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

IMPLEMENTASI KRIPTOGRAFI UNTUK PERLINDUNGAN DATA MENGGUNAKAN ALGORITMA AES-128 PADA PT PRIMA PANGAN SENTOSA

Ferian Ardyansyah[1*], Sejati Waluyo[2]

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

Email: [1*]2011501968@student.budiluhur.ac.id, [2]sejati.waluyo@ budiluhur.ac.id
(* : corresponding author)

Abstrak- Dengan kemajuan teknologi informasi saat ini menjadi sangat penting dalam banyak bidang dan salah satunya dalam bidang keamanan data. Dalam perkembangan teknologi menimbulkan dampak positif dan negatif. Dalam dampak positif dapat memberikan kemudahan dalam pengelolaan data agar tersusun dengan baik, selain dampak positif terdapat juga dampak negatifnya seperti pencurian data, dan penyalahgunaan teknologi lainnya. PT Prima Pangan Sentosa (PPS) didirikan pada tahun 2023 sebagai perusahaan distributor besar yang bergerak dibidang pangan atau kebutuhan pokok. Berdasarkan hal itu, PPS berupaya memenuhi segala macam kebutuhan pokok seperti hasil bumi. Sebagai perusahaan yang bergerak di bidang pangan , PT Prima Pangan Sentosa (PPS) memiliki laporan Pajak yang berisi Pajak penghasilan (PPh) dan Pajak pertambahan nilai (PPN). Data tersebut bersifat rahasia dan tidak boleh diakses sembarangan di PT Prima Pangan Sentosa (PPS) dan memiliki potensi kebocoran data yang dapat merugikan perusahaan, sehingga harus diamankan dengan sistem penyandian encryption). Algoritma Advanced Encryption Standard (AES) dengan panjang kunci 128 bit (AES-128) adalah salah satu solusi yang sangat andal untuk mengamankan data.(AES-128) dikenal karena memberikan tingkat keamanan yang tinggi serta efisiensi dalam kecepatan dan performa. Oleh karena itu dibuatlah aplikasi berbasis web enkripsi dan deskrpisi file yang digunakan untuk menjaga keamanan data rahasia PT Prima Pangan Sentosa yaitu laporan pajak. Aplikasi berbasis web ini dibuat menggunakan PHP dan JavaScript dengan *Framework* Bootstrap. Aplikasi web enskripsi dan deskripsi file ini diuji dengan menggunakan pengujian Alpha Testing. Berdasarkan analisa pada penelitian ini bahwa aplikasi web enkripsi dan deskripsi file berhasil dalam melindungi atau mengamankan data laporan pajak pada PT Prima Pangan Sentosa.

Kata Kunci: Kriptografi, AES-128, dan Alpha Testing

IMPLEMENTATION OF CRYPTOGRAPHY FOR DATA PROTECTION USING THE AES-128 ALGORITHM IN PT. PRIMA PANGAN SENTOSA

Abstract- *With advances in information technology, it is now very important in many fields, and one of them is in the field of data security. Technological developments have positive and negative impacts. In terms of positive impacts, it can make it easier to manage data so that it is well structured. Apart from the positive impacts, there are also negative impacts, such as data theft and misuse of other technology. PT Prima Pangan Sentosa (PPS) was founded in 2023 as a large distributor company operating in the food or basic necessities sector. Based on this, PPS tries to fulfill all kinds of basic needs, such as agricultural products. As a company operating in the food sector, PT Prima Pangan Sentosa (PPS) has a tax report containing income tax (PPh) and value-added tax (VAT). This data is confidential and cannot be accessed carelessly at PT Prima Pangan Sentosa (PPS) and has the potential for data leaks that could harm the company, so it must be secured with an encryption system. The Advanced Encryption Standard (AES) algorithm with a key length of 128 bits (AES-128) is a very reliable solution for securing data. (AES-128) is known for providing a high level of security as well as efficiency in speed and performance. Therefore, a web-based application for file encryption and description was created, which is used to maintain the security of PT Prima Pangan Sentosa's confidential data, namely tax reports. This web-based application was created using PHP and JavaScript with the Bootstrap Framework. This file encryption and description web application was tested using Alpha Testing. Based on the analysis in this research, the encryption web application and file descriptions were successful in protecting or securing tax report data at PT Prima Pangan Sentosa.*

