3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENERAPAN AES-128 DALAM KRIPTOGRAFI DATA PRODUK DAN CUSTOM PT PADMA MULIA PERKASA (PMP)

Agung Febrian[1]*, Titin.fatimah[2]

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

Email: [1*]agungfbrn290801@gmail.com, [2]titin.fatimah@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT Padma Mulia Perkasa (PMP), yang beroperasi di sektor produk mebel, menghadapi tantangan signifikan dalam hal penyimpanan data yang terstruktur dan aman. Tantangan ini berlaku terutama untuk data produk dan custom mereka, yang memegang nilai penting bagi operasional perusahaan. Mengakui ini, PT PMP memandang perlu untuk memiliki aplikasi atau situs web yang mampu melindungi dan mengamankan data tersebut dari berbagai ancaman, baik *internal* maupun *eksternal*. Untuk mengatasi tantangan ini, solusi kriptografi diperkenalkan. Melalui proses enkripsi dan dekripsi, kriptografi dapat menjaga kerahasiaan dan integritas data. Dalam skenario ini, metode "*Advanced Encryption Standard*" (AES-128) dipilih dan diterapkan karena efisiensinya dalam menjaga kerahasiaan dan integritas data. Ini merupakan algoritma yang cukup kuat dan terpercaya untuk kebutuhan keamanan data. Penelitian ini melibatkan pengujian dan evaluasi *komprehensif* dari implementasi kriptografi dan metode AES-128 dalam sistem PT PMP. Penelitian ini memiliki tujuan ganda: pertama, untuk mendalaminya dan menganalisis tantangan yang dihadapi oleh PT PMP dalam penyimpanan data terstruktur dan aman; kedua, untuk mengevaluasi efektivitas metode "*Advanced Encryption Standard" (AES-128*) sebagai solusi dalam mengatasi tantangan tersebut.. Ini termasuk analisis terperinci tentang bagaimana metode ini mempengaruhi aspek-aspek keamanan data seperti *aksesibilitas, integritas,* dan kerahasiaan.Hasil penelitian ini menunjukkan peningkatan signifikan dalam keamanan data setelah penerapan metode tersebut. Ini menunjukkan bahwa pendekatan kriptografi, dan lebih khusus lagi metode AES-128, dapat menjadi *instrumen* yang *efektif* dalam upaya perusahaan untuk melindungi data mereka. Dengan demikian, penelitian ini memberikan wawasan penting tentang penerapan dan *efektivitas* metode AES-128 dalam konteks keamanan data perusahaan.

Kata Kunci: PT Padma Mulia Perkasa (PMP), produk mebel, kriptografi, *Advanced Encryption Standard (AES-128),* enkripsi, dekripsi, keamanan data

IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD AES-128 ALGORITHM IN SECURING PRODUCT AND CUSTOMER DATA OF PT PADMA MULIA PERKASA (PMP)

Abstract- PT Padma Mulia Perkasa (PMP), which operates in the furniture product sector, faces considerable challenges concerning the structured and secure storage of data. These challenges primarily relate to their product and custom data, essential for the company's operational integrity. Recognizing this, PT PMP sees the need to establish an application or website capable of protecting this data from diverse threats, both internally and externally. To address this hurdle, cryptographic solutions were proposed. Using encryption and decryption processes, cryptography can ensure data confidentiality and integrity. Within this framework, the "Advanced Encryption Standard" (AES-128) was selected and deployed for its proficiency in maintaining data confidentiality and integrity. It stands as a robust and reliable algorithm for data security requirements. This research encompasses comprehensive testing and evaluation of the cryptographic and AES-128 method's implementation within PT PMP's system. The research aims to, firstly, delve into and assess the challenges PT PMP confronts in structured and secure data storage, and secondly, gauge the effectiveness of the "Advanced Encryption Standard" (AES-128) in mitigating these challenges. This encompasses a detailed scrutiny of how this method influences data security aspects such as accessibility, integrity, and confidentiality. The findings underscore a notable enhancement in data security following the method's implementation, implying that cryptographic approaches, especially the AES-128 method, serve as an effective mechanism for corporate data protection endeavors. Thus, this research furnishes pivotal insights regarding the implementation and efficacy of the AES-128 methodology in the domain of corporate data security.

