2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI *ADVANCED ENCRYPTION STANDARD* (AES-128) UNTUK APLIKASI KEAMANAN FILE PADA YAYASAN PERHIMPUNAN INTI

Achmad Fauzan[1], Mufti[2*], Ferdiansyah[3], Purwanto[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1]achmad190898@gmail.com, [2*]mufti@budiluhur.ac.id, [3]ferdiansyah@budiluhur.ac.id, [4]purwanto@budiluhur.ac.id
(* : *corresponding author*)

Abstrak- Yayasan Perhimpunan INTI (Indonesia-Tionghoa) sebagai lembaga yang berpartisipasi dalam organisasi sosial yang bersifat nasional, bebas, mandiri, nirlaba, dan nonpartisan. Yayasan Perhimpunan INTI memiliki urusan internal terkait informasi keuangan, informasi pegawai yang dapat merugikan instansi. Oleh karena itu, untuk mengamankan data yang memungkinkan untuk mengantisipasi terjadinya kebocoran data ke pihak yang tidak bertanggung jawab, diperlukan teknologi pengamanan data dengan sistem penyandian (encryption). Data yang digunakan dalam penelitian ini adalah data keuangan, data karyawan dan beberapa data lainnya yang merupakan dokumen penting pada Yayasan Perhimpunan INTI. Pada penelitian ini menggunakan algoritma kriptografi Advanced Encryption Standard 128-bit (AES 128-bit). Algoritma keriptografi AES-128 bertujuan untuk enkripsi dan dekripsi file. Waktu untuk menyelesaikan proses enkrip dan dekrip sebanding dengan ukuran filenya (semakin besar ukuran file yang akan diproses, semakin lambat proses enkrip dan dekrip, dan sebaliknya untuk file yang berukuran kecil). Dalam aplikasi ini hanya dapat menggunakan dokumen dengan ekstensi .doc , .docx , .xls, .xlsx, .ppt, .pptx. Dengan adanya aplikasi pengamanan file pada Yayasan Perhimpunan INTI dapat mengantisipasi terjadinya kebocoran data ke pihak yang tidak bertanggung jawab.

Kata Kunci: Kriptografi, Keamanan Data, Pengamanan Data, File, Advanced Encryption Standard.

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES-128) FOR FILE SECURITY APPLICATION IN PERHIMPUNAN INTI FOUNDATION

Abstract- *The INTI Association Foundation (Indonesian-Chinese) as an institution that participates in social organizations that are national, free, independent, non-profit and non-partisan. The INTI Association Foundation has internal affairs related to financial information, employee information that can be detrimental to agencies. Therefore, to secure data that allows for anticipating data leakage to irresponsible parties, data security technology with an encryption system is needed. The data used in this study are financial data, employee data and some other data which are important documents at the INTI Association Foundation. In this study using the Advanced Encryption Standard 128-bit (AES 128-bit) cryptographic algorithm. The AES-128 cryptographic algorithm is intended for file encryption and decryption. The time to complete the encryption and decryption process is proportional to the file size (the larger the file size to be processed, the slower the encryption and decryption process will be, and vice versa for small files). In this application you can only use documents with the extension .doc , .docx , .xls, .xlsx, .ppt, .pptx. With the existence of a file security application at the INTI Association Foundation, it can anticipate data leakage to irresponsible parties.*

Keywords*: Cryptography, Data Security, Data Security, Files, Advanced Encryption Standards.*

1. PENDAHULUAN

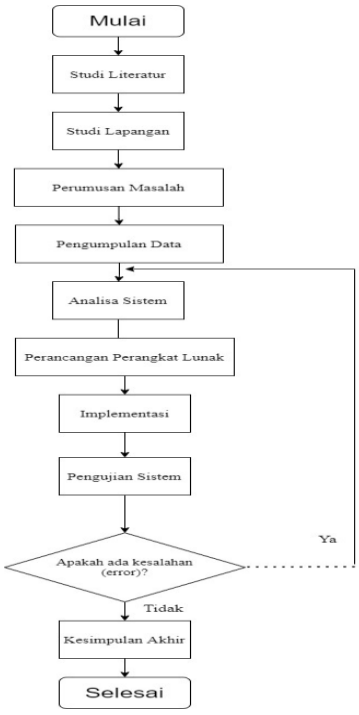
Pertumbuhan teknologi data yang pesat serta telekomunikasi membolehkan orang buat bertukar data dengan kilat serta akurat, yang ialah perihal mendasar dalam bisnis ataupun organisasi [1]. Kelebihan teknologi dalam informasi serta data malah bisa merugikan pengguna yang tidak menguasai keamanan data. Oleh sebab itu, buat mengamankan informasi yang membolehkan terbentuknya penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab, dibutuhkan sesuatu metode pengamanan informasi dengan sistem penyandian(*encryption*)[2].

