2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

PENGAMANAN FILE BERBASIS WEB DENGAN MENERAPKAN ALGORITME AES-128 PADA PT. SAMUDRA KATULISTIWA NUSANTARA

Sahdan Rediansyah[1], Rizky Tahara Shita[2*], Ferdiansyah[3], Painem[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1]sahdanrediansyah015@gmail.com, [2]rizky.taharashita@budiluhur.ac.id, [3]ferdiansyah@budiluhur.ac.id, [4]Painem@budiluhur.ac.id
(* : corresponding author)

Abstrak- Pentingnya Keamanan data informasi dalam suatu instansi swasta ataupun pemerintah agar mencegah kejahatan digital. Banyaknya khasus pencurian data di dunia digital oleh pihak yang tidak bertanggung jawab yang disebabkan rendahnya literasi pada keamanan data. Pada perusahaan PT. Samudra Katulistiwa Nusantara terdapat berbagai data asrip penting yang dimiliki oleh perusahaan ataupun client. Dan sebelumnya telah terjadi kehilangan file/dokumen arsip pada PT. PT. Samudra Katulistiwa Nusantara dikarnakan file yang ada masih belum terjaga keamanannya karena masih disimpan dalam folder komputer atau flash disk. Dalam tujuan penelitian ini akan membuat suatu rancangan aplikasi Keamanan file melalui proses modifikasi pada isi file dari yang bisa dibaca menjadi tidak bisa terbaca (encryption) dan file yang tidak bisa dibaca akan di proses kembali agar bisa terbaca seperti semula (decryption) dengan mengimplementasikan aplikasi keamanan file menggunakan algoritme kriptografi berbasis web. Metode yang dipakai dalam mengamankan file menggunakan algoritme Advanced Encryption Standard (AES-128). Hasil pada saat proses enkripsi dan dekripsi file, tidak terjadi kerusakan baik sebelum atau sesudah mengoprasikan proses enkripsi dan dekripsi.

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

WEB-BASED FILE SECURITY BY APPLYING AES-128 ALGORITHM AT PT. SAMUDRA KATULISTIWA NUSANTARA

Abstract- *The importance of securing information data in a private or government agency in order to prevent digital crimes from occurring. There are many cases of data theft in the digital world by irresponsible parties due to low data security literacy. In the company PT. Samudra Katulistiwa Nusantara contains various important archival data belonging to companies or clients. And previously there has been a loss of archive files/documents at PT. PT. Samudra Katulistiwa Nusantara because the files are still not safe because they are still stored in a computer folder or flash disk. In this research a file security application design will be made through the process of modifying file contents from readable to unreadable (encryption) and unreadable files will be processed again so that they can be read as before (decryption).) by implementing a security application. files using web-based cryptographic algorithms. The method used to secure files uses the Advanced Encryption Standard (AES-128) algorithm. The results during the file encryption and decryption process, no damage occurs either before or after the operation of the encryption and decryption process*

Keywords*: Advanced Encryption Standard (AES-128), Decryption, Ccryptographic, Encryption, File.*

1. PENDAHULUAN

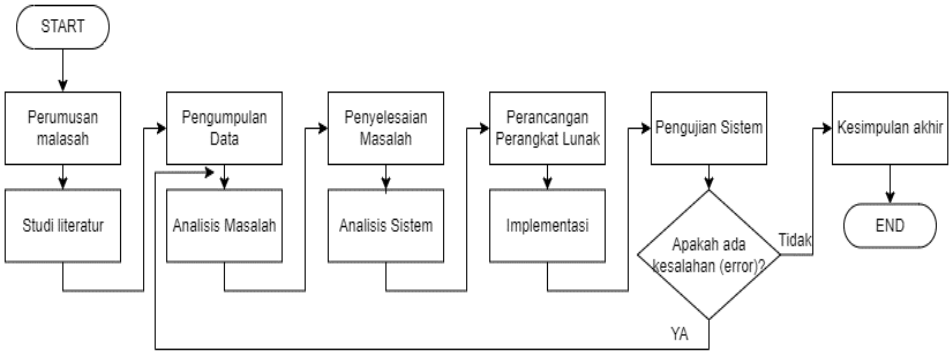
Di era perkembangan teknologi informasi segala kebutuhan aspek kehidupan manusia memerlukan peranan teknologi. Salah satu peranan teknologi tersebut ialah untuk melakukan penyimpanan data, baik itu data yang bersifat umum maupun data yang bersifat *(secret)* rahasia dan dapat dengan mudah bertukar informasi dalam berbagai format tanpa membatasi ruang dan waktu. Sebab keamanan data sangat penting sehingga hanya orang yang berwenang yang mengetahui penyimpanan data yang bersifat rahasia [1]. Maraknya pencurian data pribadi yang dilakukan pihak tidak bertanggung jawab di dunia digital yang sebabkan dengan tingginya nilai jual data pribadi. Masalah lain yang mengkhawatirkan adalah rendahnya sistem keamanan untuk file-file penting yang dimiliki oleh suatu instansi/perusahan pemerintah. Oleh karena itu, keamanan data diperlukan untuk melindungi *file* rahasia [2]. Kriptografi bisa diperuntuk dalam menjaga keamanan pesan yang dikirim berdasarkan satu pesan dengan pesan lain. Kriptografi terdiri dari kata Crypto serta Grapho dimana Crypto yang maksudnya rahasia (*secret*) serta Grapho yang maksudnya Menulis(writing) dalam Bahasa Yunani. Kriptografi ialah wujud ilmu serta seni buatmelindungi keaslian ataupun keabsahan pesan[3]. Dalam proses enkripsi, pesan yang semula akan dikirim (*plaintext*) yang akan diproses *encryption* (enkripsi) dengan kunci menjadi pesan acak tidak beraturan (*ciphertext*). hanya pengirim dan penerima yang mengetahui kuncinya (*key*). Kunci (*key*) ini juga digunakan untuk mengubah kembali *ciphertext* jadi *plaintext*[4].

