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

IMPLEMENTASI PENGAMANAN DOKUMEN MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITME AES-128 PADA CV. CIPTA MITRA PERSADA

Mohamad Arif Novianto[1*], Noni Juliasari[2]

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

Email: [1*]arinovianto1511@gmail.com, [2]noni.juliasari@budiluhur.ac.id
(* : corresponding author)

Abstrak-Penyimpanan data ke dalam folder komputer yang terlalu banyak mengakibatkan data tidak rapih dan rawan kehilangan data jika dokumen yang digunakan masih bersifat umum yang membuat data-data tersebut rawan terjadinya kehilangan *file* dan dokummen. Metode yang akan digunakan untuk mengamankan *database* dan *file* yaitu dengan algoritme kriptografi *Advanced Encryption Standard* (AES-128) untuk melakukan pengamanan data-data penting perusahaan yang akan di simpan ke dalam *database* dan mengamankan *file* penting terhadap perusahaan, agar data perusahaan yang tersimpan untuk mengamankan data-data penting dan *file* menjadi lebih aman karena sudah terenkripsi. Kriptografi AES-128 menggunakan alogpritme ntuk keamanan *file* agar kerahasiaan data terjaga dari pihak lain atau pihak yang bukan pengguna. Jika *database* pada software dilihat dari enkripsi dan dekripsi-nya, maka file tersebut tidak akan bermasalah, karena password dan key sudah dienkripsi. Hasil pada penelitian ini akan diterapkan kedalam sebuah aplikasi agar dapat memudahkan pihak dari perusahaan, terutama pada bagian dokumen yang bertugas mengamankan data atau *file* yang rahasianya terjaga, sehingga *file* yang sudah di enkripsi dan *file* yang di enkrips akan dapat diakses oleh pengguna.

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

IMPLEMENTATION OF DOCUMENT SECURITY USING CRYPTOGRAPHY WITH AES-128 ALGORITHM IN CV.CIPTA MITRA PERSADA

Abstract-Storing data in too many computer folders results in messy data and prone to data loss if the documents used are of a general nature which makes the data prone to loss of files and documents. The method that will be used to secure databases and files is the Advanced Encryption Standard (AES-128) cryptographic algorithm to secure important company data that will be stored in the database and secure important files for the company, so that company data is stored to secure important data and files are safer because they are encrypted. AES-128 cryptography uses algorithms for file security so that data confidentiality is maintained from other parties or parties who are not users. If the database in the software is seen from the encryption and decryption, there will be no problem with the file, because the password and key have been encrypted. The results of this study will be applied to an application so that it can make it easier for companies, especially in the document section in charge of securing data or files whose secrets are maintained, so that files that have been encrypted and encrypted files will be accessible to users.

Keyword: Cryptographic, AES-128, Encryption, Decryption

1. PENDAHULUAN

Sejarah Panjang dari kriptografi. Pada tahun 3000 SM, bangsa Mesir mulai menggunakan penulisan rahasia. Mereka menerapkan *hieroglyphcs* untuk menyembunyikan sebuah pesan dari sesuatu yang tidak dinginkan. *Hieroglyphcs* berasal dari bahasa Yunani *Hieroglyphica* yang artinya ukiran rahasia. *Hieroglyphs* dapat berubah atau berevolusi menjadi *hieratic*, yaitu *stylized* script yang digunakan dengan mudah dari sebelumnya. Sekitar 400 SM, kriptografi digunakan seperti sebuah *papyrus* atau perkamen militer oleh bangsa Spartan. Sistem seperti ini dikenal juga dengan konsep *Scytale.*[1], [2],[9]

Kriptografi yaitu sebuah seni yang ditujukan dengan mempelajari sebuah pesan yang akan dikirimkan kepada penerima atau disampaikan dengan cara yang aman. Kriptografi bisa juga disebut kriptologi (*cryptologi*) karena didalamnya mempunyai sebuah konsep matematka. Kriptografi memiliki tujuan untuk menjaga data informasi yang didalamnya terkandung sebuah *file* sehingga kerahasiaan pada informasi tersebut tidak dapat terbongkar terhadap pihak lain. Perancangan terhadap algoritma kriptografi disebut kriptografer.[3], [4], [5]

