KRESNA: Jurnal Riset dan Pengabdian Masyarakat
Volume 4, Nomor 1, Mei, 2024, Hal: 62-71 E-ISSN: 2809-6509

Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web

Application of Advanced Encryption Standard (AES-512) Algorithm for Web-Based File Security

Nurfauzan Humam Khoirudin[1], Windarto[2]*

[1,2]FakultasTeknologi Informasi
Universitas Budi Luhur
Email: [1]1811502614@student.budiluhur.ac.id, [2*]windarto@budiluhur.ac.id
(* corresponding author)

Abstract

The development of information technology has significantly impacted human life, especially in facilitating faster and easier data exchange. However, data security remains a major challenge due to the potential threats posed by illegal access to sensitive information. Cryptography, particularly using the Advanced Encryption Standard (AES) algorithm, has become the primary choice for securing corporate data. This research aims to enhance the security of important files at PT. Skemanusa Consultama Teknik by implementing AES-512 for data encryption and decryption. This research adopts a waterfall approach, starting from problem formulation, literature review, system design, to implementation using AES-512. Testing was conducted to compare the encryption and decryption speeds of AES-512 with other approaches such as AES-RSA combinations. The test results indicate that AES-512 is effective in securing corporate files with optimal encryption and decryption times. The application of AES-512 in this cryptographic application has successfully created a system capable of securing files such as financial reports, tax returns, and other crucial documents at PT. Skemanusa Consultama Teknik without compromising system performance. The results demonstrate a significant improvement in data security, addressing the weaknesses of traditional data storage methods like computer folders or flash drives.

Keywords **:** *Encryption, Decryption, Advanced Encryption Standard (AES-512)*

Abstrak

Perkembangan teknologi informasi telah membawa dampak signifikan terhadap kehidupan manusia, terutama dalam pertukaran data yang semakin mudah dan cepat. Namun, keamanan data menjadi tantangan utama dalam konteks ini, mengingat potensi ancaman dari akses ilegal terhadap informasi sensitif. Kriptografi, khususnya menggunakan Algoritma Advanced Encryption Standard (AES), menjadi pilihan utama untuk mengamankan data perusahaan. Penelitian ini bertujuan untuk meningkatkan keamanan file-file penting di PT. Skemanusa Consultama Teknik dengan menerapkan AES-512 untuk proses enkripsi dan dekripsi data. Metode penelitian ini mengadopsi pendekatan waterfall, dimulai dari perumusan masalah, studi literatur, perancangan sistem, hingga implementasi menggunakan AES-512. Pengujian dilakukan untuk membandingkan kecepatan enkripsi dan dekripsi dengan metode AES-512 terhadap pendekatan lain seperti kombinasi AES dan RSA. Hasil pengujian menunjukkan bahwa AES-512 efektif dalam mengamankan file-file perusahaan dengan waktu enkripsi dan dekripsi yang optimal. Penerapan AES-512 pada aplikasi kriptografi ini berhasil menciptakan sistem yang dapat mengamankan berkas-berkas seperti laporan keuangan, SPT pajak, dan dokumen-dokumen penting lainnya di PT. Skemanusa Consultama Teknik tanpa mengorbankan kinerja sistem. Hasilnya menunjukkan peningkatan signifikan dalam keamanan data, mengatasi kelemahan penyimpanan data tradisional seperti folder komputer atau flashdisk.

Kata kunci : Enkripsi, Dekripsi, Advanced Encryption Standard (AES-512)

1. PENDAHULUAN

Perkembangan teknologi informasi memiliki dampak yang sangat besar terhadap kehidupan manusia. Hal ini tercermin dari kemudahan dalam pertukaran data yang kini tidak lagi terbatas oleh ruang dan waktu. Keamanan data menjadi sangat penting, mengingat perlunya melindungi informasi rahasia dari akses yang ilegal. Kriptografi merupakan sebuah metode pengamanan data yang sering digunakan untuk menjaga keamanan data perusahaan, seperti yang pernah di lakukan penelitian yang sudah ada yang memiliki judul Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Penelitian ini memiliki tujuan untuk memahami konsep kriptografi agar bisa mengamankan informasi berbasis teks dengan mengimplementasikan algoritma Advanced Encryption Standard (AES). Algoritma Advanced Encryption Standard (AES) dipilih karena memiliki kemampuan dalam mengenkripsi dan mendekripsi data. Algoritma Advanced Encryption Standard (AES) digunakan dalam penelitian ini karena memiliki kecepatan enkripsi dan dekripsi yang tinggi, analisis statistik dan perhitungan error. Selain itu, algoritma Advanced Encryption Standard (AES) tidak memiliki serangan analisis histogram atau analisis statistik menggunakan koefisien korelasi [1].

