IMPLEMENTASI ADVANCED ENCRYPTION STANDARD 128 BIT DAN SHAMIR SECRET SHARING PADA WEBSITE DATA ULANG PENSIUN LEMBAGA DANA PENSIUN PERTAMINA

Ihvan Mulya Pradana[1*], Rizky Pradana[2]

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

Email: [1*]ihvanmulya@gmail.com, [2]rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-Keamanan dan kerahasiaan dokumen merupakan aspek yang sangat penting dan bersifat rahasia. Lembaga Dana Pensiun Pertamina saat ini belum menerapkan standar keamanan data sehingga berpotensi menimbulkan masalah kebocoran dan penyalahgunaan data. Setiap tahunnya peserta Dana Pensiun Pertamina diwajibkan untuk melakukan data ulang untuk memastikan peserta yang masih berhak menerima manfaat pensiun. Data ulang dilakukan melalui website sehingga masalah keamanan data pada prosesnya perlu diperhatikan dan dengan penelitian ini kebocoran data dapat dicegah. Tujuan dari penelitian ini melakukan pengamanan file data ulang milik Lembaga Dana Pensiun Pertamina dengan menggunakan metode algoritme Advanced Encryption Standard (AES) dan Shamir Secret Sharing terkait data peserta penerima manfaat pensiun. Dimana file dan data kunci yang digunakan untuk proses enkripsi dan dekripsi akan diamankan menggunakan skema Shamir Secret Sharing. Dari hasil implementasi dan pengujian diperoleh kesimpulan bahwa aplikasi mampu mengamankan file dan data dalam database yang dienkripsi sehingga dapat meminimalisir terjadinya penyalahgunaan atau manipulasi data oleh orang-orang yang tidak memiliki wewenang atas data tersebut. Diperoleh kesimpulan proses enkripsi rata-rata ukuran dokumen 721.783 byte lama waktu proses adalah 76 milidetik dan hasil proses dekripsi rata-rata ukuran dokumen 962.393 byte lama waktu proses adalah 80 milidetik.

Kata Kunci: data, peserta, dana pensiun, advanced encryption standard, shamir secret sharing

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD 128 BIT AND SHAMIR SECRET SHARING FOR RETIREMENT RE-REGISTRATION WEBSITE AT PERTAMINA PENSION FUND INSTITUTION

Abstract-*The security and confidentiality of documents is a very important and confidential aspect. The Pertamina Pension Fund currently has not implemented data security standards, so it has the potential to cause data leakage and misuse problems. Every year Pertamina Pension Fund participants are required to re-do data to ensure that participants are still entitled to receive pension benefits. Data reprocessing is done through the website so that data security problems in the process need to be considered and with this research data leakage can be prevented. The purpose of this study is to secure data files belonging to the Pertamina Pension Fund Institution by using the Advanced Encryption Standard (AES) algorithm and Shamir Secret Sharing related to the data of pension benefit participants. Where files and key data used for the encryption and decryption process will be secured using the Shamir Secret Sharing scheme. From the results of implementation and testing, it is concluded that the application is able to secure files and data in an encrypted database so that it can minimize the occurrence of misuse or manipulation of data by people who do not have authority over the data. It can be concluded that the average document size of 721,783 bytes of process time is 76 milliseconds and the result of the decryption process is that the average document size of 962,393 bytes takes 80 milliseconds of processing time.*

Keywords*: data, peserta, dana pensiun, advanced encryption standard, shamir secret sharing*

1. PENDAHULUAN

Seiring dengan perkembangan teknologi dan komunikasi yang begitu pesat, memudahkan kita untuk melakukan pertukaran data secara cepat melalui jaringan internet [1][2]. Namun terkadang dalam pertukaran data tersebut keamanan data kurang disadari sehingga bisa menyebabkan kebocoran data. Oleh karena itu aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting [3][4].

Dana Pensiun Pertamina adalah lembaga yang mengelola dan menjalankan program yang menjanjikan manfaat pensiun bagi para pekerja PT Pertamina dan anak perusahaannya. Saat ini jumlah penerima manfaat yang dikelola oleh Dana Pensiun Pertamina jumlahnya lebih dari lima puluh ribu peserta. Setiap tahunnya, para peserta Dana Pensiun Pertamina diwajibkan untuk melakukan data ulang untuk pengkinian data sekaligus memastikan peserta masih hidup dan berhak menerima manfaat pensiun. Di dalam formulir data ulang tersebut terdapat data

pribadi yang seharusnya dilindungi dengan baik seperti Nama, No. KTP, Alamat, Tanggal Lahir dan terdapat juga foto KTP. Namun saat ini proses tersebut belum memiliki standar keamanan data yang baik sehingga bisa menyebabkan masalah pencurian dan penyalahgunaan data. Untuk meminimalisir terjadinya tindakan tersebut diperlukan metode keamanan data, yaitu dengan memakai ilmu kriptografi [5]. Ilmu kriptografi bagian dari seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna [6].