Keywords: *PT Padma Mulia Perkasa (PMP), product company, cryptography, Advanced Encryption Standard (AES-128), data security, encryption and decryption, secure product.*

1. PENDAHULUAN

Pada zaman teknologi dan telekomunikasi yang menunjukan perkembangan cukup pesat, sebuah kerahasiaan dan juga keamanan data merupakan hal yang sangatlah penting dan harus diperhatikan dalam berkomunikasi, dengan adanya perkembangan teknologi yang sangat maju memberikan kemudahan seperti memperoleh sebuah informasi atau saling bertukar informasi dan menyimpan sebuah file yang berisi data penting.

PT Padma Mulia Perkasa (PMP) adalah perusahaan yang berfokus pada pengolahan mebel menjadi produk furnitur berkualitas. Perusahaan ini berlokasi di Tangerang, Banten. PT Padma Mulia Perkasa (PMP) memiliki data penting yang mencakup data produk dan data custom, yang tersedia dalam format file PDF.

Dalam file PDF, data produk PT Padma Mulia Perkasa (PMP) mencakup informasi mengenai jenis produk furnitur, spesifikasi teknis, dan bahan yang digunakan. data Ini sangat penting untuk memahami pilihan produk perusahaan.

Selain itu, data custom dalam file PDF berisi informasi mengenai pesanan khusus pelanggan, seperti desain, ukuran, atau spesifikasi khusus lainnya. Hal ini membantu perusahaan memenuhi preferensi pelanggan secara individual dan memberikan pelayanan yang sesuai.

Namun, perlu diingat bahwa karena data tersebut berbentuk file PDF, dapat dengan mudah diakses oleh siapa saja yang ingin melihatnya. Hal ini juga membawa risiko potensial seperti kehilangan data, pencurian data, dan manipulasi data oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting untuk melindungi dan mengamankan file PDF dengan langkah-langkah keamanan yang sesuai [1].

Dalam upaya untuk mengamankan data-data tersebut, PT Padma Mulia Perkasa (PMP) menggunakan algoritma *Advanced Encryption Standard* (AES-128). *Algoritma* ini terbukti *efektif* dan *efisien* dalam menjaga keamanan data dengan kecepatan optimal. Dengan menerapkan proses enkripsi dan dekripsi yang tepat, PT Padma Mulia Perkasa (PMP) dapat memastikan bahwa data-data sensitif, termasuk data custom dan data produk, tetap terjaga kerahasiaannya dan terlindungi dari risiko kehilangan data, pencurian data, dan manipulasi data oleh pihak yang tidak bertanggung jawab.

Penelitian sebelumnya yaitu "Perancangan keamanan data pasien di klinik kecantikan Ratu Beauty Studio menggunakan metode kriptografi *RSA*." yang mengimplementasikan aplikasi berbasis web dan menggunakan metode *RSA*. pada penelitian kali ini berbasis web untuk mengamankan data produk dan data custom dengan menggunakan metode AES-128 [2].

Penelitian ini mengadopsi Metode AES (*Advanced Encryption Standard*) dalam metodologinya. Kelebihan utama algoritma ini adalah operasionalnya yang lebih cepat dibandingkan dengan *algoritma asimetrik*, terutama dalam menghadapi operasi *matematis* yang lebih rumit, seperti manipulasi bilangan prima. Selain itu, algoritma ini tahan terhadap serangan *exhaustive key search* dan dapat diaplikasikan dalam sistem real-time, seperti GSM. Sebelum mendalami algoritma AES, kita akan membahas terlebih dahulu mengenai kriptografi. [3]

Metode AES (Advanced Encryption Standard) yang diadopsi memiliki keunggulan tersendiri. Khususnya, kecepatan operasionalnya lebih unggul dibandingkan dengan algoritma asimetrik, terutama saat berhadapan dengan operasi matematika yang kompleks. Selain itu, algoritma ini tahan terhadap serangan exhaustive key search dan dapat diterapkan dalam sistem real-time seperti GSM. Sebelum memahami lebih lanjut mengenai algoritma AES, penting untuk memahami prinsip-prinsip dasar kriptografi.

Tujuan: Tujuan utama dari penelitian ini adalah untuk mengeksplorasi efektivitas dan praktikalitas metode AES-128 dalam mengamankan data esensial PT Padma Mulia Perkasa, membandingkan keuntungan dan potensi kekurangannya dengan metode kriptografi yang digunakan sebelumnya. [4].