Salah satu permasalahan yang menjadi fokus utama adalah rendahnya tingkat keamanan *file-file* penting di instansi atau pemerintahan. Ancaman juga datang dari pihak internal yang mungkin memiliki niat buruk terhadap data. Pada kriptografi memiliki beberapa algoritma yang bisa digunakan seperti contohnya *Algoritma Advanced Encryption* (AES) yang pernah diterapkan oleh penelitian yang sudah pernah dilakukan oleh eka putrid kk, dengan judul Implementasi enkripsi dengan standar enkripsi Advanced Encryption Standard (AES) 128-bit dan steganografi menggunakan metode Java desktop-based End of File (EOF) di Dinas Pendidikan Kabupaten Tangerang. Penelitian ini menciptakan sistem keamanan yang menggunakan teori kebingungan untuk mengirimkan dan menyimpan informasi dalam bentuk kata sandi atau kode khusus. Kombinasi teknik enkripsi dan steganografi memberikan tingkat keamanan data yang sangat tinggi sehingga menjaga keamanan data tanpa mengubah gambar visual. Algoritma enkripsi yang digunakan adalah metode enkripsi Advanced Encryption Standard (AES) 128-bit dan metode steganografi End of File (EOF) [2]. Dan ada juga penelitian yang tulis oleh Hermawan dkk, dengan judul Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA. Pada penetian yang dilakukan oleh Hermawan dkk, meraka menggunakan metode AES dan RSA yang dikombinasikan untuk pengamanan data [3]

Berdasarkan latar belakang dan penelitian terdahulu, penulis mengembangkan sebuah aplikasi kriptografi yang dapat diterapkan di PT. Skemanusa Consultama Teknik dengan menggunakan metode Kriptografi Algoritme *Advanced Encryption Standard* (AES-512). Aplikasi yang dibuat ini memiliki perbedan dengan penelitian yang di lakukan oleh Herman dkk, yang mengunakan kombinasi AES dan RSA, sedangkan pada penelitian ini hanya menggunakan satu metode agar bisa mempersingkat proses enkripsi. Berbeda juga dengan penelitian yang di lakukan oleh eka putrid kk, yang mengabungkan metode enkripsi dan steganografi pada penelitianya itu, sedangkan pada pada penelitian ini hanya mengunakan metode enkripsi.

Dengan hanya menggunakan satu algoritme *Advanced Encryption Standard* (AES-512) dan metode enkripsi, diharapkan dapat memberikan tingkat keamanan yang maksimal terhadap *file-file* penting perusahaan, seperti SPT pajak, laporan keuangan, dan laporan pajak. Rumusan masalah yang diajukan mencakup peningkatan keamanan data serta penerapan AES-512 untuk proses enkripsi dan dekripsi data di PT. Skemanusa Consultama Teknik.

2. METODE PENELITIAN

2.1. Data Penelitian

Pada penelitian yang dilakukan kali ini menggunakan data instansi atau perusahaan di PT. Skemanusa Consultama Teknik dengan mengumpulkan data langsung. Data yang rentan terhadap kebocoran dan peretasan merupakan data laporan pajak perusahaan, laporan keuangan perusahaan, dan data SPT pajak perusahaan karena penyimpanan yang kurang aman dalam *folder* komputer atau *flashdisk*. Untuk meningkatkan keamanan, perusahaan membuat program enkripsi dan dekripsi data [4].

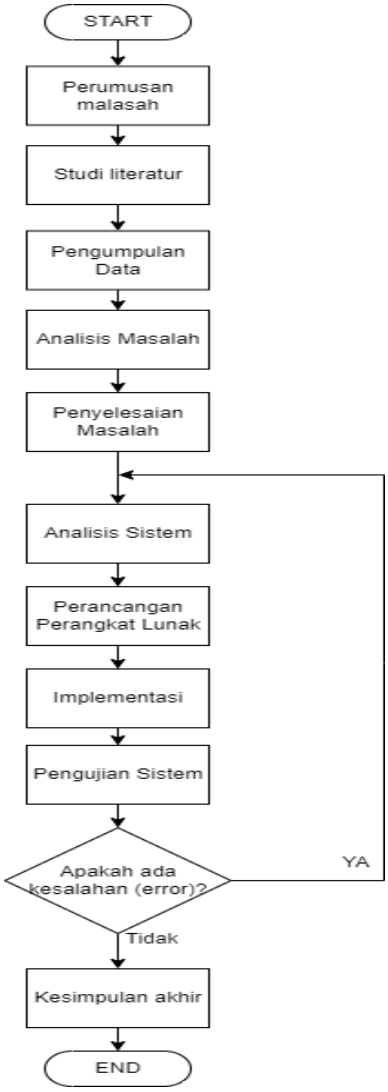
2.2. Metode Pembanding

Penelitian terdahulu menggunakan kombinasi AES dan RSA untuk enkripsi data, sementara penelitian sekarang hanya menggunakan AES. Pada penelitian ini yang hanya menggunakan satu metode dan tidak menggunakan kombinasi metode, karena menggunakan satu metode pada penelitian ini menyebabkan tingkat keamanan yang rendah dibandingkan dengan metode kombinasi, karena pesan hanya melewati satu proses enkripsi. AES digunakan untuk enkripsi dan dekripsi, sedangkan RSA digunakan untuk kunci enkripsi dan dekripsi.

