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

PENGAMANAN *FILE MARKETING* PADA YAYASAN PENDIDIKAN DESAIN INDONESIA MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB

Reza Martinus Papilaya[1*], Rizky Pradana[2]

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

Email: [1*]2011511132@student.budiluhur.ac.id, [2] rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-Yayasan Pendidikan Indonesia yang bergerak di bidang pendidikan. *file* setiap hari bertambah seiring banyaknya penjualan yang dibutuhkan pada Yayasan Pendidikan Indonesia belum mendapat pengamanan yang lebih. *File* hanya disimpan didalam sebuah ruangan yang sangat rentan untuk dicuri, hilang, atau data bisa diperjualbelikan oleh oknum yang tidak bertanggung jawab. Oleh karena itu, penelitian kali ini mempunyai tujuan untuk mengamankan *file* yang terdapat di Yayasan Pendidikan Indonesia dan ekstensi file yang lebih beragam seperti: *.docx, *.doc, *.xls, *.xlsx, *.pdf, *Tujuan utama penelitian ini adalah untuk meningkatkan tingkat keamanan data penjualan marketing sehingga informasi sensitif yang dimiliki oleh Yayasan Pendidikan Indonesia dapat terlindungi dengan baik. Pemilihan metode AES-256 didasarkan pada reputasinya yang terpercaya dalam enkripsi data yang kuat dan aman. Penelitian ini melibatkan pengembangan sistem yang mengintegrasikan algoritma AES-256 ke dalam proses pengamanan data penjualan marketing Yayasan Pendidikan Indonesia berbasis web. Evaluasi dilakukan untuk mengukur efektivitas keamanan yang diterapkan dan sejauh mana sistem ini dapat memberikan perlindungan yang memadai terhadap informasi sensitif yang dimiliki Yayasan. Potensi akses tidak sah dan kebocoran informasi dapat diminimalisir, sehingga data yang penting tetap terjaga kerahasiaannya. Dengan demikian, kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma *Advanced Encryption Standard* (AES-256) merupakan solusi efektif dalam mengamankan data sensitif Yayasan Pendidikan Indonesia dan memberikan dasar yang kuat untuk pengembangan sistem keamanan data yang lebih baik di masa depan.

Kata Kunci: Pengamanan Data, AES-256, Keamanan Siber

MARKETING FILES SECURITY AT THE INDONESIAN DESIGN EDUCATION FOUNDATION USING WEB-BASED AES-256 ALGORITHM

Abstract*-The Indonesian Education Foundation, which operates in the field of education, faces a growing need for file security due to the increasing volume of sales data. Currently, files are only stored in a room that is highly vulnerable to theft, loss, or unauthorized trading of data. Therefore, this research aims to secure the files at the Indonesian Education Foundation and extend protection to a wider range of file formats, including *.docx, *.doc, *.xls, *.xlsx, and *.pdf. The primary objective of the research is to enhance the security of marketing sales data to ensure that sensitive information held by the Foundation is well protected. The choice of the AES-256 method is based on its established reputation for strong and secure data encryption. This study involves the development of a web-based system that integrates the AES-256 algorithm into the data security process for the Foundation's marketing sales data. An evaluation is conducted to measure the effectiveness of the applied security measures and the extent to which the system can provide adequate protection for the Foundation's sensitive information. Potential unauthorized access and information leaks are minimized, ensuring the confidentiality of critical data. Consequently, the conclusion of this study is that the implementation of the Advanced Encryption Standard (AES-256) algorithm is an effective solution for securing the Indonesian Education Foundation's sensitive data and provides a solid foundation for the development of better data security systems in the future.*

