PENGAMANAN DATA KEUANGAN MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* 128 PADA PT. CHARISE DEO INDONESIA

Aif Ramadan[1*], Painem[2]

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

Email: [1*]Afrmdhn70@gmail.com, [2]Painem@budiluhur.ac.id
(* : corresponding author)

Abstrak-PT. Charise Deo Indonesia adalah perusahaan yang bergerak dibidang perdangan Air Minum Dalam Kemasan (AMDK). Data yang ada pada PT. Charise Deo Indonesia masih berupa data asli yang belum dilindungi dengan sistem pengamanan data termasuk data keuangan, data keuangan disuatu perusahaan sangatlah penting sehingga perlu dijaga agar tidak dapat dimanipulasi atau disalahgunakan oleh pihak yang tidak memiliki wewenang, maka dengan itu mengamankan data sangatlah penting untuk menjaga kerahasiaannya setiap saat. Penelitian ini bertujuan untuk membuat sistem pengamanan *file* data keuangan berbasis web dengan mengimplementasikan enkripsi pada isi data file menggunakan algoritma *Advanced Encryption Standard* (AES-128). Sehingga *file* asli tidak dapat dibaca oleh pihak yang tidak berkepentingan. salah satunya caranya adalah menggunakan algoritma kriptografi untuk enkripsi pada data yang banyak digunakan saat ini. Metode *Advanced Encryption Standard* (AES) adalah algoritma kriptografi yang dapat melakukan enkripsi dan dekripsi data dan merupakan salah satu metode kriptografi yang dapat diandalkan dalam mengamankan data. Berdasarkan penelitian yang dilakukan, didapatkan sebuah kesimpulan bahwa, aplikasi enkripsi data keuangan menggunakan metode *Advanced Encryption Standard* (AES-128) berbasis *website* ini dapat meningkatkan keamanan data pada PT. Charise Deo Indonesia. Isi data telah diacak dengan menggunakan huruf, angka, simbol, atau kombinasi ketiganya. Data yang terenkripsi tidak dapat dipahami jika dekripsi tidak dilakukan dengan kunci yang sesuai untuk mengenkripsi data. Hasil dari penelitian ini berdasarkan beberapa pengujian yang dilakukan, keamanan data ini berjalan cukup baik dengan rata-rata waktu enkripsi 1,2687 detik.

Kata Kunci: pengamanan *file*, data keuangan, enkripsi, dekripsi, kriptografi, *advanced encryption standard* 128

SECURITY OF FINANCIAL DATA USING THE ADVANCED ENCRYPTION STANDARD 128 ALGORITHM AT PT. CHARISE DEO INDONESIA

Abstract- *PT. Charise Deo Indonesia is a company engaged in the trade in Bottled Drinking Water (AMDK). Existing data on PT. Charise Deo Indonesia is still in the form of original data that has not been protected by a data security system including financial data, financial data in a company is very important so it needs to be guarded so that it cannot be manipulated or misused by parties who do not have the authority, so securing data is very important to maintain its confidentiality. at all times. This study aims to create a web-based financial data file security system by implementing encryption on the contents of the data file using the Advanced Encryption Standard (AES-128) algorithm. So that the original file cannot be read by unauthorized parties. one way is to use a cryptographic algorithm for encryption of data that is widely used today. The Advanced Encryption Standard (AES) method is a cryptographic algorithm that can encrypt and decrypt data and is one of the most reliable cryptographic methods in securing data. Based on the research conducted, it is concluded that the financial data encryption application using the Advanced Encryption Standard (AES-128) method based on this website can improve data security at PT. Indonesian Charise Deo. The contents of the data have been scrambled using letters, numbers, symbols, or a combination of the three. The encrypted data cannot be understood if the decryption is not performed with the appropriate key to encrypt the data. The results of this study based on several tests carried out, this data security runs quite well with an average encryption time of 1.2687 seconds.*

Keywords*: file security, financial data, encryption, decryption, cryptography, advanced encryption standard* 128

1. PENDAHULUAN

PT. Charise Deo Indonesia adalah perusahaan yang bergerak dibidang perdagangan air dalam kemasan. PT. Charise Deo Indonesia telah menerapkan teknologi informasi untuk pengelolaan data, tetapi data-data pada perusahaan ini berupa dokumen asli (plaintext) yang belum memiliki sebuah pengamanan dan dapat dibaca dengan mudah [1]. Hal ini dapat menyebabkan permasalahan karena data yang ada pada perusahaan tersebut khususnya data laporan keuangan adalah data pribadi yang bersifat rahasia [2]. Untuk mencegah pihak yang tidak memiliki wewenang dapat memanipulasi data-data keuangan tersebut dan menimbulkan risiko kebocoran data [3]. Berkaitan

dengan permasalahan tersebut, oleh karena itu penelitian ini diimplementasikan konsep pengamanan pada isi data atau dapat disebut dengan istilah kriptografi [4].