Orang internal mengkompromikan kerahasiaan file-file penting tersebut. Kasus pencurian data pribadi seperti dokumen elektronik, dimana pada tahun 2014 jumlah pelanggaran 1225 di tingkat penyidikan adalah 790, jadi presentasenya 64%, ditahun 2015 jumlah pelanggaran di tingkat penyidikan adalah 1569 dengan sebesar 851 dari 54% kasus, dan pada tahun 2016, jumlah total kejahatan adalah 1207, sedangkan investigasi kriminal adalah 699, dan presentasenya 57%, sehingga kasus kejahatan didunia digital keamanan data/*file* informasi ini menjadi peranan penting di era teknologi yang berkembang [5]. Tujuan dalam penelitian ini adalah agar memahani bagaimana konsep kriptografi untuk pengaman informasi berbasis *file* menggunakan algoritme AES. Kriptografi jadi menjadi sebuah solusi pada perusahaan dalam menyimpan data-data arsip seperti PT. Samudra Katulistiwa Nusantara yang memilik banyak sekali dokumen arsip yang sebelumnya pernah terjadi kehilangan dokumen yang dicuri dengan pihak yang tak berwenang, pada tahap perencanaan aplikasi proteksi *file* digunakan bahasa pemrograman berbasis web PHP dengan bantuan database MySQL. Dengsn implementasiksn ini dapat disimpulkan bahwa aplikasi mampu mendukung *file* survey yang semula dalam format *clear text* menjadi teks terenkripsi, dimana hasil akhirnya berupa file yang maknanya tidak dapat dibaca lagi.

Dalam penelitian lain yang menggunakan algoritme *Advanced Encryption Standard* Penerapan Algoritme AES ataupun RSA. Menurut penelitian sebelumnya hasil pengujian algoritme AES memiliki rata-rata kecepatan saat proses enkripsi yaitu 508,14s (detik) dan sedangkan algoritme RSA rata-rata kecepatannya yaitu 0,094s (detik). RSA jauh lebih cepat. Sementara proses dekripsi algoritme AES memiliki rata-rata kecepatanya yaitu 578,63s (detik) sedangkan algoritme RSA memiliki rata-rata kecepatan dekripsi yaitu 6,535s (detik). Menjelaskan bahwa dalam proses dekripsi algoritme AES jauh lebih cepat. kebutuhan memori untuk proses enkripsi pada algoritme AES mencapai 16.5% - 31.3% saat proses dekripsi, lalu proses enkripsi dengan algortime RSA lebih kecil dengan mecapai 5.2% - 11.2% saat proses dekripsi. Pada kebutuhan memori jelas algoritme AES lebih besar daripada algoritme RSA [6].

2. METODE PENELITIAN

Dengan menggunakan metode *waterfall* yang diawali pada perumusan masalah penelitian, setelah itu dilakukan studi literatur dengan membaca hasil dan teori yang sama pada penelitian sebelumnya serta buku dan dokumen lain yang mendukung penelitian, sehingga diperoleh hasil dibuat untuk. tidak berbeda dengan tujuan yang dicapai sebelumnya. Gambar 1 menunjukan langkah-langkah yang untuk menerapkan metode penelitian ini



Gambar 1. Tahapan Penelitian

2.1 Studi Literatur

Tahap yang dilakukan dengan mereview 10 paper jurnal dari tahun 2019 sampai dengan 2022. Pada jurnal yang di review masing-masing menggunakan berbagai macam algoritme seperti AES bit 128 dengan pengembangan system RAD, AES 128 dengan Teknik Steganografi *End of File* (EOF), kombinasi AES 128 dengan RSA, AES 128 dengan memakai SQL Injection, AES 256, algoritme RC5 dan RC6. Studi ini juga dilakukan dengan menangani masalah terkait yaitu kriptografi, khususnya dalam sistems kriptografi dengan menerapkan algoritme *Advanced Encryption Standard* (AES-128), memberikan referensi yang kuat kepada penulis untuk menentukan metode yang tepat untuk memecahkan masalah yang diteliti.

2.2 Pengumpulan Data

a. Wawancara (*Interview*)
Tahap dilakukan dengan wawancara tatap muka dan sesi tanya jawab dengan pihak kepentingan pengembangan aplikasi dan perangkat lunak dalam memenuhi data informasi yang berhubungan pada aplikasi ataupun keamanan yang ada.

b. Observasi (*Observation*)
Observasi dilaksanakan di PT.Samudra Katulistiwa Nusantara untuk mengetahui keadaan sebenarnya dari objek penelitian. Tujuannya adalah untuk memperoleh penjelasan tentang informasi dan data yang diperlukan untuk penelitian.
c. Studi Pustaka
yang dilaksanakan dengan cara membaca jurnal/e-book serta referensi yang berkaitan dengan teori kriptografi algoritme (AES-128).

