3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENGAMANAN FILE DOKUMEN MENGGUNAKAN KRIPTOGRAFI DENGAN METODE AES-128 BERBASIS WEB PADA PT MAKARA MULIA

Michael Setyawan[1*], Noni Juliasari[2]

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

Email: [1*]michaelsetyawan6@gmail.com, [2]noni.juliasari@budiluhur.ac.id
(* : corresponding author)

Abstrak-Teknologi komputer saat ini berkembang menggunakan algoritma yang dikembangkan oleh banyak ahli, terutama algoritma kriptografi yang berkembang pesat untuk menjaga keamanan data. Data atau file akuntansi biasanya dibuat di perusahaan PT Makara Mulia, seperti file gaji karyawan, perjanjian kontrak kerja, dan data pelanggan. Ini karena data atau file tersebut masih aktual dan belum tersimpan dengan aman dan masih tersimpan di folder komputer, sehingga orang yang tidak bertanggung jawab dapat melihatnya di flashdisk. Untuk menjaga keamanan data atau file di perusahaan ini, penulis melakukan proses enkripsi dan dekripsi file. Metode enkripsi yang digunakan dalam penelitian ini adalah salah satu metode yang digunakan. Jika perangkat lunak dapat mendekripsi dan mengenkripsi database aplikasi, file akan selalu aman karena kata sandi atau kunci juga dienkripsi. Dengan menambahkan karakter Randomize, konsep perlindungan data informasi untuk sistem yang mengenkripsi dan mendekripsi algoritma Advanced Encryption Standard (AES-128) telah berubah. Dalam tahap pengujian, file xlsx dengan ukuran 577 KB dienkripsi dalam 54.36 detik dan didekripsi dalam 1.43 detik, sedangkan file pdf dengan ukuran 388 KB dienkripsi dalam 37.85 detik dan didekripsi dalam 57.46 detik, yang menunjukkan bahwa waktu dekripsi lebih cepat daripada waktu enkripsi. Jika file data asli dienkripsi, mereka akan menjadi tidak dapat dibaca, tetapi file yang lebih besar akan membutuhkan waktu lebih lama untuk dienkripsi dan didekripsi. Hasil pengujian menunjukkan bahwa ukuran file tidak berubah, yang berarti algoritma enkripsi AES-128 dapat digunakan untuk menjaga konten file aman.

Kata Kunci: Kriptografi, AES-128, Enkripsi , Dekripsi, Modifikasi.

DOCUMENT FILE SECURITY USING CRYPTOGRAPHY WITH THE WEB BASED AES-128 METHOD AT PT MAKARA MULIA

Abstract-*Computer technology is currently developing using algorithms developed by many experts, especially cryptographic algorithms which are growing rapidly to maintain data security. Accounting data or files are usually made at PT Makara Mulia, such as employee salary files, work contract agreements, and customer data. This is because the data or files are still current and have not been stored safely and are still stored in computer folders, so that irresponsible people can view them on a flash drive. To maintain the security of data or files in this company, the author performs file encryption and decryption processes. The encryption method used in this study is one of the methods used. If the software can decrypt and encrypt the application database, the files will always be safe because the password or key is also encrypted. By adding the Randomize character, the concept of information data protection for systems that encrypt and decrypt the Advanced Encryption Standard (AES-128) algorithm has changed. In the testing phase, an xlsx file with a size of 577 KB was encrypted in 54.36 seconds and decrypted in 1.43 seconds, while a pdf file with a size of 388 KB was encrypted in 37.85 seconds and decrypted in 57.46 seconds, which shows that the decryption time is faster than the encryption time. If the original data files were encrypted, they would become unreadable, but larger files would take much longer to be encrypted and decrypted. The test results show that the file size has not changed, which means that the AES-128 encryption algorithm can be used to keep file contents safe.*

Keywords*: Cryptography, AES-128, Encryption, Decryption, Modification.*

1. PENDAHULUAN

Sejarah Kriptografi Pada tahun 3000 SM, Mesir menggunakan penulisan rahasia. Mereka menggunakan hieroglyphics untuk mencegah orang yang tidak diharapkan menulis. Hieroglyphs berasal dari bahasa Yunani Hieroglyphica, yang berarti ukiran rahasia [2], dan kemudian berkembang menjadi hieratic, yaitu skrip yang distylized yang lebih mudah dibaca. Sekitar tahun 400 SM, bangsa Spartan menggunakan kriptografi militer dalam bentuk sepotong papyrus atau perkamen yang dibungkus dengan batang kayu. Scytale adalah nama lain dari sistem ini [1].