Kriptografi merupakan ilmu melindungi kerahasiaan pesan dengan mengenkripsinya dalam wujud yang tidak bisa lagi dimengerti. Enkripsi mempunyai 2 proses ialah enkripsi serta dekripsi. Pesan terenkripsi diucap bacaan biasa sebab siapa juga bisa dengan gampang membaca serta menguasai data ini. Algoritma yang digunakan buat mengenkripsi serta mendekripsi bacaan biasa mengaitkan pemakaian sebagian tipe kunci[3]. *Advanced Encryption Standard*(AES) merupakan blok kode simetris yang mengambil alih algoritma Informasi *Encryption Standard*(DES). Algoritma AES mempunyai dimensi blok senantiasa 128 bit dengan panjang kunci yang berbeda. Kunci AES 128 memakai proses *loop* yang diucap *loop* yang berisi 10 putaran pola matriks 4x4, tiap pola matriks terdiri dari 1 byte ataupun 8 bit buat enkripsi serta dekripsi[4].

Riset ini mempraktikkan algoritme kriptografi AES- 128, dengan riset lebih dahulu yang memakai algoritme RC4 buat mengamankan file[5]. Algoritma *Advance Encryption Standart*(AES) 128 bisa menolong mengamankan informasi lebih efisien dibandingkan algoritma yang lain yang mana AES 128 mempunyai proses enkripsi sampai 48% serta proses dekripsi 45%[6].

2. METODE PENELITIAN

Buat ini, tata cara dijadikan selaku panduan berarti dalam melaksanakan riset. Permasalahan tersebut dirancang dengan teliti supaya hasil yang diperoleh tidak bisa berhubungan dengan tujuan dini yang sudah diresmikan lebih dahulu. Gambar 1 merupakan tahapan penelitian.



Gambar 1. Tahapan Penelitian

2.1 Pengumpulan Data

Di fase ini, mengumpulkan data tersebut di atas telah dilakukan. Semua proses langkahnya diperoleh dari Wawancara, dengan melakukan proses wawancara terhadap semua pihak yang terlibat dalam pengembangan program dan aplikasi untuk mendapatkan informasi alat keamanan dan aplikasi yang ada. Observasi adalah cara yang paling mungkin efektif saat mengumpulkan data untuk mempelajari system yang dapat dilakukan hanya dengan mengamati langsung operasi sistem yang masih dilakukan.

2.2 Kriptografi

Kriptografi merupakan Ilmu yang menekuni metode matematika yang berhubungan dengan matematika keamanan data, semacam kerahasiaan informasi, verifikasi bukti diri, integritas serta validitas informasi. Kriptografi pula bisa didefinisikan selaku penjaga kerahasaiaan pesan. Terdapat 4 tujuan mendasar ilmu kriptografi yang ialah aspek keamanan data:

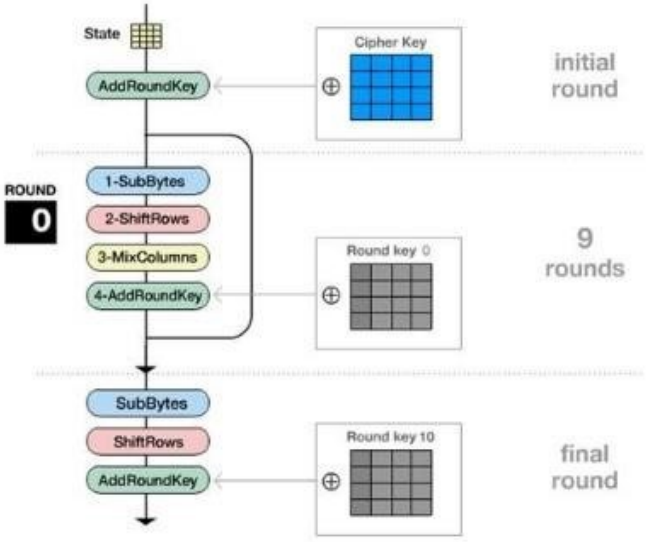
a. Kerahasiaan, merupakan layanan yang digunakan buat melindungi konten data siapa juga kecuali mereka yang mempunyai wewenangan buat membuka ataupun menghapus data terenkripsi serta kunci akses. Terdapat bermacam tata cara keamanan, mulai dari keamanan raga sampai pemakaian algoritma matematika yang membuat informasi susah dimengerti.
b. Integritas informasi, merupakan menghindari pergantian informasi yang tidak legal. Buat melindungi integritas informasi, sistem wajib bisa mengetahui pembedahan yang tidak legal pada informasi, tercantum memasukkan, menghapus, serta mengubah informasi lain dalam informasi sebenernya. Dalam kriptografi, layanan ini dicoba dengan memakai ciri tangan digital. Pesan yang ditanda tangani berarti kalau pesan yang dikirim merupakan asli.

c. Verifikasi bukti diri, merupakan tentang identifikasi ataupun pengenalan, yang ialah satu sistem serta data itu sendiri, wajib ialah bagian 2 bagian yang silih berhubungan. Data yang dikirim lewat saluran wajib diverifikasi bersumber pada keaslian konten informasi, waktu pengiriman, serta lain- lain. Oleh sebab itu, layanan integritas informasi senantiasa digabungkan dengan layanan otentikasi sumber pesan. Dalam kriptografi, layanan ini dicoba dengan memakai ciri tangan digital. Ciri tangan digital mewakili sumber pesan.
d. *Non-repudiation* ataupun nir penyangkalan, merupakan upaya buat menjauhi terbentuknya penyangkalan terhadap pengirim ataupun terciptanya sesuatu data oleh yang mengirimkan ataupun membuat.

Buat bisa melaksanakan proses kriptografi haruslah ada elemen utama didalamnya, yang berkaitan satu sama lain, ialah:
a. *Plain Text* ialah selaku pesan dini ataupun pesan asli yang di kirim pada proses komunikasi. *Plain text* inilah yang setelah itu di enkripsi serta di deskripsi.
b. *Cipher Text* ialah pesan yang tersembunyi, ialah pesan asli (*Plain text*) yang sudah di enkripsi pada proses kriptografi. *Cipher* text ini bisa diganti kembali kebentuk aslinya (*Plain text*) menggunakan *Key* yang sudah di sajikan.
c. *Cryptography Key* ialah kunci yang di pakai buat melaksanakan enkripsi serta deskripsi pada proses kriptografi. Tanpa terdapatnya kunci (*key*) yang sama hingga proses enkripsi serta deskripsi tidak bisa dicoba dengan baik. Kunci (*key*) ialah data yang bisa jadi kendali terhadap proses terbentuknya kriptografi.
d. *Encryption Decryption Algorithm,* komponen terakhir yang pula sama berartinya dalam proses kriptografi merupakan algoritma yang di pakai buat enkripsi serta deskripsi.

2.3 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) merupakan blok kode simetris yang mengambil alih algoritma *Data Encryption Standard* (DES). Algoritma AES mempunyai dimensi blok senantiasa 128-bit dengan panjang kunci yang berbeda. Buat kunci AES 128, ini memakai proses pengulangan yang diketahui selaku putaran, yang mengaitkan 10 lintasan pola matriks 4x4, tiap pola matriks terdiri dari 1 *byte* ataupun 8 bit, buat enkripsi serta dekripsi.