Keywords*: Data Security, AES-256, Cybersecurity*

1. PENDAHULUAN

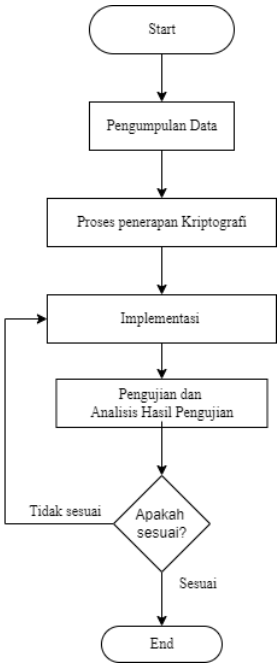
Kemajuan teknologi informasi dan Internet telah mengubah cara masyarakat berkomunikasi dan berbagi informasi. Media sosial kini telah menjadi bagian integral dari kehidupan sehari-hari, memfasilitasi akses luas dan penyebaran informasi. Pentingnya perlindungan data di media sosial dan aplikasi online lainnya menjadi perhatian utama. Penelitian ini menggunakan metode campuran dengan mengkaji literatur terkait keamanan informasi di media sosial serta mengidentifikasi aspek-aspek kritis dalam sistem aplikasi *online*, seperti keamanan data,

kesadaran, pengaturan kontrol, manajemen risiko, transparansi, dan etika. Pengelolaan sistem yang baik harus memperhatikan kebutuhan dan memberikan mekanisme kontrol yang memadai untuk melindungi data pribadi.

Algoritma kriptografi seperti *Advanced Encryption Standard* (AES) digunakan untuk mengenkripsi dan mendekripsi data, menjaga kerahasiaan dan integritas informasi. AES-256, sebagai algoritma *block cipher* simetris dengan ukuran kunci 256 *bit*, menawarkan tingkat keamanan yang tinggi dibandingkan dengan algoritma sebelumnya seperti *Data Encryption Standard* (DES). Penelitian ini bertujuan untuk menerapkan AES-256 dalam mengamankan data dokumen di Yayasan Pendidikan Design Indonesia, sebuah lembaga pendidikan terkemuka di bidang mode dengan jaringan internasional.

Yayasan Pendidikan Design Indonesia menghadapi tantangan signifikan terkait keamanan data karyawan. Data sensitif, termasuk nama, alamat, dan nomor telepon, seringkali mudah diakses dan rentan terhadap pencurian atau kebocoran informasi. format *file* yang tidak terenkripsi seperti *xlsx memperburuk masalah ini. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan aplikasi web yang mengintegrasikan AES-256 untuk melindungi dan mengamankan data karyawan, serta mengurangi risiko penyalahgunaan data oleh pihak yang tidak berwenang.

2. METODE PENELITIAN



Gambar 1. Tahapan Penelitian

Agar penerapan metode dapat berfungsi sebagai pedoman yang efektif dalam pelaksanaan penelitian, penting untuk memastikan bahwa hasil yang dicapai tetap sesuai dengan tujuan awal yang telah ditetapkan. Dengan demikian, proses penelitian harus dilakukan dengan mengikuti tahapan yang telah dirancang dan diuraikan sebelumnya, sehingga memastikan bahwa setiap langkah penelitian selaras dengan tujuan penelitian yang ingin dicapai. Tahapan penelitian ini dapat dilihat secara rinci pada gambar 1, gambar tersebut menggambarkan langkah-langkah yang diambil dalam penerapan metode penelitian, mulai dari perencanaan hingga analisis hasil, untuk memastikan bahwa semua aktivitas dilakukan dengan sistematis dan terarah, sehingga hasil akhir penelitian dapat memenuhi harapan dan kontribusi yang diinginkan.

a. Studi literatur, pada tahap ini dilakukan analisis terhadap berbagai buku, jurnal, dan kajian akademis yang relevan dengan keamanan data dan kriptografi AES-256. Tujuannya adalah untuk mendapatkan referensi yang solid dan memilih pendekatan terbaik untuk penelitian ini.
b. Studi lapangan analisis kasus dilakukan pada file di Yayasan Pendidikan *Design* Indonesia untuk mengidentifikasi masalah keamanan. Temuan dari studi ini digunakan untuk merumuskan solusi yang tepat dalam penelitian.
c. Rumusan masalah merupakan identifikasi masalah utama dalam penelitian ini meliputi pengamanan dokumen dan data penjualan menggunakan sistem enkripsi AES-256. Penelitian ini bertujuan untuk memastikan data yang dienkripsi dapat dikembalikan ke bentuk semula setelah dekripsi.

d. Identifikasi permasalahan setelah data dikumpulkan, masalah dalam sistem diidentifikasi melalui analisis data dan penerapan algoritma.
e. Implementasi aplikasi dikembangkan sesuai desain dan persyaratan sistem, menggunakan perangkat lunak Php MyAdmin, DBMS, PHP.