Kriptografi adalah seni dan ilmu yang mempelajari bagaimana membuat pesan yang dikirim oleh orang yang mengirimkannya aman sampai ke orang yang menerimanya [3]. Kriptografi adalah bagian dari cabang ilmu matematika yang disebut kriptologi (cryptologi) [4]. Tujuan kriptografi adalah untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga orang yang tidak berwenang tidak dapat mengetahuinya. Kriptografer adalah orang yang membuat algoritma kriptografi[5].

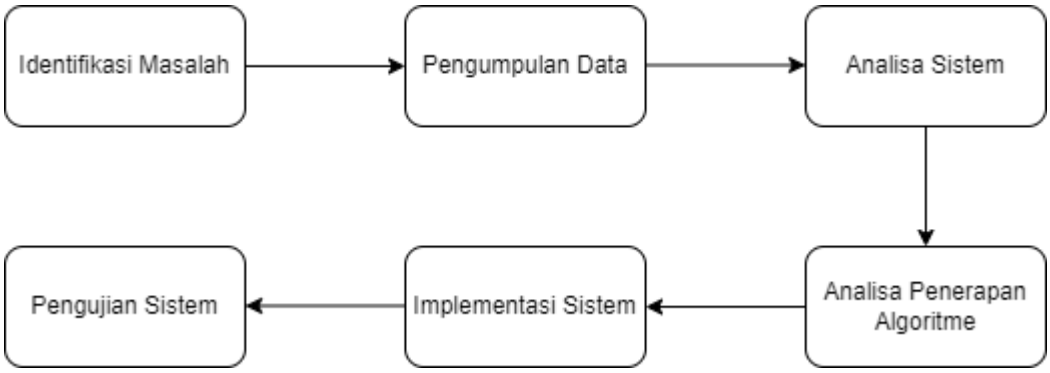
Konsep dasar kriptografi simetris adalah kunci untuk enkripsi dan dekripsi yang sama. Cryptography private key, cryptography secret key, dan cryptography konvensional adalah istilah tambahan untuk kriptografi. Dalam kriptografi kunci simetris, penerima dan pengirim pesan berbagi kunci sebelum pesan dikirim. Kerahasiaan penting sistem memastikan keamanannya [6]. Kriptografi kunci publik, atau kunci asimetris, menggunakan dua buah kunci untuk enkripsi dan dekripsi. Kriptografi kunci publik juga dikenal sebagai kriptografi kunci publik. Kriptografi asimetris ini memiliki kunci dekripsi dan enkripsi yang rahasia, yang diketahui publik. Pengirim akan menggunakan kunci publik untuk mengenkripsi pesan, sedangkan penerima akan menggunakan kunci privat untuk mendekripsi pesan [6]. Selain menjaga keamanan data, kriptografi bertujuan untuk memastikan bahwa pesan atau data tidak dapat dibaca oleh pihak yang tidak berhak. Aspek integritas menekankan bahwa tidak mungkin mengubah informasi tanpa izin pemiliknya.Jika data atau informasi yang dikirim tidak sesuai dengan yang diterima, integritas tidak akan ada.Aspek keaslian ini berkaitan dengan pendekatan yang menegaskan bahwa informasi benar-benar asli dan individu yang dapat mengaksesnya adalah individu yang dimaksud[7]. Aspek tersedia ini berkaitan dengan tersedianya data dan informasi. Dalam sistem komputer, berbagai jenis data dan informasi dapat diakses oleh pihak yang berhak. Aspek pengendalian akses ini berkaitan dengan pengaturan akses informasi. Biasanya berkaitan dengan mekanisme klasifikasi data [10]

Pengertian Advanced Encryption Standard (AES): AES adalah algoritma kriptografi yang digunakan untuk mengamankan data itu adalah simetri kunci blok untuk menggantikan DES (Standard Enkripsi Data) [10]. Data atau file seperti gaji karyawan, perjanjian kontrak kerja, dan data pelanggan adalah yang paling sering dibuat di PT Makara Mulia. Ini karena bagian akuntansi melakukannya untuk kebutuhan perusahaan atau untuk rekonsiliasi dengan vendor. Dengan demikian, data atau file yang ada tidak aman dan mungkin disimpan di folder komputer atau flash disk yang dapat diakses oleh pihak yang tidak bertanggung jawab.[9]

Tujuan penelitian ini adalah untuk membuat website yang menggunakan algoritma kriptografi Advanced Encryption Standard (AES-128) untuk enkripsi dan dekripsi file untuk perusahaan PT Makara Mulia. Ini akan membuat file rahasia perusahaan aman untuk disimpan. Manfaat dari penulisan penelitian ini adalah bahwa orang dapat menjaga file dan isi penting mereka aman.

