4th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*)

SISTEM KEAMANAN DOKUMEN BERBASIS WEB MENGGUNAKAN KRIPTOGRAFI AES 128 DI PT MENTARI MULIA BERJANGKA

Syaifudin Zuhri[1], Ferdiansyah[2*]

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

Email: [1]1811501012@student.budiluhur.ac.id, [2*]Ferdiansyah@budiluhur.ac.id
(* : corresponding author)

Abstrak-Keamanan pada dokumen sangat penting untuk keberlanjutan bisnis dan kelancaran operasional. Oleh karena itu sistem keamanan dokumen yang handal dan aman sangat penting untuk dikembangkan mengingat adanya ancaman kejahatan terhadap perlindungan dokumen perusahaan seperti akses ilegal, pencurian informasi, dan serangan siber yang semakin canggih. PT Mentari Mulia Berjangka memiliki jumlah data yang cukup banyak dan rahasia yang berbentuk dokumen digital yang tidak boleh diketahui isinya oleh semua orang hanya orang yang memiliki akses tertentu yang boleh melihat isinya. Kriptografi dapat digunakan untuk mengamankan dokumen-dokumen tersebut dengan lebih baik. Penerapan algoritme AES-128 akan dilakukan pada penelitian ini untuk mengamankan dokumen yang berformat *Doc, Docx, Pdf, Ppt, Pptx, Xls, Xlsx* dan *Txt* pada PT Mentari Mulia Berjangka. Algoritme AES-128 dipilih karena memiliki kecepatan enkripsi dan dekripsi yang lebih cepat dari algoritme yang ada dan bisa mengatasi brute force lebih baik ketimbang algoritme DES. Berdasarkan hasil pengujian dari penerapan enkripsi dan dekripsi dengan AES-128 diperoleh hasil yang baik dengan melihat hasil enkripsi yang tidak dapat dimengerti oleh orang lain dan hasil dokumen yang didekripsi memiliki isi yang sama dengan isi dokumen asli. Waktu dari hasil percobaan dokumen yang dienkripsi dan didekripsi mendapatkan perolehan waktu rata-rata 1.89 detik dengan ukuran file di bawah 3 MB.

Kata Kunci: Keamanan Dokumen, *Advanced Encryption Standard (AES)*-128, Enkripsi, Dekripsi, Kriptografi.

WEB-BASED DOCUMENT SECURITY SYSTEM USING AES 128 CRYPTOGRAPHY AT PT MENTARI MULIA BERJANGKA

Abstract*-Security of documents is very important for business continuity and smooth operations. Therefore, it is very important to develop a reliable and safe document security system considering the threat of crime to the protection of company documents such as illegal access, information theft and increasingly sophisticated cyber attacks. PT Mentari Mulia Berjangka has quite a large amount of confidential data in the form of digital documents whose contents cannot be known by anyone, only people who have certain access can see the contents. Cryptography can be used to better secure these documents. The application of the AES-128 algorithm will be carried out in this research to secure documents in Doc, Docx, Pdf, Ppt, Pptx, Xls, Xlsx and Txt formats at PT Mentari Mulia Berjangka. The AES-128 algorithm was chosen because it has faster encryption and decryption speeds than existing algorithms and can handle brute force better than the DES algorithm. Based on the test results of applying encryption and decryption with AES-128, good results were obtained by seeing that the encryption results could not be understood by other people and the results of the decrypted document had the same content as the original document. The experimental results of encrypted and decrypted documents obtained an average time of 1.89 seconds with a file size under 3 MB.*

Keywords: *Document Security, Advanced Encryption Standard (AES)-128, Encryption, Decryption, Cryptography*.

1. PENDAHULUAN

Teknologi informasi berkembang pesat belakangan ini dan digunakan diberbagai bidang dan pekerjaan seperti bisnis, termasuk di PT Mentari Mulia Berjangka. Dengan kemudahan teknologi informasi semua orang dapat menggunakannya untuk menyelesaikan permasalahan yang ada [1]. Contohnya untuk melakukan pertukaran data seperti dokumen. Keamanan pada dokumen perusahaan sangat penting untuk keberlanjutan bisnis dan kelancaran operasional. Oleh karena itu sistem kemanan dokumen yang handal dan aman sangat penting untuk dikembangkan mengingat adanya ancaman kejahatan terhadap perlindungan dokumen perusahaan seperti akses ilegal, pencurian informasi, dan serangan siber yang semakin canggih.