Atas dasar itu, maksud dari penelitian ini adalah untuk membuat aplikasi pengamanan data di PT. Charise Deo Indonesia dengan tujuan untuk membuat aplikasi pengamanan file data keuangan menggunakan teknik kriptografi dengan metode *Advanced Encryption Standard* (AES-128) berbasis *website* agar data tetap terjaga keaslian dan kerahasiannya sehingga tidak dapat dimanipulasi oleh orang yang tidak memiliki wewenang [5].

Pada kriptografi ada beberapa metode yang bisa digunakan pada keamanan data [6]. Pada hakikatnya data yang perlu diamankan harus melalui proses enkripsi, sehingga isi data tidak dapat dibaca karena telah terkunci [7]. jika *file* ingin dibaca kembali, maka dilakukan proses dekripsi untuk mengembalikan data yang terenkripsi ke data asli atau *plaintext*.

Algoritma enkripsi *Advanced Encryption Standard* (AES-128) menggunakan empat transformasi dasar dengan urutan transformasi subbytes, shiftrows, mixcolumns, dan addroundkey. Pada roses dekripsi menggunakan kebalikan dari semua transformasi dasar algoritma AES kecuali addroundkey yang memiliki urutan transformasi invshiftrows, invsubbytes, addroundkey, dan invmixcolumns. Proses enkripsi dimulai dengan menentukan plaintext dan kunci, kemudian beberapa transformasi dasar seperti subbytes, shiftrows, mixcolumns, dan addroundkey. Akan tetapi ketika melakukan trasformasi data yang diproses pada setiap trasformasi berupa data biner dari heksadesimal.

Berkenaan dengan solusi yang dijabarkan, kriptografi untuk pengamanan data algoritma *Advanced Encryption Standard* (AES) adalah algoritma yang telah menjadi standarisasi kriptografi [8]. Maka dipilihlah algoritma *Advanced Encryption Standard* (AES). Kerahasiaan isi pada data file dilakukan dengan proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah data *plaintext* menjadi data yang tidak dapat dibaca. Pada proses enkripsi pada data *plaintext* membutuhkan kunci untuk menghasilkan data *ciphertext* dan sebaliknya, pada proses dekripsi juga membutuhkan kunci yang sama pada saat proses enkripsi untuk memulihkan data asli yang dapat dibaca [9].

Penelitian sebelumnya mengimplementasikan pengamanan file berbasis desktop [10] Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan, kontribusi pada penelitian ini yaitu pengamanan file berbasis web menggunakan metode AES-128bit Pada PT. Charise Deo Indonesia. Sehingga muncul untuk membuat aplikasi untuk mengamankan file dengan metode AES-128 berbasis web. Perbedaan dari jurnal diatas, yaitu ada pada basis program.

2. METODE PENELITIAN

Metode penelitian digunakan sebagai dasar untuk melakukan penelitian agar hasil yang diperoleh tidak menyimpang dari tujuan yang telah dicapai sebelumnya. Gambar 1 merupakan tahapan yang dilakukan dalam penerapan metode yang dilakukan pada penelitian ini.

Gambar 1. Tahapan Penelitian

a. Studi Literatur

Penelitian dilakukan dengan cara meneliti berbagai macam buku ilmiah, jurnal, artikel, internet dan berbagai sumber lain yang berkaitan dengan pokok bahasan yang akan dibahas, yaitu kriptografi Advanced Encryption Standard (AES), sehingga penulis memiliki dasar yang kuat untuk menentukan metode yang tepat dalam memecahkan masalah yang akan dipelajari.

b. Studi Lapangan

Melakukan studi kasus di lokasi kegiatan/proyek berdasarkan pengalaman dan pengetahuan teoritis untuk menggali dan mengumpulkan data.

c. Perumusan Masalah

PT. Charise Deo Indonesia belum memiliki suatu pengamanan data, termasuk Data keuangan. Biasanya data hanya disimpan di komputer tanpa keamanan sehingga kemungkinan terjadinya pencurian data sangat mungkin terjadi.

d. Pengumpulan Data

Pengumpulan data dalam penelitian ini adalah dengan melakukan observasi untuk mengetahui permasalahan yang terjadi.

e. Analisa Sistem

Implementasi pengamanan dalam sistem ini adalah proses enkripsi dan dekripsi file, selanjutnya disimpan ke dalam sebuah database.

f. Perancangan Perangkat Lunak

Perancangan dilakukan sesuai dengan hasil analisis sistem khususnya pada perancangan enkripsi dan dekripsi, serta pendukung lainnya yang akan dimasukkan ke dalam perancangan aplikasi dan antarmuka.

g. Implementasi

Penerapan pengamanan data keuangan dilakukan dengan menggunakan PHP sebagai bahasa pemrograman dan MySQL sebagai *database management system*.

h. Pengujian Sistem

Pengujian dilakukan untuk memastikan bahwa sistem diimplementasikan sesuai dengan hasil analisis dan rancangan, sehingga didapatkan suatu kesimpulan bahwa sistem yang dirancang sesuai dengan yang diinginkan.