Pada saat ini teknologi sudah mengalami perkembangan dengan sangat cepat. Teknologi telah mengalami perkembangan yang dapat membantu dalam mengelola suatu data. Banyak instansi menyimpan data dan *file* yang bersifat rahasia di dalam *database* dan komputer. Keamanan yag akan disimpan ke dalam *database* dan komputer sudah menjadi hal yang diharuskan. Oleh karena itu pengamanan data untuk *database* dan *file* yang

bersifat rahasia sangat dibutuhkan.[1],[3],[8]

Dalam perusahaan CV.Cipta Mitra Persada, sebuah keamanan unutuk menjaga *file-file* penting ini belum dapat terjaga dan cara menyimpannya masih kedalam *folder* komputer, melakukan penyimpanan dengan menggunakan *flash disk* tentu data dapat dilihat pihak lain dan rawan terjadinya kehilagan data, maka penulis akan membuat suatu aplikasi yang mengunakan pengamanan enkripsi dan dekripsi *file* agar dapat menjaga keamanan dokumen dalam sebuah perusahaan. Penelitian ini akan menggunakan metode kriptografi Algoritme *Advanced Encryption Standard* (AES- 128).

Tujuan terhadap penelitian yaitu dengan mengamankan dokumen Perusahaan dengan menggunakan fungsi keamanan enkripsi dan dekripsi pada metode Advanced Encryption Standard (AES-128), menjalankan algoritma kriptografi AES-128 untuk penggunaan keamanan enkripsi dan dekripsi file untuk perusahaan CV. Cipta Mitra Persada, diupayakan bisa melakukan pengamanan *dokumen* yang sifatnya rahasia untuk sebuah perusahaan supaya bisa disimpan dengan keamanan yang memadai. Manfaat terhadap penulisan penelitian ini adalah dapat mengamankan dokumen untuk menjaga data atau *file* agar kerahasiaannya dapat terjaga dengan baik dan tidak dapat disalah gunakan.

Saat ini, data yang digunakan masih secara manual, yaitu dengan menggunakan *Microsoft Excel*. Selain itu terkait berkas dokumen pada *file* perusahaan masih disimpan didalam dokumen fisik. Tidak sedikit permasalahan yang ditemukan akibat pendataan yang masih bersifat manual. Permasalahan pertama adalah data yang disimpan yaitu didalam penyimpanan sebuah peranngkat komputer yang memudahkan rawan akan terjadinya kehilangan data. Komputer digunakan untuk hal-hal lain yang bukan untuk menyimpan data perusahaan.[5],[7] [1]

2. METODE PENELITIAN

2.1 Studi Literatur

Tahapan ini ada mengurai beberapa tahapan yang dapat digunakan terhadap metode penelitian ini. Studi akan dilakukan yaitu berupa karya tulis ilmiah, jurnal, dan permasalahan yang terjadi dengan apa yang sedang dibahas yaitu berkaitan dengan kriptografi *Advanced Encryption Standar* (AES) 128, akan mejadi referensi terhadap penulis untuk mengatasi masalah pada penelitian ini. Sedangkan mikrokontroler dapat digunakan untuk membantu peran sebuah komponen utama yang ditentukan dan dirancang sebaik mungkin.

2.2 Studi Lapangan

Pada studi lapangan yang dilakukan terhadap CV. Cipta Mitra Persada untuk mengamankan dokumen atau *file* agar dapat melihat permasalahan yang ada terhadap sisi Perusahaan atau yang lainnya.

2.3 Pengumpulan Data

Pada metode pengumpulan data, ada beberapa tahapan bagi penulis untuk mengumpulkan informasi, data, dan materi yang membahas permasalahan yang ada pada CV. Cipta Mitra Persada yaitu: Wawancara (*Interview*), Pengamatan (*Observation*), Analisa Dokumen, Studi Kepustakaan (*Library Reseacrh*).