2.1 Algorima Enkripsi dan Dekripsi

a. Algoritma Enkripsi
Dalam algoritma seperti AES, langkah-langkah utama terdiri dari *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Langkah *AddRoundKey* melibatkan XOR antara data saat ini dan kunci putaran yang dihasilkan dari kunci utama. Proses ini dilakukan di awal dan di akhir setiap putaran, termasuk pada putaran terakhir. Selanjutnya, *SubBytes* adalah langkah substitusi yang menggunakan S-*box* tetap untuk melakukan substitusi byte secara non-linier, menambah kompleksitas enkripsi. *ShiftRows* berfungsi untuk menggeser baris-baris data, memberikan difusi tambahan dengan mengacak posisi byte dalam baris. *MixColumns* adalah langkah yang mencampur data dalam setiap kolom untuk meningkatkan penyebaran lebih lanjut, namun langkah ini tidak diterapkan pada putaran final untuk menghindari kelemahan *cryptographic* tertentu. Selain itu, penjadwalan kunci adalah proses di mana kunci putaran dihasilkan dari kunci utama menggunakan algoritma penjadwalan kunci, memastikan variasi yang diperlukan dalam setiap putaran enkripsi.

```
1.  Start
2.  Input file dan password
3.  AddRaoundKey
4.  SubBytes
5.  ShiftRows
6.  MixColums
7.  AddroundKey
8.          If round = 10 Then
9.              SubBytes
10.             ShiftRows
11.             AddRoundKey
12.             Cipher Text
13. Else
14. I++
15. End
```

Gambar 2. Tahapan Enkripsi

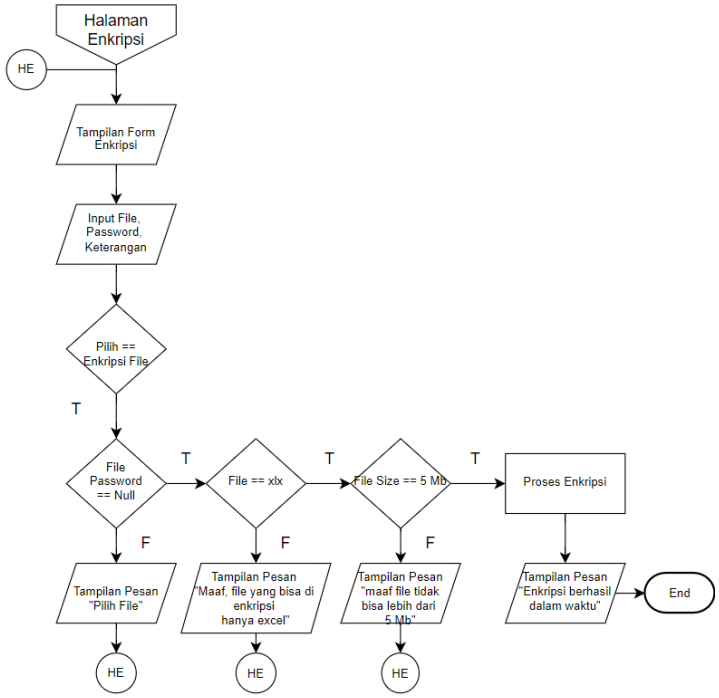
b. Algoritma Dekripsi

```
1.  Start
2.  Input file dan password
3.  AddRoundKey
4.  InvSubByte
5.  InvShiftRows
6.          If round = 10 Then
7.           AddRoundKey
8.           InvMixColumns
9.           InvSubByte
10.         InvShiftRows
11.         AddRoundKey
12.         Plain Tex
13. Else
14. I++
15. End
```