2.3 Analisa Sistem

a. Analisis Data
Analisis data yaitu salah satu langkah untuk mengatasi masalah keamanan ini, dalam analisis data dilakukan, Pengumpulan *file* yang digunakan untuk memperoleh informasi yang diperlukan dalam merancang program dan Pengumpulan *file* sesuai dengan jenisnya.Dekripsi file yang telah ditentukan *step by step* yang dipakai untuk membuat aplikasi yang mudah dipahami.
b. Anlisa Penerapan Algoritme
Setelah langkah pengumpulan data dan monitoring pengoperasian sistem. Kemudian dibuat implementasi alias dari algoritme tersebut. Analisis aplikasi algoritme menjelaskan langkah-langkah penerapan metode enkripsi *Advanced Encryption Standard* (AES) untuk proses perlindungan data penting. Maka dilakukan Proses enkripsi file dengan kunci enkripsi, yaitu proses mengubah file yang akan dienkripsi menjadi *ciphertext* dengan kunci enkripsi. Serta Proses dekripsi *ciphertext* menggunakan kunci dekripsi yang sama dengan kunci enkripsi, yaitu proses mengubah ciphertext menjadi file yang dapat dibaca kembali *(plaintext*).
c. Analisis Sistem
Implementasi keamanan yang digunakan pada sistem adalah proses enkripsi file yang kemudian disimpan dalam database. Enkripsi digunakan untuk melindungi data yang disimpan dalam database. Oleh karena itu, proses penyimpanan data dalam database membutuhkan modul untuk mengenkripsi data tersebut. Modul enkripsi tersebut terletak dalam aplikasi yang dipanggil saat pengguna ingin melihat data tersebut.

2.4 Perancangan Perangkat Lunak

Tahap ini dilakukan perancangan sesuai dengan hasil analisis sistem terutama pada perancangan enkripsi dan dekripsi. Selain itu, dukungan tambahan diintegrasikan ke dalam aplikasi dan desain antarmuka pengguna. Pengembangan sistem ini menggunakan metode waterfall, model ini harus dijalankan satu per satu secara lengkap sebelum melanjutkan ke langkah berikutnya, dan hasil dari setiap langkah harus didokumentasikan dengan baik.

2.5 Implementasi

Pada proses implementasi ini dilakukan pembuatan modul-modul yang sudah dirancang dalam tahap perencangan ke dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi yang digunakan adalah:

a) Perangkat lunak yang digunakan dalam proses penerapan pengamanan data *file* menggunakan bahasa pemograman php serta DBMS yang digunakan adalah PHPMyAdmin.
b) Perangkat keras yang digunakan diantaranya Prosesor Intel Core i3, RAM 2GB DDR3 1600Mhz, HDD 1000GB.

2.6 Pengujian Sistem

Metode pengujian adalah *blackbox* sebagai metode yang memeriksa kesalahan dan, saat dijalankan, fungsi aplikasi untuk mengklarifikasi apakah masukan diterima dengan benar dan apakah hasil yang dihasilkan demikian.

2.7 Kesimpulan

Tahapan terakhir ini di mana disimpulkan bahwa penerapan metode kriptografi *Advanced Encyption Standard* (AES) 128, berfungsi dengan baik dan dapat mengamankan *file* pada bagian *Accounting* pada PT. Samudra Katulistiwa Nusantara dengan aman dan pada tahapan ini ada saran untuk perkembangan pada sistem ini.

2.8 Metode Kriptografi AES 128

Algoritme block cipher dengan properti simetris yang menggunakan kunci simetris selama proses enkripsi dan dekripsi. Enkripsi AES menggunakan proses berulang yang disebut putaran. Jumlah putaran yang digunakan oleh AES bergantung pada panjang kunci yang digunakan. Setiap putaran membutuhkan kunci putar dan input dari putaran berikutnya. Kunci yang dihasilkan berdasarkan kunci yang ditentukan. Algoritme AES dapat melakukan enkripsi dan dekripsi dengan panjang kunci yang berbeda yaitu 128 bit, 192 bit dan 256 bit.

Jumlah putaran mempengaruhi panjangnya kunci (*key*), perbedaan antara ketiga kunci dapat dilihat pada Gambar 2 Perbandingan jumlah kunci AES [7].

