Penerapan AES pada Sistem Keanggotaan Gym untuk Perlindungan Data Pribadi

Deva Krishna Ananda[a1], I Komang Ari Mogi[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Udayana, Bali
Jln. Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, 08261, Bali, Indonesia
[1]dkrishnaananda@gmail.com
[2]arimogi@unud.ac.id

Abstract

The security of gym member data files is an important aspect of maintaining the privacy and security of personal information stored in the gym management system. In this study, we propose the application of the Advanced Encryption Standard (AES) algorithm as a solution to secure gym member data files. AES is an encryption algorithm known for its high security and has been extensively used in information security applications. In this implementation, each gym member's data files, such as profiles, addresses, and other personal information, will be encrypted using a secret key that only the system knows. With encryption using AES, even if the member's data file is stolen or accessed illegally, the information contained in it remains safe and cannot be read without the correct secret key. The results of the trial found that this application succeeded in encrypting some member data files with .pdf format into the. rda format, then decrypting them back into the original file form without changing the original file size. So, it can be shown that the use of the AES algorithm in securing gym member data files provides a high level of security and protects sensitive information from unauthorized parties.

Keywords: *Cryptography, Advanced Encryption Standard (AES), File Security, Gym Member Data*

1. Pendahuluan

Perkembangan teknologi yang pesat memberikan dampak yang sangat berguna bagi masyarakat, akan tetapi terdapat juga beberapa dampak negatif dari perkembangan teknologi tersebut, salah satunya adalah penyadapan data. Masalah keamanan data menjadi aspek penting terutama jika data tersebut berisi informasi pribadi. Data merupakan aset yang penting baik bagi individu ataupun sebuah instansi. Dalam beberapa tahun terakhir, terjadi peningkatan signifikan dalam jumlah serangan siber dan pelanggaran data di berbagai sektor, termasuk industri kebugaran [1]. Oleh karena itu, perlunya menerapkan langkah-langkah keamanan yang efektif untuk melindungi data *member gym* menjadi suatu keharusan.

Pengamanan file data *member gym* merupakan aspek penting dalam menjaga kerahasiaan informasi pribadi yang disimpan dalam sistem manajemen *gym*. Dalam sistem manajemen *gym*, biasanya data-data *member gym* disimpan dalam bentuk file yang dapat dengan mudah dilihat dan dibaca. File ini seharusnya memiliki sifat internal yang hanya dapat dilihat oleh pihak internal seperti staf tempat *gym*. Permasalahan dapat terjadi jika pihak yang tidak berwenang dapat mengakses dan membaca file data *member gym* dan kemudian menggunakannya untuk melakukan tindakan kriminal. Hal ini dapat terjadi karena instansi tidak memiliki sistem untuk mengamankan file. Untuk menyelesaikan permasalahan ini, dapat dilakukan dengan mengimplementasikan metode kriptografi untuk mengunci isi data dalam sistem pengamanan file sehingga data-data dapat terjamin keamanannya [2].

Dalam kriptografi terdapat istilah yang biasa digunakan yakni enkripsi (*encryption*) yang merupakan proses untuk mengubah data asli (*plaintext*) menjadi data tersandi (*chipertext*), dan dekripsi (*decryption*) yakni proses untuk mengembalikan data tersandi menjadi data asli [3].

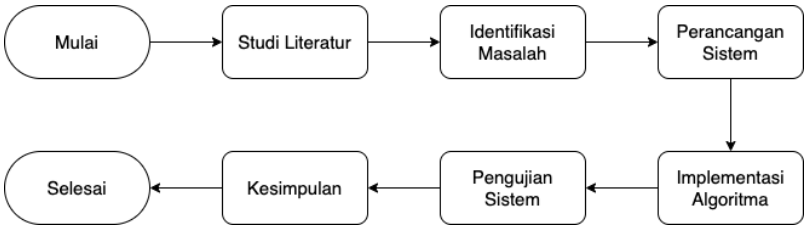
Terdapat beberapa algoritma kriptografi yang dapat digunakan untuk mengamankan file, terdapat kunci rahasia untuk mengenkripsi dan dekripsi file sehingga ketika file dienkripsi, file yang dilindungi tidak dapat dilihat oleh sembarang pihak, dan hanya pihak yang memiliki kunci rahasia itu yang dapat mendekripsi dan melihat isi file.