Gambar 3. Tahapan Dekripsi

2.2 Metode Enkripsi dan Dekripsi

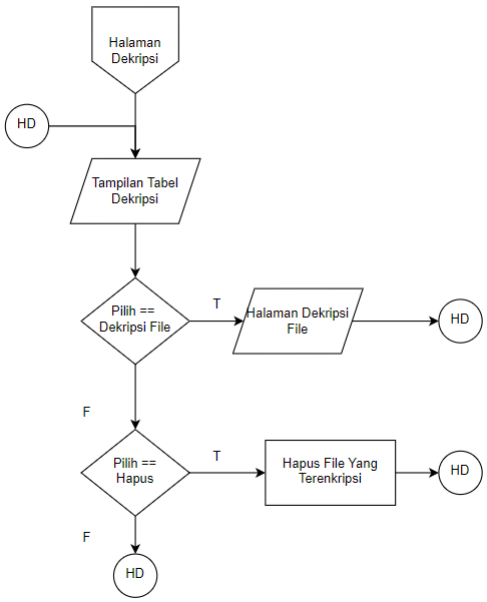
a. *Flowchart* Halaman Enkripsi
Gambar 4 adalah *flowchart* halaman enkripsi *file*, dalam alur enkripsi *file* ini menjelaskan bagaimana proses enkripsi dilakukan dapat mengenkripsi *file* yang diinginkan.



Gambar 4. *Flowchart* Halaman Enkripsi

b. *Flowchart* Halaman Dekripsi

Gambar 5 adalah *flowchart* yang menggambarkan bagaimana mengenkripsi *file* dan menghapus *file* yang telah dienkripsi untuk halaman dekripsi.



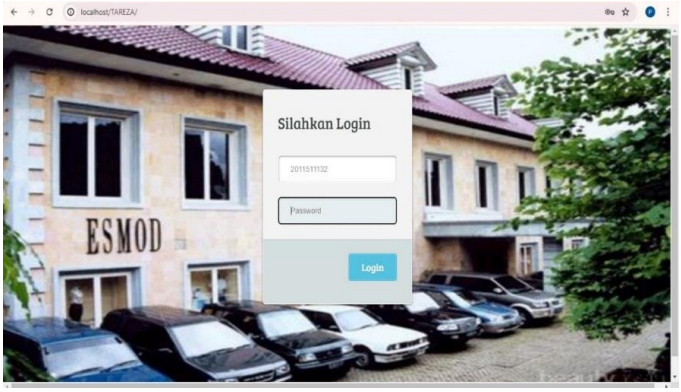
Gambar 5. *Flowchart* Halaman Dekripsi

3. HASIL DAN PEMBAHASAN

Bagian ini memuat hasil analisis, pelaksanaan atau pengujian dan pembahasan topik penelitian dan pada awalnya dapat digunakan sebagai metodologi penelitian. Bagian ini juga memberikan petunjuk berupa penjelasan, gambar, tabel, dan lain-lain.

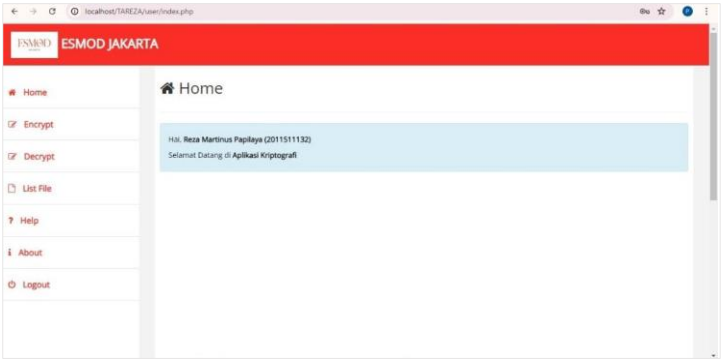
3.1 Tampilan Layar

a. Tampilan Layar *Login*
Tampilan layar halaman *login* diwajibkan untuk memasukkan kombinasi *username* dan *password* yang *valid* untuk dapat mengakses halaman utama aplikasi. Halaman *login* ini dirancang untuk memastikan bahwa hanya yang telah terdaftar dan memiliki kredensial yang benar yang dapat memasuki sistem, sehingga menjaga keamanan dan integritas data yang ada di dalam aplikasi. Proses ini melibatkan pengisian formulir dengan dua kolom *input*, satu untuk username dan satu lagi untuk *password*, yang harus diisi secara tepat sebelum tombol "*Login*" dapat ditekan untuk memverifikasi identitas dan memberikan akses ke fungsi dan informasi yang tersedia di halaman utama.