Pengujian menunjukkan bahwa rata-rata waktu yang digunakan untuk enkripsi RSA kurang dari 8ms, sementara enkripsi metode AES memerlukan waktu yang lebih lama. Namun, uji dekripsi AES lebih cepat dari RSA. Hal ini menunjukkan setiap implementasi metode yang berbeda memiliki kelebihan dan kekurangan masing-masing dalam pengujian data [5].

2.3. Penerapan Metode

Metode penelitian ini mengadopsi metode *waterfall*, diawali dengan perumusan masalah pada penelitian ini, kemudian melakukan tinjauan pustaka dan membaca hasil penelitian yang sudah ada dan beberapa buku pendukung penelitian. Tujuanya adalah supaya hasil dari penelitian ini tidak melenceng dari tujuan yang telah ditentukan sebelumnya. menjelaskan langkah-langkah yang digunakan pada penerapan metode yang dilakukan pada penelitian ini [6].

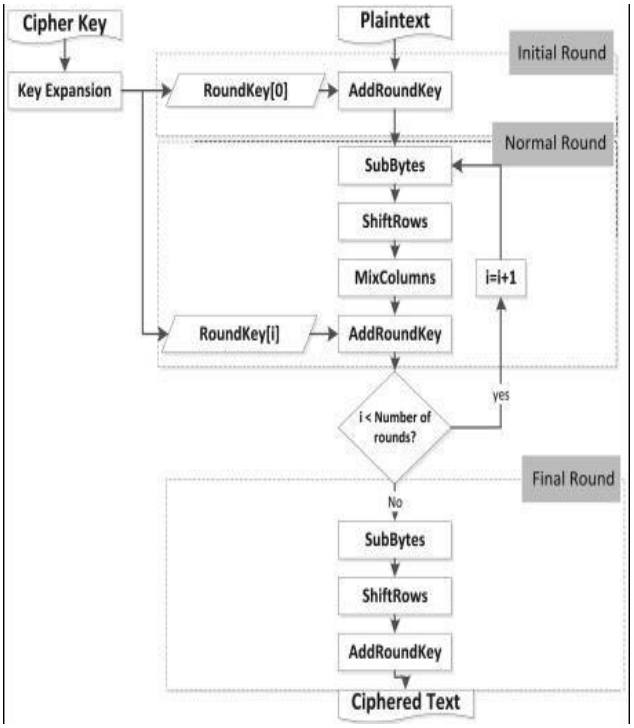


Gambar 1: Research Stage

Pada tahap ini, penelitian fokus pada pembangunan sistem pengamanan data perusahaan seperti laporan pajak, keuangan, SPT pajak, dan data karyawan PT. Skemanusa Consultama Teknik dengan metode kriptografi AES-512. Studi literatur dilakukan dengan mengulas 10 *paper* jurnal dari 2019 hingga 2022, mencakup berbagai algoritme kriptografi seperti AES, RSA, dan teknik lainnya. Data dikumpulkan melalui wawancara dan observasi di perusahaan. Selanjutnya, dilakukan analisis data, perancangan aplikasi enkripsi dan dekripsi *file*, serta implementasi menggunakan metode *waterfall*. Tahap pengujian sistem *blackbox* dilakukan untuk memastikan sistem berjalan sesuai tujuan. Hasilnya, penerapan AES-512 berhasil mengamankan *file* [7].

2.4. Enkripsi Algoritme *Advanced Encryption Standard* (AES)

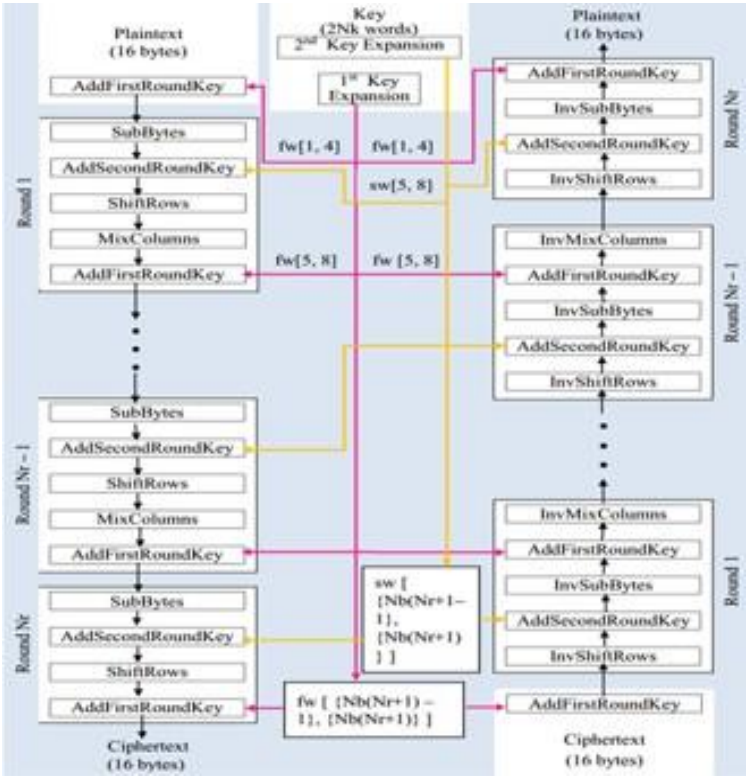
Proses enkripsi yang terjadi ketika menggunakan algoritma AES-512 ada 4 jenis perubahan *byte*, yang terdri dari *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Transformasi dimulai dengan *AddRoundKey* pada awal proses, kemudian melalui *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* lagi sesuai dengan nilai *round*. Proses ini dikenal sebagai fungsi *round function*. Pada tahap akhir, transformasi *MixColumns* tidak dilakukan seperti pada tahap sebelumnya [8].



