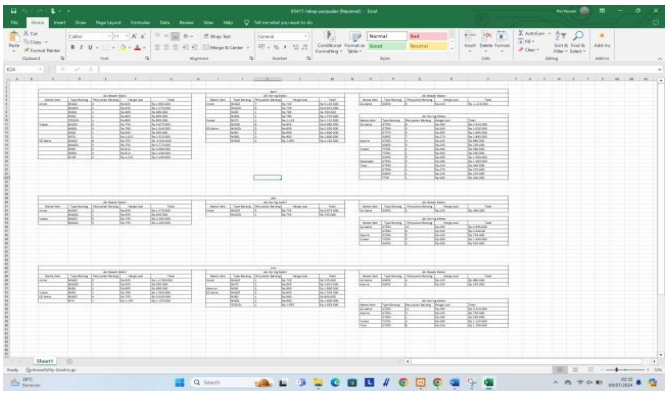
c. Tampilan Layar Hasil Proses Enkripsi

Tampilan ini menunjukkan hasil dari file yang telah berhasil dienkripsi. File hasil enkripsi dapat ditemukan di folder file_encrypt dan dapat dibuka menggunakan aplikasi notepad, seperti yang terlihat pada gambar 15.

Gambar 15. Tampilan Hasil Proses Enkripsi

d. Tampilan Layar Hasil Proses Dekripsi

Tampilan ini menunjukkan hasil dari file yang telah berhasil didekripsi. File hasil dekripsi dapat ditemukan di folder file_decrypt, di mana data tersebut masih dalam format normal dan dapat dibaca dengan jelas, seperti yang ditunjukkan pada gambar 16.



Gambar 16. Tampilan Hasil Proses Dekripsi

3.4. Hasil Uji Enkripsi Dan Dekripsi

Hasil pengujian enkripsi dan dekripsi pada file rekap penjualan serta data inventaris dengan format .doc, .xlsx, dan .pdf dapat dilihat pada tabel 3 dan 4.

Tabel 3. Tabel Hasil Uji Proses Enkripsi

No	Nama Berkas Asli	Ukuran Berkas Asli (KB)	Nama File Setelah Di Enkripsi	Ukuran File Setelah Di Enkripsi (KB)	Waktu Yang diperlukan (Detik)	Keterangan
1	Rekap Penjualan.xlsx	14 KB	19956-rekap-penjualan.rda	14 KB	0,3 Detik	Terselesaikan
2	Data Inventory Cahaya Battery.xlsx	12 KB	50730-data-inventory-cahaya-battery.rda	12 KB	0,27 Detik	Terselesaikan
3	Rekap Penjualan.docx	26 KB	45407-rekap-penjualan.rda	26 KB	0,55 Detik	Terselesaikan
4	Data Inventory.docx	21 KB	50309-data-inventory.rda	21 KB	0,48 Detik	Terselesaikan
5	Rakap Penjualan .pdf	141 KB	98141-rekap-penjualan.rda	141 KB	3 Detik	Terselesaikan
6	Data inventory.pdf	127 KB	29705-data-inventory.rda	127 KB	3 Detik	Terselesaikan

Hasil pengujian enkripsi pada file soal ujian dengan ekstensi .docx, .xslx dan .pdf menunjukkan bahwa hasil pengujian sesuai dengan tahap perancangan, di mana aplikasi sistem ini mampu melakukan enkripsi pada file dengan kapasitas yang dapat mencapai lebih dari 5 MB.

Tabel 4. Tabel Hasil Uji Proses Dekripsi

No	Nama Berkas Enkripsi	Ukuran Setelah Di Enkripsi (KB)	Nama Berkas Sesudah Di Dekripsi	Ukuran Berkas Sesudah Di Dekripsi (KB)	Waktu Yang Dibutuhkan (Detik)	Keterangan
1	19956-rekap-penjualan.rda	14 KB	40848-rekap-penjualan.xlsx	14 KB	0.23 Detik	Terselesaikan
2	50730-data-inventory-cahaya-battery.rda	12KB	6755-data-inventory-cahaya-battery.xlsx	12 KB	0,19 Detik	Terselesaikan