1. PENDAHULUAN

Dengan kemajuan teknologi informasi saat ini menjadi sangat penting dalam banyak bidang dan salah satunya dalam bidang keamanan data. Dalam perkembangan teknologi menimbulkan dampak positif dan negatif. Dalam dampak positif dapat memberikan kemudahan dalam pengelolaan data agar tersusun dengan baik, selain dampak positif terdapat juga dampak negatifnya seperti pencurian data, dan penyalahgunaan teknologi lainnya. Oleh karena itu perlindungan terhadap data rahasia sangat diperlukan. Salah satu algoritma yang populer untuk mengamankan data dalam bentuk file adalah kriptografi.

PT Prima Pangan Sentosa (PPS) didirikan pada tahun 2023 sebagai perusahaan distributor besar yang bergerak dibidang pangan atau kebutuhan pokok. Berdasarkan hal itu, PPS berupaya memenuhi segala macam kebutuhan pokok seperti hasil bumi. . Sebagai perusahaan yang bergerak di bidang pangan, PT Prima Pangan Sentosa (PPS) memiliki laporan Pajak yang berisi Pajak penghasilan (PPh) dan Pajak pertambahan nilai (PPN). Data tersebut bersifat rahasia dan tidak boleh diakses sembarangan di PT Prima Pangan Sentosa (PPS) dan memiliki potensi kebocoran data yang dapat merugikan perusahaan, sehingga harus diamankan dengan sistem penyandian encryption.

Penelitian sebelumnya di Indonesia yang dilakukan oleh Randi dan Lazuardy dengan judul "Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android", telah membahas enkripsi kriptografi menggunakan metode AES berbasis Android. Penelitian ini berkontribusi dalam mengamankan pesan aplikasi chatting dengan menggunakan metode AES [1].

Format yang dienkripsi dan basis program membedakannya dari studi sebelumnya. Penelitian ini menerapkan sistem pengamanan data berbasis web yang menggunakan algoritma AES-128.untuk menjaga laporan Pajak yang ada di PT Prima Pangan Sentosa tetap aman.

Dengan meningkatnya ancaman terhadap keamanan data kebutuhan metode pengamanan data yang lebih kuat dan efektif semakin mendesak. Algoritma Advanced Encryption Standard (AES) dengan panjang kunci 128 bit (AES-128) adalah salah satu solusi yang sangat andal untuk mengamankan data.(AES-128) dikenal karena memberikan tingkat keamanan yang tinggi serta efisiensi dalam kecepatan dan performa. AES-128 sering dipilih untuk berbagai aplikasi dan sistem karena menawarkan keseimbangan yang optimal antara keamanan dan kinerja enkripsi.

Tujuan pengembangan aplikasi berbasis web yang menggunakan Algoritma AES-128 ini adalah untuk menawarkan PT Prima Pangan Sentosa (PPS) untuk menjaga data sensitif mereka. Aplikasi ini diharapkan dapat dengan mudah diintegrasikan ke dalam sistem yang sudah ada dan memiliki antarmuka yang ramah pengguna untuk pengguna di perusahaan.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi, yang dalam bahasa Yunani terdiri dari kata "kripto" yang berarti tersembunyi dan "graphia" yang berarti tulisan, adalah ilmu yang mempelajari metode matematika untuk menjaga keamanan data. Aspek-aspek yang menjadi fokus kriptografi meliputi kerahasiaan, keabsahan, integritas, serta autentikasi data. Meskipun demikian, kriptografi tidak dapat menangani seluruh aspek terkait keamanan data. [2].

Kriptografi adalah bidang yang mempelajari cara menyandikan pesan sehingga tidak dapat dipahami lagi untuk menjaga kerahasiaan pesan [3]. Bersama dengan meningkatnya kompleksitas ancaman terhadap keamanan data, kriptografi pun turut berkembang dan menjadi lebih matang. Hal ini melahirkan berbagai istilah yang digunakan untuk merujuk pada aktivitas penyamaran pesan rahasia. Proses pengacakan pesan disebut enkripsi, sedangkan proses mengembalikan pesan yang telah diacak ke bentuk aslinya disebut dekripsi. Pesan asli, baik sebelum maupun setelah diacak, disebut plaintext, sedangkan pesan yang telah diacak disebut ciphertext.