Tabel 1. Perbedaan Putaran algoritma AES

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

Berdasarkan Tabel 1. pada (AES-128 bit) ada 2128 kunci = 3,4 x 1038. Setiap jumlah putaran menggunakan kunci internal berbeda. Secara umum, proses enkripsi (AES-128 bit) penjabarannya sebagai berikut [8]:

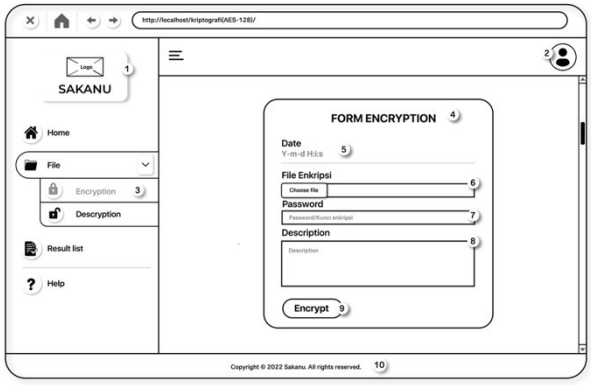
1. *AddRoundKey:* melakukan proses XOR antara state awal (*plaintext*) dengan *cipherkey*. Tahap ini disebut juga initial round.
2. *Round* : Putaran sebanyak Nr – 1 kali. Proses yang dilakukan setiap putaran adalah:
   SubBytes: *substitusi byte* yang menggunakan tabel substitusi (S-box).
   ShiftRows: pergeseran barisan array state secara wrapping.
3. *MixColumns:* mengacak data pada setiap masing- masing kolom array state.
4. *AddRoundKey:* melakukan XOR antara state sekarang round key.
5. *Final Round:* proses untuk putaran terakhir antara lain: *SubBytes* ,*ShiftRows* dan *AddRoundKey*
6. Pada proses akhir yaitu akan menghasilkan karakter/teks yang berbentuk chipertext

Secara gambaran besar proses dekripsi (AES-128 bit) berikut penjabarannya:

1. *InvShiftRows*: melakukan pergeseran pada bit dengan ke kanan pada setiap blok baris.
2. *InSubBytes*: Setiap elemen state dipetakan dengan tabel Inverse S-Box.
3. *InvMixColumns:* Setiap kolom dalam state dikalikan dengan matriks AES.
4. *AddRoundKey:* Mengombinasikan state array dan *roundKey* dengan hubungan XOR.
5. Pada proses akhir yang akan menghasilkan sebuah karakter/teks asli (*plaintext*)

2.9 Rancangan Layar

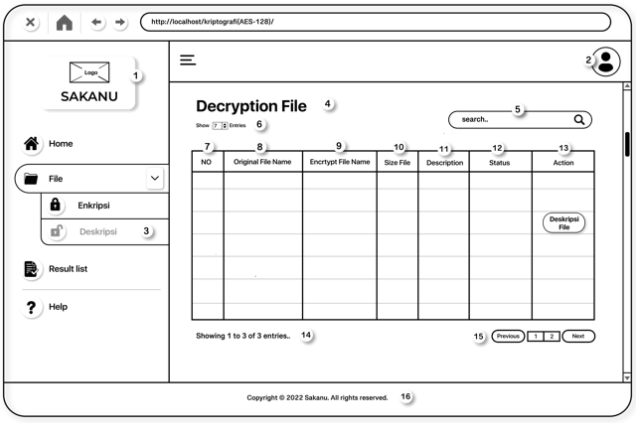
Dalam pembuatan suatu aplikasi, sangat diperlukan tahap perancangan layar sebagai bentuk dasar dalam membuat desain aplikasi yang diinginkan. Rancangan layar harus mudah dimengerti, tujuannya agar pengguna dapat merasa nyaman dan tidak kebingungan dalam menggunakan aplikasi ini.



Gambar 2. Rancangan Layar Form *Encryption*

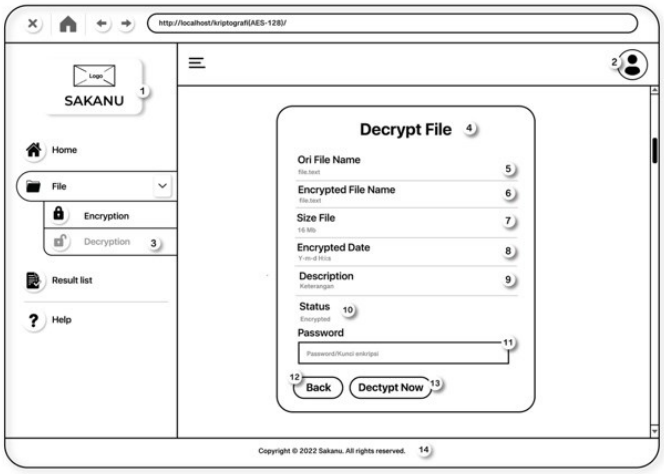
Keterangan pada gambar 3.

1. Logo perusahaan yaitu SAKANU.
2. Untuk menampilkan *username* yang sedang *login.*
3. Menu *encryption*/enkripsi.
4. *Label* from enkripsi *file.*
5. Menampilkan data tanggal pada saat enkripsi *file.*
6. Memilih/masukan *file* yang akan di enkripsi.
7. *Password/key* yang akan digunakan untuk pengamanan *file.*
8. Untuk memberikan keterangan pada *file.*
9. *Button* untuk melakukan proses enkripi.
10. *Label* tahun pembuatan aplikasi dan nama perusahaan.