2. METODE PENELITIAN

Metodologi penelitian digunakan sebagai pedoman untuk menjalankan penelitian agar tidak menyimpang dari rute dan tujuan awalnya. Gambar 1 menunjukkan metodologi penelitian.



Gambar 1. Tahapan Penelitian

2.1 Identifikasi Masalah

Pada tahapan ini dilakukan observasi untuk mengetahui permasalahan yang ada di PT Makara Mulia. Berdasarkan observasi yang dilakukan ditemukan belum adanya suatu sistem keamanan file dokumen. Oleh karena itu akan dibuatkan suatu sistem keamanan file dokumen berbasis web menggunakan metode AES 128.

2.2 Pengumpulan Data

Data yang dikumpulkan dalam penelitian ini melibatkan dua cara yaitu wawancara dan observasi. Wawancara dilakukan dengan direktur yang merupakan pakar dalam bidang ini, bertujuan untuk memperoleh pengetahuan yang akan digunakan sebagai basis pengetahuan (knowledge base). Data yang diperlukan mencakup jenis gaji karyawan, perjanjian kontrak kerja dan data customer. Observasi dilakukan secara langsung untuk mengamati penyimpanan file dokumen.

2.3 Analisa Sistem

Pengimplementasian keamanan pada sistem adalah sebuah proses enkripsi *file* yang akan disimpan ke dalam sebuah basis data. Enkripsi dilakukan untuk mengamankan *file* yang akan disimpan ke dalam *database*. Karena itu membutuhkan modul untuk melakukan enkripsi data tersebut pada saat melakukan penyimpanan *file* ke *database*. Modul pengenkripsian ditempatkan pada aplikasi yang akan dipanggil ketika user ingin melakukan pengamanan *file*. Sedangkan modul deskripsi dapat dipanggil jika user ingin melihat isi *file*.

2.4 Analisa Penerapan Algoritme

Sesudah tahapan mengumpulkan data dan mempelajari prosedur sistem maka selanjutnya melakukan analisa penerapan algoritme. Analisa penerapan algoritme menjelaskan tahapan untuk menerapkan metode kriptografi *Advanced Encryption Standard* (AES-128) pada proses pengamanan *file*. Pada tahapan ini dilakukan:

a. Menentukan kunci yang akan digunakan untuk proses enkripsi dan deskripsi *file*.
b. Pada proses enkripsi *file* menggunakan kunci enkripsi, dengan proses mengubah *file* di enkripsi menjadi *chipertext* menggunakan kunci enkripsi tersebut.
c. Proses deskripsi *chipertext* menggunakan kunci deskripsi yang sama dengan kunci enkripsi, dengan memproses perubahan *chipertext* menjadi *file* yang dapat terbaca kembali (*plaintext)*.

Algoritme AES-128 yang akan diterapkan merupakan algoritme yang sudah dimodifikasi khusus untuk diterapkan pada kasus penelitian ini.

2.5 Implementasi sistem

Tahap implementasi melibatkan proses mengubah desain rancangan sebelumnya menjadi kode-kode dalam bahasa pemrograman yang spesifik, dengan tujuan menciptakan sebuah aplikasi. Pada tahap ini, dilakukan pemrograman berdasarkan perancangan dan analisis yang telah dilakukan sebelumnya. Selain itu, tahap ini juga melibatkan penerapan aturan-aturan ke dalam mesin inferensi dengan menggunakan penalaran metode algoritme advanced encryption standard 128 dalam bahasa pemrograman PHP.