Kriptografi dibagi menjadi dua kategori: Kriptografi Klasik dan Kriptografi Modern. Kriptografi Klasik, yang digunakan sebelum dan sesudah era komputer, kurang populer dibandingkan dengan saat ini. Jenis ini hanya mengacak huruf dari A hingga Z dan tidak direkomendasikan untuk melindungi informasi penting karena mudah dipecahkan dalam waktu singkat. Prinsip utama Kriptografi Klasik adalah menjaga kerahasiaan kunci itu sendiri. Sementara itu, Kriptografi Modern jauh lebih kompleks dan memerlukan pemahaman matematika yang mendalam untuk dikuasai. Seiring dengan perkembangan komputer, kriptografi modern terus berkembang hingga saat ini. [4].

2.2 *Advanced Encryption Standard (AES)*

Algoritma AES diperkenalkan oleh NIST (National Institute of Standards and Technology) pada tahun 2001 sebagai metode enkripsi untuk menggantikan algoritma DES yang dianggap sudah usang dan mudah ditembus. AES kemudian ditetapkan sebagai standar untuk melindungi data, menggantikan peran DES. AES adalah jenis enkripsi block cipher yang mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Dalam prosesnya, blok data sepanjang 128 bit, yang dikenal sebagai plaintext dienkripsi menjadi ciphertext. Panjang kunci yang berbeda pada algoritma ini mempengaruhi jumlah putaran yang dilakukan selama enkripsi [5].

Ada tiga jenis penyandian AES, AES-128, AES-192, dan AES-256. AES-128 memiliki sepuluh putaran, sembilan putaran utama, dan satu putaran terakhir. AES-192 memiliki dua belas putaran, dan AES-256 memiliki

empat belas putaran, dengan tiga belas putaran pada transformasi awal dan satu putaran terakhir pada transformasi akhir. [6], seperti yang diilustrasikan dalam tabel berikut:

Tabel 1. Jumlah Putaran AES

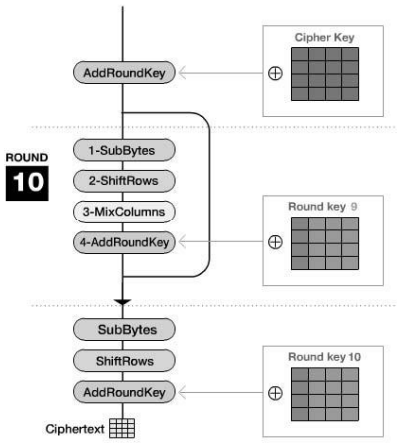
	Panjang Kunci (*NK Words*)	Panjang Blok (*Nb Words*)	Panjang Putaran (*Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Dalam proses enkripsi, terdapat empat jenis transformasi byte, yaitu SubBytes, ShiftRows, MixColumns, dan AddRound Key. Pada tahap awal, input mengalami transformasi AddRound Key sebelum dimasukkan ke dalam state. Kemudian, state mengalami serangkaian transformasi berupa SubBytes, ShiftRows, MixColumns, dan AddRound Key yang diulang sebanyak Nr kali. Proses ini dikenal sebagai function round dalam algoritma AES. Pada putaran terakhir, prosesnya berbeda dari putaran awal. Untuk dekripsi, algoritma yang digunakan adalah kebalikan dari enkripsi AES, di mana transformasi invers diterapkan pada semua transformasi dasar. [7].