2.4 *Algoritme Advanced Encryption Standard* (AES)

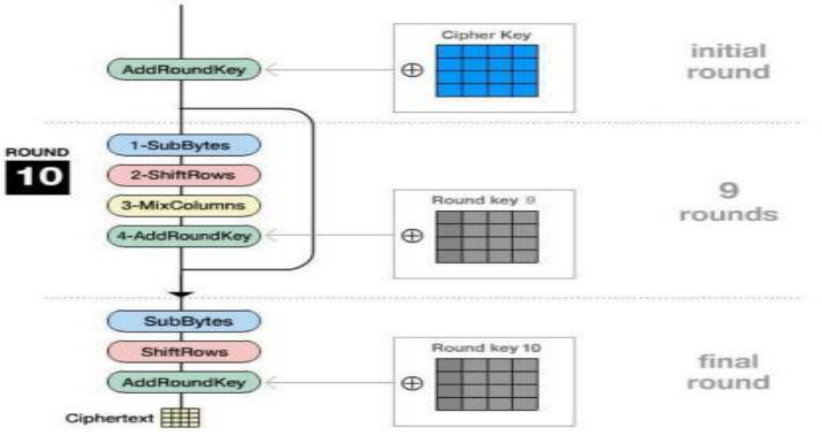
Algoritme *Advanced Encryption Standard* (AES) merupakan suatu algoritme enkripsi dan dekripsi data yang melakukan *block chiper* untuk menggunakan kunci simetri. Pada tahun 2001,NIST (*National Institute of Standard and Technology*) mempublikasikan AES sebagai standar algoritme kriptografi terbaru sebagai pengganti algoritme DES (*Data Encryption Standard*) yang sudah kuno dan mudah untuk dicuri datanya. Pada Tabel 1 menjelaskan tabel jumlah keputusan.

Tabel 1. Jumlah Putaran AES

Tipe	Jumlah Key (NK)	Jumlah Blok (Nb)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	5	4	12
AES-256	6	4	14

2.5 Proses Enkripsi *Advanced Encryption Standard (AES)*

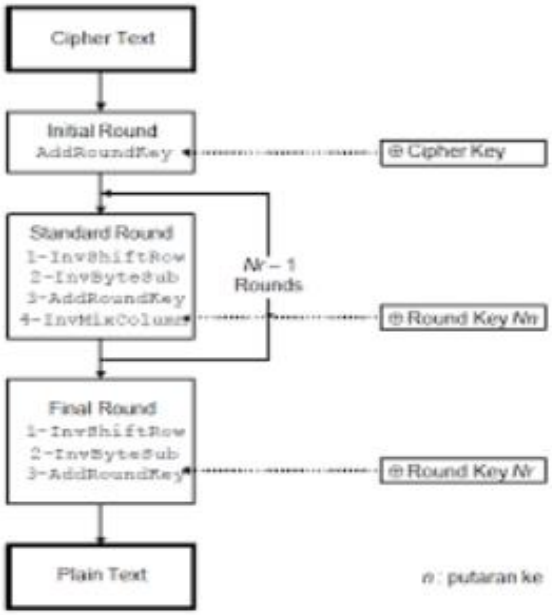
Algoritme Enkripsi adalah suatu cara mengubah pesan yang tidak dapat dimengerti dari pihak lain dalam bentuk terenkripsi. Algoritme *advanced encryption standard* memiliki Panjang kunci 128-bit yang berjumlah 16 huruf dan angka terdiri dari *AddRoundKey, SubBytes, ShiftRows dan MixColumns* Berikut adalah langkah-langkah enkripsi *AES*-128 bit. Gambar 1 ini menjelaskan proses enkripsi.



Gambar 1. Proses Enkripsi AES-128

2.6 Proses Dekripsi *Advanced Encryption Standard (AES)*

Pada transformasi yag dilakukan pada *cipher dan* dapat di implementasikan ke arah yang berlainan dan dibalikkan agar mendapatkan hasil dari sebuah *inverse cipher* yang dapat disimak algoritme AES. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.*[9]. Pada ganbar 2 ini menjelaskan proses dekripsi AES-128.



