5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITMA AES 128 BERBASIS *WEB* UNTUK KEAMANAN *FILE* PT. TUMBAKMAS NIAGA SAKTI

Yossy Anggara[1*], Mufti[2]

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

Email: [1*]2011511090@student.budiluhur.ac.id, [2]mufti@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT. Tumbakmas Niaga Sakti adalah perusahaan yang bergerak di bidang penjualan dan distribusi, pada PT. Tumbakmas Niaga Sakti terdapat data-data penting khususnya data penjualan yang menjadi tanggung jawab bagi beberapa pihak yang bersangkutan. Data penjualan perlu dilindungi dari akses yang tidak berhak agar tidak digunakan atau dimanfaatkan sebagai acuan perbandingan penjualan untuk kategori produk yang penjualannya tinggi di pasar. Kebocoran data penjualan dapat menyebabkan menurunya *omset* penjualan sehingga akan menyebabkan kerugian *finansial* pada perusahaan PT. Tumbakmas Niaga Sakti. Pada penelitian ini mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* (AES) 128 bit pada aplikasi berbasis web untuk mengamankan data penjualan milik PT. Tumbakmas Niaga Sakti. Algoritma AES 128 bit dipilih karena lebih efisien dalam hal kecepatan dan tingkat keamanan yang tinggi sehingga sangat sulit dipecahkan dengan serangan *brute force* dibandingkan dengan Algoritma DES. Dari hasil pengujian yang dilakukan mampu mengenkripsi dan mendekripsi data penjualan PT. Tumbakmas Niaga Sakti menggunakan algoritma AES 128 bit dengan baik. Hal ini dilihat dari *file* hasil enkripsi yang isinya tidak dapat dibaca atau tidak dimengerti oleh orang lain dan hasil dari *file* yang didekripsi memiliki isi yang sama dengan *file* asli tanpa adanya kekurangan sehingga tetap menjaga integritas data. Implementasi ini memberikan solusi *keamanan file* yang efektif bagi PT. Tumbakmas Niaga Sakti dalam melindungi data penjualan dari akses tidak sah dan menghindari kebocoran data.

Kata Kunci: Algoritma, Kriptografi, *Advanced Encryption Standard* (AES), *waterfall*, AES 128 bit.

WEB-BASED AES 128 ALGORITHM IMPLEMENTATION FOR FILE SECURITY PT. TUMBAKMAS NIAGA SAKTI

Abstract- *PT. Tumbakmas Niaga Sakti is a company engaged in sales and distribution, at PT. Tumbakmas Niaga Sakti contains important data, especially sales data, which is the responsibility of several parties concerned. Sales data needs to be protected from unauthorized access so that it is not used or exploited as a sales comparison reference for product categories with high sales in the market. Sales data leaks can cause a decrease in sales turnover, which will cause financial losses to the PT company. Tumbakmas Niaga Sakti. In this research, we implemented the Advanced Encryption Standard (AES) 128-bit cryptographic algorithm in a web-based application to secure sales data belonging to PT. Tumbakmas Niaga Sakti. The 128-bit AES algorithm was chosen because it is more efficient in terms of speed and has a high level of security, so it is very difficult to break with brute force attacks compared to the DES algorithm. From the results of the tests carried out, it was able to encrypt and decrypt PT sales data. Tumbakmas Niaga Sakti uses the AES 128-bit algorithm well. This can be seen from the encrypted file whose contents cannot be read or understood by other people and the results of the decrypted file have the same contents as the original file without any shortcomings, thereby maintaining data integrity. This implementation provides an effective sales data security solution for PT. Tumbakmas Niaga Sakti in protecting sales data from unauthorized access and avoiding data leaks.*

Keywords*: Algorithms, Cryptography, Advanced Encryption Standard (AES), waterfall, AES 128 bit.*

1. PENDAHULUAN

Pada zaman yang serba digital saat ini, keamanan data menjadi salah satu hal yang mempunyai peran penting bagi perusahaan. Salah satu data penting bagi perusahaan adalah data penjualan yang di*maintenance* setiap bulannya. Kebocoran data penjualan dapat menyebabkan kalahnya persaingan bisnis terutama pada produk-produk dengan permintaan tinggi di pasar. Persaingan bisnis yang semakin ketat mendorong setiap pengusaha memeras habis pikirannya untuk merumuskan strategi pemasaran yang hebat. Tidak jarang pelaku bisnis menempuh hal-hal tidak terpuji dengan melakukan pencurian data penjualan agar dapat selangkah lebih maju untuk mengalahkan pesaing. Jika data perusahaan bocor ke tangan pesaing bisnis, data tersebut dapat dimanfaatkan oleh pesaing untuk meningkatkan penjualannya.