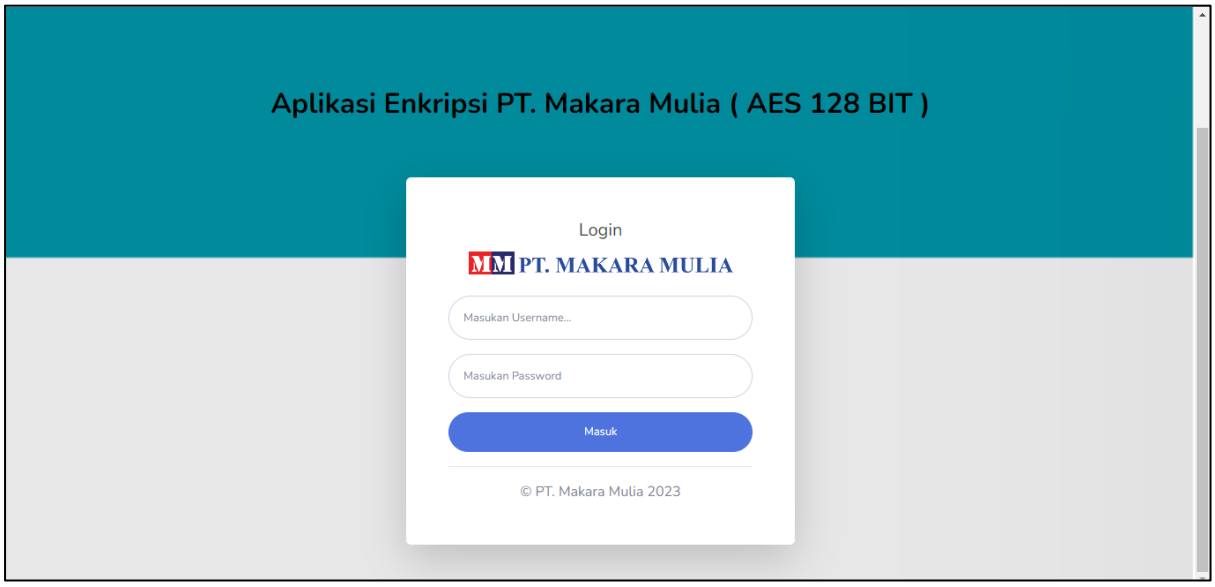
2.6 Pengujian Sistem

Tujuan dari tahapan ini adalah untuk memastikan bahwa sistem berjalan sesuai dengan proses analisa dan perancangan yang diharapkan. Selama proses pengujian ini, ditemukan bahwa sistem sesuai dengan tujuan awalnya dan dapat digunakan dengan baik untuk memenuhi fungsi yang diinginkan.

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Halaman *Login*

Pada tampilan layar halaman *login* ini terdapat tampilan background, *login* dan *form login* berisi *username*, *password* dan button masuk. Berikut tampilan layar halaman *login*.



Gambar 3. Tampilan Halaman *Login*

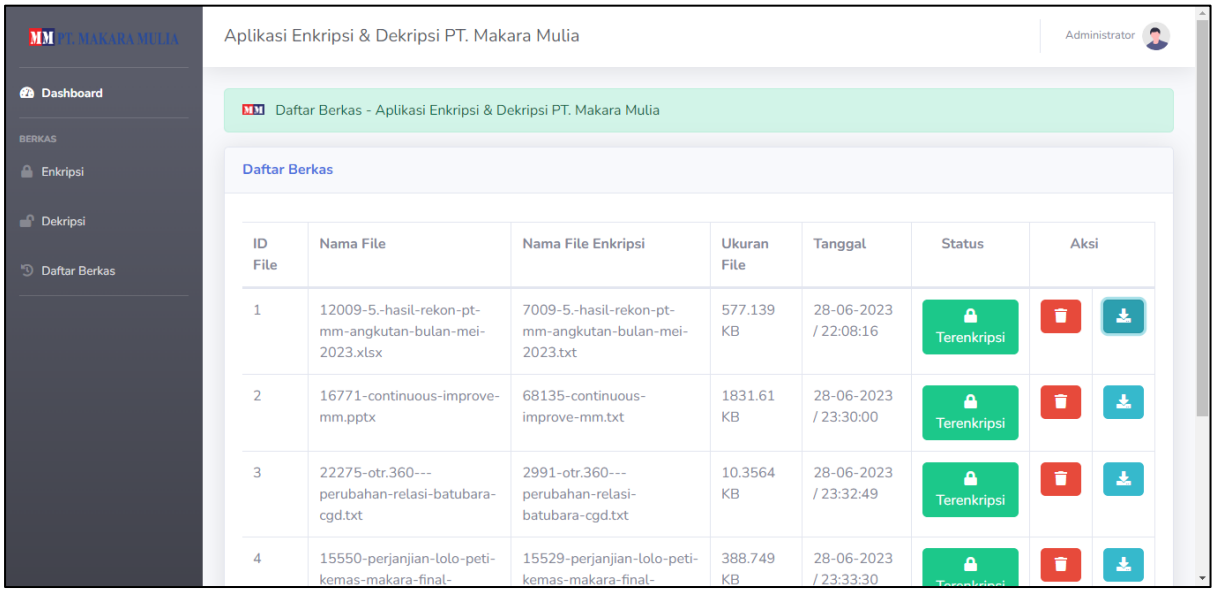
3.2 Tampilan Halaman Utama

Pada tampilan layar halaman utama ini terdapat gambar pada *profile*, menu-menu yaitu: *Dashboard*, daftar berkas, Enkripsi dan Dekripsi, terdapat logo dari perusahaan PT Makara Mulia, tampilan yang berisi total file yang terenkripsi dan terdekripsi, dibagian bawah terdapat penjelasan singkat dari aplikasi enkripsi, terakhir terdapat tombol dengan logo *logout*. Berikut tampilan layar halaman utama.