PT Mentari Mulia Berjangka adalah perusahaan berjangka komiditi yang berdiri pada januari 2013. Berlokasi di Graha Aktiva Lt.6 Suite 601 JL. HR. Rasuna Said Blox X-1 Kav. 03 Jakarta Selatan. Sebagai perusahaan pialang

resmi PT Mentari Mulia Berjangka Jakarta telah menjadi anggota Bursa Berjangka Jakarta dan Kliring Berjangka Indonesia. Serta telah mendapatkan persetujuan dari Badan Pengawas Berjangka Komiditi (BAPPEBTI). PT Mentari Mulia Berjangka memiliki jumlah data yang cukup banyak dan rahasia yang berbentuk dokumen digital yang tidak boleh diketahui isinya oleh semua orang hanya orang yang memiliki akses tertentu yang boleh melihat isinya. Dokumen digital ini terdiri dari *Doc*, *Docx*, *Pdf*, *Ppt*, *Pptx*, *Xls*, *Xlsx* dan *Txt*.

Kriptografi dapat digunakan untuk mengamankan dokumen–dokumen tersebut dengan lebih baik. Kriptografi dapat mengenkripsi dokumen sehingga isinya menjadi acak dan mendekripsikan dokumen ke bentuk awal [2]. Hal ini bisa mencegah orang lain mengetahui isi dari dokumen. Beberapa algoritme kriptografi yang digunakan untuk mengamankan dokumen adalah AES -128 [2], DES [3].

Algoritme AES–128 adalah simetrik dan *cipher block* untuk menggantikan *Encryption System* (DES) [4], [5]. Algoritme ini menggunakan kunci yang sama saat proses enkripsi dan pada saat proses dekripsi, keluaran dari algoritme AES-128 adalah berupa blok yang terdiri dari jumlah bit tertentu. Algoritme AES mendukung berbagai macam kunci dan jumlah blok yang dapat digunakan. Tetapi AES memiliki ukuran kunci dan blok yang tetap yaitu sebesar 128, 192, 256 bit [6]. Informasi akan lebih aman setelah dienkripsi oleh algoritme AES-128 karena data akan diubah kedalam bentuk acak sehingga tidak sembarang orang yang bisa membacanya kecuali memiliki kunci.

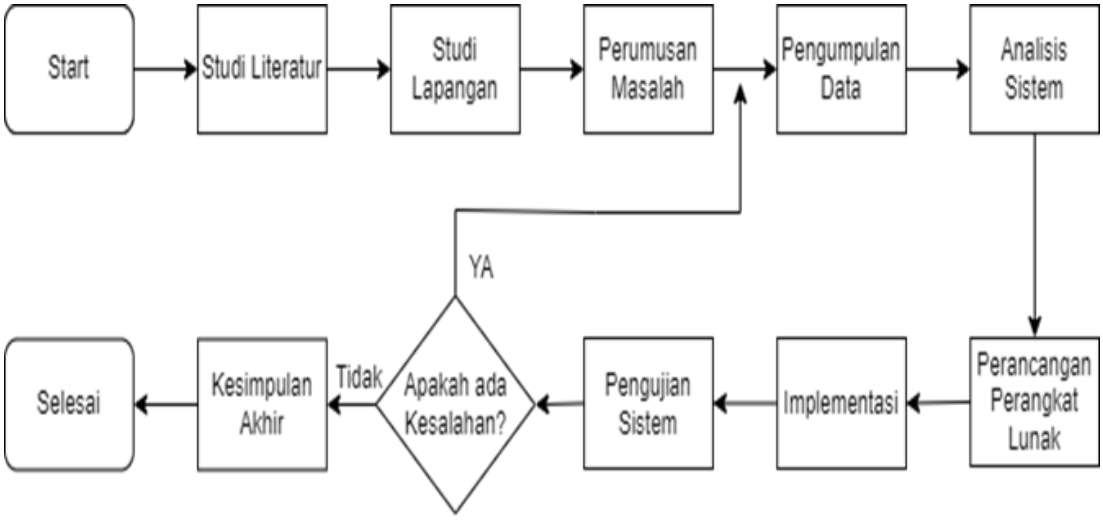
Penelitian sebelumnya yang terkait meliputi penelitian Nayuni Dwitri dkk dengan judul "Pengaman Data File Document Mengunakan Kriptografi *Encryption System* (DES)" [3], algoritme *Encryption System* (DES) memiliki kekurangan yaitu mudah terkena serangan *brute force* karena panjang kuncinya yang terlalu pendek yaitu hanya 56 bit yang dengan mudah dibobol dengan menggunakan kemampuan prosesor saat penulisan ini dibuat, sebagai ganti dari algoritme *Encryption System* (DES) adalah algoritme *Advanced Encryption Standard* (AES) yang memiliki Panjang kunci lebih Panjang ketimbang *Encryption System* (DES) [7].