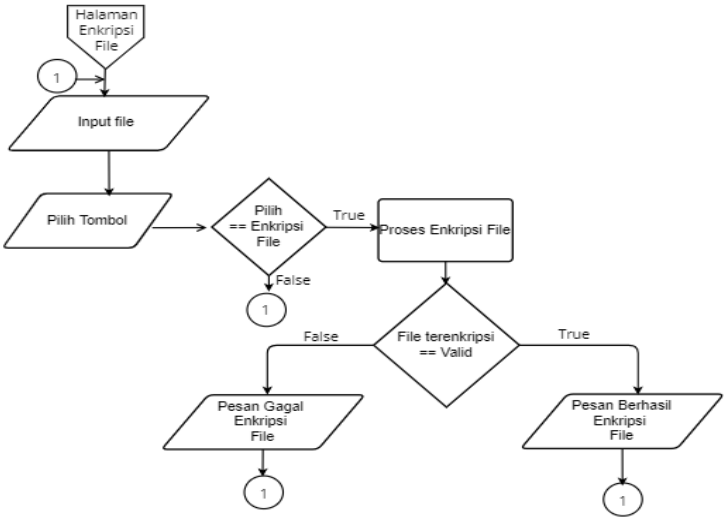
Gambar 2. Proses Dekripsi AES-128

3. HASIL DAN PEMBAHASAN

Berdasarkan dari bab sebelumnya, proses penulisan ini akan membahas tentang hasil dan pembahasan pada algortima kriptografi AES 128bit dengan mengamankan sebuah dokumen atau *file*. Implementasi terhadap tahapan ini menjelaskan tentang *flowchart*, hasil dari enkripsi dekripsi *file, dan* proses.

3.1 Flowchart Form Enkripsi *File*

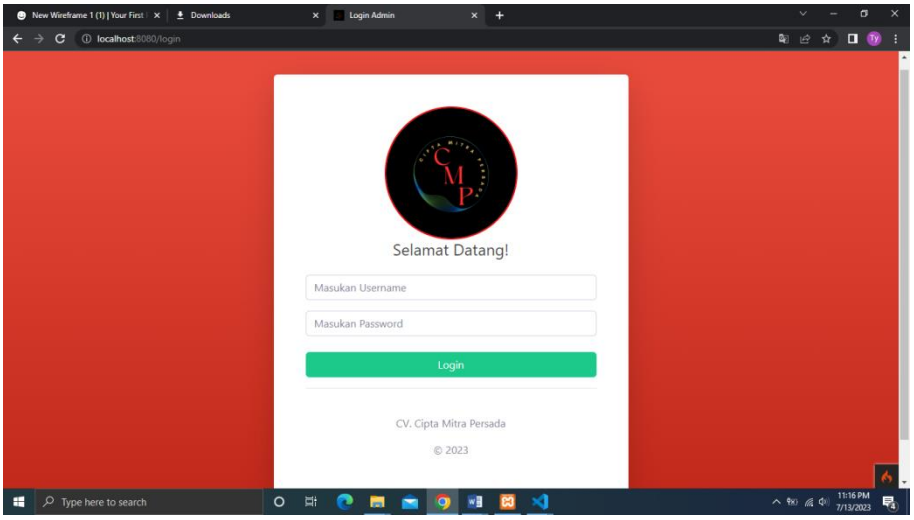
Skema dari fowchart ini menjelaskan dalam melaksanakan atau menjalankan enkripsi *file*, jika akan menuju ke menu masuk dalam halaman utama untuk melakukan sebuah senkripsi *file*, atau menyertakan password dan memberikan penjelasan, akan ada tombol untuk melakukan enkripsi *file* dan melakukan pekerjaan enkripsi *file* dengan *AES*-128 yang berjalan dari *subbytes, shiftrows, mixcolumns* dan *addroundkey*, setelah selesai melakukan itu semua dan melakukan enkripsi *file* gagal, maka akan ada pesan dan tampilan gagal enkripsi, dan jika enkripsi berhasil maka yang terjadi adalah akan kembali ke halaman enkripsi *file.* Gambar 3 merupakan proses dari *flowchart form* enkripsi *file.*