Gambar 4. Tampilan Halaman Utama

3.3 Tampilan Halaman Daftar Berkas

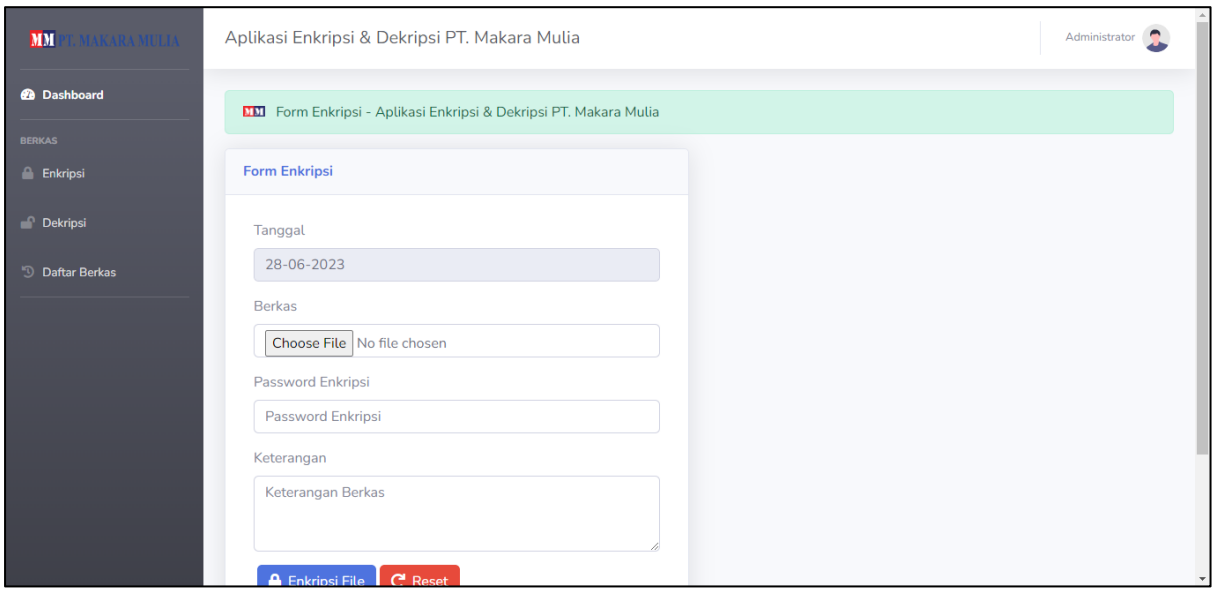
Pada tampilan layar daftar berkas ini terdapat tampilan berbentuk tabel yang berisi berkas yang telah di enkripsi dengan isi pada tabel yaitu id *file*, nama *file*, nama *file* enkripsi, ukuran *file*, tanggal, status dan aksi di mana status ini bisa berubah jika *file* sudah terdekripsi, sementara pada tabel ini *file* masih dalam status terenkripsi, serta dilengkapi dengan pilihan menu *Dashboard*, daftar berkas, Enkripsi, Dekripsi dan sign out. Berikut tampilan layar daftar berkas.