Dalam penelitian ini, akan diimplementasikan algoritma kriptografi *Advanced Encryption Standard* (*AES*) untuk pengamanan file data *member gym*. Dengan menggunakan algoritma *AES*, informasi yang disimpan dalam sistem manajemen *gym* akan menjadi tidak terbaca dan tidak dapat diakses oleh pihak yang tidak berwenang. Hal ini membantu menjaga kerahasiaan dan integritas data *member*, serta mencegah kemungkinan penyalahgunaan atau pencurian informasi pribadi.

2. Metode Penelitian

2.1. *Flowchart* Penelitian

Metode yang digunakan pada penelitian ini adalah dengan Metode Waterfall. Metode waterfall adalah salah satu metode pengembangan perangkat lunak yang mengikuti pendekatan linear, berurutan, dan terstruktur [4]. Metode ini dijadikan prinsip dalam melakukan penelitian agar dapat meminimalisir penyimpangan dan kesalahan sehingga penelitian dapat dilakukan dengan lebih baik. Pada Gambar 1 dijelaskan mengenai *flowchart* penelitian.



Gambar 1. *Flowchart* Penelitian

2.2. Identifikasi Masalah

Pada penelitian ini, identifikasi dilakukan dengan mencari beberapa kerentanan yang ada pada menajemen sistem *member gym*. Terdapat beberapa permasalahan seperti kebocoran informasi pribadi karena tidak adanya sistem untuk pengamanan data sehingga pihak yang tidak berwenang dapat dengan mudah mengetahui informasi pribadi dari *member gym*. Untuk itu diperlukannya implementasi kriptografi untuk mengamankan data file.

2.3. Kriptografi

Kriptografi merupakan ilmu untuk menjaga keamanan dan kerahasiaan pesan [5]. Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk melindungi informasi agar tetap rahasia, otentik, dan terjamin keutuhannya. Tujuan utama kriptografi adalah mengamankan komunikasi dan data dari akses yang tidak sah atau perubahan yang tidak diinginkan. Secara umum, kriptografi melibatkan penggunaan algoritma matematis yang kompleks untuk mengubah data asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*) menggunakan kunci kriptografi. Proses ini disebut enkripsi. Untuk membaca kembali isi asli dari *ciphertext*, diperlukan kunci yang sesuai untuk melakukan proses dekripsi.

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

AES (*Advanced Encryption Standard*) adalah sebuah algoritma kriptografi yang digunakan secara luas untuk mengamankan data. Algoritma ini dikenal sebagai standar enkripsi yang kuat dan efisien. *AES* menggunakan pendekatan blok cipher, artinya data dipecah menjadi blok-blok yang sama ukurannya sebelum dienkripsi. Setiap blok data kemudian diolah menggunakan serangkaian operasi matematis yang kompleks, termasuk substitusi byte, pergeseran baris, dan

pencampuran kolom. Proses ini dilakukan berulang pada setiap blok data untuk menghasilkan ciphertext.

a. Proses Enkripsi *AES*
Proses enkripsi pada algoritma AES terdiri dari beberapa jenis perubahan *byte*, yakni *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Operasi yang digunakan dalam *AES* merupakan operasi yang ditentukan dalam domain *finite field* GF (2^8) dengan polinomial irreducible pembangkit $m(x) = x8 + x4 + x3 + x + 1$ [6].

1. Dalam tahap *AddRoundKey*, setiap *byte* dalam blok data di-XOR-kan dengan *byte* kunci yang sesuai.
2. Pada tahap *SubBytes,* Setiap *byte* dalam blok data digantikan dengan *byte* yang sesuai dalam tabel substitusi (S-Box).
3. Pada tahap *ShiftRows*, *byte* dalam setiap baris blok data digeser ke kiri berulang secara teratur.
4. Pada tahap *MixColumns*, kolom-kolom dalam blok data diubah menggunakan transformasi matriks.

Tahap-tahap ini diulang beberapa kali tergantung pada ukuran kunci yang digunakan (128-bit, 192-bit, atau 256-bit).

b. Proses Dekripsi *AES*
Proses dekripsi untuk mengembalikan *chipertext* menjadi *plaintext* dapat dilakukan terbalik dengan menerapkan arah yang berlawanan dari proses enkripsi, hal ini sering disebut dengan istilah *inverse chiper*. Perubahan byte yang digunakan pada proses ini adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*.