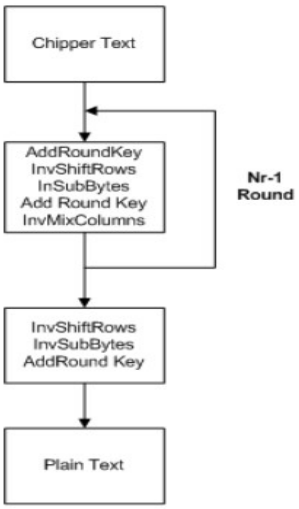
Gambar 2. Proses Enkripsi Menggunakan Algoritma AES

Pada Gambar 2, secara garis besar proses enkripsi AES 128 dengan kunci 128 bit merupakan selaku berikut:
1. *AddRoundKey* : melaksanakan XOR antara *state* dini(plainteks) dengan *cipher key*. Pada sesi ini diucap pula *initial round*.
2. *Round* : Putaran sebanyak Nr- 1 kali. Proses yang dicoba pada tiap putaran merupakan:
   1) *SubBytes* : substitusi *byte* dengan memakai tabel substitusi (*S-box*).
   2) *ShiftRows* : perpindahan baris-baris *array state* secara *wrapping*.
3. *MixColumns* : mengacak data pada tiap-tiap kolom *array state* dengan persamaan selaku berikut :
   $A(x) = \{03\}x^2 + \{01\}x^2 + \{01\}x^2 + \{02\}$
4. *AddRoundKey* : melaksanakan XOR antara *state* saat ini *round key*.

5. *Final Round* : proses buat putaran terakhir antara lain :
   1) *SubBytes*
   2) *ShiftRows*
   3) *AddRoundKey*

Pada proses terakhir hendak menciptakan karakter atau teks yang berbentuk *chipertex*.

Transformasi enkripsi bisa dicoba secara terbalik buat sediakan enkripsi balik yang gampang dimengerti buat algoritme AES. Konversi *byte* yang gampang dimengerti dari algoritma AES. Pada proses dekripsi AES, transformasi yang digunakan pada enkripsi balik pada proses dekripsi AES merupakan *InvShiftRows*, *InvSubBytes*, *InvMixColumns* serta *AddRoundKey*.



Gambar 3. Skema Proses Dekripsi AES

2.4 Rencana Pengujian

Sesi ini tujuannya buat mengenali kalau sistem yang lagi terbuat cocok dengan hasil analisis serta perancangan dan buat membuat statment apakah sistem sudah penuhi harapan. Oleh sebab itu dibutuhkan tata cara pengujian selaku dimensi ataupun parameter buat merumuskan kalau sistem tersebut betul- betul bekerja sebagaimana mestinya. Tata cara pengujian merupakan *Blackbox Testing* yang digunakan buat mengecek kesalahan serta, dikala aplikasi lagi berjalan, buat mendemonstrasikan fungsionalitas aplikasi, merupakan input yang diterima dengan benar serta apakah hasil menciptakan semacam yang diharapkan.

2.5 Kesimpulan

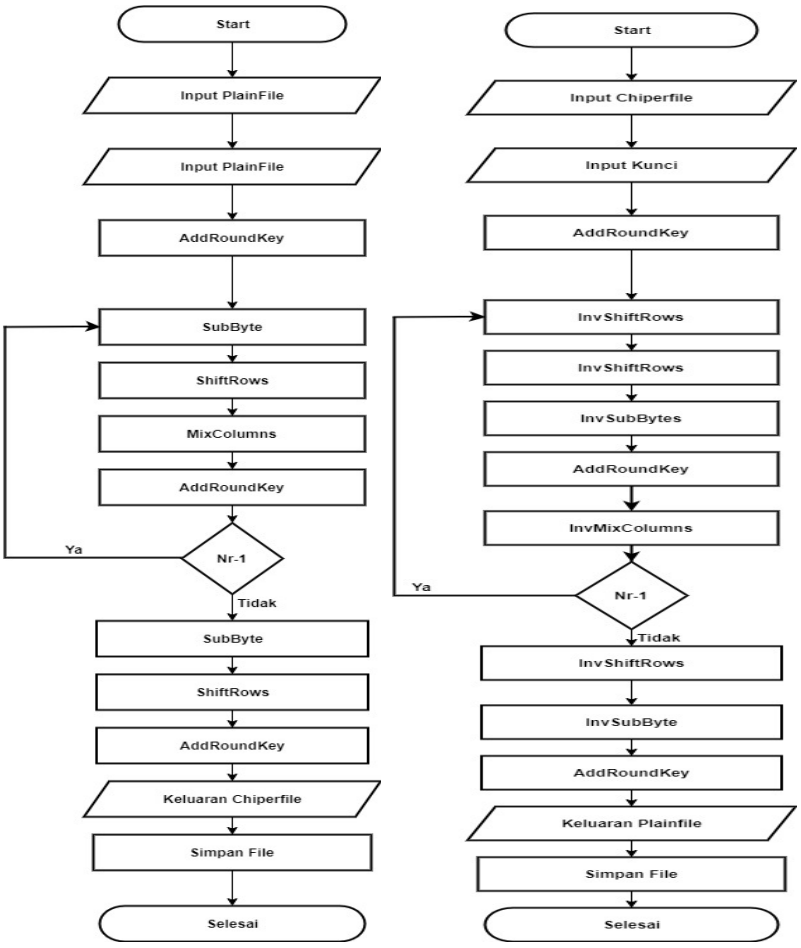
Untuk tahap ini, berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan penerapan metode enkripsi AES-128 terhadap keamanan file, untuk menentukan apakah implementasi *Advanced Encryption Standard* (AES). metode dapat melindungi file dengan benar. Saran untuk perbaikan pengembangan sistem juga dilakukan pada tahap ini .