PT. Tumbakmas Niaga Sakti adalah perusahaan yang bergerak di bidang penjualan dan distribusi yang didirikan pada tahun 2003 dan berpusat di Jl. Letjen S. Parman. Sebagai perusahaan memiliki jaringan dari Sabang sampai Merauke membuat TNS berkembang menjadi perusahaan yang berkompeten. Sebagai perusahaan yang

berkembang, PT. Tumbakmas Niaga Sakti memiliki banyak *file* penting terutama data penjualan yang perlu dilindungi dari akses yang tidak berhak agar tidak digunakan atau dimanfaatkan untuk hal-hal yang dapat menyebabkan kerugian secara *finansial*.

Kriptografi adalah suatu teknik pengamanan data yang berguna untuk menjaga kerahasiaan data dan keaslian data[1]. Pengamanan *file* dengan menggunakan teknik kriptografi telah banyak dilakukan diberbagai penelitian [2]. Salah satu algoritma yang digunakan untuk mengamankan *file* adalah AES 128 [3]. Algoritma AES adalah blok ciphertext simetris yang mampu mengenkripsi (encipher) dan mendekripsi informasi (decipher) [3].

Pada penelitian sebelumnya, Rista Maya dkk melakukan penelitian yang berjudul "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES". Pada penelitian sebelumnya menjelaskan manfaat kriptografi dengan metode DES untuk mengamankan data nilai siswa agar tidak tidak dimanipulasi oleh pihak yang tidak bertanggung jawab [4]. Pada algoritma DES melakukan operasi pada ukuran blok 64 bit dan menggunakan panjang kunci 64 bit tetapi hanya 56 bit yang dipakai sisa 8 bit paritas tidak digunakan. Proses enkripsi algoritma DES pada tahap pertama yaitu plainteks dan kunci diubah kedalam bentuk biner. Setelah itu blok plainteks dipermutasi dengan Tabel IP dan blok kunci dipermutasi dengan Tabel PC untuk pembangkitan kunci. Pada proses pembangkitan kunci 56 bit ini dilakukan pembagian menjadi dua, kiri dan kanan, yang panjang masing-masing 28 bit. Kedua bagian itu digeser ke kekiri sebanyak 1 atau 2 *byte*. Proses ekspansi kunci ini dilakukan sebanyak 16 putaran. Dari hasil kunci yang diperoleh pada 16 putaran ini selanjutnya akan dilakukan proses enkripsi pada setiap blok plainteks sebanyak 16 putaran.

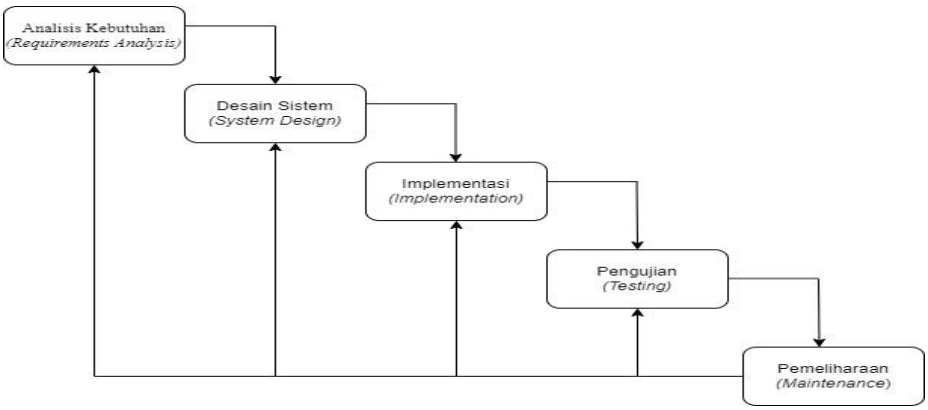
Sedangkan pada penelitian yang penulis lakukan menggunakan Algoritma *Advanced Encryption Standard* (AES) untuk mengatasi kekurangan pada Algoritma *Data Encryption Standard* (DES). Pada algoritma AES melakukan operasi pada ukuran blok 128 bit dan panjang kunci yang dipakai dari 128 bit, 192 bit, 256 bit yang membuatnya lebih tahan terhadap serangan *brute force* [5]. Proses enkripsi algoritma AES pada tahap pertama yaitu plainteks dan kunci diubah kedalam bentuk biner. Setelah itu lakukan proses ekspansi kunci yang melalui beberapa tahap. Tahap pertama ubah kunci dalam *hexadesimal* dengan ukuran matrik 4x4, lalu lakukan pergeseran ke kiri sebanyak 1 bit, selanjutnya lakukan subtitusi menggunakan *S-BOX* pada matrik yang sudah dilakukan pergeseran dan lakukan XOR dengan *round constant*. Hasil XOR dengan *round constant* tersebut lakukan XOR dengan matriks awal. Proses ini diulang sebanyak 10 putaran. Dari hasil kunci yang diperoleh pada 10 putaran ini adalah kunci yang dipakai untuk proses enkripsi pada setiap blok plainteks sebanyak 10 putaran.