Gambar 2: Encryption Process Advanced Encryption Standard (AES)

2.5. Dekripsi *Algoritme Advanced Encryption Standard* (AES)

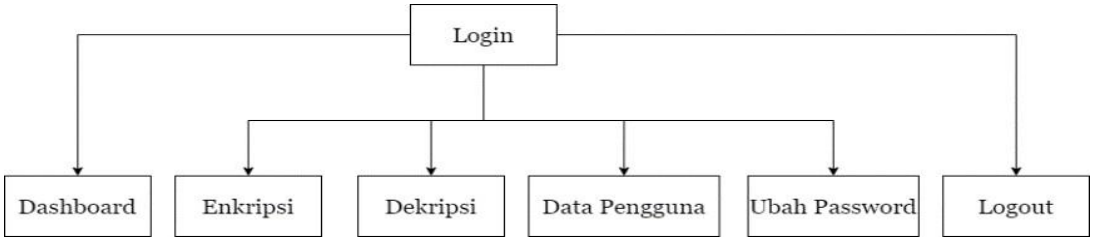
Proses dekripsi pada AES melibatkan transformasi *cipher* yang dibalik agar bisa menghasilkan *inverse cipher*. Tahapan pada proses ini meliputi *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* [9]. Untuk bisa menjelaskan secara fisual dari proses dekripsi pada algoritma *Advanced Encryption Standard* (AES) saya mengunakan gambar berikut.



Gambar 3: Decryption Process Advanced Encryption Standard (AES)

2.6. Rancangan Menu

Program ini memiliki beberapa Halaman yang akan dibuat, termasuk Halaman *Login*, Halaman Menu *Dashboard*, Halaman Menu Enkripsi, dan Halaman Menu Dekripsi. Pada Halaman *Login*, pengguna harus masuk dengan mengisi *username* dan *password* sebelum menggunakan aplikasi. Menu Enkripsi memungkinkan pengguna untuk mengenkripsi *file* dengan mengisi berkas, *password*, dan deskripsi. Menu Dekripsi digunakan untuk mengembalikan berkas yang sudah dienkripsi menjadi aslinya dengan memasukkan *password* dan memilih dekripsi *file*. Program ini memproses langkah-langkah tersebut untuk penggunaan yang lebih aman dan efisien [10].