Dalam bidang ilmu kriptografi, dikenal dua istilah yaitu enkripsi dan dekripsi [7]. Enkripsi merupakan proses pengacakan naskah asli (*plain*) menjadi naskah acak yang sulit dibaca (*cipher*) sedangkan dekripsi adalah proses pengembalian *cipher* ke dalam *plain* [8]. Kedua proses ini membutuhkan satu komponen yang disebut kunci. Kunci dan *plain* akan dikombinasikan dengan serangkaian rumus matematika dalam algoritme enkripsi sehingga menghasilkan *cipher* [9]. Kunci yang digunakan untuk proses dekripsi bisa merupakan kunci yang sama saat proses enkripsi (kunci simetris) maupun kunci yang berbeda saat proses enkripsi (kunci asimetris). Kunci simetris dapat dibedakan lagi berdasarkan cara melakukan enkripsinya yaitu berdasarkan bit-bit data (*stream cipher*) dan berdasarkan blok-blok data (*block cipher*) [10][11].

Pada salah satu penelitian tahun 2021 [12], dimana AES sebagai algoritma kriptografi dapat digunakan untuk mengamankan data di dalam *smart card* yang menunjukkan bahwa penggunaan AES dengan *key* yang bersifat dinamis ini mampu mengamankan data 40 *byte plainteks* menjadi 48 *byte cipherteks*, dengan rata-rata waktu komputasi sebesar 71.2 ms untuk penulisan data dan 89.4 ms untuk pembacaan data menggunakan *key* 128 bit, 70.8 ms untuk penulisan data dan 88 ms untuk pembacaan data menggunakan *key* 192 bit, dan 72 ms untuk penulisan data dan 88.4 ms untuk pembacaan data menggunakan key 256 bit. Waktu komputasi ini hanya mempunyai selisih sekitar 2 ms dibandingkan dengan penulisan dan pembacaan data tanpa mekanisme enkripsi dan dekripsi. Selanjutnya penelitian yang berjudul "Implementasi Algoritma SPECK *Block Cipher* dan *Shamir 's Secret Sharing* Pada File Teks" pada tahun 2019 [13]. Hasil pengujian rata-rata pemakaian CPU pada ukuran file 4 KB dengan isi 3 baris yaitu 7,058%, ukuran file 4 KB dengan isi 8 baris yaitu 25,855%, sedangkan ukuran file 4 KB dengan isi 13 baris yaitu 31,095%. Hasil pengujian rata-rata banyaknya pemakaian RAM pada ukuran file 4 KB dengan isi 3 baris yaitu 377,277 MB, ukuran file 4 KB dengan isi 8 baris yaitu 414,283 MB, sedangkan ukuran file 4 KB dengan isi 13 baris yaitu 440,231 MB. Atas dasar hal tersebut, penelitian ini memiliki tujuan untuk mengamankan file dan *database* pada aplikasi website data ulang milik Dana Pensiun Pertamina dengan menggunakan metode algoritme *Advanced Encryption Standard* (AES) dan *Shamir Secret Sharing*. Dimana file dan data pada *database* tersebut akan dienkripsi untuk mencegah penyalahgunaan data oleh orang yang tidak bertanggung jawab dan kunci yang digunakan untuk proses enkripsi dan dekripsi akan diamankan menggunakan skema *Shamir Secret Sharing*.

2. METODE PENELITIAN

2.1 Data Sumber Penelitian

Data yang digunakan dalam penelitian merupakan data yang diambil dari data penelitan pada Dana Pensiun Pertamina yaitu merupakan data peserta pensiun yang terdaftar pada lembaga Dana Pensiun Pertamina dan data yang terdapat pada formulir data ulang pensiun.

2.2 Tahapan Penelitian

Penelitian ini memiliki gambaran tahapan-tahapan penelitian dari awal hingga akhir yang terdiri sebagai berikut.

a. Studi Literatur
   Studi Literatur merupakan tahap untuk mempelajari konsep dan alat bantu yang akan digunakan untuk membangun sistem dalam penelitian ini. Studi dapat dilakukan dengan mempelajari beberapa referensi seperti buku teks, jurnal, karya tulis maupun diktat kuliah yang berkaitan dengan penelitain yaitu kriptografi algoritme *Advanced Encryption Standard* (AES) dan algoritme *Shamir Secret Sharing*. Dipelajarinya studi ini bertujuan mendapatkan referensi yang baik untuk menyelesaikan permasalahan yang akan diteliti.
b. Studi Lapangan
   Studi Lapangan merupakan studi kasus untuk mempelajari lebih dalam untuk mengetahui permasalahan yang ada pada data aplikasi Data Ulang Pensiun, yang kemudian akan dirangkum menjadi masalah penelitian.
c. Perumusan Masalah
   Perumusan Masalah merupakan tahap dalam menentukan masalah yang diambil dari tahap sebelumnya, yaitu bagaimana mengamankan data pada database dan formulir data ulang pensiun dengan mengimplementasikan kriptografi algoritme *Advanced Encryption Standard* (AES) dan algoritme *Shamir Secret Sharing*.