Penelitian ini menggunakan *Advanced Encryption Standard* (AES)-128 untuk membantu mengamankan dokumen pada PT Mentari Mulia Berjangka, karena algoritme ini bisa mengatasi masalah *brute force* lebih baik ketimbang *Encryption System* (DES) [7]. Kecepatan waktu enkripsi dan dekripsi *Advanced Encryption Standard* yang lebih cepat dari beberapa algoritme yang ada juga menjadi alasan untuk menggunakan algoritme ini [8], [9], [10].

Pada penelitian ini, mengembangkan sistem keamanan dokumen yang handal dan aman, khususnya untuk PT Mentari Mulia Berjangka, dengan mengusulkan penerapan kriptografi menggunakan algoritme AES-128 untuk menjamin keamanan dokumen digital dalam berbagai format. Penilitian ini menunjukkan bahwa teknik enkripsi dan dekripsi berfungsi dengan baik untuk melindungi dokumen sensitif, hasil enkripsi tidak dapat dipahami oleh orang yang tidak berwenang, dan dekripsi dokumen dapat dilakukan tanpa kehilangan isi asli.

2. METODE PENELITIAN

Untuk memastikan bahwa penelitian tidak menyimpang dari tujuan awalnya, metode penelitian ini digunakan sebagai garis besar langkah-langkah yang akan diikuti dalam penelitian ini. Tahapan-tahapan Gambar 1 berikut akan diikuti dalam penelitian ini.



Gambar 1. Tahapan Penelitian

2.1 Studi Literatur

Studi Literatur dilakukan dengan cara mempelajari buku text, jurnal dan karya tulis ilmiah terdahulu sehingga ditemukan algoritme yang digunakan untuk pengamanan dokumen digital pada penelitian sebelumnya.

2.2 Studi Lapangan

Studi lapangan dilakukan di PT Mentari Mulia Berjangka Indonesia untuk mengidentifikasi masalah yang terjadi, yang kemudian saat melakukan perumusan masalah, akan dirumuskan. Metode yang dipilih adalah metode AES–128 karena metode ini membantu proses pengamanan dokumen digital.

2.3 Perumusan Masalah

Pada tahap ini, masalah yang akan diselesaikan ditentukan, yaitu mengamankan dokumen yang belum memiliki sistem keamanan dengan merancang sistem keamanan file pada PT Mentari Mulia Berjangka dengan kriptografi AES-128.

2.4 Pengumpulan Data

Pada tahapan ini, data yang diperlukan untuk merancang sistem keamanan dikumpulkan. Beberapa tahapan yang diambil antara lain:

a. Wawancara (*Interview*), adalah proses pengumpulan data dengan membuat pertanyaan tentang keamanan file pada staff di PT Mentari Mulia Berjangka sebagai pihak yang berwenang untuk membuat aplikasi kriptografi.
b. Observasi (*Observation*), Pengamatan dilakukan dengan cara melakukan pengamatan langsung pada obyek penelitian yang sebenarnya. Hal ini bertujuan agar memperoleh informasi tentang hal–hal yang berkaitan tentang data-data yang dibutuhkan untuk merancang sistem keamanan dalam penelitian ini.
c. Analisa Dokumen, dilakukan dengan cara menganalisis dokumen yang digunakan pada PT Mentari Mulia Berjangka.
d. Studi Kepustakaan (*Library Research*), dilakukan dengan membaca jurnal, buku text, dan referensi tambahan tentang teori kriptografi, standar pengamanan file, dan *Advanced Encrytion Standard* (AES), serta teori-teori tambahan yang berkaitan dengan pembuatan perancangan sistem kemanan kriptografi pengamanan file dokumen ini.

2.5 Analisis Sistem

Implementasi pengamanan sistem adalah proses enkripsi isi file yang akan disimpan ke dalam database. Ini dilakukan untuk memastikan bahwa file yang disimpan ke dalam database adalah file rahasia yang hanya dapat diakses oleh pihak berwenang. Oleh karena itu, modul diperlukan untuk melakukan enkripsi data saat file disimpan ke dalam database. Sistem keamanan memiliki modul enkripsi, yang merupakan aplikasi yang digunakan oleh pengguna ketika mereka ingin mengenkripsi file. Modul dekripsi, di sisi lain digunakan ketika pengguna ingin melihat isi file.