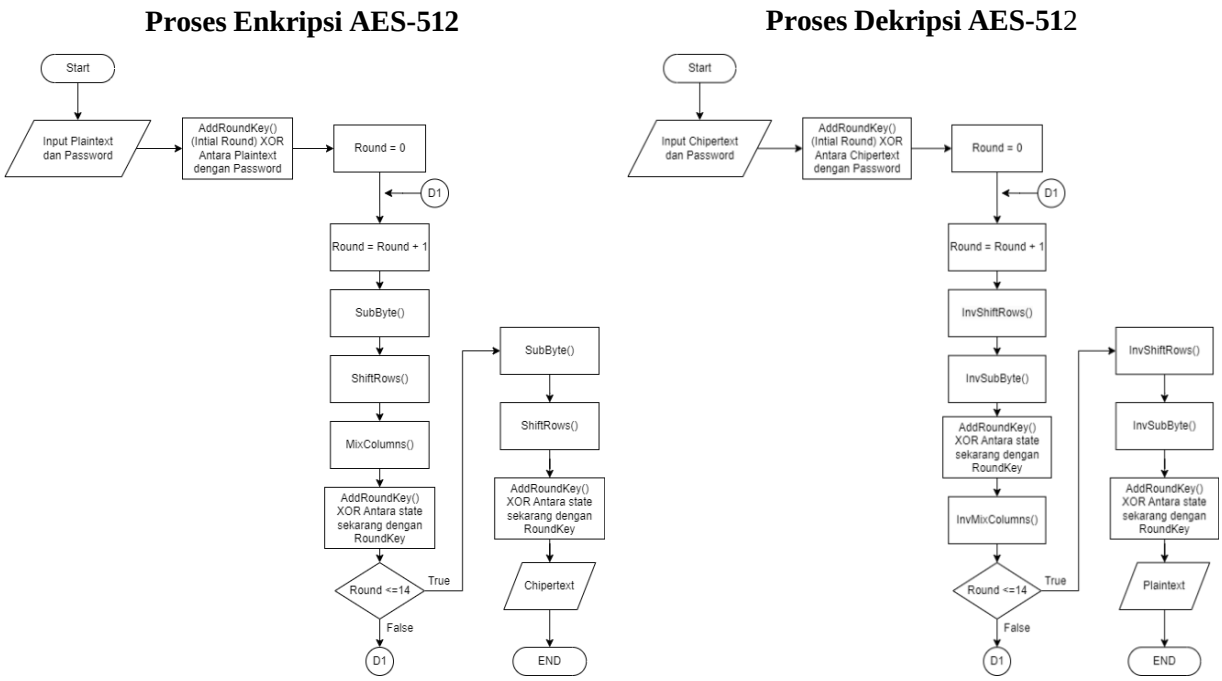


Gambar 4: Menu Design

3. HASIL DAN PEMBAHASAN

3.1. *Flowchart* Enkripsi dan Dekripsi AES-512

Pada Gambar 5 menggambarkan *flowchart* yang menjelaskan tahap-tahap dari enkripsi dan dekripsi kriptografi AES-512.

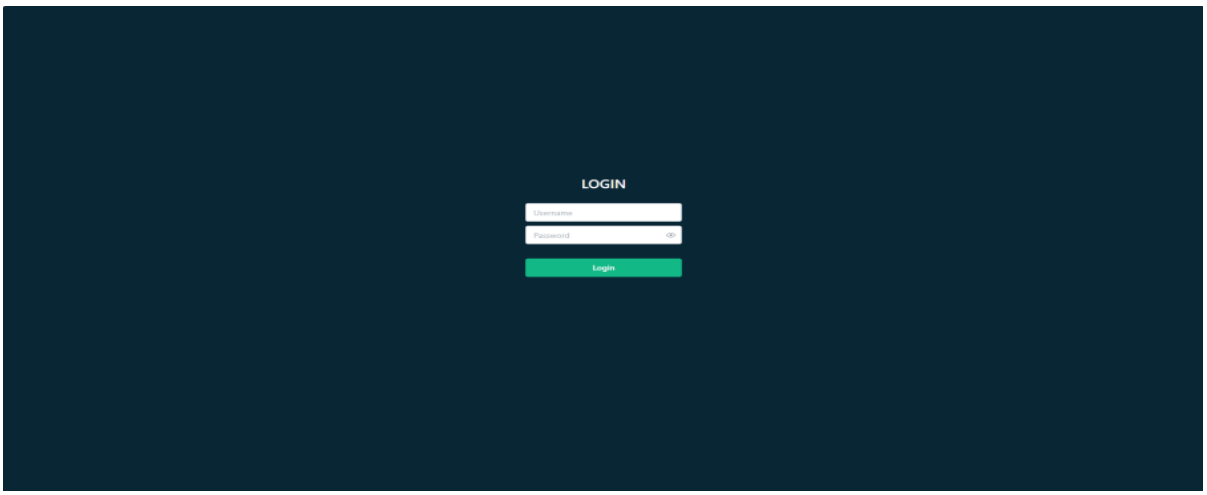


Gambar 5: AES-512 Encryption and Decryption Flowchart

3.2. Tampilan Layar

3.2.1. Tampilan Layar Halaman *Login*

Pada tampilan halaman *login* ini pengguna harus memasukkan id pengguna dan kata sandi untuk dapat masuk ke halaman *dashboard* seperti yang ditunjukkan pada Gambar 6.



Gambar 6: Login Page Screen View

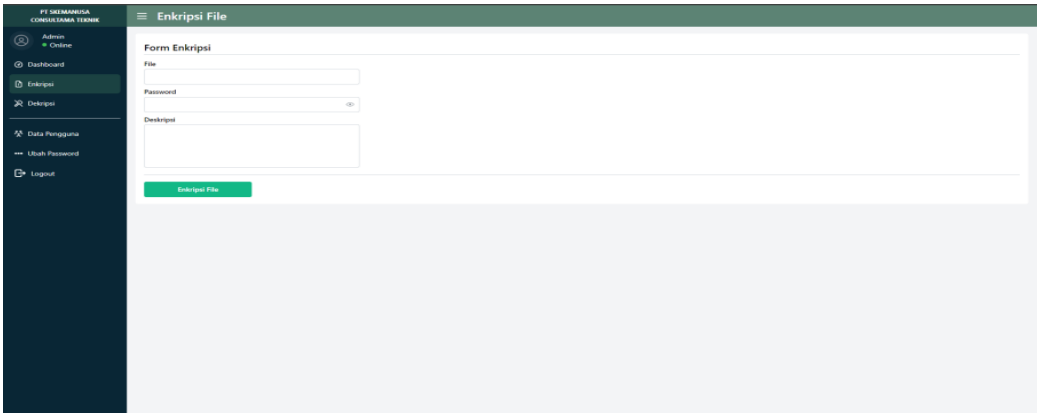
3.2.2. Tampilan Layar Halaman *Dashboard*

Pada halaman *dashboard* aplikasi ini, pengguna dapat mengakses beberapa menu, termasuk Berkas dan Daftar Hasil. Di bawah menu Berkas terdapat sub menu Data Berkas yang berisi Enkripsi Berkas dan Dekripsi Berkas. Gambar 7 menampilkan tampilan halaman *dashboard*.