d. Pengumpulan Data
Pengumpulan data merupakan tahap dalam pengumpulan data menurut masalah yang ditentukan dari tahap sebelumnya. Beberapa tahap yang dapat dilakukan adalah.
1. Wawancara
Melakukan wawancara dengan pihak Dana Pensiun Pertamina dan peserta pensiun untuk mendapat informasi dalam penelitian.
2. Observasi (Pengamatan)
Melakukan pengamatan secara langsung terhadap prosedur sistem yang sedang berjalan.

e. Analisa Sistem
Analisa Sistem merupakan analisis untuk menyelesaikan masalah dalam penelitian ini. Beberapa tahapan yang dilakukan antara lain.
1) Analisis Data
Dalam analisis data dilakukan pengelompokan data sesuai jenisnya dan endekripsikan data sebagai bantuan untuk membangun program yang lebih baik.
2) Analisis Penerapan Algoritma
Analisis penerapan algoritme menjelaskan bagaimana mengimplementasikan algoritme kriptografi *Advanced Encryption Standard* (AES) dan algoritme *Shamir Secret Sharing* untuk mengamankan data. Pada tahap ini, antara lain: menentukan kunci sebagai salah satu proses kriptografi Advanced Encryption Standard (AES) untuk enkripsi dan dekripsi data, proses memecah kunci menjadi beberapa bagian dengan algoritma *Shamir Secret Sharing* untuk mengamankan kunci agar tidak mudah diketahui, proses enkripsi, yaitu mengubah data plaintext menjadi ciphertext dengan menggunakan kunci dan algoritme *Advanced Encryption Standard* (AES). Proses dekripsi, yaitu mengubah kembail data dari *ciphertext* menjadi *plaintext* dengan menggunakan kunci yang sama pada proses enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES).

f. Perancangan Perangkat Lunak
Perancangan perangkat lunak merupakan tahap perancangan layar, rancangan pendukung, serta hasil dari analisis sistem tahap sebelumnya yang akan diintegrasikan dengan program. Beberapa rancangan pendukung yang dimaksud adalah proses login, proses unggah file, proses modifikasi data dan lain-lain.

g. Implementasi
Implementasi merupakan proses pengerjaan atau pembuatan sistem aplikasi sesuai dengan rancangan yang telah ditentukan sebelumnya. Menggunakan sistem aplikasi berbasis web dengan *framework Codeigniter* dan bahasa pemograman PHP dan juga perangkat lunak DBMS yaitu MySQL untuk mengimplementasikan algoritme *Advanced Encryption Standard* (AES) dan algoritme *Shamir Secret Shari*ng.

h. Pengujian Sistem
Pengujian sistem merupakan tahap yang dibutuhkan untuk menjamin sistem yang telah dibuat sesuai dengan perancangan dan analisis sehingga sistem berjalan dengan baik secara fungsional, berjalan sesuai dengan tujuan, dan menghasilkan output yang diharapkan. Metode pengujian sistem yang akan digunakan adalah metode *Blackbox Testing*.

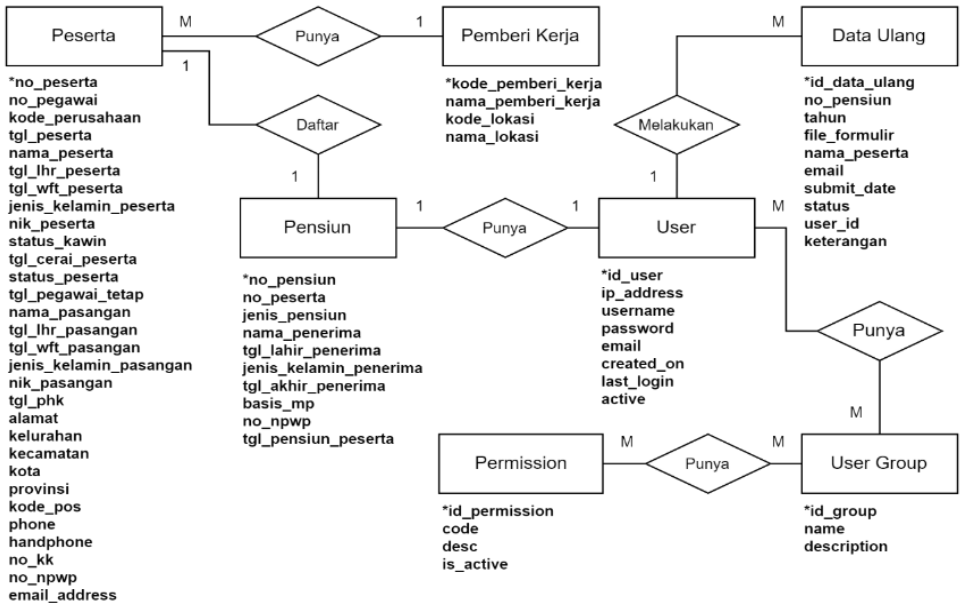
i. Kesimpulan
Pada tahap ini diambil kesimpulan akhir, berdasarkan hasil pengujian dan beberapa tahap yang telah dilakukan, Apakah implementasi kriptografi algoritme *Advanced Encryption Standard* (AES) dan algoritme *Shamir Secret Sharing* mampu mengamankan data pada aplikasi Data Ulang Dana Pensiun Pertamina dengan baik.