Gambar 4. Rancangan Layar Decrpyion File

Keterangan pada gambar 4
1. Logo perusahaan yaitu SAKANU.
2. Untuk menampilkan *username* yang sedang *login.*
3. Menu *descryption*/dekripsi *file.*
4. *Label* dekripsi *file.*
5. Untuk mencari data file
6. Menampilkan berapa baris data.
7. Menampilkan nomor *file.*
8. Menampilkan nama *file* asli.
9. Menampilkan nama *file* yang sudah terenkripsi.
10. Menampilkan ukuran *file.*
11. Menampilkan keterangan pada *file*.
12. Menampilkan status pada *file.*
13. Menampilkan aksi untuk melakukan dekripsi *file.*
14. Menampilkan label 1 hingga 3 dari 3 masukanya data.
15. Untuk memilih kehalaman table sebelumnya atau selanjutnya jika ada atau *file* berjumlah banyak. *Label* tahun pembuatan aplikasi dan nama perusahaan.



Gambar 5. Rancangan Layar Form Decrypt File

Keterangan pada gambar 5.
1. Logo perusahaan yaitu SAKANU.
2. Untuk menampilkan *username* yang sedang *login.*
3. Menu *descryption*/dekripsi file.
4. *Label* dekripsi *file.*
5. Menampilkan nama *file* asli.
6. Menampilkan nama *file* terenkipsi.
7. Menampilkan ukuran size file.

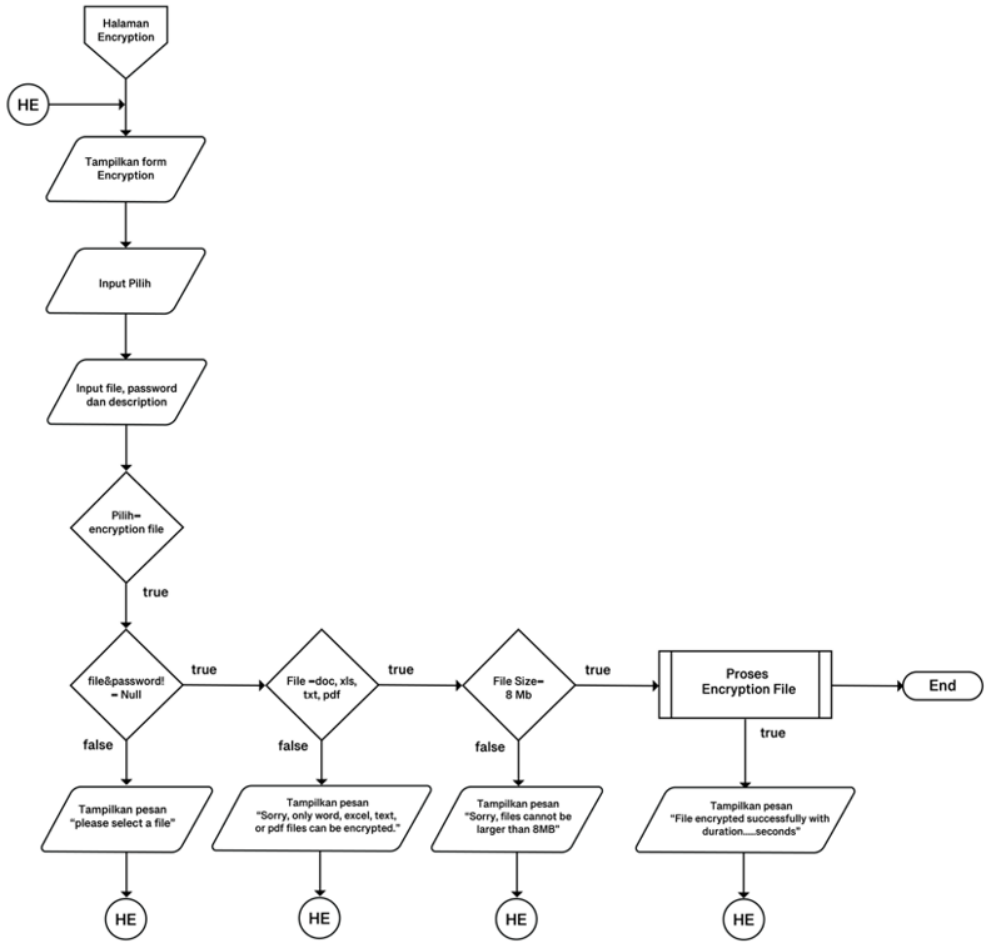
8. Memapilkan tanggal file dienkripsi.
9. Menampilkan keterangan pada file.
10. Menampilkan Status file.
11. Untuk mengisi password enkripsi.
12. Button jika tidak jadi melakukan proses enkripsi
13. Button untuk mendekripsi file yang telah di masukan password enkripsi.
14. Label tahun pembuatan aplikasi dan nama perusahaan.

3. HASIL DAN PEMBAHASAN

Berdasarkan penjabaran dari metode, bab selanjutnya yaitu tentang algoritme kriptografi (AES-128 bit) yang digunakan mengenkripsi dan dekripsi dokumen. Peimplementasi ini akan dijelaskan *flowchart*, algoritme, proses dan hasil dari enkripsi dan dekripsi dokumen pada aplikasi.