2.2.1 Proses Enkripsi AES-128

AES-128 bit yang membutuhkan 10 putaran enkripsi, Proses enkripsi melibatkan empat transformasi utama:

1. *AddRoundKey* : Putaran awal proses enkripsi menetapkan tahapan untuk mengamankan teks biasa dengan melakukan operasi XOR (Exclusive OR) antara teks biasa.
2. Melakukan sebanyak $Nr-1$ putaran, dengan setiap langkah yang diambil dalam setiap putaran adalah :
   a. *SubByte* : Substitusi byte dengan menggunakan tabel substitusi (S-box).
   b. *ShiftRows* : Pergeseran baris-baris array state secara wrapping.
   c. *MixColumns* : mengalikan data di masing-masing kolom array state.
   d. *AddRoundKey :* Memanfaatkan round key untuk menghasilkan XOR antara kondisi saat ini.
3. Final Round :
   a. *SubByte*
   b. *ShiftRows*
   c. *AddRoundKey*



Gambar 1. Proses Enkripsi AES-128

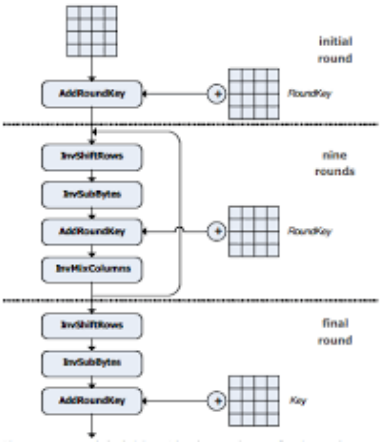
2.2.2 Proses Deskripsi AES-128

Proses deskripsi AES-128 kebalikan atau invers dari proses Enkripsi, berikut langkah-langkah yang harus dilakukan, antara lain:

1. *AddRoundKey* : Putaran awal proses enkripsi menetapkan tahapan untuk mengamankan teks biasa dengan melakukan operasi XOR (Exclusive OR) antara teks biasa.
2. Melakukan sebanyak $Nr-1$ putaran, dengan setiap langkah yang diambil dalam setiap putaran adalah :
   a. *InvShiftRows* : Kebalikan Pergeseran baris-baris array state secara wrapping.
   b. *InvSubByte* : Kebalikan Substitusi byte dengan menggunakan tabel substitusi (S-box).

c. *InvAddRoundKey :* Operasi XOR antara byte-byte matriks state yang disusun dari ciphertext dengan byte-byte roundkey yang dibangkitkan sebelumnya.
d. *InvMixColumns* : Mengalikan setiap kolom hasil dari Inverse *AddRoundKey*.

3. Final Round :
   a. *InvShiftRows*
   b. *InvSubByte*
   c. *AddRoundKey*



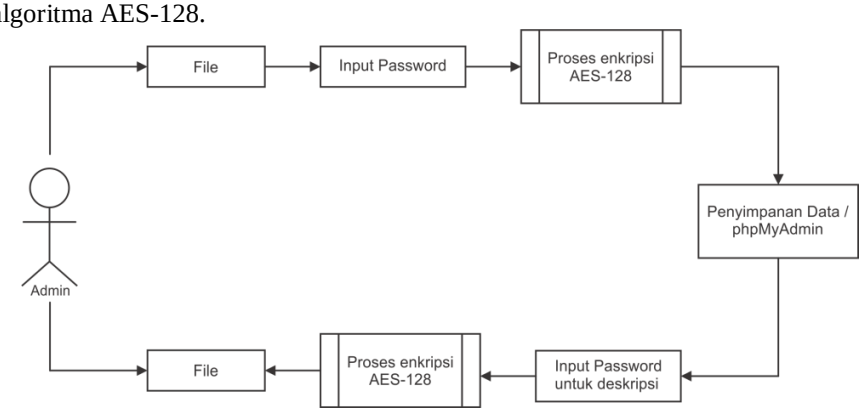
Gambar 2. Proses Deskripsi AES-128

2.3 Metode Pembanding

Pada tahapan ini penulis melakukan perbandingan dengan pelitian yang telah dikerjakan oleh Habib Husain Amirullah jurnalnya yang berjudul "Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android". Dengan menggunakan Algoritma AES-128, penelitian yang dilakukan dapat mengembangkan aplikasi yang mampu melakukan enkripsi menggunakan algoritma AES dan mengintegrasikannya dengan Biometric Prompt peningkatan keamanan data pada era digital [8].

2.4 Proses Penerapan Metode AES-128

Satu masalah pada PT Prima Pangan Sentosa adalah tidak mempunyai program perlindungan file penting terutama untuk data pajak. Oleh karena itu, program enkripsi diperlukan untuk memastikan kerasahasian file. Gambar 1 menunjukkan alur metode diterapkan pada program perlindungan file data pajak yang dibuat dengan menggunakan algoritma AES-128.