1. *InvShiftRows* merupakan operasi yang memulihkan posisi *byte* dalam setiap baris blok cipher ke posisi aslinya. Pada tahap enkripsi, *ShiftRows* menggeser *byte-byte* dalam setiap baris ke kiri. Pada tahap dekripsi, *InvShiftRows* menggeser *byte-byte* tersebut kembali ke posisi aslinya dengan pergeseran ke kanan.
2. *InvSubBytes* merupakan operasi yang mengembalikan *byte-byte* dalam blok *cipher* ke nilai asli mereka menggunakan *Inverse S-Box*. Pada tahap enkripsi, *SubBytes* menggantikan setiap *byte* dengan *byte* yang sesuai dalam tabel substitusi. Pada tahap dekripsi, *InvSubBytes* mengembalikan *byte-byte* tersebut ke nilai asli mereka dengan menggunakan *Inverse S-Box*.
3. *InvMixColumns* merupakan operasi yang membalikkan transformasi matriks yang dilakukan pada blok *cipher.* Pada tahap enkripsi, *MixColumns* menggabungkan dan mengalikan kolom-kolom dalam blok *cipher* dengan matriks tetap. Pada tahap dekripsi, *InvMixColumns* membalikkan operasi tersebut dengan menggunakan matriks *invers*.

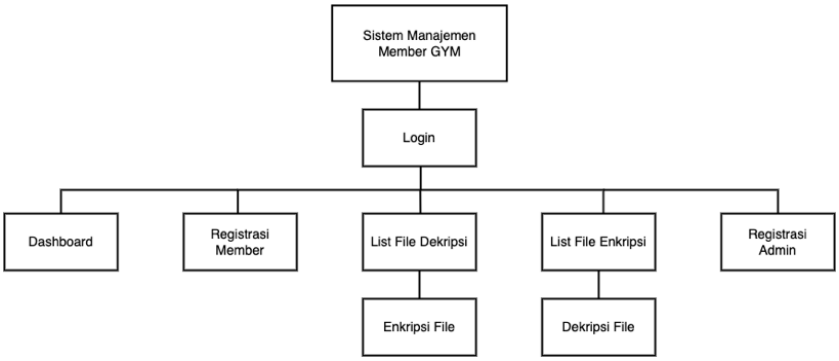
3. Hasil dan Pembahasan

3.1. Rancangan Sistem

Rancangan sistem pada penelitian ini akan menggunakan aplikasi berbasis web, algoritma kriptografi *Advanced Encryption Standard* akan ditulis dalam bahasa pemrograman PHP. Perancangan ini bertujuan untuk mengetahui apakah algoritma dapat berjalan dengan benar dan file data *member gym* dapat terenkripsi dan didekripsi dengan benar dan sesuai.

3.2. Rancangan Menu

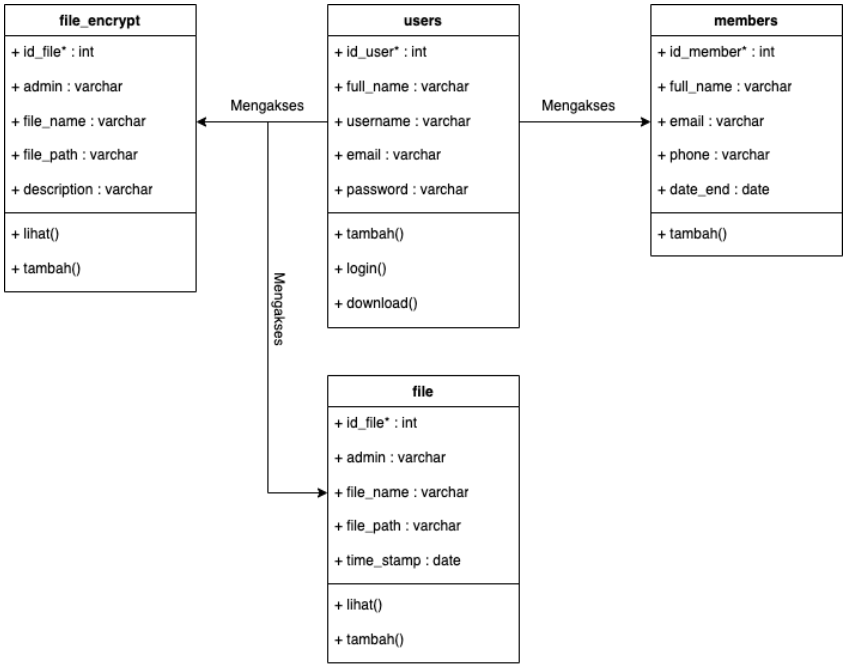
Struktur rancangan tampilan menu web pengamanan file data *member gym* pada sistem manajemen *gym* yang akan dirancang dapat dilihat pada Gambar 2.