Gambar 5. Tampilan Halaman Daftar Berkas

3.4 Tampilan Halaman Enkripsi

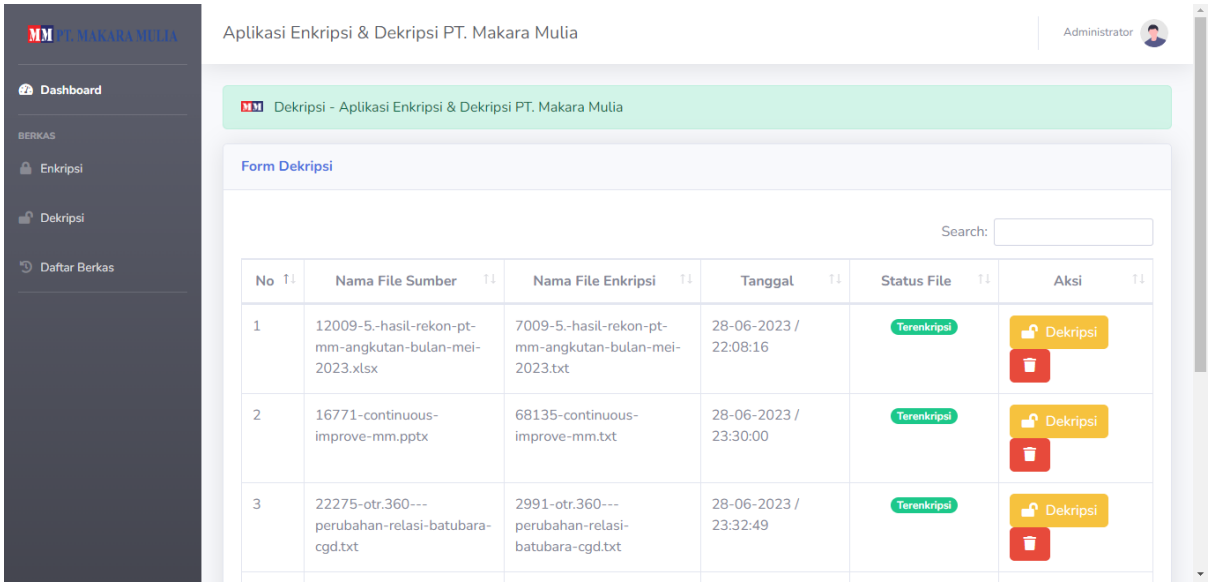
Pada tampilan layar enkripsi berkas ini terdapat judul enkripsi berkas , dibagian bawah logo terdapat form yang diisi pada saat ingin mengenkripsi berkas yang perlu diisi yaitu: tanggal, berkas di mana kita memilih berkas pada penyimpanan pada komputer berkas yang ingin di enkripsi, lalu terdapat *password* untuk *file* yang ingin di enkripsi, keterangan dan tombol button untuk melakukan proses enkripsi *file*, serta dilengkapi dengan pilihan menu *Dashboard*, daftar berkas, Enkripsi, Dekripsi dan *sign out*. Berikut tampilan layar enkripsi berkas.



Gambar 6. Tampilan Halaman Enkripsi

3.5 Tampilan Halaman Dekripsi

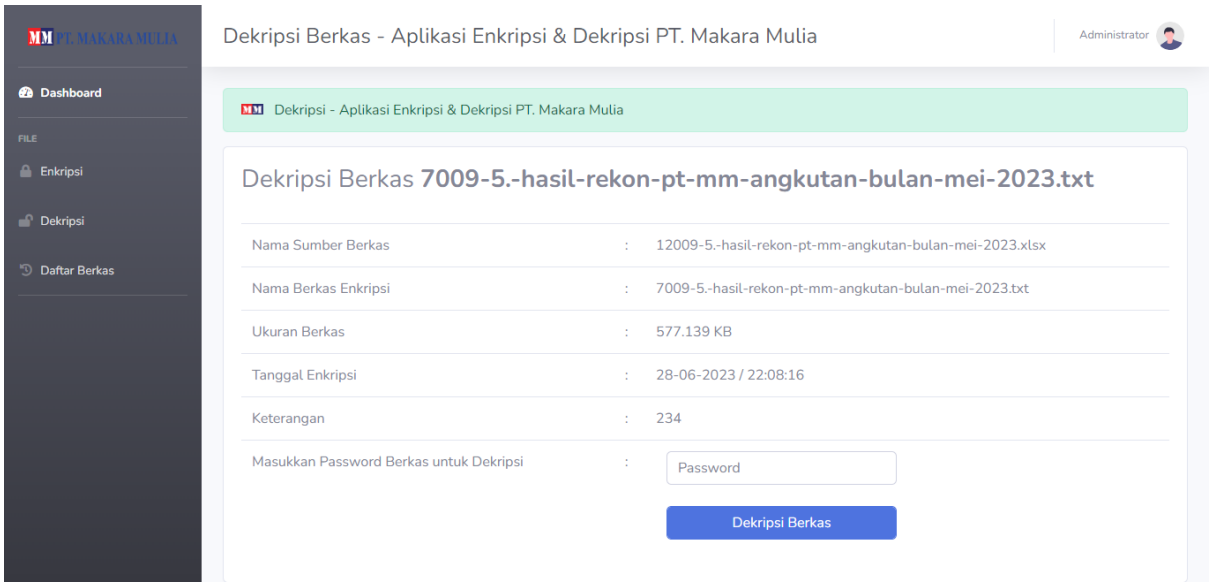
Pada tampilan layar dekripsi berkas ini terdapat tampilan berbentuk tabel yang berisi *file* yang telah di enkripsi dan dekripsi dengan isi pada tabel yaitu no, nama *file* sumber, nama *file* Enkripsi, tanggal, status *file* dan aksi status di mana aksi status ini bisa merubah berkas yang ingin di dekripsi, serta dilengkapi dengan pilihan menu *Dashboard*, Daftar Berkas, Enkripsi, Dekripsi dan *sign out*. Berikut tampilan layar dekripsi berkas.