3	45407-rekap-penjualan.rda	26 KB	39164-rekap-penjualan.docx	26 KB	0,6 Detik	Terselesaikan
4	50309-data-inventory.rda	21 KB	59795-data-inventory.docx	21 KB	0,46 Detik	Terselesaikan
5	98141-rekap-penjualan.rda	141 KB	66687-rekap-penjualan.pdf	141 KB	3 Detik	Terselesaikan
6	29705-data-inventory.rda	127 KB	94312-data-inventory.pdf	127 KB	3 Detik	Terselesaikan

Hasil pengujian dekripsi dengan ekstensi .docx, .xlsx dan .pdf berhasil melakukan proses dekripsi file. Selain itu, hasil dari seluruh pengujian proses dekripsi mencapai tingkat keberhasilan 100% pada file yang diuji.

4. KESIMPULAN

Berdasarkan analisis terhadap website yang telah dikembangkan, dapat disimpulkan bahwa program ini memiliki potensi yang baik, meskipun masih memerlukan pengembangan lebih lanjut untuk meningkatkan kualitas dan performanya. Implementasi aplikasi menggunakan AES-128 menunjukkan bahwa aplikasi ini dapat mengenkripsi file dalam berbagai format, seperti *.doc, *.docx, *.xls, *.xlsx, dan *.pdf. Tahap enkripsi dan dekripsi dipengaruhi oleh ukuran file yang diinput. semakin besar ukuran file, semakin lama waktu yang dibutuhkan untuk menyelesaikan proses tersebut. Aplikasi ini juga memiliki batasan ukuran file maksimal yang dapat diproses, yaitu 5 MB. Berdasarkan penjelasan dalam penelitian ini, dapat dilihat bahwa algoritma AES-128 bisa diterapkan dalam aplikasi yang dikembangkan, dengan keberhasilan 100% dalam proses enkripsi dan dekripsi. Hal ini menunjukkan bahwa aplikasi tersebut efektif dalam melindungi file rekap penjualan dan data inventaris dari akses yang tidak sah.

DAFTAR PUSTAKA

[1] I. D. Widyawan, “Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi”, vol 11, no.2, pp. 167-174, 2023.

[2] B. E. Widodo and A. S. Purnomo, “Implementasi *Advanced Encryption Standard* Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY,” Jurnal Teknik Informatika (Jutif), vol. 1, no. 2, pp. 69–77, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[3] M. Fahri, H. Damanik, I. Gunawan, Z. M. Nasution, S. Sumarno, and I. O. Kirana, “PemanfaatanAlgoritma Aes Untuk Keamanann Data Karyawan PT. Telkom Indonesia Pematangsiantar,” vol. 1, no. 1, pp. 32–37, 2022, doi: 10.55123.

[4] A. Putra, R. Tarigan, P. S. Ramadhan, and K. Ibnutama, “Nomor 1, Edisi April,” vol. 5, 2023, [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jct/index

[5] A. I. Suranta, D. Virgian, and S. Y. Sakti, “Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi,” SKANIKA: Sistem Komputer dan Teknik Informatika, vol. 5, no. 1, pp. 1–10, 2022.

[6] M. Azhari, J. Perwitosari, and F. Ali, “Implementasi Pengamanan Data pada Dokumen Menggunakan AlgoritmaKriptografi *Advanced Encryption Standard* (AES),” Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[7] H. Wijaya, “Penerbit Implementasi Kriptografi AES-128 Untuk Mengamankan URL (*Uniform Resource Locator*) Dari SQL Injection,” *Akademika Jurnal*, vol. 17, no. 1, 2020, pp. 8-13.

[8] B. O. P. I. Irawan, et al., “Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard (AES),” *Jurnal Simantec*, vol. 11, no. 2, pp. 167-174, 2023.

[9] T. B. Tahir, M. A. H. Sirad, and M. Rais, “Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel,” *PATRIA ARTHA Technological Journal*, vol. 4, no. 1, pp. 41-46, 2020, doi: 10.33857/patj.v4i1.326.

[10] I. Priambudi, “Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web PadaSMP Yapipa,” *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 6, no. 1, pp. 22-31, 2023.