2. METODE PENELITIAN

A. Studi Literatur

Selama fase studi literatur, penulis mengkaji berbagai literatur dan riset terdahulu yang berkaitan dengan kriptografi dan kompresi. Kajian ini memberikan pemahaman mendalam tentang berbagai teknik, aplikasi, dan implementasi algoritma enkripsi serta metode kompresi. Hal ini dilakukan untuk mendapatkan dasar teoretis yang kokoh dan memahami perkembangan terkini dalam kedua bidang tersebut [5].

B. Tahapan Pengumpulan Data

Melakukan wawancara dengan pihak-pihak terkait bertujuan untuk mengantisipasi dan memahami permasalahan yang ada, sehingga dapat dihasilkan sebuah desain sistem yang mampu mengatasi masalah tersebut.

Selain itu, observasi dilakukan pada PT Padma Mulia Perkasa (PMP) untuk memahami kondisi sebenarnya dari objek yang diteliti. Tujuan utamanya adalah mendapatkan penjelasan yang mendalam tentang informasi dan data yang dibutuhkan untuk penelitian ini..

C. Analisis sistem

1. Analisis Data

   Untuk menangani isu keamanan ini dalam analisis data, salah satu langkah yang dapat diambil adalah mengorganisir file-file yang dibutuhkan untuk menghimpun informasi esensial dalam merancang aplikasi. Klasifikasikan file berdasarkan tipe mereka. Proses dekripsi file mencakup penentuan tahapan dalam menciptakan aplikasi yang intuitif dan mudah dipahami.

2. Menganalisis penerapan algoritma.

   Setelah melalui tahap pengumpulan data dan pengawasan proses sistem, berikutnya adalah penerapan algoritma. Analisis Aplikasi Algoritma merinci tahapan dalam menerapkan metode enkripsi *Advanced Encryption Standard* (AES) untuk melindungi data yang penting. Demikian juga:

   A. Menentukan kunci yang akan digunakan untuk enkripsi dan dekripsi file.
   B. Proses mengenkripsi file dengan kunci enkripsi, khususnya proses mengubah file terenkripsi menjadi ciphertext menggunakan kunci enkripsi.
   C. Proses dekripsi ciphertext menggunakan kunci yang sama dengan kunci enkripsi, yaitu proses mengubah ciphertext menjadi pesan yang dapat diputar ulang (plaintext).

3. Analisis sistem.

   Proses pengamanan yang diimplementasikan pada sistem ini melibatkan enkripsi konten file. Enkripsi ini dilakukan dengan tujuan melindungi isi file yang sensitif, sehingga hanya pihak-pihak yang memiliki otoritas yang dapat mengaksesnya. Proses ini memerlukan sebuah modul khusus untuk mengenkripsi data. Modul enkripsi ini, yang diletakkan dalam aplikasi, akan diaktifkan saat pengguna berusaha mengamankan konten file. Sebaliknya, modul dekripsi akan dipanggil saat pengguna ingin mengakses dan membaca isi file.

D. Desain Perangkat Lunak

Dalam tahap desain, berdasarkan hasil analisis sistem, terutama terkait dengan desain enkripsi dan dekripsi, dukungan tambahan juga diintegrasikan ke dalam aplikasi beserta dengan desain antarmuka pengguna. Pengembangan sistem ini memanfaatkan metode *waterfall*, di mana setiap tahap harus diselesaikan secara menyeluruh sebelum bergerak ke tahap berikutnya, dan setiap hasil dari tiap tahap harus didokumentasikan dengan tepat.

E. Implementasi

Dalam implementasi ini, apa yang dikandung pada tahap desain direalisasikan dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi ini digunakan:

1. Perangkat lunak yang digunakan dalam implementasi pengamanan file data menggunakan bahasa pemrograman PHP dan phpMyAdmin sebagai databasenya.
2. Hardware yang digunakan adalah Lenovo Ideapad 310 Intel CoreI5, RAM 4 GB DDR4.