3.1 Flowchart Menu *Encryption* (Enkripsi)

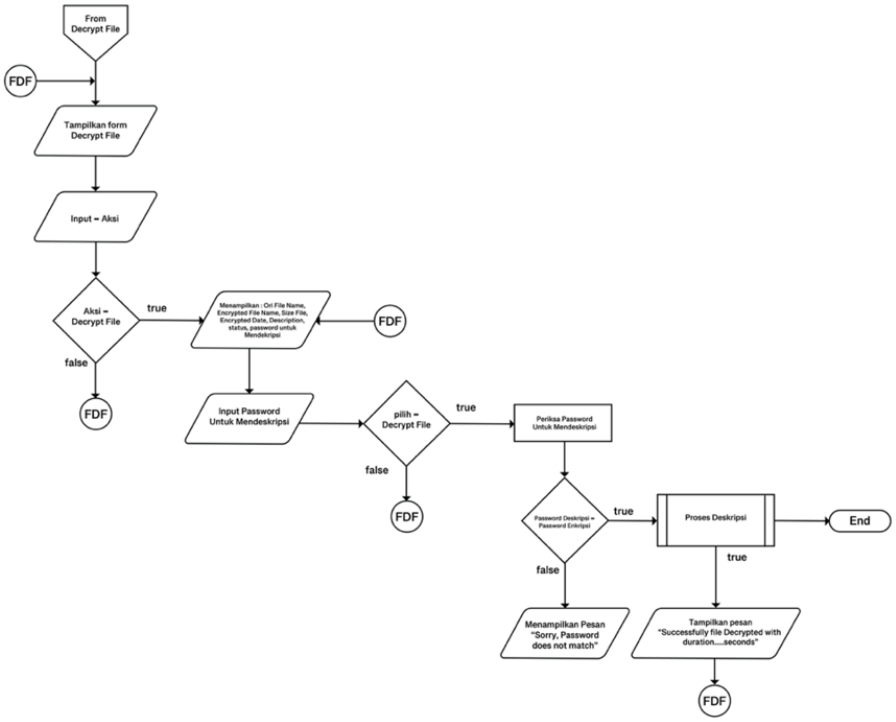
Pada gambar 6 merupakan *flowchart* dari halaman form enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi *file*, dalam menenkripsi *file* admin dan user haru memasukkan password, setelah itu program akan memproses *Encryption* (enkripsi).



Gambar 6. Flowchart Proses *Encryption* Enkripsi

3.2 Flowchart Menu *Decryption* (Dekripsi)

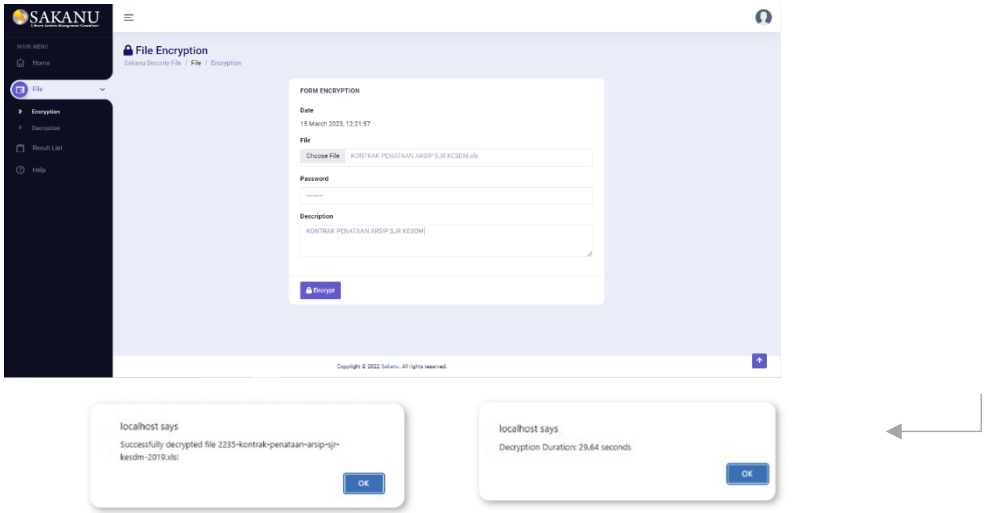
Pada gambar 7 merupakan *flowchart* dari halaman *form Decryption* (dekripsi), dimana *flowchart* ini menjelaskan tentang melakukan dekripsi *file*, dalam dekripsi *file* pengguna harus memasukkan *password* yang sesuai dengan *password* enkripsi, setelah itu program akan memproses dekripsi.



Gambar 7. Flowchart Proses *Decryption* (Dekripsi)

3.3 Proses Encryption (Enkripsi)

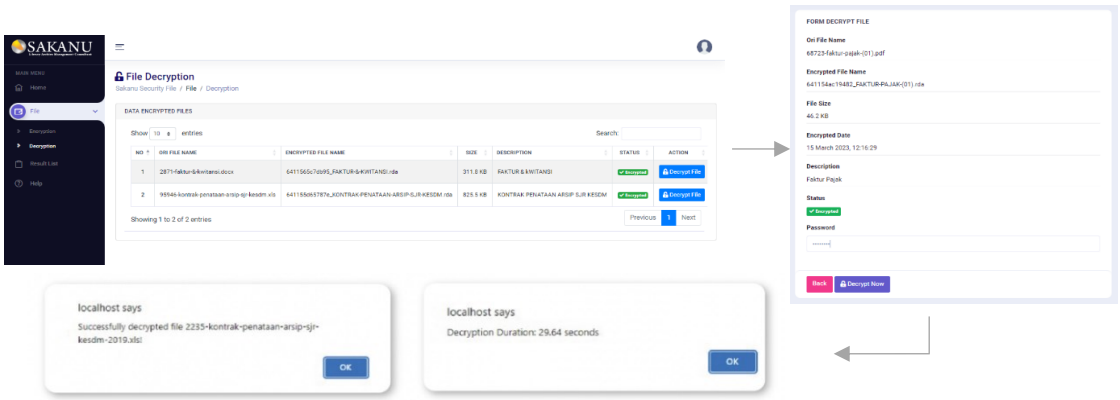
Masuk kehalaman *encryption* (enkripsi) pada sub menu *file* akan ada form yang mengharuskan upload *file* yang ingin dienkripsi, serta password sebagai kunci (*key*), *description* untuk memberi keterangan pada *file,* lalu klik *button "encrypt"*. Jika *file* berhasil akan ada *pop-up "File encrypted successfully!"* dan *Encryption Duration:* ".*$total_time_in_seconds.*"