Gambar 2. Rancangan Menu

3.3. Rancangan Basis Data

a. *Class Diagram*
Pada *Class Diagram* menjelaskan struktur dari aplikasi ini. Struktur ini merupakan atribut dan metode pada masing-masing *Class*. *Class Diagram* dapat dilihat pada gambar 3.



Gambar 2. *Class Diagram*

b. Spesifikasi Basis Data
Terdapat 4 tabel pada basis data yang akan digunakan dalam aplikasi ini, untuk spesifikasi basis data dapat dilihat pada table-tabel berikut.

Tabel 1. Spesifikasi Basis Data Users

Nama	Tipe Data	Keterangan
Id_user	int (11)	Id User
full_name	varchar (255)	Nama Admin
username	varchar (30)	Username
email	varchar (255)	Email Admin

Nama	Tipe Data	Keterangan
password	varchar (255)	Password

Tabel 2. Spesifikasi Basis Data Members

Nama	Tipe Data	Keterangan
Id_member	int (11)	Id Member
full_name	varchar (255)	Nama Member
email	varchar (255)	Email Member
phone	varchar (15)	No HP Member
date_end	date	Tanggal Akhir Membership

Tabel 3. Spesifikasi Basis Data *File*

Nama	Tipe Data	Keterangan
id_file	int (11)	Id File
admin	varchar (255)	Username Admin
file_name	varchar (255)	Nama File
file_path	varchar (255)	Letak File
time_stamp	datetime	Waktu File Dibuat/Didekripsi

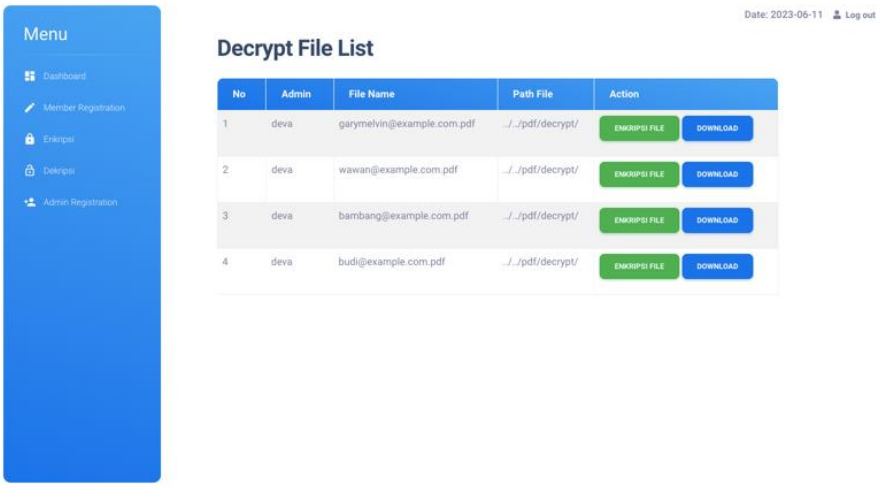
Tabel 4. Spesifikasi Basis Data *File_Encrypt*

Nama	Tipe Data	Keterangan
id_file	int (11)	Id File
admin	varchar (255)	Username Admin
file_name	varchar (255)	Nama File
file_path	varchar (255)	Letak File
description	Varchar (255)	Keterangan File

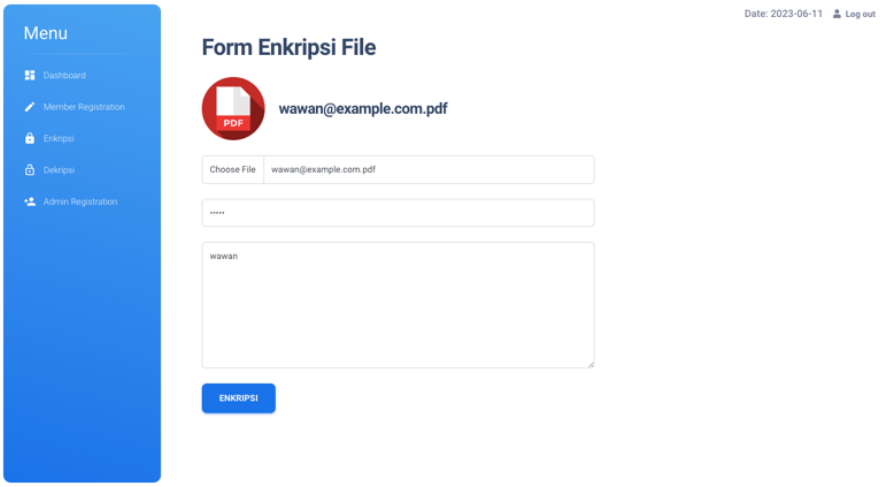
3.4. Implementasi *Advanced Encryption Standard* (*AES*) pada Aplikasi