2.6 Perancangan Perangkat Lunak

Pada tahap ini, perancangan akan disesuaikan dengan hasil analisis sistem, terutama untuk modul enkripsi dan dekripsi serta modul pendukung lainnya yang akan diintegrasikan ke dalam aplikasi dan perancangan antar muka.

2.7 Implementasi

Selama proses implementasi, modul-modul dibuat dalam tahap perancangan ke dalam bahasa pemrograman tertentu. Aplikasi yang digunakan meliputi penerapan data menggunakan PHP dan MySQL. Perangkat keras yang digunakan adalah *Processor Intel Core i3-2370M*, RAM 4GB, dan HDD 200GB.

2.8 Pengujian Sistem

Pada tahap ini, sistem diuji untuk memastikan apakah ia sudah sesuai dengan hasil analisis sebelumnya dan sesuai dengan harapan. Metode pengujian ini berfungsi sebagai ukuran atau parameter pengujian sistem.

2.9 Kesimpulan

Pada tahap ini kesimpulan akhir diambil dari penerapan metode kriptografi *Advanced Encrytion Standard* (AES) untuk mengamankan file dokumen pada PT Mentari Mulia Berjangka, berdasarkan hasil pengujian implementasi metode *Advanced Encrytion Standard* (AES) berjalan dengan baik dan dapat mengamankan dokumen dengan aman.

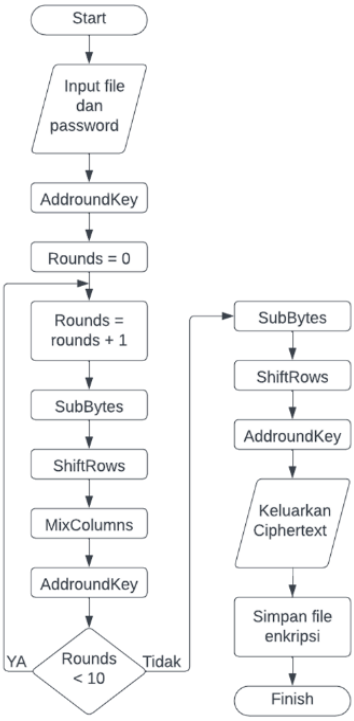
3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

Pada *flowchart* ini merupakan *flowchart* dimana pengguna memilih dokumen yang ingin dienkripsi dan membuat *password* untuk dokumen. *Flowchart* dari submenu enkripsi ditunjukkan pada Gambar 2 berikut.