2.3 Rancangan Basis Data

Pada rancangan basis data ini menerangkan tentang *Entity Relationship Diagram* (ERD) dan *Logical Record Structure* (LRS) dari *database* yang digunakan oleh aplikasi Data Ulang Dana Pensiun Pertamina.

a. Rancangan *Entity Relationship Diagram* (ERD)

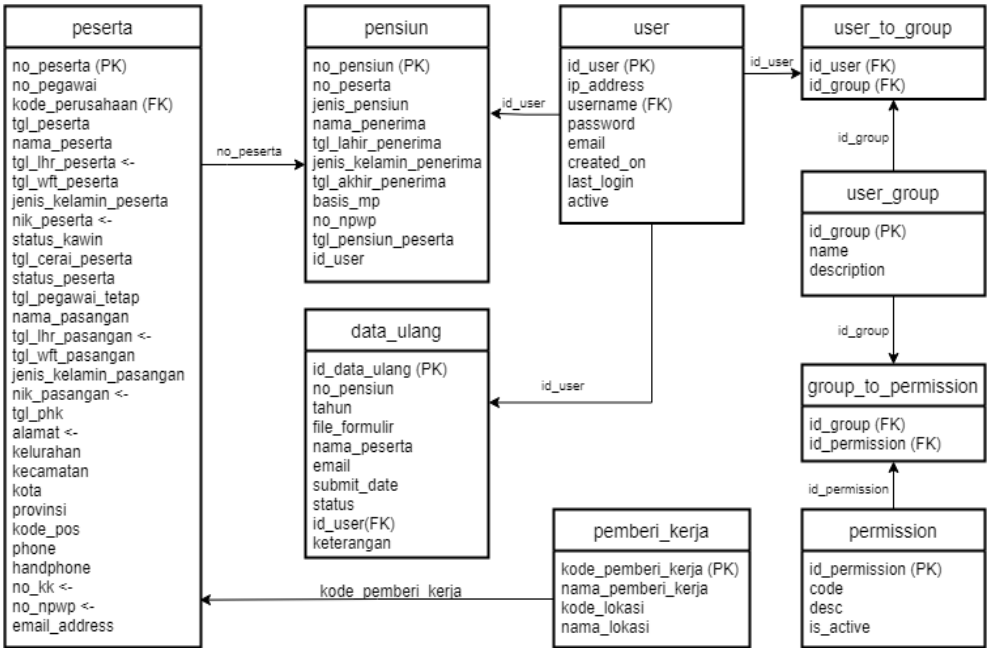
Entity Relationship Diagram (ERD) ini berisi komponen-komponen himpunan entitas dan himpunan relasi. Masing-masing dilengkapi dengan atribut-atribut yang mewakili seluruh data yang ada dapat dilihat pada Gambar 1 dibawah ini.



Gambar 1. *Entity Relationship Diagram*

b. Rancangan *Logical Record Structure*

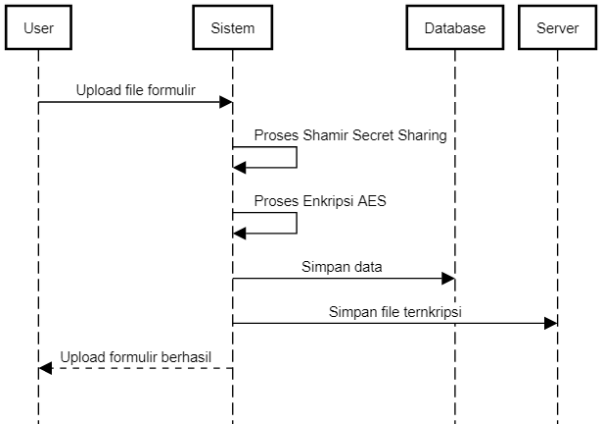
Pada *Logical Record Structure* menggambarkan keterkaitan dan hubungan antar tabel satu dengan yang lain yang terdapat pada *website* Data Ulang Dana Pensiun Pertamina. *Logical Record Structure* dapat dilihat pada Gambar 2 di bawah ini.