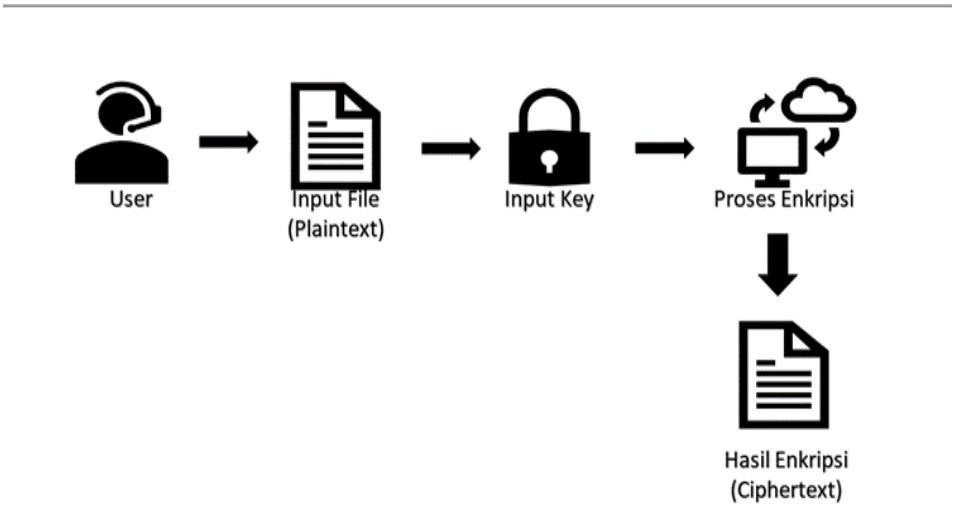
3. HASIL DAN PEMBAHASAN

3.1 Implementasi Program

Berikut ini tahapan proses pengamanan data keuangan pada PT. Charise Deo Indonesia.

a. Enkripsi

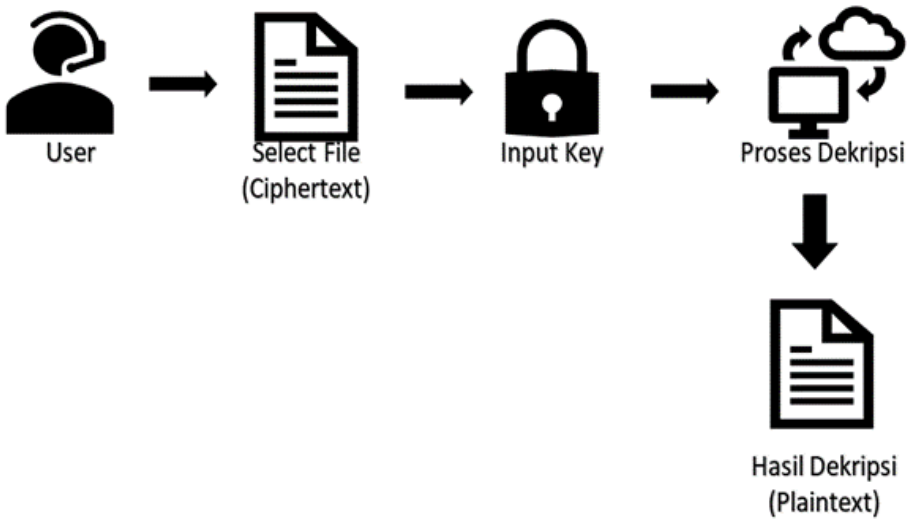
Pada proses enkripsi, pengguna memasukan data yang berupa *plaintext* lalu memberikan *key* atau *password* untuk dilakukan proses enkripsi data, setelah data berhasil dienkripsi maka isi data tersebut telah diacak sehingga tidak dapat dibaca atau bisa disebut juga *ciphertext.*



Gambar 2. Proses Enkripsi Data

b. Dekripsi

Pada proses dekripsi, pengguna akan membuka data yang berupa *ciphertext* menggunakan *key* atau *password* yang sesuai dengan proses enkripsi sebelumnya untuk melakukan proses dekripsi data, setelah data berhasil didekripsi maka isi data akan kembali sepeti semula atau bisa disebut juga *plaintext.*