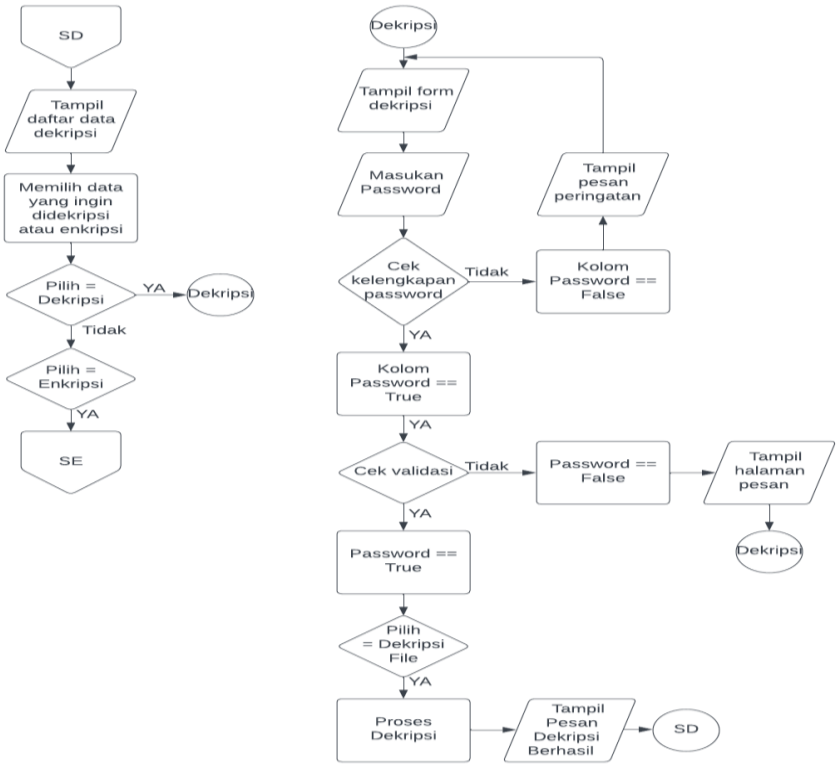
Gambar 2. *Flowchart* Submenu Enkripsi

Pada proses enkripsi menggunakan AES 128 dilakukan 10 putaran dan setiap putaran menggunakan *roundkey* yang berbeda. *Flowchart* dari enkripsi AES 128 bisa dilihat pada Gambar 3 berikut.



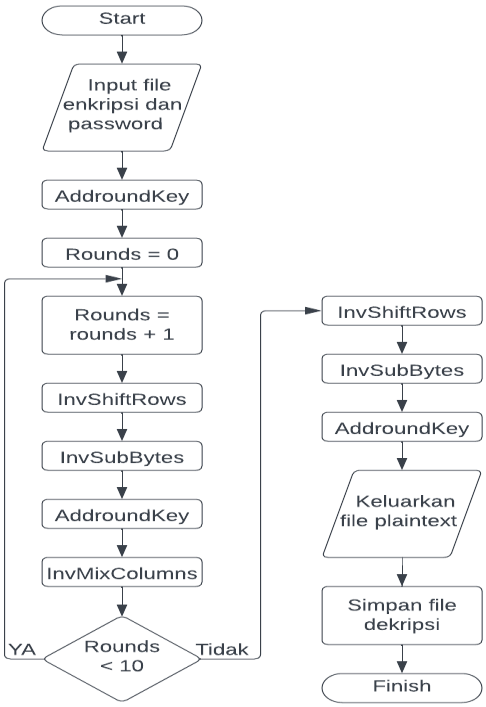
Gambar 3. *Flowchart* Enkripsi AES-128

Pada *flowchart* submenu data dekripsi adalah *flowchart* yang menjelaskan tentang alur halaman dekripsi. Di halaman ini akan muncul daftar data–data enkripsi yang telah dilakukan pengguna berikut dengan informasi tambahan seperti no, nama file sumber, nama file enkripsi, path file, status file, dan aksi. Aksi yang bisa dilakukan di halaman ini adalah aksi dekripsi dan aksi enkripsi. *Flowchart* dari submenu dekripsi digambarkan pada gambar 4.



Gambar 4. *Flowchart* Submenu Dekripsi

Pada diagram *flowchart* untuk dekripsi AES-128 adalah alur jalannya proses dekripsi AES-128. *Flowchart* dekripsi AES-128 ditunjukkan pada Gambar 5 berikut.



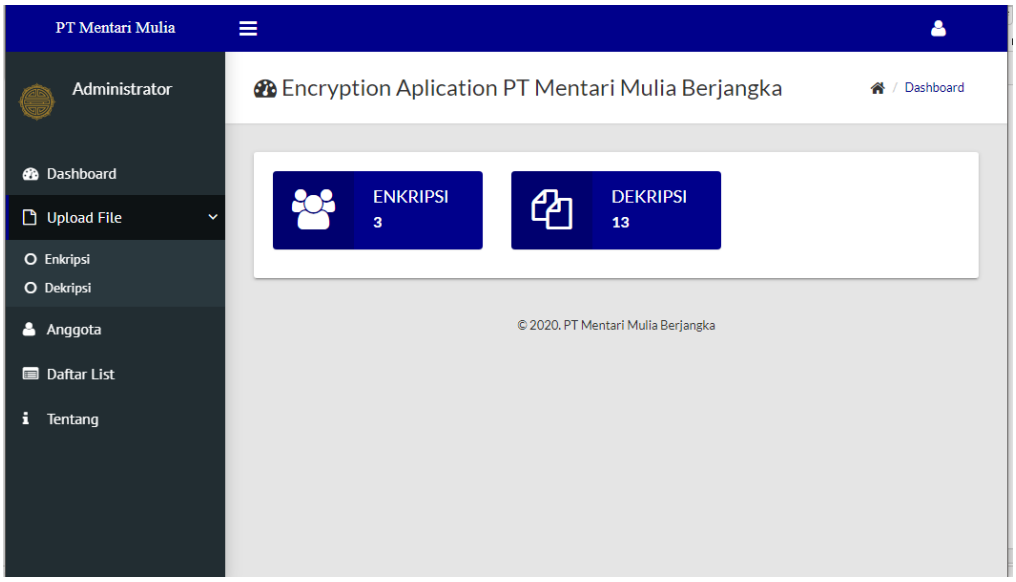
Gambar 5. *Flowchart* Proses Dekripsi AES-128