Gambar 2. *Logical Record Structure*

2.4 Rancangan Sistem

Proses enkripsi dilakukan ketika pengguna mengunggah file formulir data ulang ke website, sebelum proses enkripsi dan dekripsi AES dilakukan perlu proses *Shamir Secret Sharing* untuk membuat kunci yang sebelumnya sudah dipecah dan disimpan pada lokasi yang berbeda-beda dan kunci tersebut digunakan untuk proses AES.



Gambar 3. Proses Enkripsi

3. HASIL DAN PEMBAHASAN

Algoritma mendeskripsikan suatu sistem yang terdapat tahap-tahap dalam melakukan sesuatu dan penerapannya dalam bentuk yang sederhana. Langkah tersebut dapat di implementasikan dalam alur untuk melakukan sesuatu. Algoritme bertujuan untuk mempermudah penulisan baris program yang akan dibuat serta dapat membantu dalam menjelaskan proses yang akan berjalan

3.1 Algoritma Halaman *Download* Formulir Data Ulang

Algoritma ini menjelaskan proses detail pada halaman *download* formulir data ulang yang terdapat pada aplikasi Data Ulang Dana Pensiun Pertamina. Dapat dilihat pada Gambar 3 dibawah ini.

```
START
INPUT no_pensiun
IF no_pensiun is null THEN
    RETURN ERROR
ENDIF
data_pensiun <- ambil detail data dari database berdasarkan no_pensiun
IF data_pensiun is null THEN
    RETURN ERROR
ELSE
    dekripsi data_pensiun dengan algoritme AES dan SSS
    generate formulir data ulang berdasarkan data_pensiun
    RETURN formulir_data_ulang
ENDIF
RETURN
```

Gambar 4. Algoritma *Download* Formulir Data Ulang Peserta

3.2 Algoritma Halaman *Upload* Formulir Data Ulang

Algoritma ini menjelaskan proses detail pada halaman *upload* formulir data ulang yang terdapat pada aplikasi Data Ulang Dana Pensiun Pertamina. Dapat dilihat pada Gambar 4 dibawah ini.

```
START
INPUT no_pensiun
INPUT file formulir
IF no_pensiun is NULL OR file is NULL THEN
    RETURN ERROR
ENDIF
data_pensiun <- ambil detail data dari database berdasarkan no_pensiun
IF data_pensiun is NULL THEN
    RETURN ERROR
ENDIF
upload file formulir ke server
enkrip file formulir dengan algoritme AES dan SSS
OUTPUT success_message
RETURN
```

Gambar 5. Algoritma *Upload* Formulir Data Ulang Peserta

3.3 Algoritma Halaman Detail Formulir Data Ulang

Algoritma ini menjelaskan proses detail pada halaman detail formulir data ulang.

```
START
INPUT id_data_ulang
data_ulang <- ambil detail data dari database berdasarkan id_data_ulang
IF data_ulang is NULL THEN
    RETURN ERROR
ENDIF
formulir <- dekripsi formulir data_ulang dengan AES dan SSS
OUTPUT data_ulang
OUTPUT formulir
RETURN
```