Gambar 7. Tampilan Halaman Dekripsi

3.6 Tampilan Halaman Mendekripsi Berkas

Pada tampilan layar untuk mendekripsi berkas ini terdapat judul berkas yang sudah terenkripsi, dibawahnya terdapat form yang sudah diisi yaitu: nama sumber berkas, nama berkas enkripsi, ukuran berkas, tanggal enkripsi, keterangan, dan *password* yang harus diisi yang untuk mendekripsi *file* atau membuka *file*, setelah *password* diinput terdapat button untuk melakukan proses dekripsi berkas, serta dilengkapi dengan pilihan menu *Dashboard*, daftar berkas, Enkripsi, Dekripsi dan *sign out*. Berikut tampilan layar untuk mendekripsi berkas.



Gambar 8. Tampilan Halaman Mendekripsi Berkas

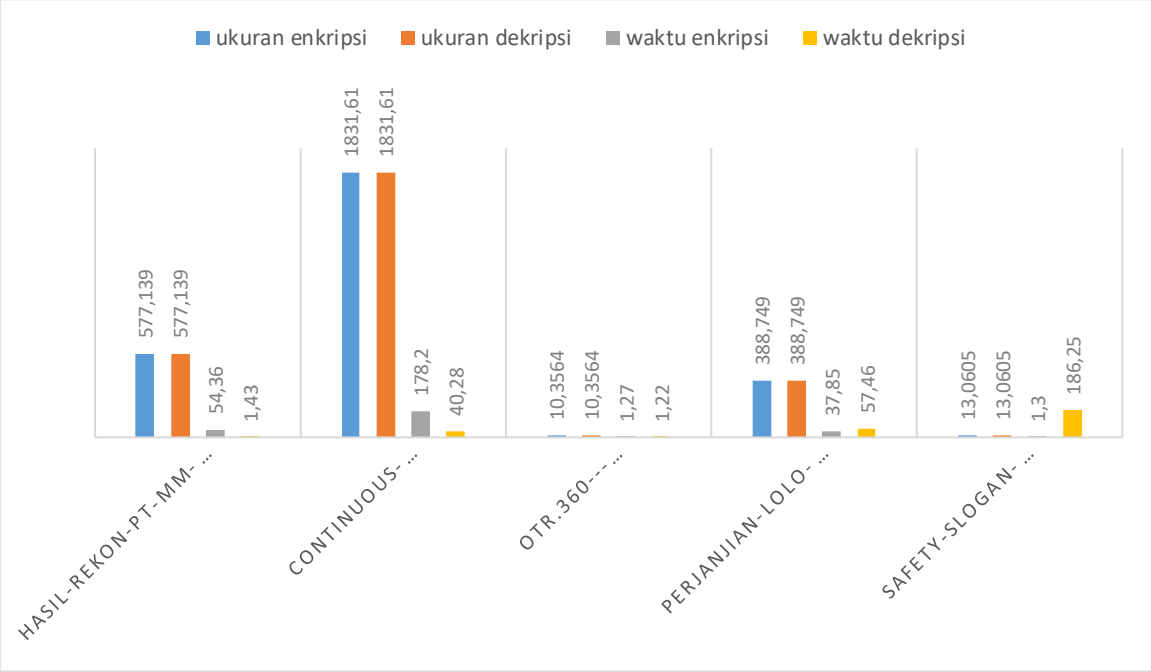
3.7 Tabel Pengujian

Tabel 2. Pengujian Enkripsi dan Dekripsi Berkas

Nama File	Nama File Setelah di Enkripsi	Ukuran File			Waktu	
		Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
hasil-rekon-pt-mm-angkutan-	150825.-hasil-rekon-pt-mm-angkutan-bulan-mei-2023.txt	577,139 KB	577,139 KB	577,139 KB	54.36 detik	1.43 Detik