Pada implementasi algoritma *Advanced Encryption Standard* terdapat beberapa hal yang akan dilakukan yakni enkripsi dan dekripsi file. Berikut adalah implementasinya.

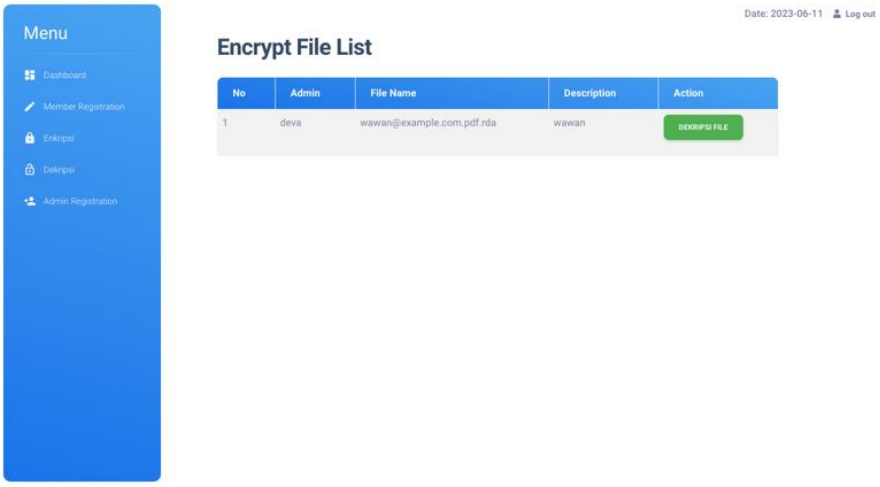
a. Enkripsi *File*
Pada Proses ini, yang dilakukan pertama oleh admin adalah mengakses menu *list file* dekripsi dan kemudian memilih file data *member* yang ingin di enkripsi, setelah itu admin akan memasukkan file, kunci rahasia dan keterangan, lalu menekan tombol enkripsi untuk mengenkripsi file dan aplikasi akan memproses file untuk dienkripsi. Proses ini dapat dilihat pada gambar-gambar berikut.