Gambar 3. Proses Implementasi Metode

Pada gambar 3 diatas, proses metode AES-128 dijelaskan dengan memodifikasi kunci program, sebagai berikut:

1. Proses enkripsi pada web, proses enkripsi bisa dilakukan dengan login sebagai admin dan pilih menu file enkripsi pada halaman dashboard, upload file, input password dan klik enkripsi *file*, jika berhasil *file* disimpan pada databse.

2. Saat proses dekripsi, admin menggunakan password yang sama yang digunakan saat enkripsi dan mengambil password yang telah tersimpan di database untuk memastikan bahwa proses dekripsi berjalan dengan baik dan file dapat dikembalikan ke kondisi semula.

2.5 Rancangan Pengujian

Pengujian website dilakukan melalui metode alpha testing, yang bertujuan untuk mengevaluasi aplikasi dari perspektif pengembang. Metode ini memungkinkan pengembang untuk mengamati bagaimana pengguna berinteraksi dengan aplikasi dan mengidentifikasi setiap masalah yang muncul selama penggunaan [9].

3. HASIL DAN PEMBAHASAN

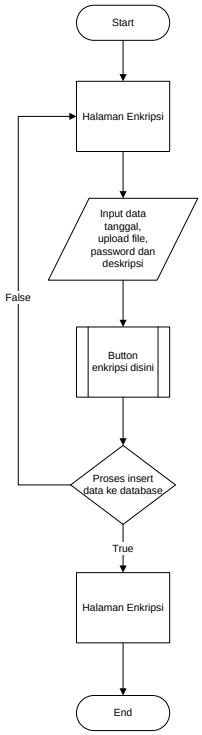
Bagian ini menyajikan hasil dari pengujian sistem yang telah dikembangkan sebelumnya, dengan menggunakan metode penelitian. Penjelasan disertai dengan gambar, tabel, dan elemen relevan lainnya untuk memperjelas hasil dan temuan dari penelitian ini.

3.1 *Flowchart*

Flowchart adalah representasi grafis yang menunjukkan langkah-langkah dan urutan prosedur dalam suatu program [10].

3.1.1 *Flowchart* Halaman Enkripsi

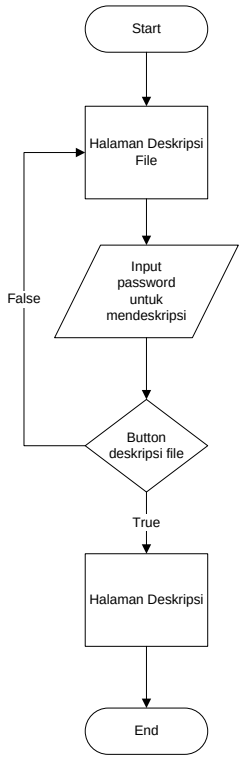
Gambar 2 menunjukkan flowchart pada halaman enkripsi, yang menjelaskan proses admin mengenkripsi file. Langkah pertama adalah mengupload file dan mengisi password. Format file yang dapat dimasukkan termasuk Excel, Word, Text, PDF, dan PowerPoint.



Gambar 4. *Flowchart* Halaman Enkripsi

3.1.2 *Flowchart* Halaman Deskripsi *File*

Gambar 3 menunjukkan alur kerja halaman dekripsi file, yang memungkinkan pengguna memproses file yang terenkripsi dengan mengembalikannya ke file asli. Pertama, pengguna memilih file bedarken statusnya, dan kemudian memberikan kata sandi untuk proses dekripsi, yang, jika kata sandi sesuai, mengembalikannya ke file asli.