F. Pemeriksaan Sistem

Metode yang digunakan untuk pengujian aplikasi ini adalah metode *Black Box*. Pengujian *Black Box* adalah pendekatan pengujian yang menggunakan struktur kontrol yang telah dirancang secara prosedural untuk melaksanakan pengujian dan melihat bagaimana perangkat lunak beroperasi. Seluruh komponen internal perangkat lunak diuji untuk memastikan bahwa mereka berfungsi sesuai dengan spesifikasi dan desain yang telah ditentukan [6]

G. Kesimpulan

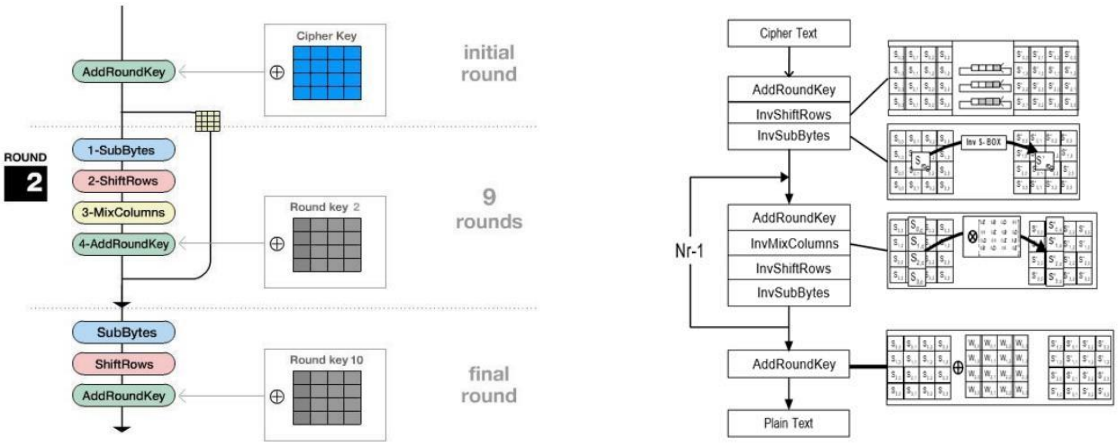
Tahap akhir ini menyimpulkan bahwa penerapan metode kriptografi *Advanced Encryption Standard* (AES) 128, berjalan dengan baik, dan dapat mengamankan file data produk dan custom diPT Padma Mulia Perkasa, ada usulan pengembangan dalam sistem ini [7].

2.1 *Advanced Encryption Standard*

Algoritma AES (*Advanced Encryption Standard*) adalah algoritma cipher simetris dan blok yang menggunakan kunci simetris untuk enkripsi dan dekripsi. Pada tahun 2002, digunakan sebagai referensi standar untuk algoritma terbaru yang dirilis oleh NIST (Lembaga Standar dan Teknologi Nasional) untuk menggantikan istilah algoritma DES (Data Encryption Standard) yang sudah usang [8]

2.2 Proses Enkripsi

Metode enkripsi algoritma AES memiliki empat jenis, yaitu yaitu *transformasi* byte, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada bagian pertama dari proses enkripsi, input akan disalin ke dalam ruang status untuk dikonversi menggunakan *byte AddRoundKey*. Setelahnya, *konversi SubBytes*, *ShiftRows*, *MixColumns, dan AddRoundKey* secara berulang kali sejumlah Nr. Pada metode ini disebut algoritma AES *(round function*). Pada putaran terakhir terdapat sedikit perbedaan dibandingkan dengan putaran sebelumnya, dimana keadaan state tidak mengalami transformasi Mix Columns.[9].