Gambar 6. Algoritma Detail Formulir Data Ulang Peserta

3.4 Algoritma Halaman Persetujuan Data Ulang Pensiun

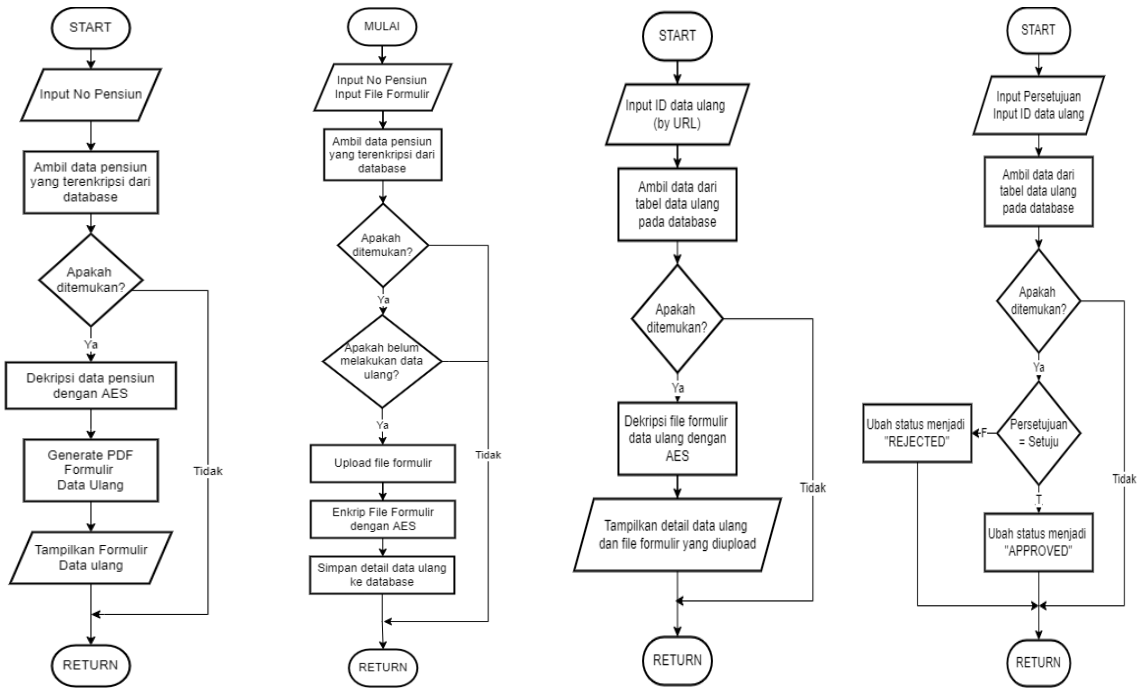
Algoritma ini menjelaskan proses detail pada proses persetujuan formulir data ulang.

```
START
INPUT persetujuan
INPUT id_data_ulang
DATA_ULANG <- dapatkan data dari database berdasarkan id_data_ulang
IF data_ulang IS NULL THEN
    RETURN ERROR
ELSE
    IF persetujuan == 'SETUJU' THEN
        update status data ulang menjadi 'APPROVED'
    ELSE
        update status data ulang menjadi 'REJECTED'
    ENDIF
ENDIF
OUTPUT success_message
RETURN
```

Gambar 7. Algoritma Persetujuan Data Ulang Pensiun

3.5 *Flowchart Sistem*

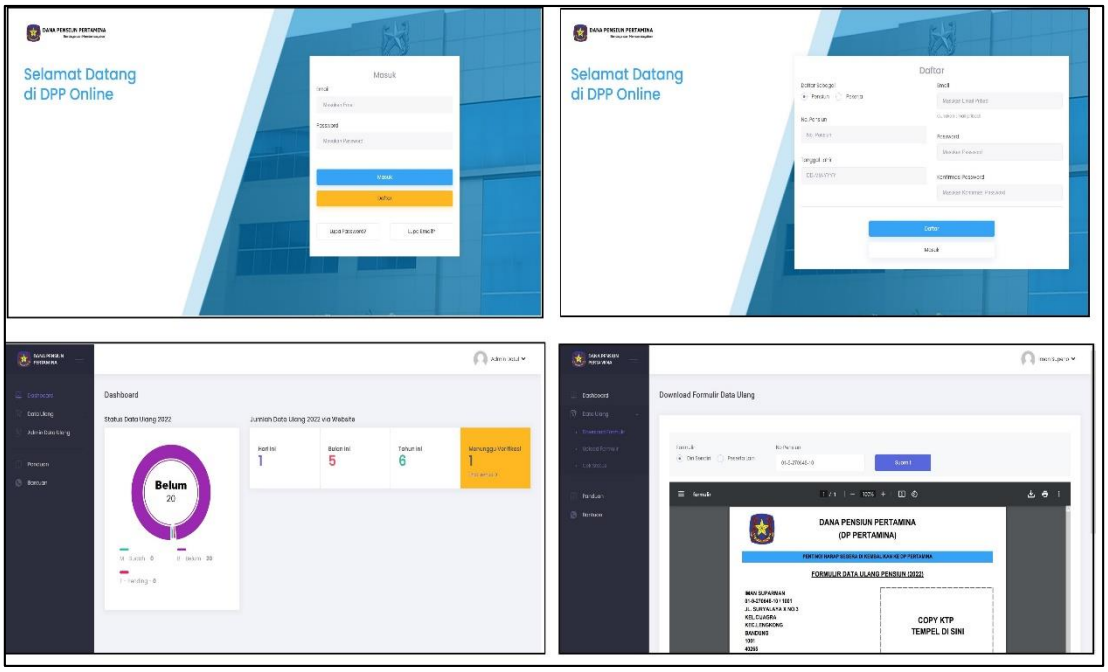
Flowchart pada beberapa proses yang terdapat pada sistem adalah untuk mengerjakan sesuatu yang disusun dalam sederet aksi. Untuk memudahkan pemahaman proses, kerangka berfikir akan disajikan dalam bentuk *flowchart* sebagai berikut. Pada *flowchart* aplikasi menjelaskan proses pada aplikasi sistem, dimana terdapat beberapa fitur menu dan Pada *flowchart* ini menjelaskan proses yang terjadi pada halaman *download* formulir data ulang. Mulai dari input, dekripsi data yang diperoleh dari *database* hingga menampilkan file formulir, selanjutnya formulir data ulang di-*upload*. Mulai dari proses *input*, *upload*, enkripsi hingga menyimpan data data ulang pada *database* hingga proses dekripsi file formulir hingga menampilan formulir serta alir sistem pada proses data ulang pensiun pada peserta.