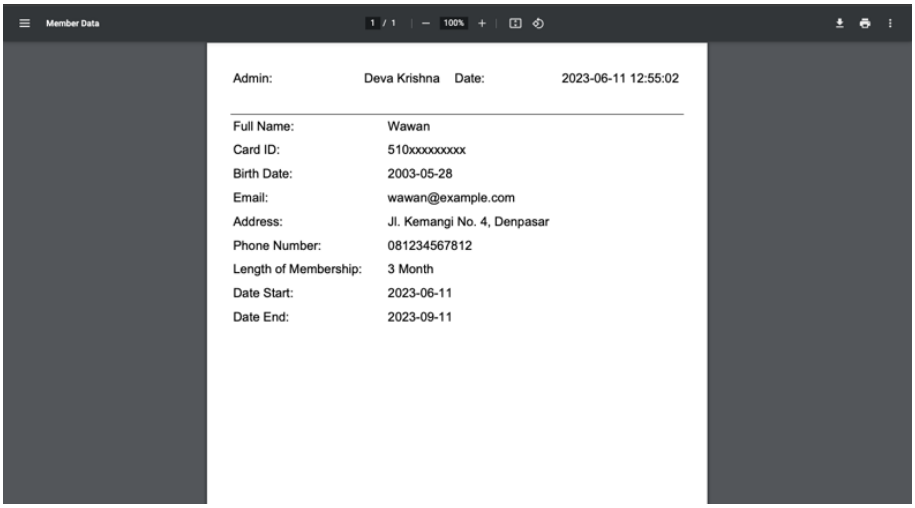
Gambar 3. Proses Enkripsi



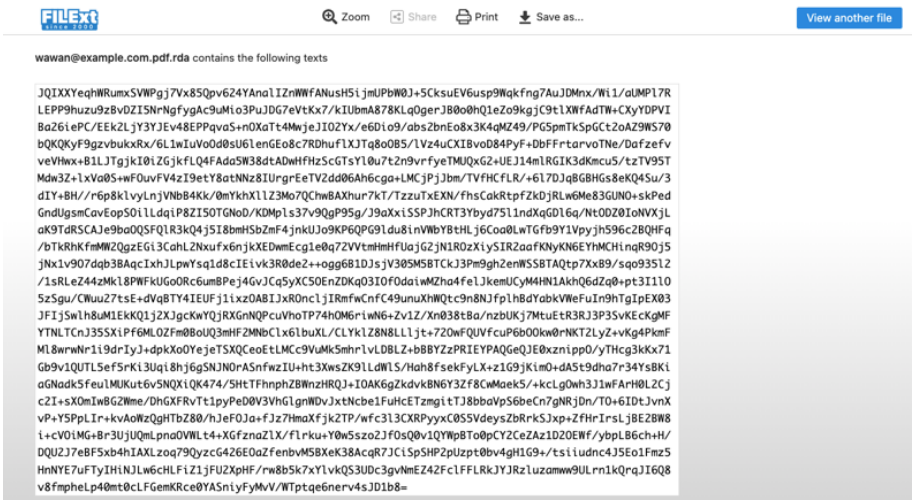
Gambar 4. Proses Enkripsi (2)



Gambar 5. Proses Enkripsi (3)