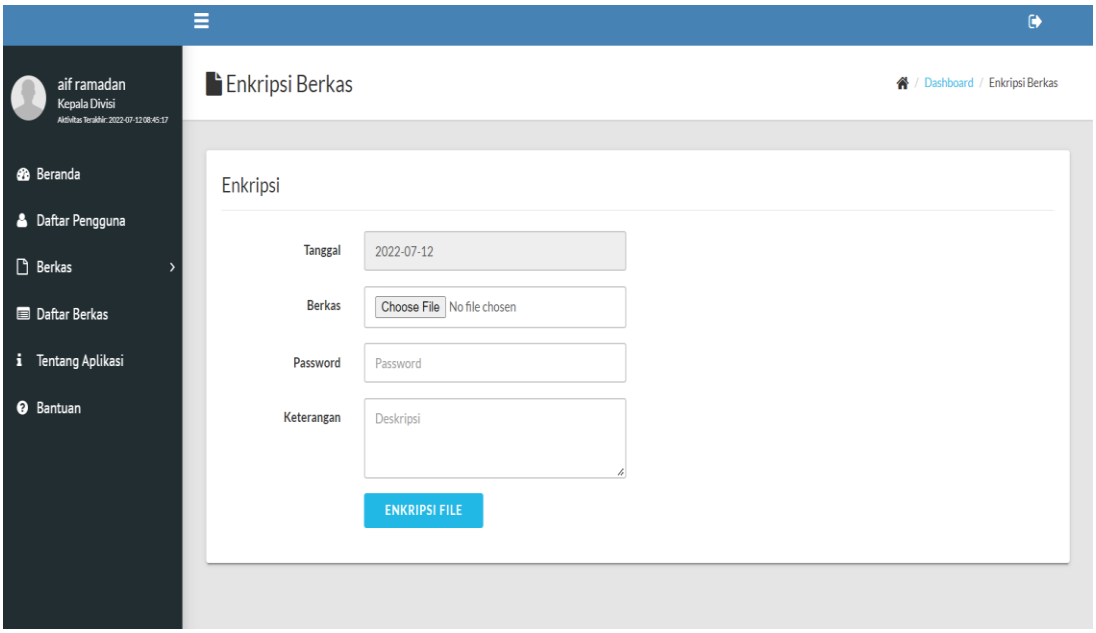


Gambar 3. Proses Dekripsi Data

3.2 Tampilan Layar

3.2.1 Tampilan Halaman Enkripsi

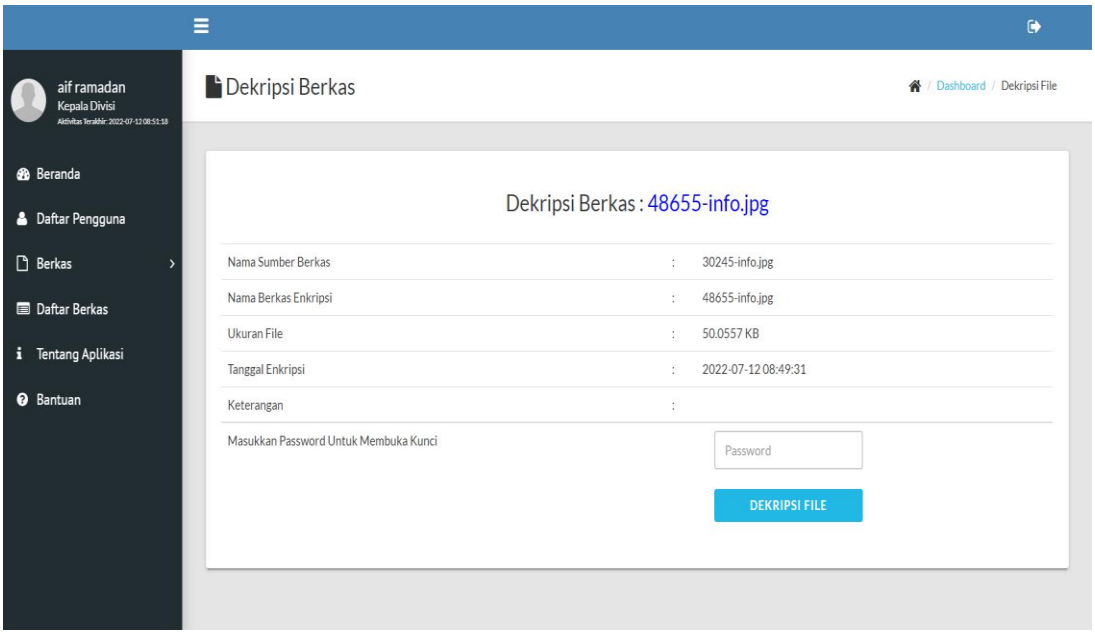
Pada Tampilan Layar Halaman *Form* Enkripsi Berkas, admin akan memilih *file* untuk yang ingin dienkripsi, kata kunci keamanan enkripsi dan deskripsi *file* lalu tekan tombol enkripsi *file* untuk menyimpan data inputan.