Gambar 8. *Flowchart* Sistem

3.6 Tampilan Layar Aplikasi

Pada bagian ini, akan di uraikan mengenai tampilan layar mulai dari hasil perancangan aplikasi yang telah dibuat dari awal sampai selesai. Berikut ini beberapa hasil tampilan dari aplikasi dapat dilihat pada Gambar 8 dibawah ini.



Gambar 9. Beberapa Tampilan Layar Pada Aplikasi

3.7 Pengujian Data Proses Enkripsi dan Dekripsi

Pada tahap ini dilakukan proses pengujian enkripsi dan dekripsi dengan algoritme *Advanced Encryption Standard* (AES-128) dan *Shamir Secret Sharing* dari segi rata-rata waktu proses enkripsi dan dekripsi serta rata-rata ukuran dan perubahan ukuran file yang diproses. Berikut adalah hasil pengujian dari 10 sampel data pada aplikasi.

Tabel 1. Pengujian Proses Enkripsi AES dan Shamir Secret Sharing (*Encrypt*)

No	Nomor Pensiun	Nama File Asli	Nama File Terenkripsi	Ukuran File Asli (bytes)	Ukuran File Terenkripsi (bytes)	Durasi Proses Enkripsi (ms)
1	019-270648-10	019-270648-10-DATUL.pdf	019-270648-10-DATUL.enc.pdf	1.082.881	1.443.864	124
2	019-298529-10	019-298529-10-DATUL.pdf	019-298529-10-DATUL.enc.pdf	1.069.287	1.425.728	98
3	019-430858-10	019-430858-10-DATUL.pdf	019-430858-10-DATUL.enc.pdf	869.380	1.159.192	112
4	019-480446-10	019-480446-10-DATUL.pdf	019-480446-10-DATUL.enc.pdf	869.380	1.159.192	83
5	019-589408-10	019-589408-10-DATUL.pdf	019-589408-10-DATUL.enc.pdf	816.530	1.088.728	61
6	019-625996-10	019-625996-10-DATUL.pdf	019-625996-10-DATUL.enc.pdf	613.265	817.708	68
7	019-633074-10	019-633074-10-DATUL.pdf	019-633074-10-DATUL.enc.pdf	565.804	754.412	47
8	029-000007-10	029-000007-10-DATUL.pdf	029-000007-10-DATUL.enc.pdf	539.737	719.660	69
9	069-110047-10	069-110047-10-DATUL.pdf	069-110047-10-DATUL.enc.pdf	422.484	563.328	58
10	069-117192-10	069-117192-10-DATUL.pdf	069-117192-10-DATUL.enc.pdf	369.085	492.120	39
		Total		7.217.833	9.623.932	759
		Rata-rata		721.783	962.393	76

Pada proses enkripsi dengan algoritme AES dan Shamir Secret Sharing dari 10 sampel file formulir data ulang pensiun. ukuran rata-rata adalah 721.783 byte, dan rata-rata proses waktu enkripsi adalah 76 milidetik, dan ukuran rata-rata file yang sudah ter-enkripsi meningkat sekitar 33 % menjadi 9.623.932 byte.

Tabel 2. Pengujian Proses Dekripsi AES dan Shamir Secret Sharing (*Decrypt*)