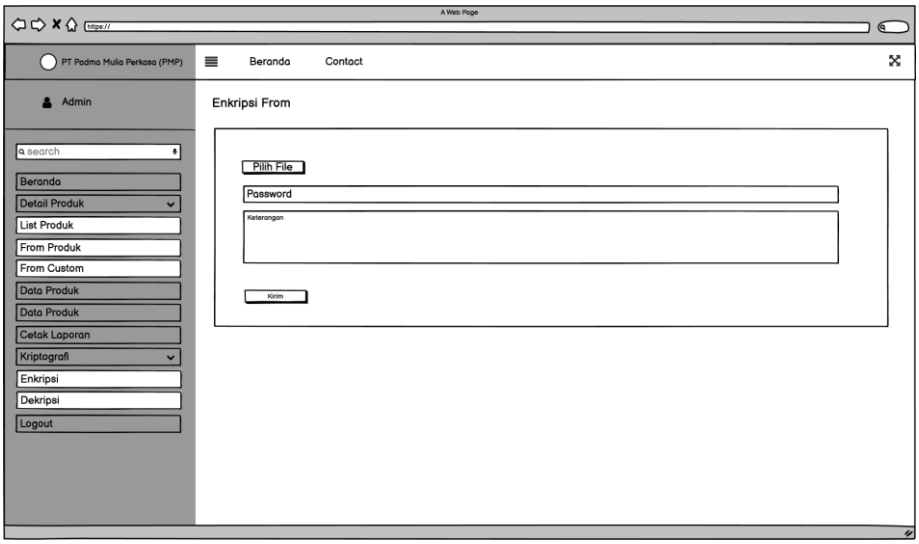
Gambar 1. Proses Enkripsi dan Dekripsi

2.3 Proses Dekripsi

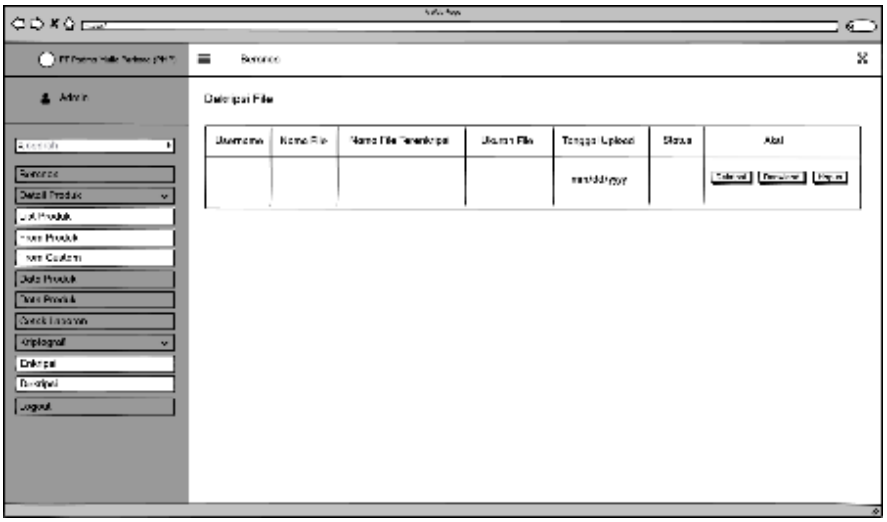
Konversi enkripsi dapat dibalik Proses enkripsi dan disediakan untuk datang ke arah yang berlawanan enkripsi balik yang mudah dipahami algoritme AES. Konversi byte digunakan dalam kasus enkripsi terbalik, yaitu *invShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey* [10]. Diagram proses dekripsi AES-128.Gambar 1 berikut menunjukkan proses enkripsi AES-128 dapat dilihat pada gambar 1. berikut:

2.3 Rancangan Layar

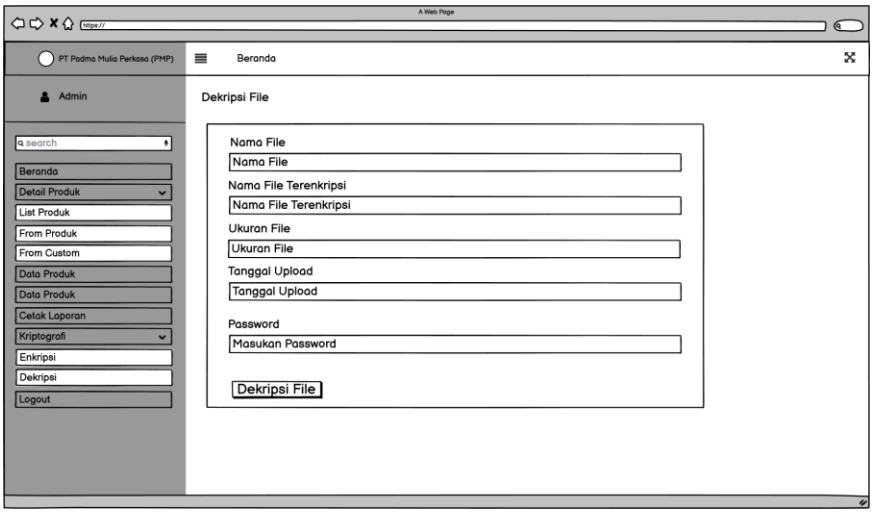
Dalam pembuatan suatu aplikasi, sangat diperlukan tahap perancangan layar sebagai bentuk dasar dalam membuat desain aplikasi yang diinginkan. Rancangan layar harus mudah dimengerti, tujuannya agar pengguna dapat merasa nyaman dan tidak bingung dalam menggunakan aplikasi ini.. Dapat dilihat pada gambar 2.
berikut:



Gambar 2. Rancangan Layar Halaman Enkripsi



Gambar 3. Rancangan Halaman Dekripsi



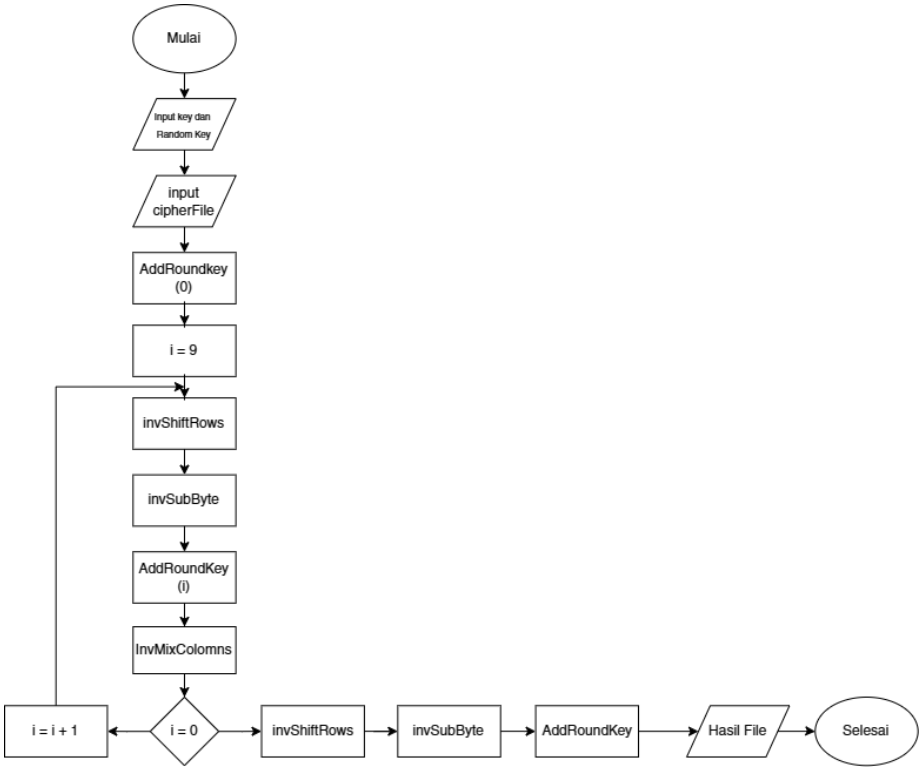
Gambar 4. Rancangan Halaman Form Dekripsi

3. HASIL DAN PEMBAHASAN

Bab ini menguraikan implementasi algoritma AES-128 untuk enkripsi dan dekripsi data PT Padma Mulia Perkasa (PMP). Uraian ini mencakup pembahasan flowchart, detail algoritma, proses, serta hasil dari enkripsi dan dekripsi dokumen melalui aplikasi yang telah dikembangkan.

3.1 Flowchart Proses Enkripsi

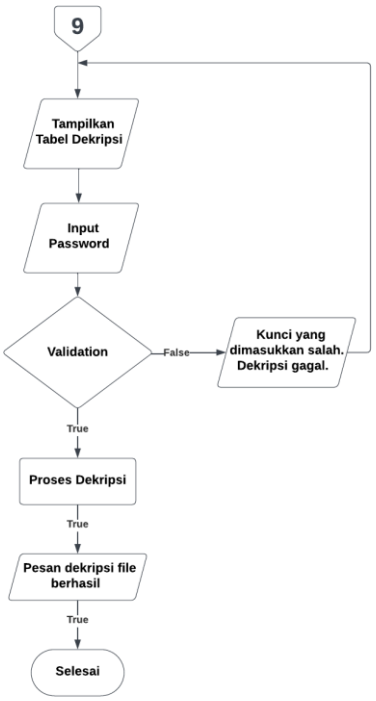
Pada gambar 3. merupakan *flowchart* dari halaman *form* enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi file admin harus memasukkan *password*, setelah itu program akan memproses *enkripsi*.