Gambar 3. Flowchart Proses Enkripsi File

3.2 Tampilan Halaman Login

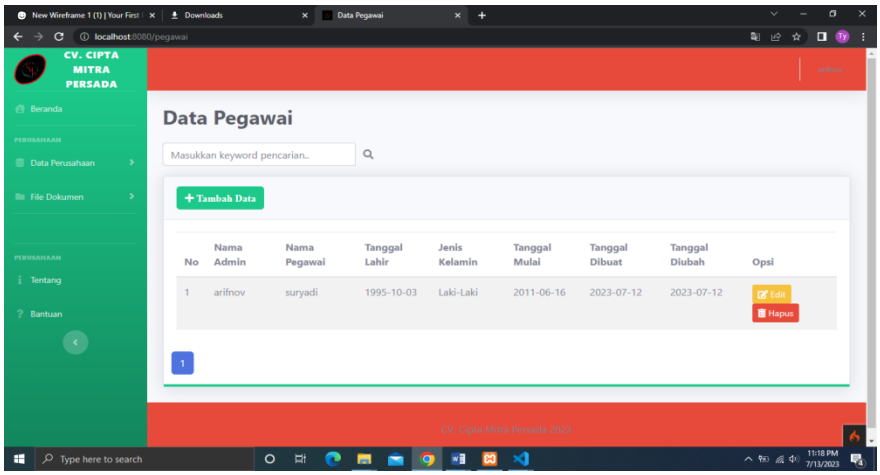
Pada tampilan layar halaman login ini terdapat tampilan background, login dan form login berisi username, password dan button masuk. Berikut tampilan layar halaman login.Pada gambar 4 menampilkan halaman login.



Gambar 4. Tampilan Halaman Login

3.3 Tampilan Data Pegawai

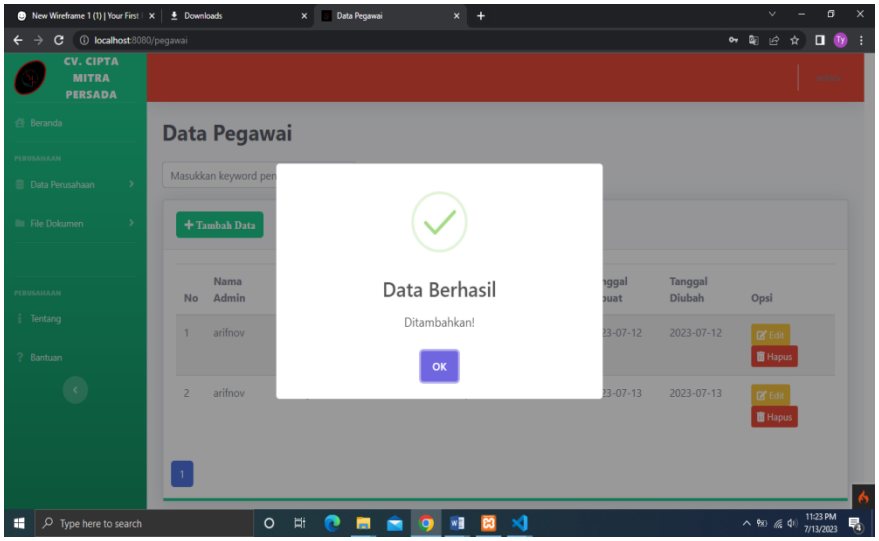
Berikut ini adalah tampilan layar halaman data pegawai, ketika *user* memilih data pegawai. Pada halaman ini terdapat tombol tambah data, tombol ubah data dan tombol hapus.pada tampilan data pegawai berisi no, nama admin, nama pegawai, tanggal lahir, jenis kelamin, tanggal mulai Pada gambar 5 menampilkan halaman data pegawai.