3. HASIL DAN PEMBAHASAN

Perihal ini didasarkan pada tata cara yang hendak periset implementasikan pada bab lebih dahulu, ialah dengan memakai enkripsi AES- 128 buat melindungi informasi berbentuk file. Implementasi tata cara ini menarangkan *flowchart* enkripsi serta dekripsi tata cara pengujian sistem AES- 128¸ serta tampilan layar proses enkripsi serta dekripsi.

3.1 *Flowchart*

Flowchart enkripsi serta dekripsi AES-128 menarangkan alur proses endkripsi serta dekripsi algoritma AES-128. Pada Gambar 4 adalah proses enkripsi serta dekripsi.

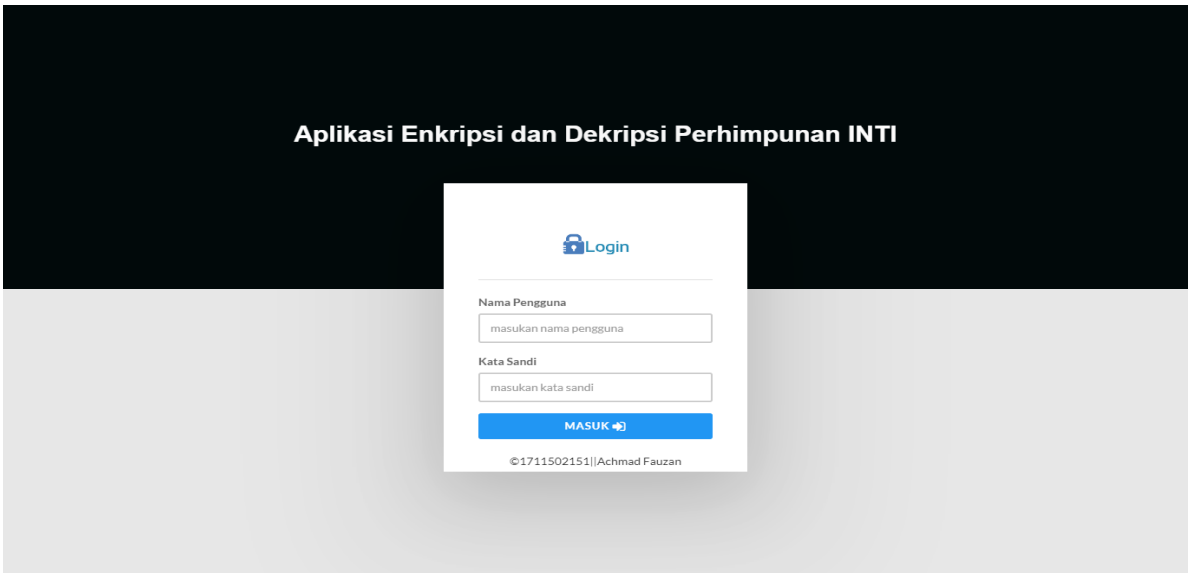


Gambar 4. *Flowchart* Proses Enkripsi dan Dekripsi

3.2 Tampilan Layar

a. Tampilan Layar *Login*

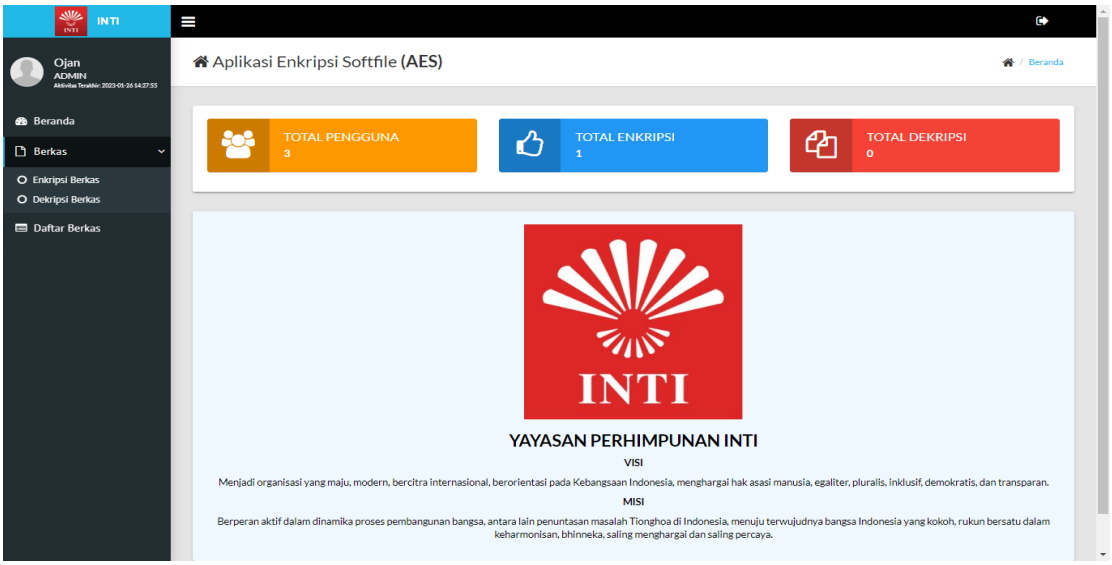