Gambar 7: *Dashboard Page Screen View*

3.2.3. Tampilan Layar Halaman Form Enkripsi

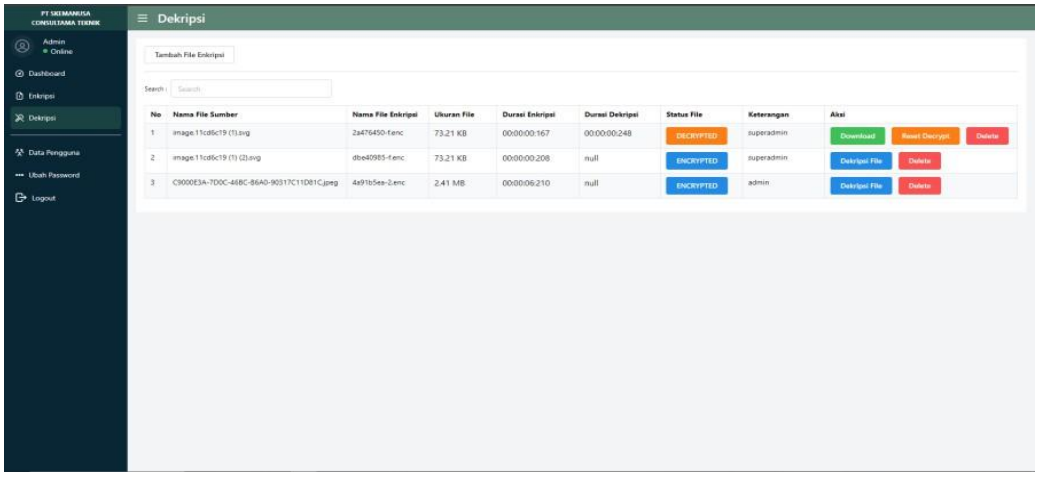
Halaman *Form* Enkripsi memungkinkan pengguna untuk memilih *file* yang akan dienkripsi, kemudian mengisi kata sandi, keterangan, dan memilih tombol enkripsi. Gambar 8 menampilkan tampilan halaman enkripsi.



Gambar 8: *Screen View of Encryption Form Page*

3.2.4. Tampilan Layar Halaman Tabel Dekripsi

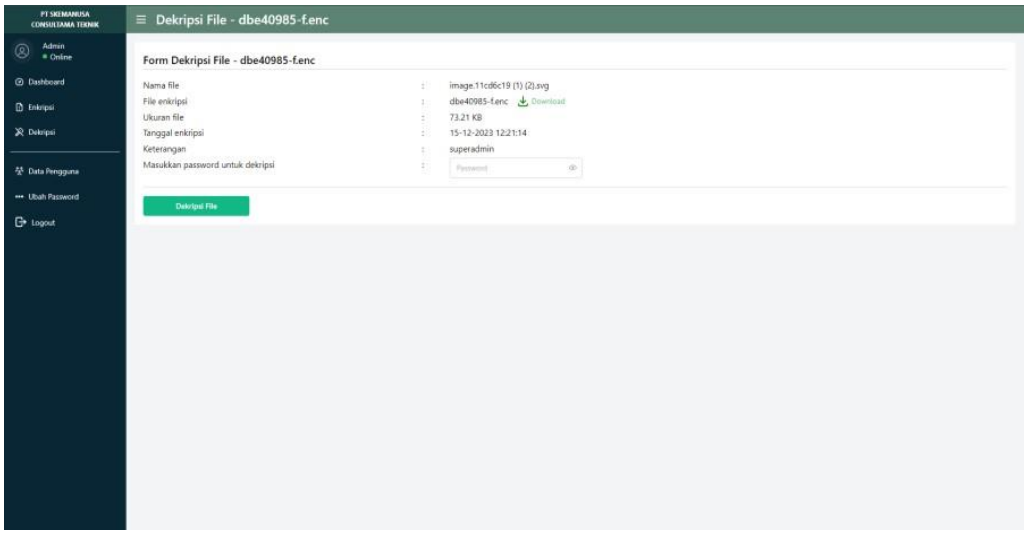
Halaman tabel dekripsi pada formulir ini menampilkan *file-file* yang telah dienkripsi dan akan didekripsi. Gambar 9 menunjukkan tampilan halaman dekripsi.