Gambar 3 *Flowchart* Menu Enkripsi

3.2 *Flowchart* Menu Dekripsi

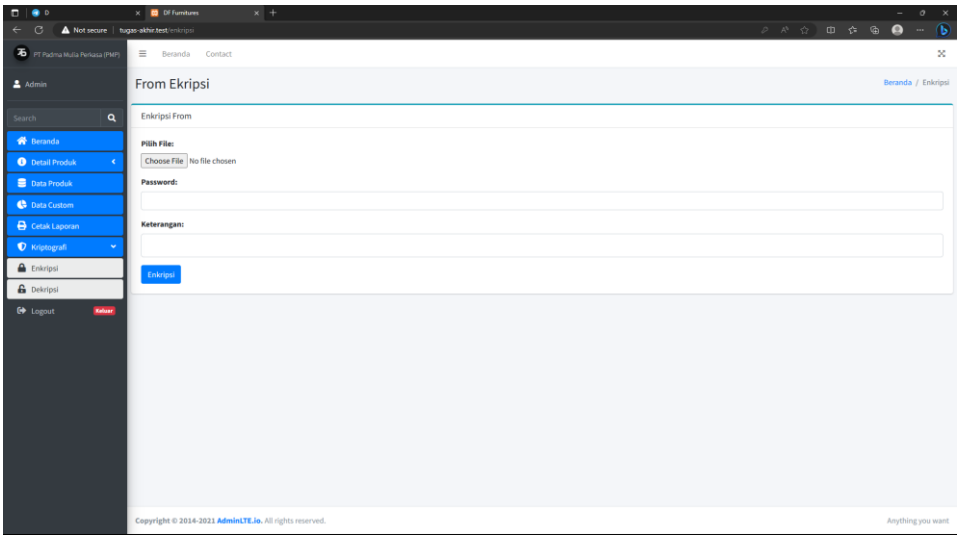
Pada gambar 4 merupakan *flowchart* dari halaman dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan *dekripsi* . Dalam *dekripsi* admin harus memasukkan *password* yang sesuai dengan *enkripsi*, setelah itu program akan memproses *dekripsi*.