Gambar 5. Tampilan Data Pegawai

3.4 Tampilan Layar Tambah Data Pegawai

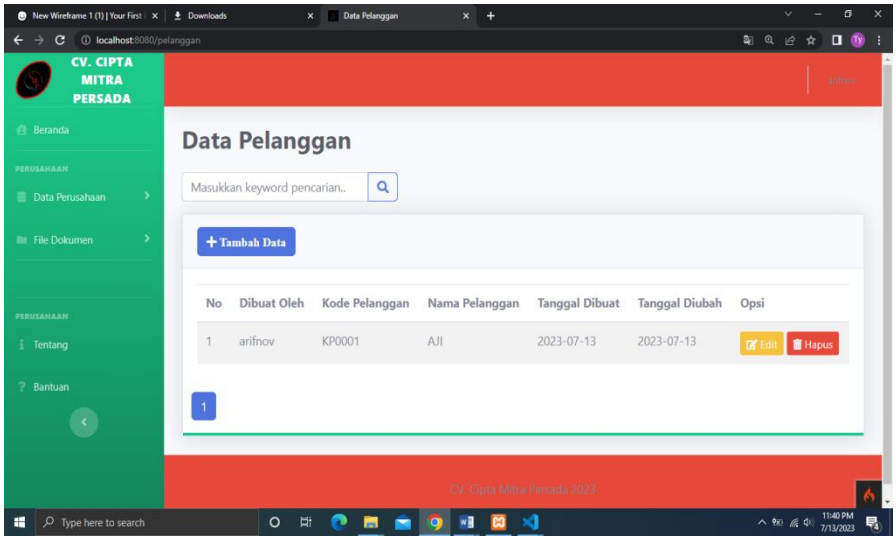
Form ini berfungsi untuk menambah data pegawai baru dan *user* dapat mengisi data pegawai pada *form* yang sudah ada, jika *user* akan mengisi form tambah data, maka data tersebut akan tersimpan dan terenkripsi di dalam *database* serta akan tampil *pop up* data berhasil. Pada tombol batal digunakan untuk membatalkan tambah data pegawai. Gambar 6 menampilkan halaman tambah data pegawai



Gambar 6. Tampilan Halaman Tambah dataPegawai

3.5 Tampilan Halaman Data Pelanggan

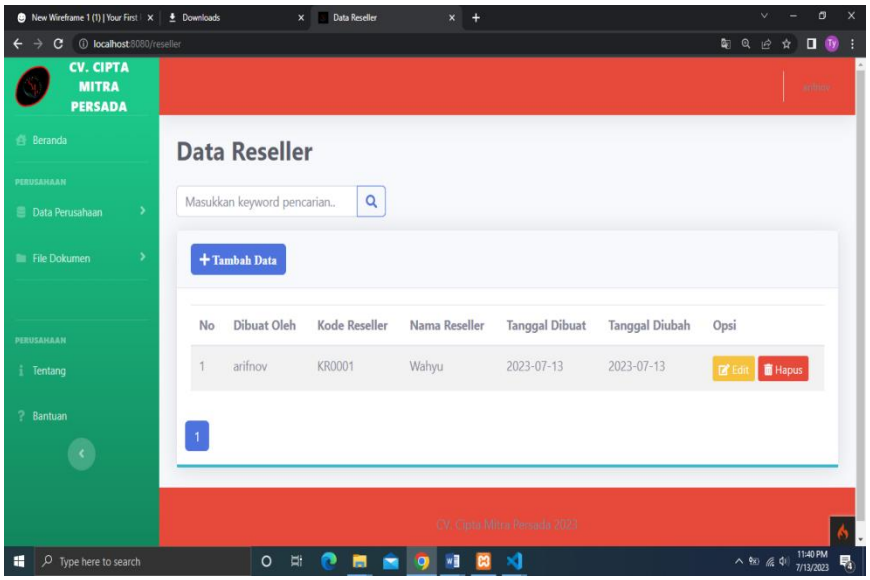
Berikut ini adalah tampilan layar halaman data pelanggan, ketika *user* memilih menu data pelanggan. Pada halaman ini terdapat tombol tambah data, tombol ubah data dan tombol hapus. Pada gambar 7 menampilkan halaman data pelanggan**.**