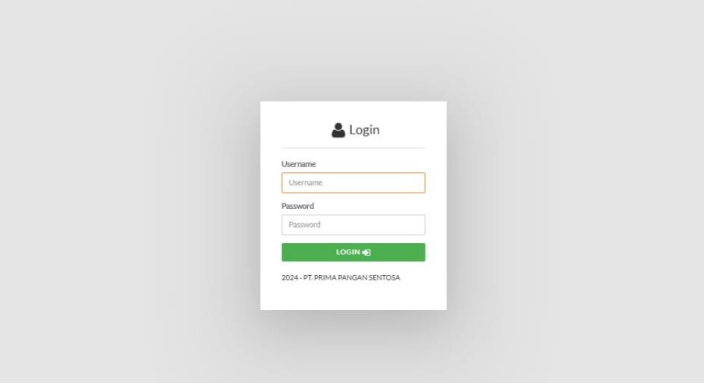


Gambar 5. *Flowchart* Halaman Deskripsi *File*

3.2 Tampilan Layar

a. Tampilan Layar Login

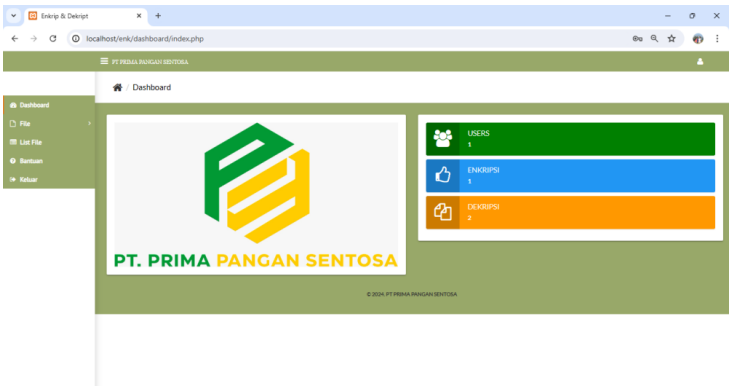
Tampilan awal pada web aplikasi Perlindungan file data pajak. Tampilan login berisikan username dan password, jika pengguna mengisi username dan password dengan benar pengguna akan dialihkan ke dalam halaman dashboard, apabila pengguna salah mengisi username dan password sistem akan menampilkan notifikasi username dan password salah.



Gambar 6. Tampilan Login

b. Tampilan Layar Dashboard

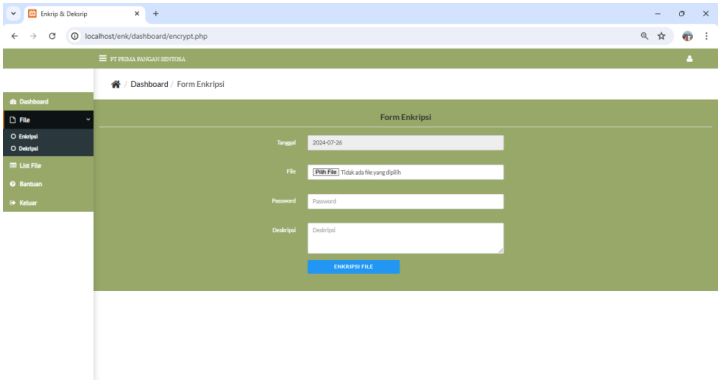
Setelah login langsung diarahkan ke tampilan Dashboard, yang mana pada menu dashboard dapat melihat logo tempat riser yaitu logo PT Prima Pangan Sentosa, tampilan banyaknya user, jumlah ata yg telah dienkripsi, dan deskripsi.



Gambar 7. Tampilan Layar Dashboard

c. Tampilan Layar Enkripsi

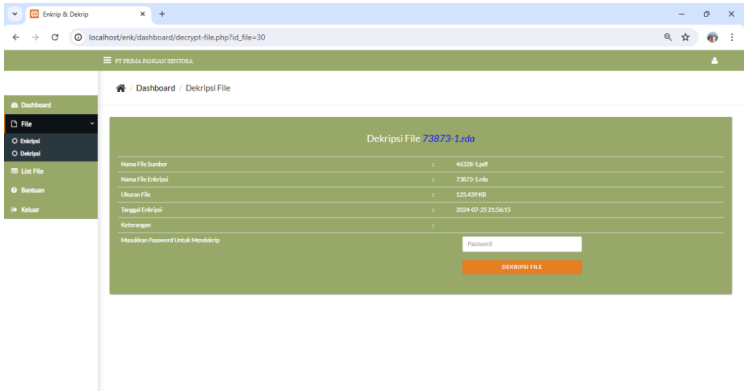
Tampilan menu file terdapat dua pilihan antara menu enkripsi dan deskripsi, dalam menu enkripsi terdapat menu form yang nantinya diisi oleh admin. Pada menu form terdiri atas tanggal, input file, password, deskripsi dan tombol button enkripsi.