Gambar 9: *Decryption Table Page Screen View*

3.2.5. Tampilan Layar Halaman Form Dekripsi Berkas

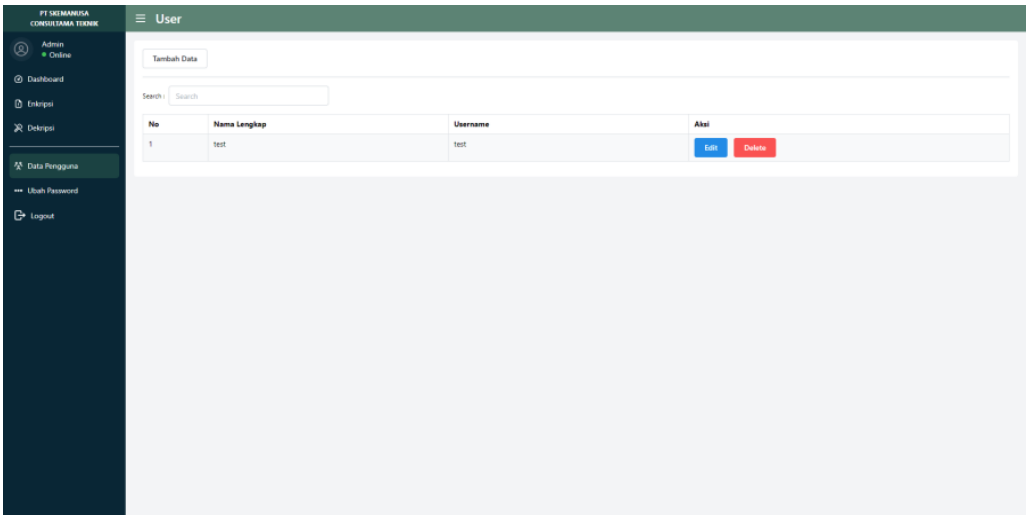
Halaman *form* dekripsi berkas memerlukan pengguna untuk memasukkan kata sandi atau kunci yang sama yang digunakan saat proses enkripsi. Gambar 10 menampilkan tampilan form dekripsi berkas.



Gambar 10: *File Decryption Page Screen View*

3.2.6. Tampilan Layar Halaman Data Pengguna

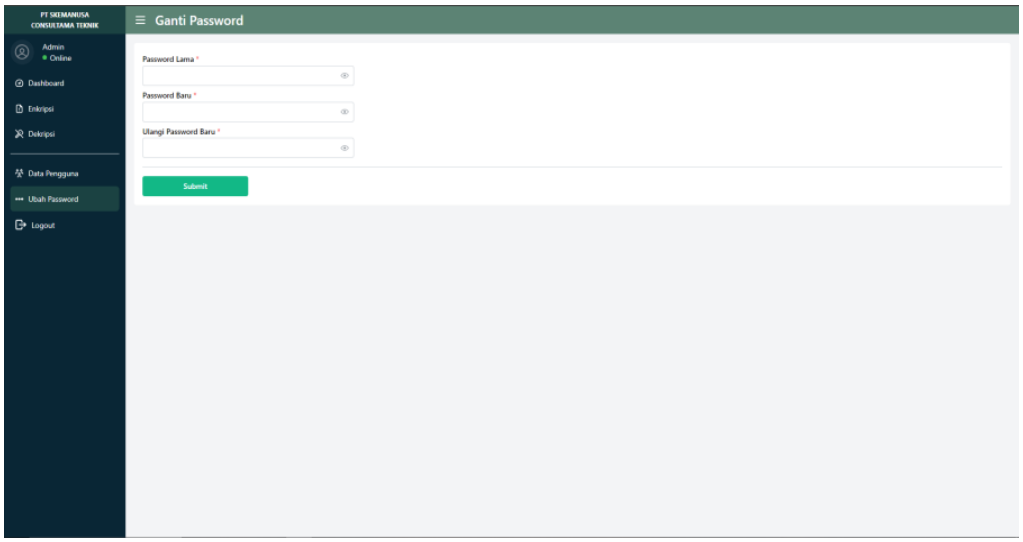
Tampilan halaman data pengguna adalah halaman yang menampilkan informasi pengguna dan memungkinkan untuk menambahkan, menghapus, dan mengubah data pengguna. Hal ini ditunjukkan dalam Gambar 11.



Gambar 11:: *User Data Page Screen View*

3.2.7. Tampilan Layar Halaman Ubah Password

Tampilan halaman ubah *password* adalah halaman untuk mengubah kata sandi pengguna. Hal ini ditunjukkan dalam Gambar 12.



Gambar 12: Change Password Page Screen View

3.2.8. Hasil Pengujian

Tabel 1 adalah hasil dari proses enkripsi berkas yang dilakukan oleh sistem menggunakan aplikasi. Berikut adalah tabel hasil pengujian berkas.

Table 1. Encryption Testing Results

No	Nama *File* Awal	Ukuran *File*	Nama *File* Hasil Enkripsi	Ukuran *File* Setelah Enkripsi	Durasi Enkripsi	Keterangan
1	Account Payable Customer.xlsx	143 KB	dd795ecc-3.enc	143 KB	5.19 Detik	BERHASIL
2	Wajib Lapor PT. SKEMANUSA 2019-2020.pdf	540 KB	4a8885b7-a.enc	539.2 KB	1.68 Detik	BERHASIL
3	Denah Perusahaan.pptx	3.6 MB	20e771b-b.enc	3.6 MB	7.43 Detik	BERHASIL
4	Surat Pernyataan.doc	63 KB	6a301197-0.enc	63 KB	0.41 Detik	BERHASIL
5	Pembahasan.txt	3.7 KB	d2158c1-4.enc	3.7 KB	0.28 Detik	BERHASIL
6	IMG_20231005_210.jpg	151 KB	e4160361-1.enc	151 KB	0.52 Detik	BERHASIL

Dari tabel di aras bisa dilihat hasil uji coba dari sistem yang dibuat, hasil dari enkripsi berhasil dengan ukuran file yang sama dengan file aslinya. Durasi tercepat dari proses enkripsi terdapat pada file jpg yang berdurasi enkripsinya 0.52 detik dengan hasil berhasil, durasi terlama enkripsi berada pada file excel yang berdurasi 5.19 detik dengan hasil berhasil.