Bisa dilihat pada Gambar 5, ini merupakan tampilan halaman *login*, untuk bisa masuk kedalam halaman beranda, user harus memasukkan *username* dan *password* dengan sesuai.



Gambar 5. Tampilan Layar *Login*

b. Tampilan Layar *Dashboard*

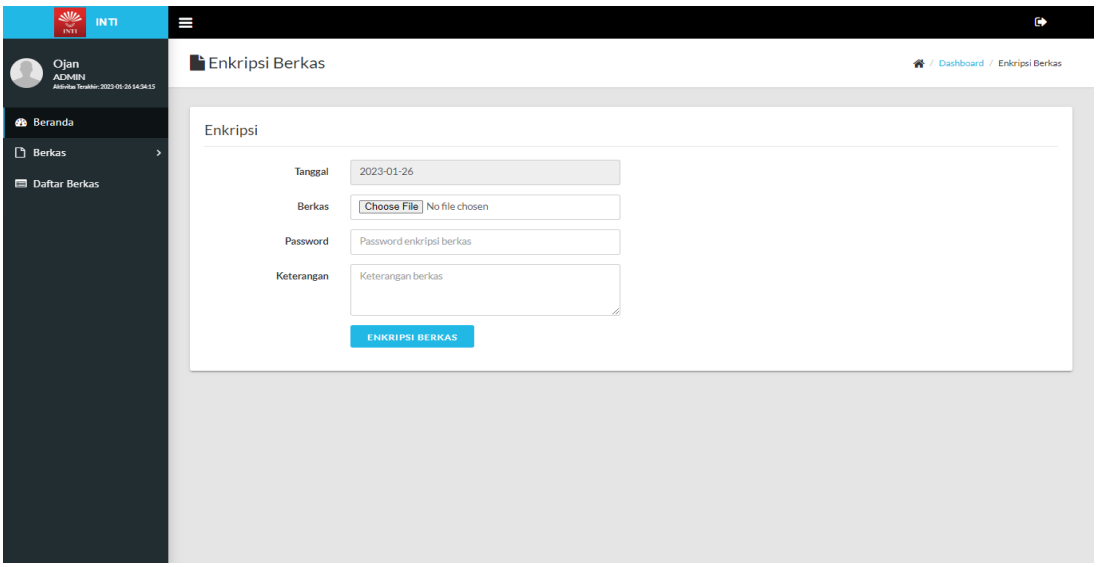
Ketika *user* berhasil *login* dan sistem mengenali *user* yang terdaftar pada *database*, maka akan ditampilkan halaman *dashboard* seperti yang disajikan pada Gambar 6. Pada halaman *dashboard*, terdapat menu-menu file. Terdapat 2 *submenu* dari file yang isinya adalah enkripsi, dekripsi. Lalu terdapat menu Daftar *list*. Dan di dalam halaman beranda terdapat beberapa fitur yang dapat menampilkan jumlah *user*, jumlah file enkripsi, dan jumlah file dekripsi.