Pada Penerapan algoritma AES, dengan ukuran kunci yang lebih besar, ukuran blok yang lebih besar, proses ekspansi kunci yang lebih kompleks membuat algoritma AES lebih unggul dari Algoritma DES yang digunakan pada penelitian sebelumnya. Dari keunggulan Algoritma AES maka penulis mengusulkan metode algoritma AES untuk mengamankan data penjualan PT. TUMBAKMAS NIAGA SAKTI sehingga dapat mengurangi risiko kerugian finansial dan reputasi kebocoran data yang dapat menyebabkan menurunya persentase penjualan yang sebelumnya sudah meningkat. Dengan adanya solusi keamanan data yang efektif, risiko tersebut dapat diminimalkan.

2. METODE PENELITIAN

2.1 Penerapan Metode

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode *waterfall*. Gambar 1 menunjukkan tahapan metode *waterfall*.



Gambar 1. Tahapan Metode *Waterfall*

Berikut tahapan dalam metode *waterfall* meliputi:

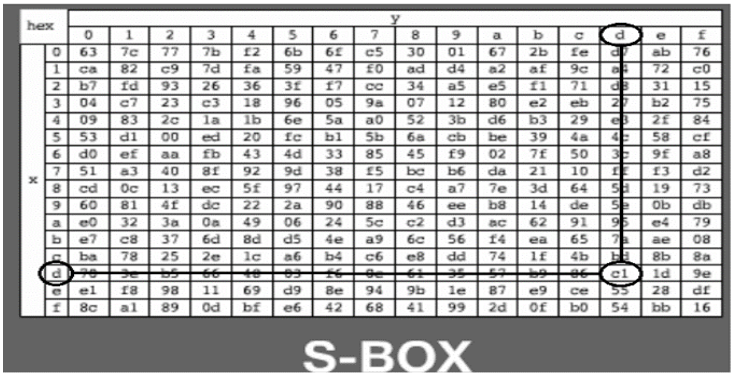
a. Analisis Kebutuhan *(Requirements Analysis)*
   Pada tahap ini dilakukan pengumpulan dan menganalisis kebutuhan perangkat lunak yang di inginkan oleh PT. Tumbakmas Niaga Sakti. Kegiatan ini dilakukan dengan wawancara, survei, dan studi kelayakan untuk spesifikasi perangkat lunak.
b. Desain Sistem *(System Design)*
   Setelah semua kebutuhan sistem terkumpul, tahap selanjutnya adalah melakukan desain dan perancangan sistem. Hasil dari tahap ini adalalah spesifikasi lengkap yang menggambarkan bagaimana perangkat lunak akan dibangun.
c. Implementasi *(Implementation)*
   Pada tahap ini mulai dilakukan menuliskan kode program *(Coding)* berdasarkan desain yang telah dirancang sebelumnya. Kode program ditulis, dilakukan pengujian *(unit testing)*, dan diintegrasikan menjadi satu kesatuan perangkat lunak.
d. Pengujian *(Testing)*
   Setelah implementasi selesai, dilakukan pengujian terhadap seluruh perangkat lunak guna memastikan semua persyaratan telah terpenuhi. Jika ditemukan *error* atau *bug*, maka dilakukan perbaikan sebelum melanjutkan ke tahap berikutnya.
e. Pemeliharaan *(Maintenance)*
   Pada tahap ini adalah tahap terakhir yaitu dilakukan pemeliharaan perangkat lunak setelah diimplementasikan. Pemeliharaan yang dilakukan meliputi perbaikan *error* atau *bug*, penyempurnaan fungsi, dan pembaruan sesuai dengan kebutuhan PT. Tumbakmas Niaga Sakti..