3.2 Tampilan Layar

Pada halaman *login* adalah halaman yang pertama kali dilihat pada aplikasi enkripsi dan dekripsi pada PT Mentari Mulia Berjangka. Pada halaman ini memiliki form *login* untuk mengisi *username*, *password* dan tombol *login*. Tampilan layar halaman *login* ditunjukkan pada Gambar 6.

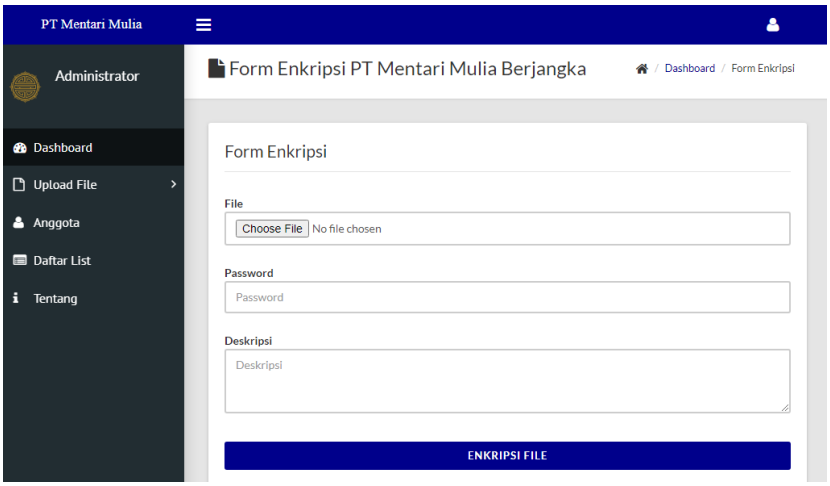
Gambar 6. Tampilan Layar Halaman *Login*

Setelah *login* sebagai admin maka tampilan layar halaman *dashboard* admin akan muncul, halaman *dashboard* admin adalah halaman yang terdapat informasi mengenai jumlah dokumen yang telah dienkripsi dan dekripsi. Di halaman ini juga terdapat menu lain seperti menu anggota, menu upload file, menu tentang dan menu daftar list dan di bagian atas terdapat tombol *logout*. Tampilan layar halaman *dashboard* admin ditunjukkan pada Gambar 7.



Gambar 7. Tampilan Layar Halaman *Dashboard* Admin

Jika pengguna aplikasi memilih submenu enkripsi maka akan tampil halaman layar submenu enkripsi, menu ini tidak tersedia bagi pengguna dengan akun *user*. Pada halaman ini terdapat halaman yang digunakan untuk mengenkripsi dokumen yang berformat *Doc*,*Docx*, *Pdf*, *Ppt*, *Pptx*, *Xls*, *Xlsx* dan *Txt* dan ukuran dokumen tidak lebih dari 3 MB. Tampilan layar halaman submenu enkripsi ditunjukkan pada Gambar 8.

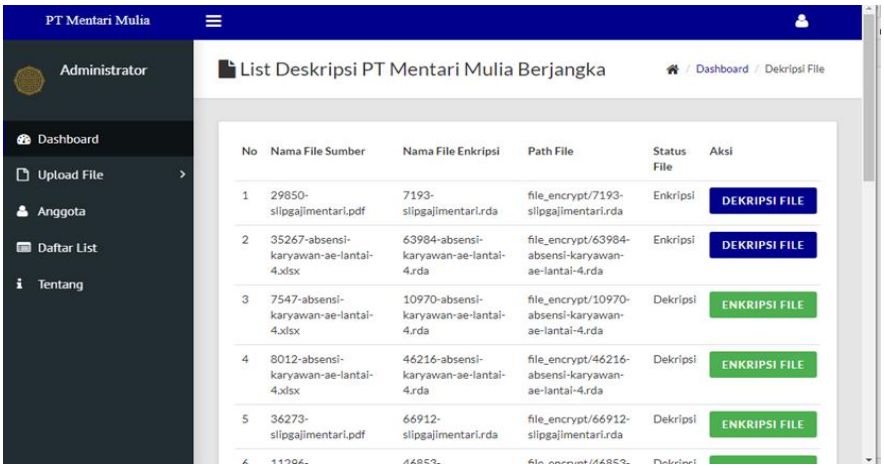


Gambar 8. Tampilan Layar Halaman Submenu Enkripsi

Jika pengguna mengupload melebihi ukuran 3 MB maka akan muncul pesan eror pada aplikasi. Pesan eror ditunjukan pada Gambar 9.