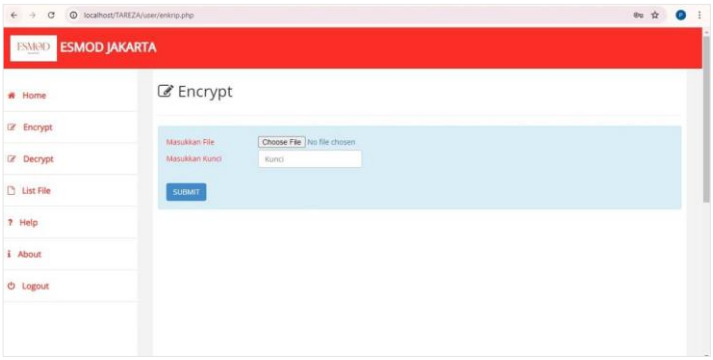
Gambar 6. Tampilan Layar *Login*

b. Tampilan Layar *Home*
Setelah berhasil menyelesaikan proses autentikasi di halaman *login*, diarahkan ke tampilan layar halaman utama aplikasi. Di halaman utama ini, akan disuguhi berbagai opsi menu yang meliputi: "*Home*" yang menyediakan informasi umum dan navigasi dasar, "Enkripsi" yang memungkinkan untuk mengamankan data dengan teknik enkripsi, "Dekripsi" yang memberikan fasilitas untuk mengembalikan data yang telah dienkripsi ke bentuk aslinya, "Dokumen" yang berfungsi sebagai pusat untuk mengelola dan mengakses dokumen-dokumen yang relevan, serta "Cek Bilangan Prima" yang menawarkan alat untuk memeriksa apakah bilangan tertentu merupakan bilangan prima atau tidak. Menu-menu ini dirancang untuk memberikan akses cepat dan mudah ke berbagai fitur penting dalam aplikasi, memfasilitasi pengalaman yang efisien dan efektif.



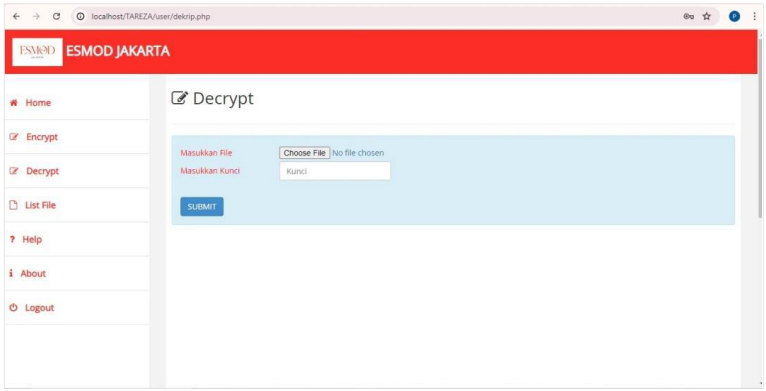
Gambar 7. Tampilan Layar Halaman Utama

c. Tampilan Layar Enkripsi
Pada tampilan layar enkripsi, diberikan kemampuan untuk mengamankan data melalui proses enkripsi yang intuitif. Dalam menu ini, dapat meng-upload file yang ingin dienkripsi, serta memasukkan dua kunci yang diperlukan untuk proses enkripsi, yaitu kunci 1 dan kunci 2. Kunci-kunci ini harus berupa bilangan prima, yang memastikan tingkat keamanan tambahan dalam proses enkripsi. dapat melihat contoh format kunci dan panduan pada gambar yang disediakan, yang menjelaskan secara detail cara memasukkan kunci dengan benar untuk memastikan bahwa data yang diunggah terlindungi secara optimal sebelum diproses lebih lanjut.