Gambar 8. Tampilan Layar Enkripsi

d. Tampilan Layar Deskripsi *File*

Tampilan Deskripsi file akan muncul saat mengklik tombol deskripsi pada menu deskripsi, pada tampilan menu deskripsi file akan tertera beberapa info mengenai file yang akan di deskripsi antara lain, nama file sumber dengan format aslinya, nama file enkrispi dengan format rda, ukuran file, tanggal enkripsi, keterangan, dan yang paling penting menu password yang nantinya diisi dengan password enkripsi sebelumnya.



Gambar 9. Tampilan Layar Deskripsi File

3.3 Pengujian

Pengujian aplikasi dilakukan dengan menguji fungsionalitas sistem menggunakan metode *alpha testing*.

3.3.1 *Login*

Tabel 2 merupakan skenario pengujian fungsionalitas yang dilakukan pada bagian login.

Tabel 2. Pengujian login

Kasus dan uji coba (data normal)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input Username : admin Inpu Password : admin	Login berhasil dan diarahkan ke halaman dashboard	Login berhasil dan diarahkan ke halaman dashboard	[√]Diterima [ ]Ditolak
Kasus dan uji coba (data salah)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input Username : [input kosong] Inpu Password : [input kosong]	Menampilkan pesan error "Harap isi bidang ini" yang terdapat pada username dan password	Menampilkan pesan error "Harap isi bidang ini" yang terdapat pada username dan password	[√]Diterima [ ]Ditolak
Input Username : ferian Inpu Password : ferian	Menampilkan pesan error "username dan password salah!"	Menampilkan pesan error "username dan password salah!"	[√]Diterima [ ]Ditolak

3.3.2 Enkripsi

Tabel 3 merupakan skenario pengujian fungsionalitas yang dilakukan pada bagian pengujian enkripsi.

Tabel 3. Pengujian Enkripsi

Kasus dan uji coba (data normal)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input File : dataset.docx [maksimal 3mb] Input password : [kombinasi dengan random key] input deskripsi : [input bebas]	Menampilkan pesan “Enkripsi Berhasil”	Menampilkan pesan “Enkripsi Berhasil”	[√]Diterima [ ]Ditolak
Kasus dan uji coba (data salah)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input File : dataset.doc [maksimal 3mb] Input password : [input password 12345678910] Input deskripsi : [input bebas]	Menampilkan error dengan pesan “Perpanjang teks ini hingga 16 karakter atau lebih (saat ini anda menggunakan 11 karakter)	Menampilkan error dengan pesan “Perpanjang teks ini hingga 16 karakter atau lebih (saat ini anda menggunakan 11 karakter)	[√]Diterima [ ]Ditolak

Tabel 4. File Testing Upload Enkripsi

No	Nama File Asli	Ukuran File (KB)	Nama File setelah di enkripsi	Ukuran File setelah di enkripsi (KB)
1	Pajak.xlsx	17	79658-pajak.rda	0.0156403
2	Faktur Pajak.pdf	181	96064-faktur-pajak.rda	0.176514
3	PPN.pdf	47	89704-ppn.rda	0.04498

3.3.3 Proses Unggah

Tabel 4 merupakan skenario pengujian fungsionalitas yang dilakukan pada bagian pengujian Proses Unggah.

Tabel 5. Pengujian Proses Unggah

Kasus dan uji coba (data normal)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input File : dataset.docx Input password: [input bebas dengan panjang 16 karakter atau kombinasi dengan angka] Input deskripsi : [input dengan bebas]	Dapat menyimpan dan menampilkan daftar hasil unggah file asli dan file enkripsi serta path file di menu deskripsi	Dapat menyimpan dan menampilkan daftar hasil unggah file asli dan file enkripsi serta path file di menu deskripsi	[√]Diterima [ ]Ditolak
Kasus dan uji coba (data salah)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Tidak ada data uji			

3.3.4 Deskripsi *File*

Tabel 5 merupakan skenario pengujian fungsionalitas yang dilakukan pada bagian pengujian Deskripsi *File*.