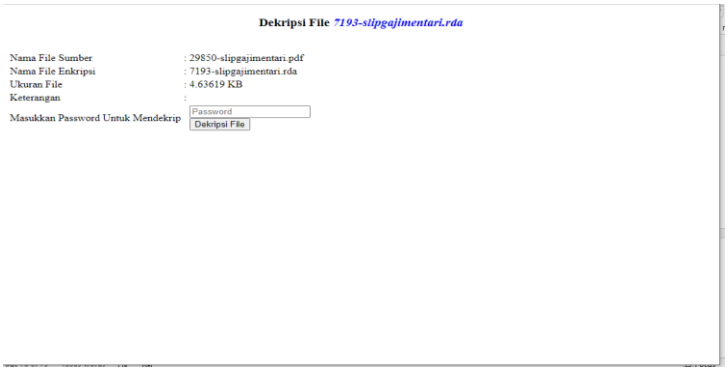
Gambar 9. Pesan eror saat pengguna mengupload file dokumen lebih besar dari kapasitas aplikasi.

Jika pengguna ingin melakukan dekripsi maka pengguna bisa memilih submenu dekripsi untuk memilih file dokumen yang ingin didekripsi. Tampilan layar submenu dekripsi ditunjukkan pada Gambar 10 berikut.



Gambar 10. Tampilan Layar Halaman Submenu Dekripsi

Jika pengguna menekan tombol dekripsi file maka akan menuju ke halaman baru yaitu halaman untuk melakukan proses dekripsi dan jika pengguna menekan tombol enkripsi maka akan menuju ke halaman submenu enkripsi, pengguna harus mengisikan *password* untuk melakukan proses dekripsi. Tampilan halaman proses dekripsi ditunjukkan pada Gambar 11 berikut.



Gambar 11. Tampilan Layar Halaman Proses Dekripsi

3.3 Pengujian

Setelah kebutuhan *software* dan *hardware* terpenuhi, maka bisa dilakukan proses pengujian sistem keamanan dokumen berupa aplikasi yang telah dibuat. Pada pengujian ini akan diuraikan proses enkripsi dan proses dekripsi file dokumen dari *plaintext* ke *ciphertext* dan proses mengembalikan *ciphertext* ke *plaintext*. Pengujian tersebut akan menghasilkan perbandingan antara *plaintext* dan *ciphertext* pada aplikasi ini. Tabel 1 di bawah ini menunjukan hasil dari proses enkripsi dan proses dekripsi yang dilakukan oleh aplikasi ini.

Tabel 1. Pengujian Enkripsi Dokumen

Nama File	Password	Nama File Enkripsi	Tempat File Enkripsi	Ukuran File Asli	Ukuran File Enkripsi	Waktu Enkripsi
slipGajiMentari.pdf	123	17719-slipgajimentari.RDA	C:\xampp\htdocs\TA_181150 1012\dashboard\file_encrypt\ 17719-slipgajimentari.rda	13.9 KB	13.9 KB	2.09 detik
Absensi Karyawan AE lantai 4.xlsx	`123	1229-absensi-karyawan-ae-lantai-4.RDA	C:\xampp\htdocs\TA_181150 1012\dashboard\file_encrypt\ 1229-absensi-karyawan-ae-lantai-4.rda	11.0 KB	11.0 KB	1.89 detik

Tabel 2. Pengujian Dekripsi Dokumen

Nama File	Password	Nama File Dekripsi	Tempat File Dekripsi	Ukuran File Asli	Ukuran File Dekripsi	Waktu Dekripsi
slipGajiMentari.pdf	123	44195-slipgajimentari.pdf	C:\xampp\htdocs\TA_18115 01012\dashboard\file_decrypt\44195-slipgajimentari.pdf	13.9 KB	13.9 KB	2.01 detik
Absensi Karyawan AE lantai 4.xlsx	`123	7571-absensi-karyawan-ae-lantai-4.xlsx	C:\xampp\htdocs\TA_18115 01012\dashboard\file_decrypt\7571-absensi-karyawan-ae-lantai-4.xlsx	11.0 KB	11.0 KB	1.75 detik

Dapat dilihat pada Tabel 2 di atas waktu enkripsi AES-128 pada dokumen slipGajiMentari.pdf adalah 2.09 detik dan untuk waktu dekripsinya adalah 2.01 detik sedangkan kecepatan enkripsi AES-128 pada dokumen Absensi Karyawan AE lantai 4.xlsx adalah 1.89 detik dan waktu dekripsinya adalah 1.75 detik. Rata-rata waktu enkripsi AES-128 pada data di atas adalah 1.89 detik dan rata-rata waktu dekripsi AES-128 adalah 1.88 detik.