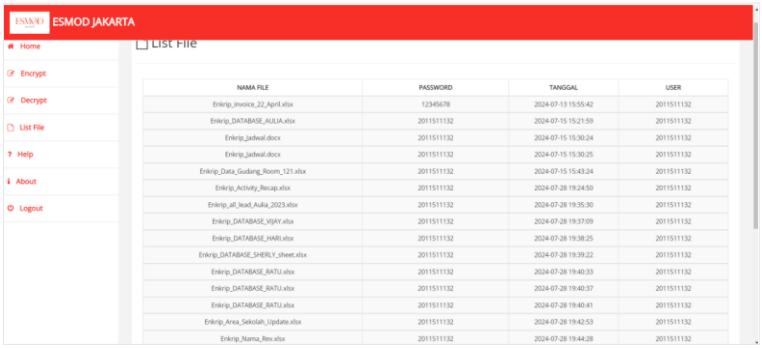
Gambar 8. Tampilan Layar Enkripsi

d. Tampilan Layar Dekripsi
Berikut ini adalah tampilan layar menu dekripsi, diharuskan untuk memasukkan file yang telah dienkripsi sebelumnya bersama dengan kunci privat yang sesuai untuk proses dekripsi. Kunci privat ini, yang harus dicantumkan oleh peneliti, berfungsi untuk mengembalikan *file* terenkripsi ke bentuk aslinya. Instruksi serta format kunci privat yang diperlukan dapat ditemukan pada gambar 9, yang menyediakan panduan visual untuk memastikan bahwa peneliti dapat memasukkan informasi yang tepat agar proses dekripsi dapat dilakukan dengan benar dan efisien.



Gambar 9. Tampilan Layar Dekripsi

e. Tampilan Layar Tampilan Layar Menu File
Berikut ini merupakan tampilan layar menu Dokumen, di mana peneliti dapat mengakses berbagai fungsi terkait dengan file yang telah dienkripsi sebelumnya. Dalam menu ini, memiliki kemampuan untuk melihat riwayat file yang telah melalui proses enkripsi, mengunduh ulang file hasil enkripsi yang mungkin perlu diakses kembali, serta menghapus file hasil enkripsi dari database jika tidak lagi diperlukan. Fitur-fitur ini dirancang untuk memberikan kemudahan dalam mengelola file yang telah dienkripsi, memastikan dapat melakukan pengelolaan file dengan fleksibel dan efisien sesuai kebutuhan mereka..



Gambar 10. Tampilan Layar Dokumen

3.2 Analisis Hasil

Tujuan dari Penelitian yang sedang dilakukan melalui peneliti dan proses pengujian aplikasi ini untuk mempelajari lebih lanjut tentang kemungkinan hasil dari sistem aplikasi keamanan file Yayasan Pendidikan *Design* Indonesia. Proses penulisan file enkripsi dan file dekripsi diuji secara bergantian dalam dua tahap pengujian ini.

3.2.1 Pengujian Proses Enkripsi

Pada tahap ini berisi tentang hasil pengujian proses enkripsi yang dilakukan pada sepuluh *file* dokumen, dengan hasil dari sistem pengolahan *file* mampu menangani berbagai ukuran *file* dengan berhasil. Pada waktu pemprosesan *file* cenderung meningkat seiring dengan peningkatan ukuran *file*, dengan jumlah *file* yang lebih besar maka waktu yang dibutuhkan lebih lama untuk diproses. Sistem menunjukkan performa yang sangat baik untuk *file* berukuran kecil dan menengah, tetapi ada peningkatan waktu yang signifikan untuk *file* berukuran besar.

Tabel 1. Tabel Pengujian Proses Enkripsi

No	Dokumen	Ukuran Hasil Enkripsi	Ukuran Hasil Dokumen	Status	
				Enkripsi	Waktu
1	Data Gudang.xlsx	96 KB	96 KB	Berhasil	13.34 Detik
2	*Inventory* Asset	32 KB	32 KB	Berhasil	3.07 Detik
3	*ActivityRecap*.xlsx	19 KB	19 KB	Berhasil	0.61 Detik
4	*all lead* Aulia 2023.xlsx	72 KB	72 KB	Berhasil	2.53 Detik
5	*DATABASE* VIJAY.xlsx	42 KB	42 KB	Berhasil	1.37 Detik
6	*DATABASE* HARI.xlsx	56 KB	56 KB	Berhasil	1.82 Detik
7	*DATABASE SHERLY sheet.xlsx*	49 KB	49 KB	Berhasil	1.77 Detik
8	*DATABASE* RATU.xlsx	109 KB	109 KB	Berhasil	3.54 Detik

3.2.2 Pengujian Proses Dekripsi

Pada tahap ini berisi tentang hasil pengujian proses dekripsi yang dilakukan pada sepuluh *file* dokumen yang sama. Hasil dari pengujian proses enkripsi lalu di Proses dalam program dekripsi *file* yang dilakukan oleh aplikasi yang dirancang sedemikian rupa sehingga tidak mengubah isi *file* dan ukuran *file* sama sekali. Setelah *file* dienkripsi dan kemudian didekripsi, hasilnya identik dengan *file* aslinya. Artinya, integritas dan keakuratan data dalam *file* tetap terjaga sepenuhnya, tanpa adanya perubahan atau kehilangan informasi pada proses tersebut.