Gambar 6. Proses Enkripsi

3.4 Proses Decryption (Dekripsi)

Proses pengubahan *file chipertext* (terenkripsi) menjadi *file plaintext* (Dekripsi), masuk halaman menu *decryption* yang pada sub *button file, klik "Decrypt file"* nantinya akan muncul *form decrypt file* yang mengharuskan user mencantumkan password (key) yang sama pada saat melalukan proses encrypt (enkripsi). Jika berhasil akan ada *pop-up* "*Successfully decrypted file*".*$data_file!*" lalu dan "*Decryption Duration:* ".*$total_time_in_seconds*."



Gambar 8. Proses *Decryption* (Dekripsi)

3.5 Pengujian

Pada Tabel 2 dan 3 adalah hasil dari pengujian *file* pada pogram aplikasi Enkripsi dan Dekripsi AES-128. Bertujuan agar dapat dilihat hasil prosesnya berhasil/tidak.

Tabel 2. Hasil Pengujian Enkripsi

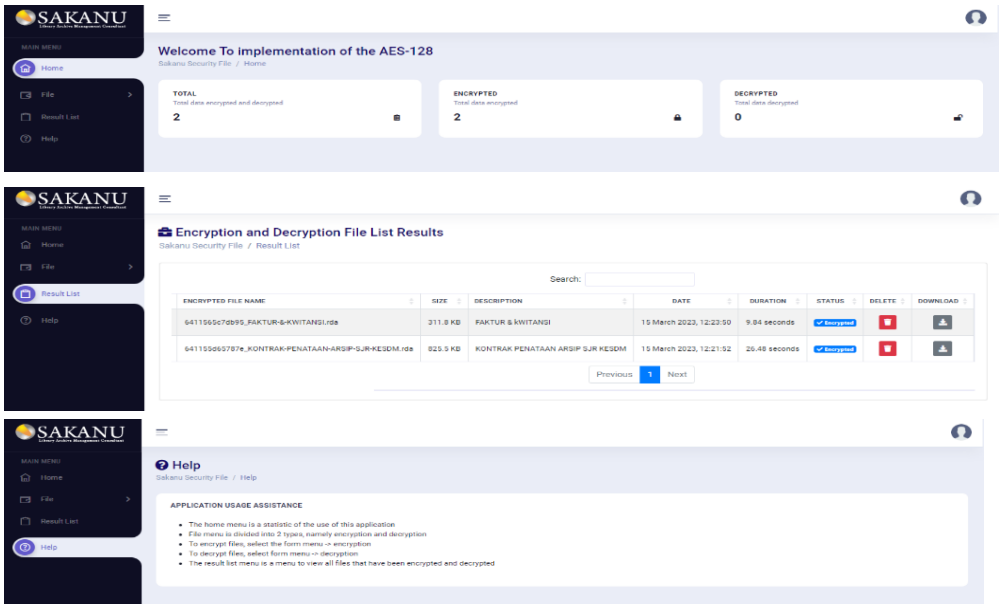
Tabel 3. Hasil Pengujian Dekripsi

No	Nama file awal	Ukuran file asli	Nama file enkripsi	Ukuran file enkripsi	Status	
					Enkripsi	Durasi
1	Laporan laba_rugi 2019.pdf	110 kb	63d3db02a0fff_laporan-laba_rugi-2019.rda	110 kb	Berhasil	3.58 detik
2	Kontrak penataan arsip sjr kesdm.xls	825.5 kb	63d3daa89f653_kontrak-penataan-arsip-sjr-kesdm.rda	825.5 kb	Berhasil	26.3 detik
3	Faktur pajak.pdf	46.2 kb	63d3da670070a_faktur-pajak.rda	46.2 kb	Berhasil	1.47 detik
4	Faktur & kwitansi.docx	311.8 kb	63d3da3c32f96_faktur-&-kwitansi.rda	311.8 kb	Berhasil	9.47 detik
5	Rab penataan arsip.xlsx	16.8 kb	63d3d91cf0bfd_rab-penataan-arsip-.rda	16.8 kb	Berhasil	0.54 detik
6	Pemilihan berkas.jpg	18000 kb	File hanya bisa word, excel, text dan pdf	-	Gagal	-
7	Surat-surat	9220 kb	File tidak boleh lebih dari 8mb	-	Gagal	-