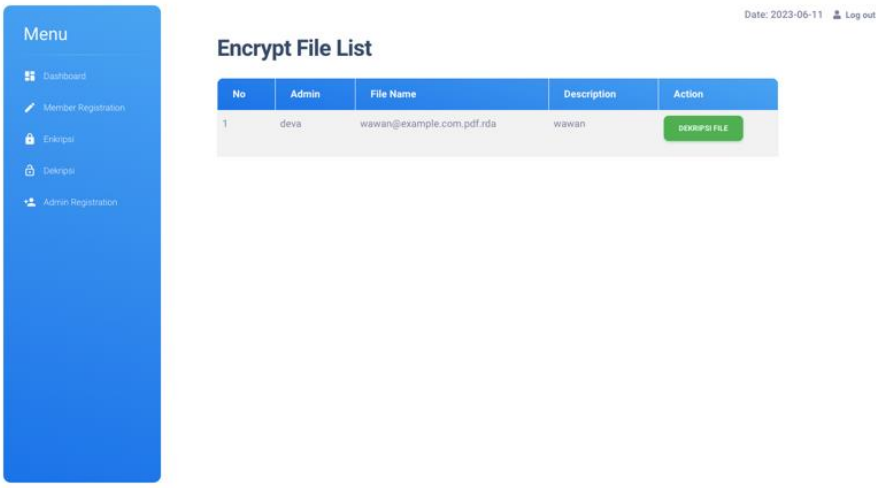


Gambar 6. Isi File Sebelum Enkripsi

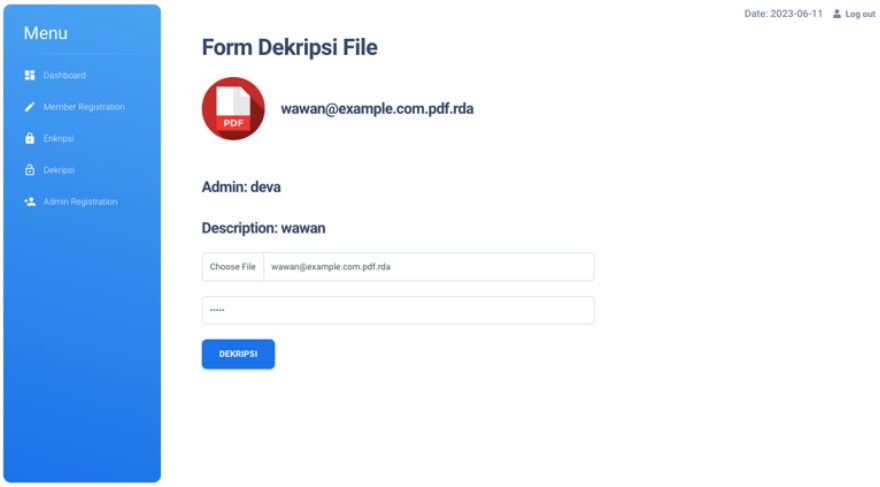


Gambar 7. Isi File Setelah Enkripsi

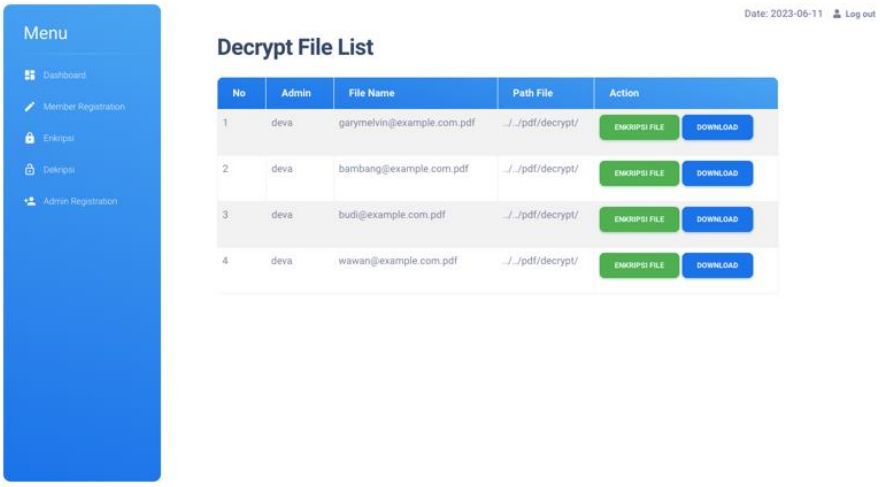
b. Dekripsi *File*
Pada Proses ini, yang dilakukan pertama oleh admin adalah mengakses menu *list file* enkripsi dan kemudian memilih file data member yang ingin di dekripsi, setelah itu admin akan memasukkan file dan kunci rahasianya lalu menekan tombol dekripsi untuk mendekripsi file dan aplikasi akan memproses file untuk didekripsi. Proses ini dapat dilihat pada gambar-gambar berikut.



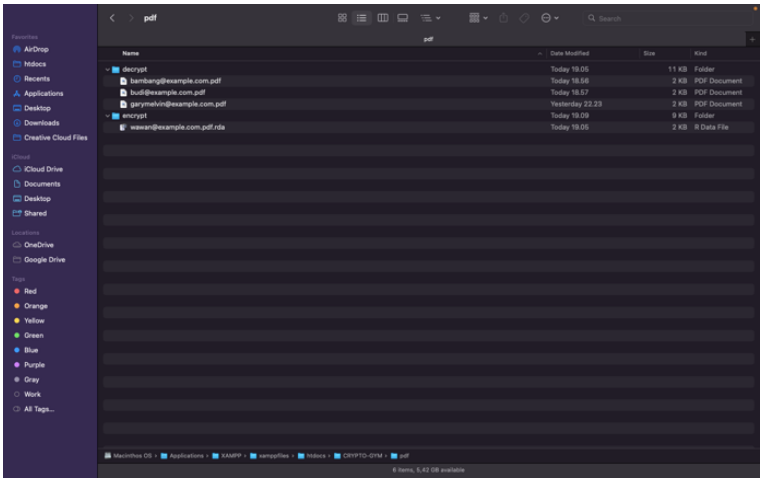
Gambar 8. Proses Dekripsi



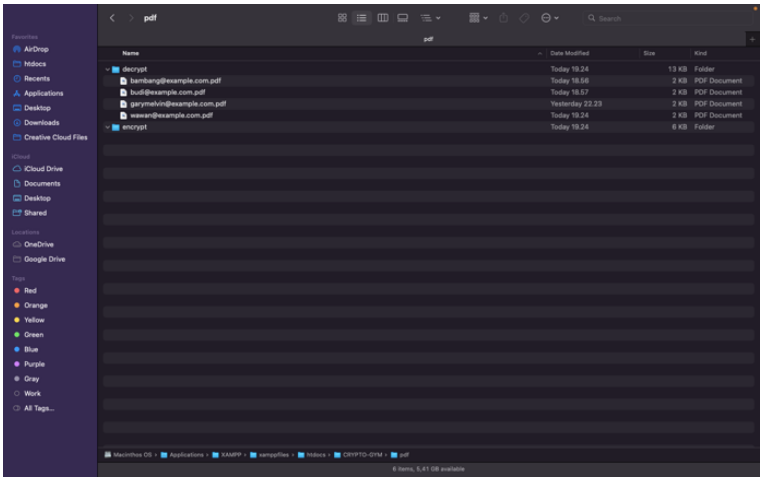
Gambar 9. Proses Dekripsi (2)