Gambar 4. Tampilan Halaman Enkripsi

3.2.2 Tampilan Halaman Dekripsi

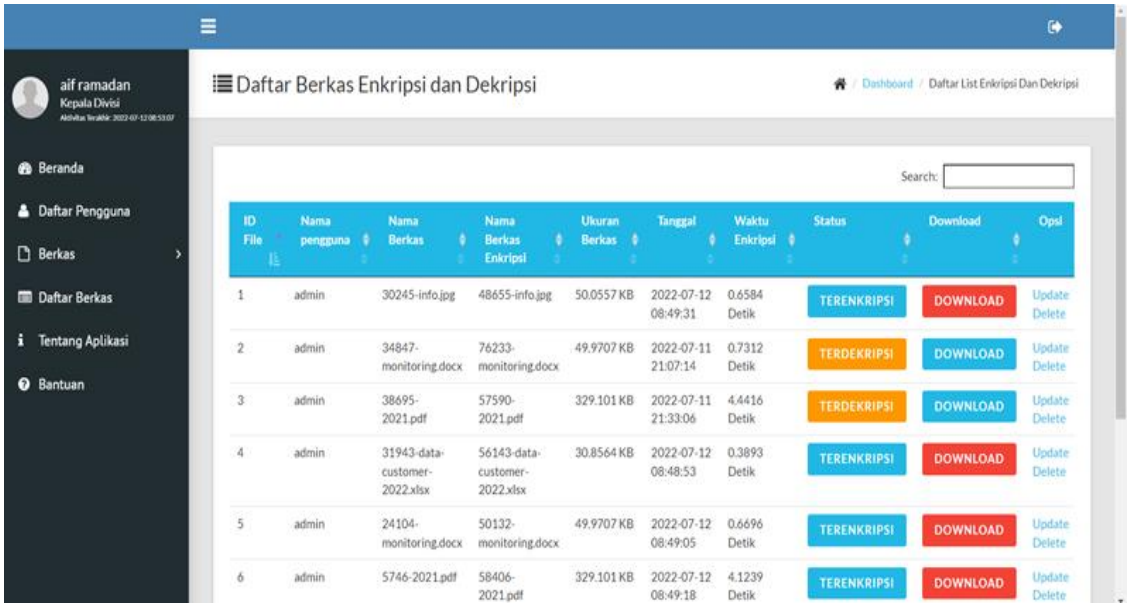
Pada Tampilan Layar Dekripsi Berkas ini pengguna dapat mendekripsi berkas untuk mengembalikan berkas yang telah dienkripsi menjadi berkas asli dengan cara memasukkan password atau kunci yang sama saat enkripsi.



Gambar 5. Tampilan Halaman Dekripsi

3.2.3 Tampilan Halaman Daftar Berkas

Pada Tampilan Layar Daftar Berkas ini berisi berkas enkripsi dan dekripsi yang telah di input kedalam aplikasi, pengguna dapat mendekripsi *file*, mendownload *file*, mengganti *password* baru bila terjadi lupa *password* dan menghapus *file* jika terjadi kesalahan *input file.*



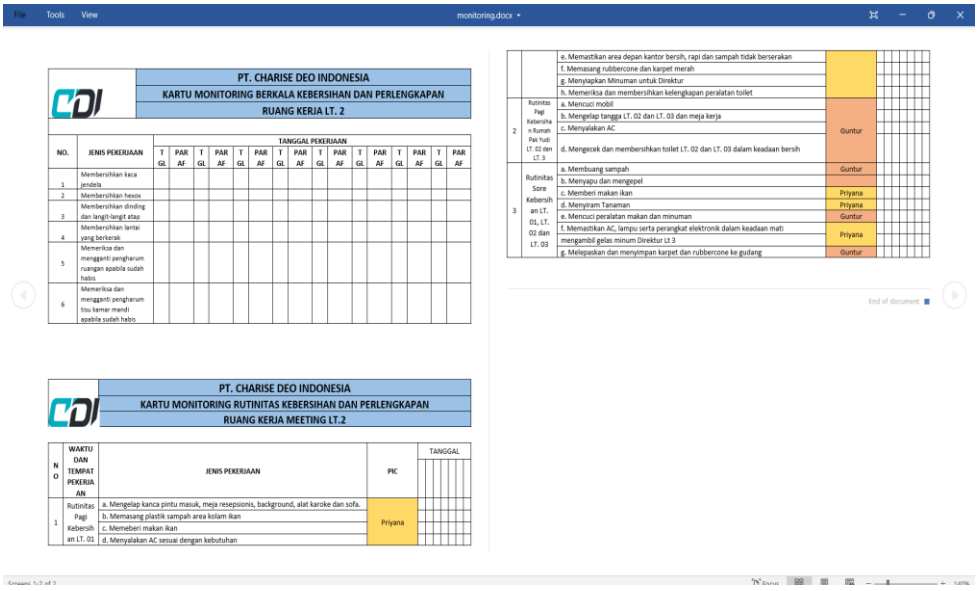
Gambar 6. Tampilan Halaman Daftar Berkas

3.3 Analisis Hasil

Berikut ini adalah hasil uji coba *file* asli dan *file* yang telah dienkripsi, hasil pengujian berupa tampilan *file* sebelum di enkripsi atau *plaintext* dan setelah dienkripsi atau *ciphertext*. Pada uji coba ini *file* akan di uji dengan format **docx* dan **xlsx*.

a. Uji coba file *docx.