No	Nomor Pensiun	Nama File Asli	Nama File Terenkripsi	Ukuran File Asli (bytes)	Ukuran File Terenkripsi (bytes)	Durasi Proses Enkripsi (ms)
1	019-270648-10	019-270648-10-DATUL.enc.pdf	019-270648-10-DATUL.pdf	1.443.864	1.082.881	118
2	019-298529-10	019-298529-10-DATUL.enc.pdf	019-298529-10-DATUL.pdf	1.425.728	1.069.287	102
3	019-430858-10	019-480446-10-DATUL.enc.pdf	019-430858-10-DATUL.pdf	1.159.192	869.380	110
4	019-480446-10	019-589408-10-DATUL.enc.pdf	019-480446-10-DATUL.pdf	1.088.728	816.530	130
5	019-589408-10	019-430858-10-DATUL.enc.pdf	019-589408-10-DATUL.pdf	1.159.192	869.380	97
6	019-625996-10	019-625996-10-DATUL.enc.pdf	019-625996-10-DATUL.pdf	817.708	613.265	53
7	019-633074-10	019-633074-10-DATUL.enc.pdf	019-633074-10-DATUL.pdf	754.412	565.804	51
8	029-000007-10	029-000007-10-DATUL.enc.pdf	029-000007-10-DATUL.pdf	719.660	539.737	63
9	069-110047-10	069-110047-10-DATUL.enc.pdf	069-110047-10-DATUL.pdf	563.328	422.484	47
10	069-117192-10	069-117192-10-DATUL.enc.pdf	069-117192-10-DATUL.pdf	492.120	369.085	33
		Total		9.623.932	7.217.833	804
		Rata-rata		962.393	721.783	80,4

Pada proses enkripsi dengan algoritme AES dan Shamir Secret Sharing dari 10 sampel file formulir data ulang pensiun. ukuran rata-rata adalah 721.783 byte, dan rata-rata proses waktu enkripsi adalah 76 milidetik, dan ukuran rata-rata file yang sudah ter-enkripsi meningkat sekitar 33 % menjadi 9.623.932 byte.

4. KESIMPULAN

Dari hasil analisis terhadap masalah dan aplikasi yang dikembangkan maka dapat ditarik beberapa kesimpulan, antara lain: Enkripsi algoritme Advanced Encryption Standard dengan key 128 bit (AES-128) dapat diimplementasikan pada aplikasi Data Ulang Pensiun Dana Pensiun Pertamina untuk mengamankan file dan database menggunakan bahasa pemrograman PHP dan database MySQL Algoritme Shamir secret sharing dapat diimplementasikan pada aplikasi Data Ulang Pensiun untuk mengamankan key yang digunakan pada algoritme AES-128 sehingga keseluruhan sistem kriptografi menjadi lebih aman. Aplikasi ini dapat mengamankan file dan data yang masuk ke dalam server dan database dengan metode algoritma Advanced Encryption Standard (AES) dan algoritme Shamir Secret Sharing sehingga data yang tersimpan sulit untuk dibaca secara langsung. Hasil akhir pengujian aplikasi ini diperoleh hasil proses enkripsi rata-rata ukuran dokumen 721.783 byte, lama waktu proses adalah 76 milidetik dan hasil proses dekripsi rata-rata ukuran dokumen 962.393 byte lama waktu proses adalah 80 milidetik.

DAFTAR PUSTAKA

[1] A. P. Nugroho and H. B. Suseno, "Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES," *QUERY: Jurnal Sistem Informasi*, vol. 04, no.01, pp. 9–17, 2020.

[2] I. Fitriani and A. B. Utomo, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa," *JISKA: Jurnal Inform. Sunan Kalijaga*, vol. 5, no. 3, pp. 153–163, 2020.

[3] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Proc. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

[4] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," *JURIKOM: Jurnal Ris. Komputer*, vol. 7, no. 1, pp. 148-155, 2020.

[5] Y. Dwi Putri, R. Rosihan, and S. Lutfi, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," *JIKO: Jurnal Inform. dan Komputer*, vol. 2, no. 2, pp. 87–94, 2019.

[6] R. Andriyanto, K. Khairijal, and D. Satria, "Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION," *J. Unitek*, vol. 13, no. 1, pp. 34–48, 2020.

[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.
[8] N. Taliasih and I. Afrianto, "Sistem Keamanan Basis Data Klien PT. INFOKES Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *J. Nas. Teknol. dan Sist. Inf.*, vol. 06, no. 01, pp. 009–018, 2020.
[9] W. S. Raharjo, A. R. C, and P. N. A, "Implementasi Secure Multi-Party Computation Menggunakan Metode Shamir Secret Sharing pada Pengamanan Dokumen Digital Rahasia," *J. Inform. dan Sist. Inf. Univ. Ciputra*, vol. 04, no. 01, 2018.
[10] A. Kusyanti2, K. Amron, and F. Mohammad, "Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. Vol. 2, No. 11,u, no. 11, pp. 4863–4869, 2018.
[11] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, pp. 52-58, 2018.
[12] N. Noprianto, V. N. Wijayaningrum, and R. Ariyanto, "Pemanfaatan AES dengan Key Dinamis sebagai Metode Pengamanan Data pada Smart Card," *Jurnal SISTEMASI: Sistem Informasi*, vol. 10, no. 3, pp. 575-585, 2021.
[13] N. K. Diarti, A. Kusyanti, and M. Data, "Implementasi Algoritme SPECK Block Cipher dan Shamir 's Secret Sharing Pada File Teks," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 4, pp. 3742–3748, 2019.