3.6 Tampilan Layar

No.	Nama File Awal	Ukuran File Asli	Nama File Enkripsi	Ukuran File Enkripsi	Status	
					Enkripsi	Durasi
1	Laporan Laba_Rugi 2019.Pdf	110 KB	33370-Laporan-Laba_Rugi-2019.Pdf	110 KB	Berhasil	3.54 Detik
2	Kontrak Penataan Arsip Sjr Kesdm.Xls	825.5 KB	13860-Kontrak-Penataan-Arsip-Sjr-Kesdm.Xls	825.5 KB	Berhasil	25.42 Detik
3	Faktur Pajak.Pdf	46.2 KB	75537-Faktur-&-Kwitansi.Docx	46.2 KB	Berhasil	1.48 Detik
4	Faktur & Kwitansi.Docx	311.8 KB	75537-Faktur-&-Kwitansi.Docx	311.8 KB	Berhasil	9.7 Detik
5	Rab Penataan Arsip.Xlsx	16.8 KB	8671-Rab-Penataan-Arsip.xlsx	16.8 KB	Berhasil	0.56 Detik

Pada tampilan layar yang diuraikan mengenai tahap awal program dijalankan. Yaitu ada tampilan layar *home* yang berfungsi untuk menampilkan berapa total *file* yang sudan di *encrypted* & *decrypted* , selanjutnya ada tampilan layar *result file*, yang berfungsi menampilkan hasil *file* yang sudah di *encrypted* & *decrypted* dan bisa menghapus serta mendownload file, yang terakhir *help*, berisi tentang bantuan jika *users* mengalami kendala saat penggunaan aplikasi terdapat pada gambar 9.



Gambar 9. Tampilan Layar

4. KESIMPULAN

Berdsarkan uraian dalam bab sebelumnya dan aplikasi dikembangkan, dari sini disimpulkan bahwa program aplikasi pengamanan file berbasis web untuk PT. Samudra Katulistiwa dengan menerapkan metode *Advanced Encryption Standard* (AES-128 bit) menggunakan aplikasi kriptografi bisa menjadi tindakan pengamanan yang dapat merekam data berdasarkan agresi/pihak yang bertanggung jawab. Adapun, ukuran file yang diproses mempengaruhi durasi yang ditempuh dalam proses *encryption* (enkripsi) dan *decryption* (dekripsi). Dimana semakin minim ukuran pada file yang akan diproses, semakin cepat juga *encryption* (enkripsi) dan *decryption* dekripsi, dan semakin tinggi/besar ukuran file, semakin lama enkripsi dan dekripsi. aplikasi ini sudah dapat didukung dengan format dan ekstensi *file* Office *.doc, *.docx,*.xls,*.xlsx,* *.pptx, *.txt dan *.pdf . Dari hal-hal tersebut pula, diharapkan program ini dapat diperbaiki dalam segi waktu yang ditempuh pada enkripsi dan dekripsi supaya bisa lebih cepat lagi pada ukuran file yang lebih besar.

DAFTAR PUSTAKA

[1] Azanuddin, Suardi Yakub dan Jaka Prayuda. Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server. JURASIK, Volume 7, No. 1(ISSN: 2527-5771), pp. 51-61, 2022.

[2] Aji Permana dan Elan jaelani. Implementasi Algoritma Aes 128 Bit Sebagai Pengaman Teks Di Aplikasi Note Berbasis Android. Jejaring, Volume 5, No. 2(E-ISSN : 2614-5448) pp. 9-17, 2020.

[3] Binanda Wicaksana dan Ma'mun Setiawan. Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Berkas Soal Ujian. TEKNOIS, Volume 10, No. 1(e-ISSN : 2087-3891), pp. 25-34, 2020.

[4] Chaerul Umam, Muslih dan Daffa Fadillah. Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna. 2st Proceeding STEKOM, Volume 2, No.1 no. ISSN: 2809-1566, pp. 110-111 2022.

[5] Delisman Hulu, Berto Nadeak dan Soeh Aripin. DOI: 10.30865/komik.v4i1.2590 Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. KOMIK, Volume 4, No.1(ISSN 2597-4645), pp. 78-86, 2020.

[6] Imelda Asih Rohani Simbolon, Indra Gunawan, Ika Okta Kirana, Rafiqa Dewi,dan S. Solikhun. Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. Journal of Computer System and Informatics (JoSYC), Volume1, No.2(SSN 2714-8912), pp. 54-60, 2020.

[7] Mhd.Fachrul Fachrozi, Hasanul. Fahmi. Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint Di Balai Penelitian Sungei Putih. JIKOMSI , Vol.3 No.3(E-ISSN : 2723-6129), pp 1-8, 2021.

[8] Triyas Hevianto Saputro, N. H. (2020). Survei Tentang Algoritma Kriptografi Asimetris. JIP (Jurnal Informatika Polinema)(Vol 6 No 2), ISSN: 2614-6371 E-ISSN: 2407-070X, pp. 67-77, 2020.

[9] Hamid Wijaya. (2020). Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection . Akademika, Vol.17 No.1(e-ISSN : 2548-4184), pp. 8-13, 2020.

[10] Zahrul Basim, Painem. (2020). Implementasi Kriptografi Algoritma Rc4 Dan 3des Dan Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As-Su'udiyyah. Skanika, Volume 3, No.4(E-ISSN: 2721-478),pp. 54-60, 2020.