Pada uji coba ini terdapat *file* docx asli atau *plaintext* seperti gambar 7 dan gambar 8 merupakan file yang sudah dienkripsi atau *ciphertext.*



PT. CHARISE DEO INDONESIA
KARTU MONITORING BERKALA KEBERSIHAN DAN PERLENGKAPAN
RUANG KERJA LT. 2

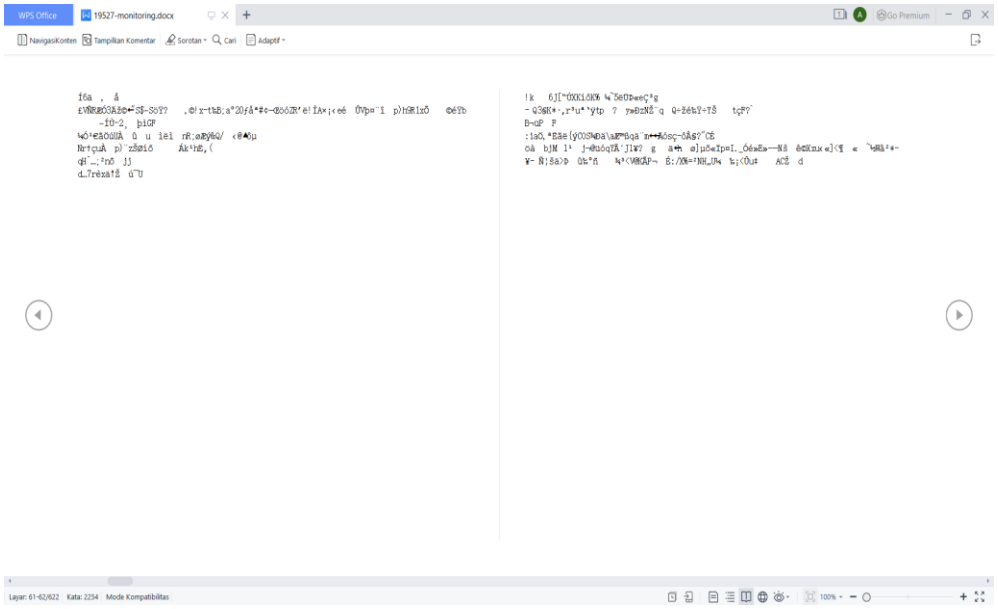
NO.	JENIS PEKERJAAN	TANGGAL PEKERJAAN															
		T GL	PAR AF	T GL	PAR AF	T GL	PAR AF	T GL	PAR AF	T GL	PAR AF	T GL	PAR AF	T GL	PAR AF	T GL	PAR AF
1	Membersihkan kaca jendela																
2	Membersihkan hexox																
3	Membersihkan dinding dan langit-langit atap																
4	Membersihkan lantai yang berkerak																
5	Memeriksa dan mengganti pengharum ruangan apabila sudah habis																
6	Memeriksa dan mengganti pengharum tisu kamar mandi apabila sudah habis																

		e. Memastikan area depan kantor bersih, rapi dan sampah tidak berserakan	
		f. Memasang rubbercone dan karpet merah	
		g. Menyiapkan Minuman untuk Direktur	
		h. Memeriksa dan membersihkan kelengkapan peralatan toilet	
2	Rutinitas Pagi Kebersihan Rumah Pak Yudi LT. 02 dan LT. 3	a. Mencuci mobil b. Mengelap tangga LT. 02 dan LT. 03 dan meja kerja c. Menyalakan AC d. Mengecek dan membersihkan toilet LT. 02 dan LT. 03 dalam keadaan bersih	Guntur
3	Rutinitas Sore Kebersihan LT. 01, LT. 02 dan LT. 03	a. Membuang sampah	Guntur
		b. Menyapu dan mengepel	
		c. Memberi makan ikan	Priyana
		d. Menyiram Tanaman	Priyana
		e. Mencuci peralatan makan dan minuman	Guntur
		f. Memastikan AC, lampu serta perangkat elektronik dalam keadaan mati	Priyana
		mengambil gelas minum Direktur Lt 3	
		g. Melepaskan dan menyimpan karpet dan rubbercone ke gudang	Guntur

PT. CHARISE DEO INDONESIA
KARTU MONITORING RUTINITAS KEBERSIHAN DAN PERLENGKAPAN
RUANG KERJA MEETING LT.2

NO	WAKTU DAN TEMPAT PEKERJAAN	JENIS PEKERJAAN	PIC	TANGGAL
1	Rutinitas Pagi Kebersihan LT. 01	a. Mengelap kanca pintu masuk, meja resepsionis, background, alat karoke dan sofa. b. Memasang plastik sampah area kolam ikan c. Memeberi makan ikan d. Menyalakan AC sesuai dengan kebutuhan	Priyana	