Gambar 6. Tampilan Layar Dashboard

c. Tampilan Layar Enkripsi Berkas

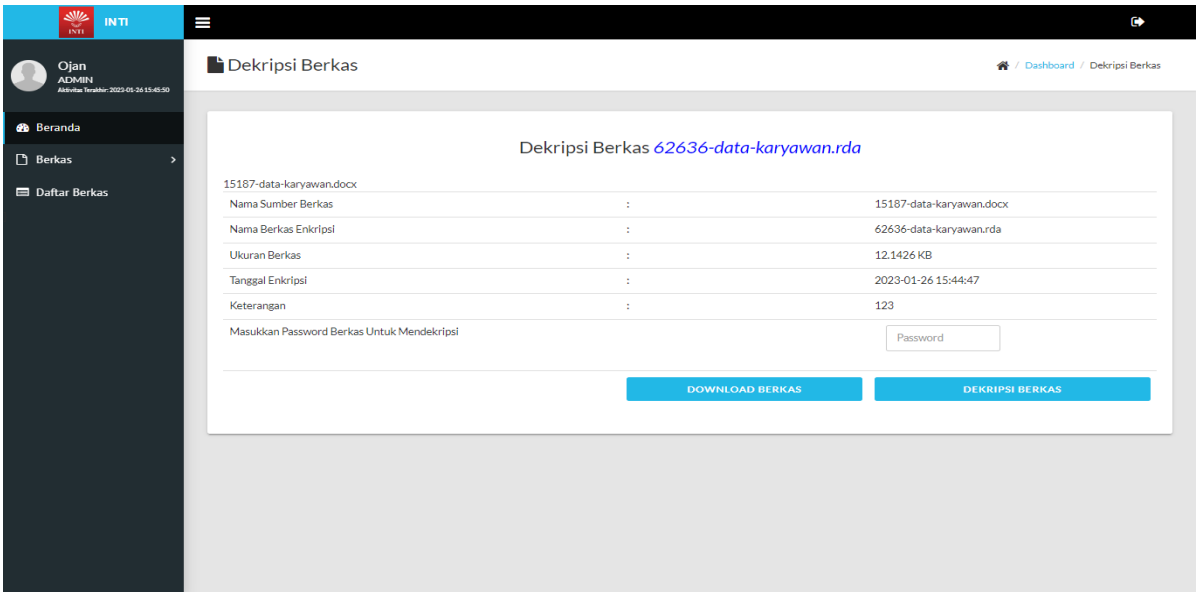
Ketika sistem mengenali pengguna, maka akan ditampilkan halaman enkripsi berkas seperti yang disajikan pada Gambar 7. Pada halaman enkripsi berkas, *user* dapat melakukan enkripsi file.



Gambar 7. Tampilan Layar Enkripsi Berkas

d. Tampilan Layar Dekripsi Berkas

Jika *user* ingin melakukan dekripsi berkas maka *user* mengklik tombol dekripsi berkas, maka akan muncul tampilan layar halaman dekripsi berkas pada Gambar 8.