Gambar 7. Tampilan Data Pelanggan

3.6 Tampilan Data Reseller

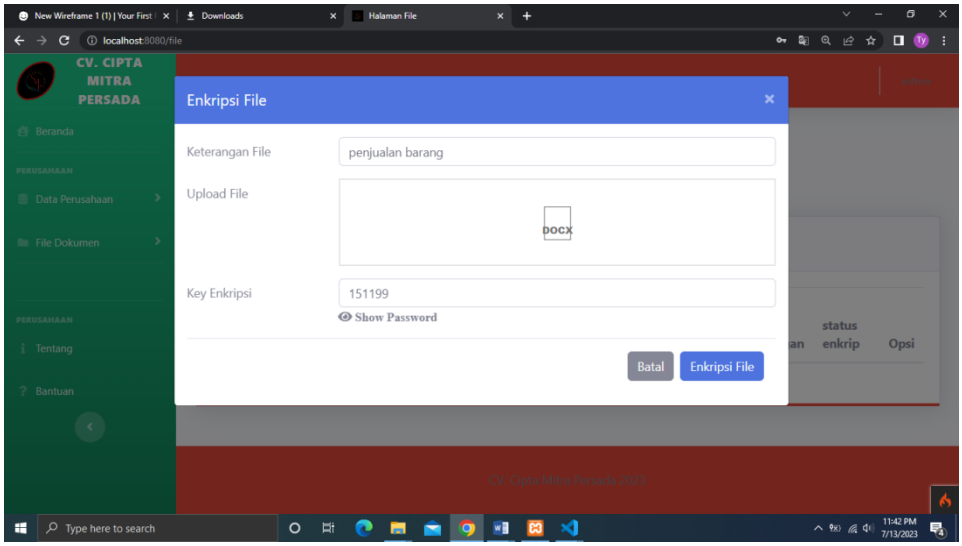
Berikut ini adalah tampilan layar halaman data *reseller*, ketika *user* memilih menu data *reseller*, maka akan muncul nomor, dibuat oleh, kode, nama, tanggal dibuat dan diubah, tombol edit dan hapus. Pada gambar 8 menampilkan tampilan data *reseller.*



Gambar 8. Tampilan Data reseeller

3.7 Tampilan Halaman Enkripsi

Berikut ini adalah tampilan layar *form* enkripsi *file* kembali, *form* ini berfungsi untuk enkripsi kembali *file* yang sudah terdekripsi dan jika *user* sudah mengisi *form* enkripsi *file* dan klik tombol enkripsi *file* maka data tersebut akan terenkripsi kembali di dalam penyimpanan yang sudah ditentukan aplikasi, serta akan tampil *pop up* data berhasil dienkripsi. Pada gambar 9. menampilkan data *enkripsi.*



Gambar 9. Halaman enkripsi

3.8 Tabel Data Enkripsi

Dalam melakukan tahapan pengujian terhadap enkripsi *file* ini sudah sama dengan pola kriptografi dengan menggunakan metode AES-128, tujuan dari adanya uji coba enkripsi *file* ini agar dapat memberitahu apakah *file* yang sudah di enkripsi dinyatakan berhasil atau sebaliknya, proses pengujian dimulai dengan jenis *file* yang berbeda-beda mulai dari ppt, mp4, excel, word, pdf, rar, jpg, png. Sementara itu, f*ile* yang dikasih pada perusahaan CV. Cipta Mitra Persada hanya *file* excel saja. *Table* 2 menyajikan dari pengujian enkripsi *file* di EnDe *File.*