Tabel 2. Tabel Pengujian Proses Dekripsi

No	Dokumen	Ukuran Hasil Enkripsi	Ukuran Hasil Dokumen	Status	
				Enkripsi	Waktu
1	Data Gudang.xlsx	96 KB	96 KB	Berhasil	9.11 Detik
2	*Inventory Asset*	32 KB	32 KB	Berhasil	3.28 Detik
3	*ActivityRecap*.xlsx	19 KB	19 KB	Berhasil	1.31 Detik
4	*all lead* Aulia 2023.xlsx	72 KB	72 KB	Berhasil	2.03 Detik
5	*DATABASE* VIJAY.xlsx	42 KB	42 KB	Berhasil	0.55 Detik
6	*DATABASE* HARI.xlsx	56 KB	56 KB	Berhasil	2.12 Detik
7	*DATABASE* SHERLY *sheet*.xlsx	49 KB	49 KB	Berhasil	2.07 Detik
8	*DATABASE* RATU.xlsx	109 KB	109 KB	Berhasil	4.04 Detik

3.2.3 Pengujian Program

Semua fitur dan proses dalam aplikasi diuji dan berjalan sesuai dengan harapan. Proses login, enkripsi, dekripsi, penghapusan file, pengunduhan file, akses halaman tambahan, dan logout semuanya berfungsi dengan baik dan sesuai dengan ekspektasi yang telah ditetapkan. Aplikasi ini tampak stabil dan memenuhi kebutuhan fungsional yang diharapkan.

Tabel 3. Tabel Pengujian Proses Dekripsi

No	Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
1	Mengisi *Form Login*	Tampilan Halaman *Dashboard*	Sesuai Harapan
2	Memasukan berkas file dan menekan tombol enkripsi *file*	Tampilan halaman hasil enkripsi	Sesuai Harapan
3	Menekan dekripsi	Menampilkan halaman dekripsi	Sesuai Harapan
4	*File* yang telah dienkripsi dan didekripsi dan dihapus	Berkas *file* terhapus	Sesuai Harapan
5	Dapatkan *file* yang telah mengalami enkripsi dan dekripsi	Berkas *file* berhasil di-*download*	Sesuai Harapan
6	Pilih halaman tentang.	Tampilan halaman tentang	Sesuai Harapan
7	Memilih halaman panduan	Menampilkan halaman panduan	Sesuai Harapan

3.3 Kelebihan Aplikasi

Program aplikasi berbasis web ini menawarkan kemudahan penggunaan yang tinggi dan mampu melampirkan serta memproses berkas dengan ukuran maksimal hingga 5 MB. Batas ukuran ini memberikan keleluasaan kepada peneliti untuk mengunggah dokumen atau *file* besar tanpa mengalami masalah, sehingga proses enkripsi dan dekripsi dapat dilakukan dengan efisien. Selain itu, aplikasi ini dirancang untuk memastikan bahwa proses enkripsi dan dekripsi tidak mengubah isi *file* sama sekali; hasil dari dekripsi akan identik dengan *file* aslinya. Dengan kata lain, integritas dan keakuratan data dalam *file* tetap terjaga sepenuhnya tanpa adanya perubahan atau kehilangan informasi.

3.4 Kekurangan Aplikasi

Meskipun program aplikasi ini mendukung ukuran *file* hingga 5 MB, yang memadai untuk banyak kasus, beberapa pengguna mungkin membutuhkan dukungan untuk file yang lebih besar, sehingga batasan ini dapat menjadi kendala bagi mereka yang bekerja dengan dokumen atau data yang sangat besar. Selain itu, tampilan aplikasi yang masih sederhana mungkin kurang memenuhi kebutuhan pengguna yang menginginkan antarmuka yang lebih canggih atau fitur tambahan. Meskipun penggunaan *password* untuk enkripsi dan dekripsi meningkatkan keamanan, hal ini juga menambah kompleksitas penggunaan, karena peneliti harus mengingat dan mengelola *password* dengan baik untuk menghindari masalah akses atau kesalahan.