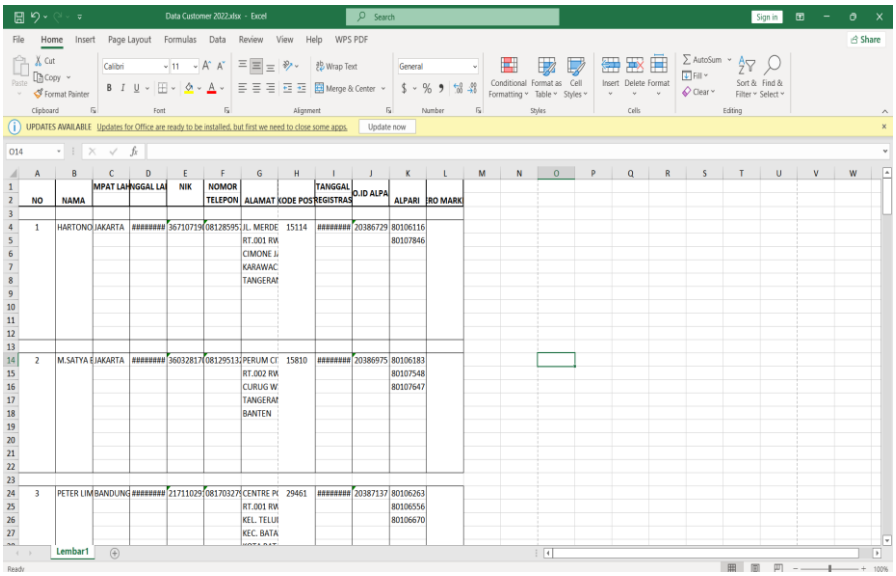
Gambar 7. *File* Docx Asli atau *Plaintext*



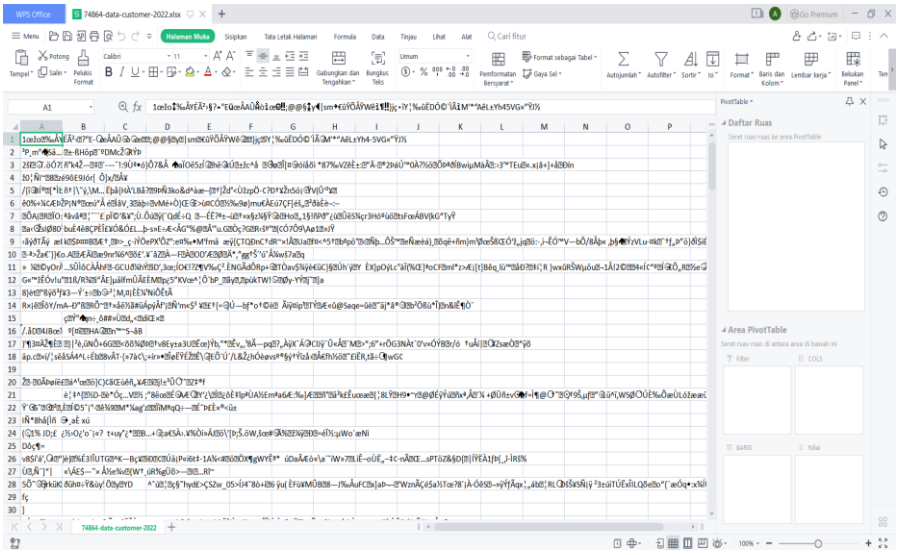
Gambar 8. *File* Docx Hasil Enkripsi atau *Ciphertext*

b. Uji coba file *xlsx.

Pada uji coba ini terdapat file asli atau *plaintext* seperti gambar 9 dan gambar 10 merupakan file yang sudah dienkripsi atau *ciphertext.*



Gambar 9. File Xlsx Asli atau Plaintext



Gambar 10. File Xlsx Hasil Enkripsi atau Ciphertext

3.4 Tabel Pengujian

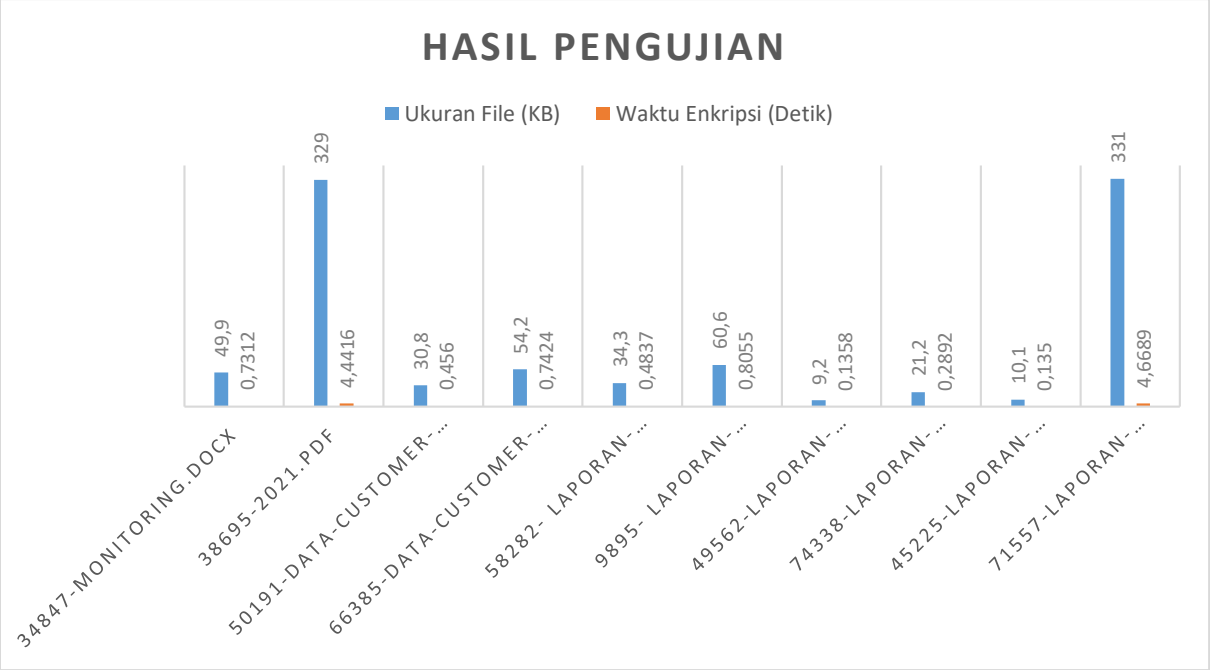
Dalam pengujian kali ini, akan dilakukan pengujian antara proses enkripsi dan dekripsi file.