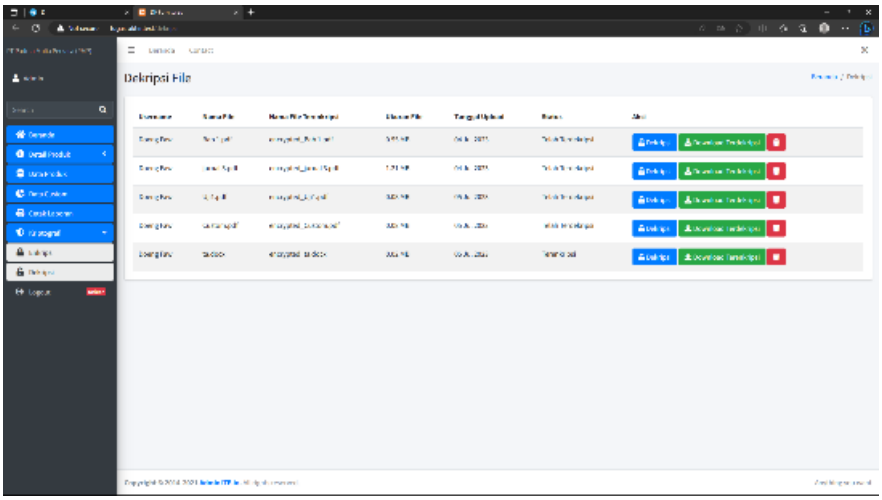
Gambar 4. *Flowchart* Menu Dekirpsi

3.3 Tampilan Layar

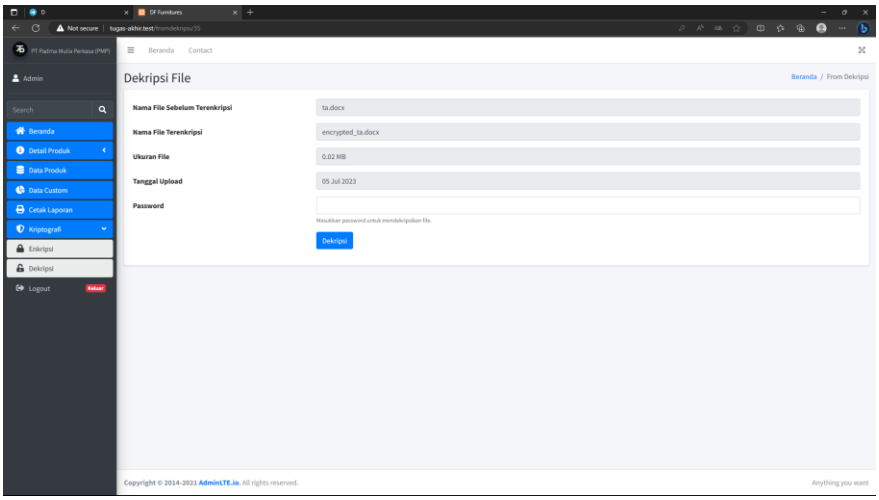
Pada gambar 5 terdapat tampilan layar tampilan aplikasi enkripsi hingga menu dekripsi file. Dapat dilihat pada gambar 5 berikut:.



Gambar 5. Tampilan Layar Enkripsi



Gambar 6. Tampilan Layar Dekripsi



Gambar 7. Tampilan Layar Form Dekripsi

3.4 Pengujian

Pengujian dilakukan untuk menilai keefektifan dan keandalan implementasi algoritma AES-128 dalam aplikasi. Hal-hal yang dievaluasi meliputi kecepatan proses, integritas hasil enkripsi (dokumen yang dienkripsi seharusnya tidak bisa dibuka tanpa dekripsi yang tepat), serta perbandingan ukuran data sebelum dan sesudah enkripsi. Tabel 1 menampilkan hasil dari pengujian yang telah dilaksanakan.

Tabel 1. Hasil Pengujian Enkripsi dan Dekripsi File

Nama File	Ukuran File (*Kilobyte*)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Data Custom.pdf	75kb	76kb	75kb	1,46 detik	1,23 detik
Data Produk.pff	66kb	67kb	66kb	1,31 detik	1,10 detik

4. KESIMPULAN

Aplikasi kriptografi berbasis web yang dirancang khusus untuk PT Padma Mulia Perkasa (PMP) telah berhasil memberikan solusi keamanan data optimal, khususnya untuk file PDF. Dengan efisiensi dalam proses enkripsi dan dekripsi serta modifikasi penggunaan random key, tingkat keamanan aplikasi ini meningkat signifikan. Ke depannya, kombinasi metode AES-128 dengan teknik lainnya dapat dipertimbangkan untuk meningkatkan ketahanan terhadap upaya peretasan. Selain itu, pengembangan aplikasi mobile di masa depan akan meningkatkan fleksibilitas penggunaan.

DAFTAR PUSTAKA

[1] Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). PERANCANGAN KEAMANAN DATA PASIEN DI KLINIK KECANTIKAN RATU BEAUTY STUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA. Jurnal Informatika Teknologi dan Sains (Jinteks), 4(4), 437-443.

[2] Sodikin, L., & Hidayat, T. (2020). Analisa Keamanan E-Commerce Menggunakan Metode AES Algoritma. Teknokom, 3(2), 8-13.

[3] Auliyah, A. I. (2020). Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document. Indonesian Journal of Data and Science, 1(1), 23-28.

[4] Firdaus, R., & Santika, R. R. (2022, September). Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security. In Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) (Vol. 1, No. 1, pp. 111-120).

[5] Ananda, S. P., & Lukman, S. (2022). Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital: Array. Jurnal Ilmiah KOMPUTASI, 21(3), 333-344.

[6] Widyawan, D., & Imelda, I. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi. SKANIKA: Sistem Komputer dan Teknik Informatika, 4(1), 15-22.

[7] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES dari Serangan Brute Force", TECHSI-Jurnal Teknik Informatika, 13(1), 14-25.

[8] Irawan, C. (2019). Implementasi ALgoritma Autokey Cipher dan AES-128 Pada Enkripsi File.

[9] Hidayatulloh, N. W., Tahir, M., Amalia, H., Basyar, N. A., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data. Digital Transformation Technology, 3(1), 1-10.

[10] Zaliluddin, D., & Rully, A. (2020). Implementasi E-Government Berbasis Android. JSiI (Jurnal Sistem Informasi), 7(2), 83-88.