4. KESIMPULAN

Program keamanan *file* ini dirancang khusus untuk melindungi data transaksi penjualan dan dokumen penting lainnya dengan menggunakan metode enkripsi yang kuat. Program ini memungkinkan peneliti untuk menyandikan dan mendekode *file* dalam format *.xlsx secara akurat menggunakan teknik enkripsi AES-256, yang merupakan salah satu standar enkripsi terkuat saat ini. Penting untuk dicatat bahwa ukuran file yang sedang diproses mempengaruhi waktu yang dibutuhkan untuk menyelesaikan prosedur enkripsi dan dekripsi. Semakin besar ukuran *file*, semakin lama waktu yang diperlukan untuk menyelesaikan proses tersebut. Oleh karena itu, untuk efisiensi optimal, disarankan agar ukuran *file* yang diproses tidak melebihi batas yang diperlukan dan, jika memungkinkan, *file* dikompresi sebelum enkripsi untuk mempercepat proses dan mengurangi waktu tunggu. Untuk meningkatkan efisiensi program keamanan file ini, Anda bisa mempertimbangkan implementasi fitur kompresi *file* otomatis sebelum proses enkripsi dimulai. Ini membantu mengurangi waktu yang dibutuhkan untuk enkripsi dan dekripsi, terutama saat menangani file dengan ukuran besar. Selain itu, melakukan pengujian rutin terhadap performa enkripsi pada berbagai ukuran file dapat memberikan wawasan lebih lanjut untuk mengoptimalkan kecepatan proses.

DAFTAR PUSTAKA

[1] M. R. Alfani, M. Furqan, and Y. R. Nasution, "*Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (DSA) dan Advanced Encryption Standard (AES)*," *Journal of Science and Social Research*, vol. 7, no. 1, pp. 301–306, 2024. http://jurnal.goretanpena.com/index.php/JSSR

[2] N. Cristy, and F. Riandari, "*Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan*," *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, vol. 4, no. 2, pp. 75–85, 2021. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181

[3] R. D. A. Huday, S. Waluyo, "Pengamanan File Rekam Medis Pada Puskesmas Larangan Utara Menggunakan Algoritma Kriptografi Rsa Berbasis Web," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, vol. 1, no. 1, pp. 277–286, 2022. http://senafti.budiluhur.ac.id/index.php/senafti/article/view/221/38

[4] I. M. Sukarsa, I. M. R. Pradana, and P. W. Buana, "Implementasi Enkripsi dan Otentikasi Transmisi Data ZeroMQ Menggunakan Advanced Encryption Standard," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 6, pp. 1149–1156, 2020. https://doi.org/10.29207/resti.v4i6.2581

[5] R. Laia, "Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio," *Pelita Informatika: Informasi dan Informatika*, vol. 8, no. 4, pp. 467–469, 2020. https://www.ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/2445

[6] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Terapan)*, vol. 1, no. 2, pp. 108–114, 2021. https://doi.org/10.30998/jrkt.v1i02.4096

[7] R. Nuari, and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *Journal of Artificial Intelligence and Innovative Applications*, vol. 1, no. 2, pp. 2716–1501, 2020. http://openjournal.unpam.ac.id/index.php/JOAIIA

[8] D. Nurnaningsih, and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)," *Jurnal Teknik Informatika*, vol. 11, no. 2, pp. 177–186, 2018. https://doi.org/10.15408/jti.v11i2.7811

[9] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, pp. 564–573, 2022. https://doi.org/10.31933/jemsi.v3i5.992

[10] S. Oktaviani, F. Rizky, and I. Gunawan, "*Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES),*" *Jurnal Media Informatika*, vol. 4, no. 2, pp. 97–101, 2023. https://doi.org/10.55338/jumin.v4i2.435

[11] M. B. Yel, and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, pp. 92–101, 2022. https://doi.org/10.59697/jik.v6i1.144