Tabel 6. Pengujian Deskripsi *File*

Kasus dan uji coba (data normal)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input Proses : dekrip Input password: [password yang telah dibuat pada menu enkrip]	Menampilkan hasil proses dekrip	Menampilkan hasil proses dekrip	[√]Diterima [ ]Ditolak
Kasus dan uji coba (data salah)			
Data Masukan	Diharapkan	Pengamatan	Kesimpulan
Input Proses : Dekrip Input password: [password salah]	Menampilkan pesan error " Maaf, Password tidak sesuai"	Menampilkan pesan error " Maaf, Password tidak sesuai"	[√]Diterima [ ]Ditolak

Tabel 7. File Testing Upload Deskripsi

NO	Nama File Enkripsi	Ukuran setelah di Enkrpsi (KB)	Nama File Setelah di Deskripsi	Ukuran File Setelah di Deskripsi (KB)
1	79658-pajak.rda	0.0156403	72966-pajak.xlsx	17
2	96064-faktur-pajak.rda	0.176514	83649-faktur-pajak-28-jun-apr-24.pdf	181
3	89704-ppn.rda	0.04498	83649-faktur-pajak-28-jun-apr-24.pdf	47

4. KESIMPULAN

Setelah dilakukan implementasi dan uji coba Aplikasi Perlindungan File Data menggunakan algoritma AES-128 Pada PT. Prima Pangan Sentosa. Berdasarkan analisis dan evaluasi yang telah dilakukan, dapat disimpulkan bahwa Penerapan Algoritma Advanced Encryption Standard (AES-128) berhasil mengamankan file data dalam format xlsx, xls, docx, doc, txt, pdf, ppt, pptx. Berdasarkan Kesimpulan diatas, terdapat beberapa saran untuk meningkatkan pengembangan Program web antara lain, perlu dilakukan pengembangan lebih lanjut pada program web yang ada, seperti meningkatkan infrastruktur agar bisa digunakan pada semua format file.

DAFTAR PUSTAKA

[1] A. Randi, K. Lazuardy, S. Chandra, and A. Dharma, "Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android," *J. Ilmu Komput. dan Sist. Inf.*, vol. 3, no. 2, pp. 1–10, 2020.

[2] M. I. Affandy *et al.*, "Kombinasi Kriptografi Affine Cipher dengan Algoritma AES (Advanced Encryption Standart) Untuk Pengamanan Data Gaji Karyawan Pada CV. Interyasa Lubuk Pakam," *J. CyberTech*, 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/

[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[4] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.v4i2.428.

[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, 2021, doi: 10.36080/skanika.v4i1.2216.

[6] D. Aldianto and A. Wibowo, "Implementasi Kriptografi Dengan Aes 256 Dan Md 5 Untuk Mengamankan Data Di Pt. Ebdesk Teknologi," *Pros. Semin. Nas. ...*, vol. 2, no. September, pp. 288–295, 2023, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/article/view/972%0Ahttps://senafti.budiluhur.ac.id/index.php/senafti/article/download/972/392

[7] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[8] H. H. Amirullah, "Aplikasi Keamanan Berkas d engan Enkripsi A ES d an Biometrik Sidik Jari Berbasis Android Android File Security Application w ith A ES Encryption a nd Fingerprint Authentication," vol. 14, no. 1, pp. 23–32, 2024.

[9] B. Santosa, F. Ahmad Juni Haryanto, R. Indra Perwira, and D. B. Prasetyo, "Implementation of Steganography on Voice Over Internet Protocol (VOIP)," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 5, pp. 195–204, 2019, doi: 10.28989/senatik.v5i0.334.

[10] A. Zalukhu, P. Swingly, and D. Darma, "Perangkat Lunak Aplikasi Pembelajaran Flowchart," *J. Teknol. Inf. dan Ind.*, vol. 4, no. 1, pp. 61–70, 2023, [Online]. Available: https://ejurnal.istp.ac.id/index.php/jtii/article/view/351