Tabel 2. Hasil File Yang Sudah Di Enkripsi

Nama File	Ukuran File (byte)			Waktu (milli detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Bab I Arif.pdf	59.586 byte	105.934 byte	59.687 byte	3.48457	3.067881
Bab II.pdf	153.344 byte	329.952 byte	187.344 byte	7.824535	8.987868
Logo CV. Cipta MitraPersada.pdf	158.785 byte	272.156 byte	258.705 byte	7.155158	7.197219
Bab II.pdf	738.150 byte	1.312.280 byte	738.150 byte	39.820641	43.286179
DataArifxlsx	70.218 byte	161.472 byte	90.818 byte	5.734265	6.245535
Data Order April.xlsx	132.432 byte	219.480 byte	123.452 byte	6.926616	7.784671
Presentasi 1.pptx	833.432 byte	1.465.176 byte	824.152 byte	49.861466	49.271033
Presentasi.pptx	2.495.822 byte	3.703.604 byte	2.185.722 byte	121.282768	139.764057
Rata-Rata	546.754 (byte)	972.021 (byte)	546.754 (byte)	30.260.321 (millidetik)	33.182.193 (millidetik)

4. KESIMPULAN

Pada hasil perancangan, Sistem dengan menggunakan keamanan dokumen atau *file* dapat dijadikan solusi dengan melakukan pengamanan dokumen. Dari hasil pengimplementasian tersebut, system yang dibuat dapat mendorong CV. Cipta Mitra Persada untuk melakukan pengamanan dokumen atau *file* dengan menggunakan metode algoritme *advanced encryption standard*. Tahap dalam melakukan pengujiannya yaitu di mana sebuah dokumen atau *file* menggunakan format xlsx dengan size 2,56 KB dengan waktu enkripsi 02:33 menit dan melakukan proses dekripsi 02.16 menit dengan *file* lain seperti xlsx 228 KB waktu enkripsi 15.27 detik untuk proses dekripsi 14.26 detik. Dari hasil beberapa *file* dijelaskan yaitu jika waktu dekripsi lebih cepat dibanding pada waktu enkripsi. Diharapkan aplikasi ini dapat dikembangkan pada platform lain, seperti dikembangkan di platform Android atau IOS dan diharapkan penelitian ini dalam tahapan selanjutnya dapat menyempurnakan dan mengembangkan aplikasi ini dari sisi tampilan agar terlihat menarik.

DAFTAR PUSTAKA

[1] Putri, E.A., Kartikadewi, A. and Rosyid, A.A.L. (2020) Implementasi Kriptografi Dengan Algoritme *Advanced Encryption Standard* (AES) 128 Bit Dan Steganografi Menggunakan Metode *End Of File* (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang. 3(2), pp. 69-78.

[2] Basim, Z. and Painem (2020) Implementasi Kriptografi Algoritme RC4 Dan 3DES dan Steganografi Dengan Algoritme EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah. *SKANIKA*, 3(4), pp. 45–52.

[3] Kodir, A. and Pramusinto, W. (2021) Implementasi Kriptografi Dengan Menggunakan Metode RC4 Dan BASE64 Untuk Mengamankan Database Sekolah Pada Sdn Grogol Utara 10. *SKANIKA*, 4(1), pp. 7–14.

[4] Dewi Cita Anggraeni, C. K. (2017). Perancangan Aplikasi Algoritme AES Rijndael Pada Enkripsi Citra Digital File Jpeg 128 Bit, 91.

[5] Widyawan, D. and Imelda (2021) Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi. *SKANIKA*," 4(1), pp. 15–22.

[6] Zalukhu, K., Syahra, Y. and Syahputra, T. (2020) Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritme *Advanced Encryption Standard* 128 Bit Pada Pengadilan Militer I-02 Medan. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, 3(2), pp. 138–150.

[7] Cristy, N. and Riandari, F. (2021) Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan. *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]*, 4(2), pp. 75–85.

[8] Prayudha, J., Saniman and Ishak (2019) Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (AES). *Sains dan Komputer (SAINTIKOM)*, 18(2), pp. 119–129.

[9] H. Kridalaksana, A., Arriyanti, E., & Widodo, W. (2018). Aplikasi Pengaman Sms Dengan Metode Kriptografi Advanced Encryption Standard (Aes) 128 Berbasis Android. Sebatik, 10(1), 8–14.

[10] Z. Musliyana, T. Y. Arif, and R. Munadi. (2018). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritme AES dan OneTime Password Studi Kasus: SSO Universitas Ubudiyah Indonesia, 12(2), pp. 12-21.