bulan-mei-2023.xlsx						
continuous-improve-mm.pptx	89671-ontinuous-improve-mm.txt	1831,61 KB	1831,61 KB	1831,61 KB	178.2 Detik	40.28 Detik
otr.360---perubahan-relasi-batubara-cgd.txt	33448-otr.360---perubahan-relasi-batubara-cgd.txt	10,3564 KB	10,3564 KB	10,3564 KB	1.27 Detik	1.22 Detik
perjanjian-lolo-peti-kemas-makara-final-23082018(1).pdf	16136-perjanjian-lolo-peti-kemas-makara-final-23082018(1).txt	388,749 KB	388,749 KB	388,749 KB	37.85 Detik	57.46 Detik
safety-slogan-atau-moto-k3.docx	88689-safety-slogan-atau-moto-k3.txt	13,0605 KB	13,0605 KB	13,0605 KB	1.3 Detik	186.25 Detik

3.8 Grafik Pengujian



Gambar 9. Grafik Pengujian

3.9 Kelebihan Aplikasi

a. File setelah di enkripsi terdapat perubahan dengan dua bentuk yaitu perubahan dan penambahan angka pada baris awal nama file dan penambahan atau penjelasan pada nama file seperti "*file_enrypt*"
b. File ketika terenkripsi terkunci dengan aman karena terpassword
c. File yang sudah dienkripsi tidak bisa dibaca sebelum melakukan dekripsi terhadap file tersebut.
d. Tampilan website yang simple sehingga mudah dipahami oleh pengguna.

3.10 Kekurangan Aplikasi

a. File yang dapat diproses untuk dienkripsi tidak lebih dari 5mb
b. Semakin besar file maka semakin lama enkripsi filenya
c. Aplikasi hanya bisa enkripsi dan dekripsi file.

4. KESIMPULAN

Setelah perancangan selesai, Sistem Keamanan Data atau File menjadi solusi untuk mengamankan data atau file di bagian akuntansi seperti gaji karyawan, data pelanggan, dan perjanjian kontrak kerja. Setelah diimplementasikan, sistem ini dapat membantu PT Makara Mulia perusahaan dalam mengamankan data atau file dengan menggunakan algoritma enkripsi standar yang canggih. Dalam tahap pengujian, file xlsx dengan ukuran 577 KB dienkripsi dalam 54.36 detik dan didekripsi dalam 1.43 detik, sedangkan file pdf dengan ukuran 388 KB dienkripsi dalam 37.85 detik dan didekripsi dalam 57.46 detik, yang menunjukkan bahwa waktu dekripsi lebih cepat daripada waktu enkripsi. Diharapkan aplikasi ini dapat dikembangkan tidak hanya di platform web, tetapi juga di platform Android atau IOS. Penelitian selanjutnya diharapkan dapat menyempurnakan dan mengembangkan tampilan aplikasi untuk menjadi lebih menarik.

DAFTAR PUSTAKA

[1] I. Asih, R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, 2020.

[2] Dian Widyawan and Imelda, "PENGAMANAN FILE MENGGUNAKAN KRIPTOGRAFI DENGAN METODE AES-128 BERBASIS WEB DI KOMITE NASIONAL KESELAMATAN TRANSPORTASI ," vol. 4, pp. 15–22, Jan. 2021.

[3] 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, doi: 10.47709/jpsk.v2i1.1390.

[4] B. Sihombing, D. Patresia, S. Manrung, E. Ahadi, and I. Gunawan, "PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOFRAFI ALGORITMA VIGENERE CHIPER DARI SERANGAN EAVESDROPPING," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 4, no. 1, 2020.

[5] Edi Susanto, "PERANGKAT LUNAK KEAMANAN BERBASIS FILE MENGGUNAKAN ALGORITMA KRIPTOGRAFI VIGENERE CIPHER," *Comasie*, vol. 4, no. 6, pp. 80–88, 2021.

[6] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2590.

[7] N. Cristy and F. Riandari, "Niolinda Cristy 1 , Fristi Riandari 2 [Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," vol. 4, no. 2, p. 75, 2021.

[8] R. Firmansyah and A. A. Permana, "IMPLEMENTASI KEAMANAN PESAN TEKS MENGGUNAKAN KRIPTOGRAFI ALGORITMA RSA DENGAN METODE WATERFALL BERBASIS JAVA," 2019.

[9] A. Eka Putri, A. Kartikadewi, and L. A. Abdul 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, doi: 10.15408/aism.v3i2.14722.

[10] R. Andriyanto *et al.*, "Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION," vol. 13, no. 1, 2020.