4. KESIMPULAN

Kesimpulan yang diperoleh setelah melakukan melakukan perancangan, pembuatan, serangkaian uji coba analisis program sistem keamanan berupa aplikasi pengamanan dokumen ini adalah aplikasi ini dapat membantu mengamankan dokumen dan merahasiakannya dari pihak yang tidak memiliki hak. Kelebihan dari aplikasi ini adalah dapat mengamankan dokumen yang sudah dienkripsi dan hasil dekripsi dari aplikasi ini tidak mengalami perubahan sama seperti file dokumen aslinya. Sedangkan kekurangan aplikasi ini yaitu ukuran file dokumen yang dienkripsi tidak boleh dari 3 MB. Saran untuk penelitian selanjutnya adalah diharapkan ukuran file dokumen yang bisa diupload ditingkatkan melebihi 3 MB dan waktu untuk proses enkripsi dan proses dekripsi ditingkatkan supaya lebih cepat.

DAFTAR PUSTAKA

[1] R. Firdaus dan R. R. Santika, “Penerapan Algoritme AES-128 Untuk Enkripsi Dokumen di PT Caveo Biometric Security”, SENAFTI, vol. 1, no. 1, hlm. 111–120, Sep 2022.

[2] S. I. H. Abimanyu, D. Kusumaningsih, P. Purwanto, dan W. Windarto, “Implementasi Algoritme Advanced Encryption Standar (AES-128) Untuk Mengamankan Dokumen Pada PT. JIA DREAMS COMMUNICATIONS”, SENAFTI, vol. 2, no. 1, hlm. 88–96, Apr 2023.

[3] N. Dwitri, S. Sindi, dan I. A. Sihombing, "Pengamanan Data File Document Menggunakan Kriptografi Encryption System (DES)," JISICOM (Journal of Information System, Informatics and Computing), vol. 4, no. 1, hal. 40-45, Juni 2020.

[4] K. Zalukhu, Y. Syahra, and T. Syahputra, “Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritme Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan,” J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD), vol. 3, no. 2, p. 138, 2020, doi: 10.53513/jsk.v3i2.2419.

[5] R. Andriyanto, K. Khairijal, and D. Satria, “Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION”, JURNAL TEKNOLOGI UNIVERSAL, vol. 13, no. 1, pp. 34-48, Jun. 2020.

[6] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, “Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritme Kriptografi Advanced Encryption Standard (AES) Jurnal Pendidikan Sains dan Komputer”, Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 1, hlm. 163–171, 2022.

[7] P. A. Wijaya, M. Damanik, P. Hartati, I. Gunawan, “Implementasi Enkripsi Dan Deskripsi Data SIAK (Sistem Informasi Administrasi Kependudukan) Menggunakan Algoritme DES, AES dan MD5”, TECHSI - Jurnal Teknik Informatika, vol. 12, no. 1, hlm. 43–51, 2020.

[8] M. B. P. Sansaya, A. Farisi, “Perbandingan Kinerja Algoritme Kandidat AES Dalam Enkripsi dan Dekripsi File Dokumen”, MDP Student Conference, vol. 2, no. 1, hlm. 282– 289, Apr 2023.

[9] E. E. Awal, E. H. Nurkifli, T. N. Padilah, “Analisis Perbandingkan Hasil Enkripsi dan Dekripsi Algoritme Kriptografi Rijndael Dan Twofish Untuk Penyandian Data”, Jurnal Mahasiswa Ilmu Komputer (JMIK), vol. 3, no. 1, hlm. 260–265, Mar 2022.

[10] B. E. Nino, “Perbandingan Performa Algoritme AES dan Twofish Menggunakan Metode Strict Avalanche Criterion pada Nomor Induk Kependudukan Indonesia”, Jurnal Teknologi Informasi, vol. 9, no. 1, hlm. 19-29, Juni 2023.