Table 2. Decryption Testing Results

No	Nama *File* Enkripsi	Ukuran *File* Enkripsi	Nama *File* Hasil Dekripsi	Ukuran *File* Dekripsi	Durasi Enkripsi	Keterangan
1	dd795ecc-3.enc	143 KB	Account Payable Customer.xlsx	143 KB	0.67 detik	BERHASIL
2	4a8885b7-a.enc	539.2 KB	Wajib Lapor PT. SKEMANUSA 2019-2020	540 KB	1.19 detik	BERHASIL
3	20e77717b-b.enc	3.6 MB	Denah Perusahaan.pptx	3.6 MB	7.56 detik	BERHASIL
4	6a301197-0.enc	63 KB	Surat Pernyataan.doc	63 KB	0.51 detik	BERHASIL
5	d21585c1-4.enc	3.7 KB	Pembahasan.txt	3.7 KB	0.39 detik	BERHASIL
6	e4160361-1.enc	151 KB	IMG_20231005_201109_210.jpg	151 KB	0.73 detik	BERHASIL

Dari tabel di aras bisa dilihat hasil uji coba dari sistem yang dibuat, hasil dari *decryption* berhasil dengan ukuran file yang sama dengan file aslinya. Durasi tercepat dari proses *decryption* terdapat pada file txt yang berdurasi *decryption* 0.39 detik dengan hasil berhasil, durasi terlama *decryption* berada pada file pptx yang berdurasi 7.56 detik dengan hasil berhasil.

4. KESIMPULAN

Setelah perancangan dan pembuatan sistem, dilanjutkan dengan implementasi, dapat disimpulkan dibagi menjadi 3, yaitu:

a. Pada penelitian yang dilakukan, ditemukannya kebocoran data di PT. Skemanusa Consultama Teknik disebabkan dari cara penyimpanan data yang dilakukan oleh perusahan hanya dalam bentuk folder di komputer dan flashdisk.

b. Penelitian yang dilakukan saya kali ini menciptakan suatu sistem yang bertujuan untuk meningkatkan keamanan data yang dianggap penting di PT. Skemanusa Consultama Teknik.
c. PT. Skemanusa Consultama Teknik membuat sistem pengaman data dengan cara enkripsi dan dekripsi mengimplementasikan cara kerja kriptografi dengan Algoritma *Advanced Encryption Standard* (AES-512).

DAFTAR PUSTAKA

[1] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022.
[2] A. E. Putri, A. Kartikadewi, and L. A. A. Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Applied Information System and Management (AISM)*, vol. 3, no. 2, pp. 69–78, Jan. 2021.
[3] A. Hermawan, E. Iman, and H. Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 325–330, 2021.
[4] R. Toyib and A. Wijaya, "Analisis Perbandingan Algoritma Simetris Rivest Code 5 Dengan Algoritma Simetris Rivest Code 6," *Jurnal Informatika Upgris*, vol. 4, no. 2, pp. 203–209, 2018.
[5] C. Yadav, V. Yadav, and J. Kumar, "Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-based Encryption in Cloud Environment," *International Journal of Electrical and Electronics Research*, vol. 9, no. 3, pp. 48–56, 2021.
[6] A. K. Azad and M. Y. Mollah, "EAES: Extended advanced encryption standard with extended security," *Advances in Science, Technology and Engineering Systems*, vol. 3, no. 3, pp. 51–56, 2018.
[7] H. H. S. Pasaribu, S. S. Dhilon, P. D. Galingging, and S. Syaputra, "Implementasi SHA 512 BIT on Routingurl," *Jurnal Ipteks Terapan: Research of Applied Science and Education*, vol. 17, no. 3, p. 2023, 2023.
[8] G. Dhanalakshmii and G. V. S. George, "An Enhanced Data Integrity for the E-Health Cloud System using a Secure Hashing Cryptographic Algorithm with a Password Based Key Derivation Function2 (KDF2)," *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 290–297, Sep. 2022.
[9] F. Fadlullah, M. Tahir, B. P. Bintari, M. L. Dewi, and M. F. Ilmy, "Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi," *Jurnal Bintang Pendidikan Indonesia (JUBPI)*, vol. 1, no. 2, pp. 251–263, 2023.
[10] D. Aldianto and A. Wibowo, "Implementasi Kriptografi Dengan AES 256 dan MD 5 Untuk Mengamankan Data di PT. Ebdesk Teknologi," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi*, vol. 2, no. 2, 2023.