Gambar 8. Tampilan Layar Dekripsi Berkas

3.3 Pengujian

Pada Tabel 1 adalah hasil dari pengujian file asli yang sudah melalui proses enkripsi, dan pada Tabel 2 adalah hasil proses dekripsi.

Tabel 1. Hasil Enkripsi

No.	Nama Asli File	Ukuran File Asli Per (KB)	Nama File Setelah Di Enkripsi	Ukuran File Setelah Di Enkripsi per (KB)
1.	data-penerima-beasiswa.xlsx	27	36980-data-penerima-beasiswa.rda	26.249
2.	data-karyawan.docx	13	13468-data-karyawan.rda	12.1426
3.	laporan-keuangan.pdf	339	35838-laporan-keuangan.rda	338.3
4.	laporan-desember2022.xlsx	13	98031-laporan-desember2022.rda	12.9961

Tabel 2. Hasil Dekripsi

No.	Nama File Enkripsi	Ukuran Setelah di Enkripsi per (KB)	Nama File Setelah Di dekripsi	Ukuran File Setelah di Dekripsi per (kb)
1.	36980-data-penerima-beasiswa.rda	26.249	19550-data-penerima-beasiswa.xlsx	26.249
2.	13468-data-karyawan.rda	12.1426	13468-data-karyawan.docx	12.1426
3.	35838-laporan-keuangan.rda	338.3	35838-laporan-keuangan.pdf	338.3
4.	98031-laporan-desember2022.rda	12.9961	26738-laporan-desember2022.xlxs	12.9961

4. KESIMPULAN

Berdasarkan analisis, perancangan dan uji coba program aplikasi kriptografi, dapat disimpulkan bahwa penelitian ini dengan Algoritma kriptografi AES berhasil diimplementasikan pada aplikasi pengamanan file berbasis web pada Yayasan Perhimpunan INTI. Waktu untuk menyelesaikan proses enkrip dan dekrip sebanding dengan ukuran filenya (semakin besar ukuran file yang akan diproses, semakin lambat proses enkrip dan dekrip, dan sebaliknya untuk file yang berukuran kecil). Aplikasi ini hanya menggunakan file yang berektensi *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf.

DAFTAR PUSTAKA

[1] A. F. I. R. Achmad Nugrahantoro, Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) *Mode Chiper Block Chaining* (CBC), vol. XII, Yogyakarta: JURNAL ILMIAH FIFO, 2020, pp. 12 - 21.
[2] Yusfrizal, Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper dan RSA Berbasis Android, vol. 3, Medan: Jurnal Teknik Informatika Kaputama, 2019, pp. 29 - 37.
[3] H. Wijaya, Implementasi Kriptografi Aes-128 Untuk Mengamankan URL (*Uniform Resource Locator*) Dari SQL Injector, vol. 17, Baubau: JURNAL AKADEMIKA, 2020, pp. 8 - 13.
[4] D. A. Meko, Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data, Vol. 4, Kupang: Jurnal Teknologi Terpadu, 2018, pp. 8 - 15.
[5] A. S. Lisnayani Silalahi, Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1, vol. 3, Medan: Nasional Komputasi dan Teknologi Informasi, 2020, pp. 182 - 186.
[6] A. I. H. F. R. U. Ferdiansyah, Penggunaan Qr Code Berbasis Kriptografi Algoritma Aes Advanced Encryption Standard Untuk Administrasi Rekam Medis, vol. 03, Cimahi: JOINT (Journal of Information Technology), 2021, pp. 20 - 27.
[7] B. N. S. A. Delisman Hulu, Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan, vol. 4, Medan: KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 2020, pp. 78 - 86.
[8] N. P. S. Asri Prameshwari, Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen, vol. 8, Denpasar Bali: Eksplora Informatika, 2018, pp. 52 - 58.
[9] D. N. Angga Aditya Permana, Rancangan Aplikasi Pengamanan Data Dengan Algoritma *Advanced Encryption Standard* (AES), vol. 11, Tangerang: Jurnal Teknik Informatika, 2018, pp. 177 - 186.