Gambar 10. Proses Dekripsi (3)



Gambar 11. File Sebelum Dekripsi



Gambar 12. File Setelah Dekripsi

3.5. Pengujian

Tahap ini akan melakukan pengujian proses enkripsi dan dekripsi file dari aplikasi manajemen *member gym*. File yang akan didekripsi merupakan file data diri dari *member gym*. Sebagai contoh akan digunakan 4 file data diri yang akan diuji untuk enkripsi dan dekripsinya. Berikut adalah hasilnya.

a. Hasil Pengujian Proses Enkripsi File
   Tabel berikut menunjukkan hasil dari proses enkripsi file

Tabel 5. Hasil Pengujian Proses Enkripsi

No	Nama File	Ukuran File	Nama File Enkripsi	Ukuran File Enkripsi	Keterangan
1	garymelvin@example.com.pdf	1.675 bytes	garymelvin@example.com.pdf.rda	2.244 bytes	Berhasil
2	bambang@example.com.pdf	1.697 bytes	bambang@example.com.pdf.rda	2.276 bytes	Berhasil

No	Nama File	Ukuran File	Nama File Enkripsi	Ukuran File Enkripsi	Keterangan
3	budi@example.com.pdf	1.685 bytes	budi@example.com.pdf.rda	2.260 bytes	Berhasil
4	wawan@example.com.pdf	1.689 bytes	wawan@example.com.pdf.rda	2.264 bytes	berhasil

b. Hasil Pengujian Proses Dekripsi File
Tabel berikut menunjukkan hasil dari proses dekripsi file.

Tabel 6. Hasil Pengujian Proses Dekripsi

No	Nama File Enkripsi	Ukuran File	Nama File Dekripsi	Ukuran File Dekripsi	Keterangan
1	garymelvin@example.com.pdf.rda	2.244 bytes	garymelvin@example.com.pdf	1.675 bytes	Berhasil
2	bambang@example.com.pdf.rda	2.276 bytes	bambang@example.com.pdf	1.697 bytes	Berhasil
3	budi@example.com.pdf.rda	2.260 bytes	budi@example.com.pdf	1.685 bytes	Berhasil
4	wawan@example.com.pdf.rda	2.264 bytes	wawan@example.com.pdf	1.689 bytes	berhasil

4. Kesimpulan

Berdasarkan penjelasan yang telah dibahas, dapat ditarik kesimpulan bahwa aplikasi berbasis web dari sistem manajemen *member gym* dapat mengimplementasikan algoritma kriptografi Algoritma *Advanced Encryption Standard* (*AES*) untuk mengamankan file-file yang berisi data diri para *member gym*. Aplikasi ini berhasil melakukan proses enkripsi menjadi format. rda dan mendekripsikannya kembali menjadi bentuk file asli dan tidak mengubah ukuran file aslinya. Sehingga dapat ditunjukkan bahwa penggunaan algoritma AES dalam pengamanan file data member gym memberikan tingkat keamanan yang tinggi dan melindungi informasi sensitif dari pihak yang tidak berwenang. Diharapkan penelitian selanjutnya dapat mengkombinasikan metode kriptografi untuk pengamanan data pada sistem lain, sehingga dapat meningkatkan keamanan file atau data dan mencegah terjadinya penyadapan data oleh pihak yang tidak bertanggung jawab.

Daftar Pustaka

[1] A. B. Putra, A. Kusyanti, dan M. Data, “Implementasi Algoritme Grain V1 Untuk Enkripsi Gambar Pada Aplikasi Berbasis Web,” 2018. [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id
[2] H. Saputra Djong dan S. Siswanto, “Implementasi Kriptografi Dengan Menggunakan Metode Rc4 dan Aes-256 Untuk Mengamankan File Dokumen Pada Pt Varnion Technology Semesta,” 2022.
[3] Y. Wiharto dan A. Irawan, “Enkripsi Data Menggunakan Advanced Encryption Standard 256,” vol. 7, no. 2, 2018.
[4] A. A. Wahid, “Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK Oktober (2020) Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi,” 2020.
[5] Harun Mukhtar, “Kriptografi untuk Keamanan Data,” 2018.
[6] F. Muharram, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard,” *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 2, 2018.