Tabel 1. Pengujian Enkripsi dan Dekripsi

No	Pengujian	Harapan	Hasil
1	Enkripsi *file*	Data yang dienkripsi harus di buka menggunakan *password* yang sesuai dan ukuran data tetap sama.	Sesuai dengan yang telah diharapkan.
2	Enkripsi data pada perangkat yang sama	*File* yang telah dienkrip tidak bisa dibaca kembali.	*File* masih bisa dibaca di folder yang sama.
3	Hasil Enkripsi	Menampilkan isi data yang tidak tidak bisa dibaca.	Sesuai dengan yang telah diharapkan.

4	Dekripsi *file*	Data yang telah di dekripsi bisa dibaca kembali dengan isi yang masih sama seperti semula.	Sesuai dengan yang telah diharapkan.
5	Hasil dekripsi	Menampilkan text asli dari *file* kembali seperti semula.	Sesuai dengan yang telah diharapkan.

Hasil dari pengujian ini dibuat menjadi sebuah grafik untuk mengetahui kecepatan waktu enkripsi dengan beberapa file dengan ukuran yang berbeda. Ukuran file yang dapat diuji maksimal 5 MB. Hasil dari pengujian ini selain berjalan baik waktu enkripsi file juga tergolong cepat dengan rata-rata waktu enkripsi adalah 1,2687 detik.



Gambar 11. Grafik Hasil Pengujian

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, didapatkan sebuah kesimpulan bahwa aplikasi enkripsi data keuangan dengan menggunakan teknik kriptografi dengan metode *Advanced Encryption Standard* (AES-128) berbasis *website* ini dapat meningkatkan keamanan data pada PT. Charise Deo Indonesia. Isi data telah diacak dengan menggunakan huruf, angka, simbol, atau kombinasi ketiganya. Data yang terenkripsi tidak dapat dipahami jika dekripsi tidak dilakukan dengan kunci yang sesuai untuk mengenkripsi data, berdasarkan beberapa pengujian yang dilakukan, keamanan data ini berjalan cukup baik

Untuk perkembangan selanjutnya data yang telah dienkripsi tidak dapat dibaca di perangkat yang sama dan diharapkan dapat memperbesar kapasitas ukuran file untuk dienkripsi.

DAFTAR PUSTAKA

[1] A. I. Suranta and D. V. Shaka Yudha Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," *Skanika*, vol. 5, no. 1, pp. 1–10, 2022.

[2] S. Vivi Wahdini, D. Hartama, and I. Okta Kirana, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021.

[3] I. Gunawan, S. Tunas, and B. Pematangsiantar, "Peningkatan Pengamanan Data File menggunakan Algoritma Kriptografi AES dari Serangan Brute Force," *TECHSI*, Vol. 13, No. 1, pp. 14–25, 2021.

[4] T. S. Alasi, "Implementasi Kriptografi Dengan Algoritma Ceasar Cipher Untuk Keamanan Data Microsoft Office Word Dan Excel," *J. Inf. Komput. Log.*, vol. 1, no. 2, pp. 1–4, 2019.

[5] A. P. Nugroho and H. B. Suseno, "Keamanan Data Transaksi Nasabah Pada Aplikasi Bank Sampah Berbasis Web Menggunakan Algoritma AES," *Keamanan Data Transaksi Nasabah Pada Apl. Bank Sampah Berbas. Web Menggunakan Algoritm. AES*, vol. 5341, no. April, pp. 9–17, 2020.

[6] B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 1, p. 30, 2019.

[7] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma

Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022.
[8] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021.
[9] W. Pramusinto, N. Wizaksono, and A. Saputro, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 dan Metode Kompresi Huffman," *J. Bit*, vol. 17, no. 2, pp. 46–52, 2020.
[10] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI: Jurnal Ilmu Komput. dan Sist. Informasi*, vol. 4, no. 2, pp. 75–85, 2021.