2.2 *Advanced Encryption Standard* (AES)

a. Proses enkripsi AES 128
   Pada proses enkripsi AES 128 terdapat 4 jenis transformasi adalah sebagai berikut:
   1. *Addroundkey* adalah melakukan XOR antara plainteks (*state* awal) dengan *cipher key*. Tahap ini disebut juga *initial round*. Pertama ubah bilangan heksadesimal menjadi biner: 0x95 = 10010101 (dalam biner) 0x48 = 01001000 (dalam biner). Lakukan operasi XOR bit per bit: 10010101 ⊕ 01001000 = 11011101 (dalam biner). Ubah hasil biner menjadi heksadesimal: 11011101 (dalam biner) = 0xdd (dalam heksadesimal), hasil dari operasi XOR antara 0x95 dan 0x48 adalah 0xdd. Pada gambar 1 dapat dilihat pada matrik sebelah kiri merupakan plainteks yang diXORkan dengan *Chiper key*.

95	1e	a1	3d	XOR	48	f6	0f	b7	=	dd	e8	ae	8a
61	73	d6	db		c5	28	84	6f		a4	5b	52	b4
6c	3b	9f	00		48	ac	06	f9		24	97	99	f9
70	34	81	8c		c0	58	82	0b		b0	6c	03	87

   2. *Subbytes*, pada tahap ini dilakukan penggantian setiap isi matriks dengan menggunakan tabel S-BOX. Langkah pertama yang dilakukan ambil nilai heksadesimal misalnya dd, kemudian cari pada tabel S-BOX untuk nilai x=d dan nilai y=d. Maka hasil yang didapatkan adalah c1.



Gambar 2. Tabel S-BOX

3. *Shift Rows* adalah proses menggeser atau memindahkan setiap blok atau elemen tabel baris demi baris. Pada baris pertama tidak dilakukan pergeseran, pada baris kedua dilakukan pergeseran 1 *byte*, pada baris ketiga dilakukan pergeseran 2 *byte*, dan pada baris keempat dilakukan pergeseran 3 *byte*. Pergeseran tersebut terlihat pada contoh sebuah blok yang berisi nilai heksadesimal terdapat pergeseran tiap elemen ke kiri tergantung berapa banyak *byte* yang tergeser, setiap tergeser 1 *byte* artinya bergeser ke kiri sebanyak 1 kali.

c1	9b	e4	7e
49	39	00	8d
36	88	99	ee
e7	50	7b	17

⟹

c1	9b	e4	7e
39	00	8d	49
99	ee	36	88
17	e7	50	7b

4. *MixColumns* adalah mengalikan setiap kolom dalam *block chiper* 4x4 dengan matriks tetap. Transformasi *MixColumns* beroperasi pada *state* matriks 4x4 *byte*. Setiap kolom dari matriks diperlakukan sebagai polinomial 4 suku pada GF (2^8). Kolom ini dikalikan modulo $x^4 + 1$ dengan polinomial tetap $c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + 02$. $s'(x) = c(x) \oplus s(x)$. Untuk perhitungan perkalian yang berlaku adalah perkalian dengan 01 berarti tidak ada perubahan, perkalian dengan 02 adalah menggeser *byte* kekiri kemudian lakukan XOR dengan 0x1B jika bit MSB adalah 1. Perkalian dengan 03 adalah XOR hasil perkalian dengan 02 dan *byte* asli.

$S'_{0,c}$	=	02	03	01	01	X	$S_{0,c}$
$S'_{1,c}$		01	02	03	01		$S_{1,c}$
$S'_{2,c}$		01	01	02	03		$S_{2,c}$
$S'_{3,c}$		03	01	01	02		$S_{3,c}$

Perhitungan perkalian dengan matriks tetap *MixColumns* :

$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$

$S'_{1,c} = S_{0,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c}$

$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{3,c})$

$S'_{3,c} = (\{03\} \bullet S_{0,c}) \oplus S_{0,c} \oplus S_{1,c} (\{02\} \bullet S_{3,c})$

b. Proses Dekripsi AES 128

Pada proses dekripsi terdapat 4 jenis transformasi yang merupakan kebalikan dari proses enkripsi adalah sebagai berikut:

1. *Addroundkey* pada proses dekripsi adalah dengan melakukan XOR antara *Chipertext* dengan kunci putaran terakhir. Dapat dilihat pada gambar 3, disebelah kiri merupakan *Chipertext* yang diXORkan dengan kunci putaran terakhir.

ea	77	a2	50	⊕	33	e5	34	58	=	d9	92	96	08
4d	e3	fb	27		8c	ea	75	e0		c1	09	8e	c7
20	d0	fa	b7		2a	4f	3d	0c		0a	9f	c7	bb
99	8e	4b	f3		e1	8c	7c	6e		78	02	37	9d

2. *Inverse ShiftRows* merupakan operasi kebalikan dari *ShiftRows* yang dilakukan pada proses enkripsi. Pada transformasi *Inverse ShiftRows* dilakukan pergeseran bit ke kanan. Pada baris ke-0 tidak dilakukan pergeseran, pada baris ke-1 lakukan pergeseran kekanan sebanyak 1 *byte*, pada baris ke-2 lakukan pergeseran ke kanan sebanyak 2 *byte*, dan pada baris ke-3 lakukan pergeseran ke kanan sebanyak 3 *byte*.

d9	92	96	08
c1	09	8e	c7
0a	9f	c7	bb
78	02	37	9d

⟹

d9	92	96	08
c7	c1	09	8e
c7	bb	0a	9f
02	37	9d	78

3. *Inverse SubBytes* merupakan transformasi *bytes* yang berkebalikan dengan transformasi *SubBytes*. Pada *Inverse SubBytes*, tiap elemen pada *state* dipetakan dengan menggunakan tabel *Inverse* S-Box.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 3. Tabel *Inverse* S-BOX

4. *Inverse MixColumns* beroperasi dengan cara yang sama seperti enkripsi, tetapi menggunakan matriks *inverse* dari matriks tetap enkripsi yang digunakan dalam *MixColumns*. Matriks *inverse* ini digunakan untuk mengembalikan efek pengacakan yang dilakukan oleh *MixColumns* pada proses enkripsi. Proses ini dihitung dengan aturan pola *irreducibel polynomial.*

S'_0	=	0e	0b	0d	09	X	29	a2	e4	d3
S'_1		09	0e	0b	0d		ed	bb	df	61
S'_2		0d	09	0e	0b		31	9b	d1	5f
S'_3		0b	0d	09	0e		4c	df	85	d3

S'_0 = 0e x 29
Hex 0e = binary 00001110 (Di pola *polynomial* = $(x^3 + x^2 + x)$
Hex 29 = binary 00101001 (Di pola *polynomial* = $(x^5 + x^3 + 1)$
S'_1 = 0b x ed
Hex 0b = binary 00001011 (Di pola *polynomial* = $(x^3 + x + 1)$
Hex ed = binary 11101101 (Di pola *polynomial* = $(x^7 + x^6 + x^5 + x^3 + x^2 + 1)$
S'_2 = 0d x 31
Hex 0d = binary 00001101 (Di pola *polynomial* = $x^3 + x^2 + 1$)
Hex 31 = binary 00110001 (Di pola *polynomial* = $(x^5 + x^4 + 1)$
S'_3 = 09 x 4c
Hex 09 = binary 00001001 (Di pola *polynomial* = $(x^3 + 1)$
Hex 4c = binary 01001100 (Di pola *polynomial* = $(x^6 + x^3 + x^2)$

2.3 Data Penelitian

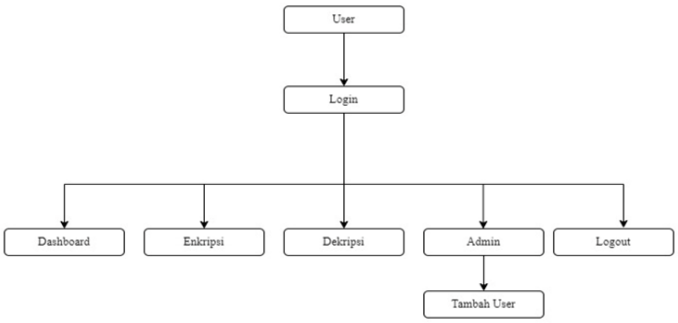
Data yang digunakan dalam penelitian ini adalah data hasil penjualan PT. Tumbakmas Niaga Sakti, data *monitoring* penjualan setiap harinya. Data ini diberikan langsung dari sumbernya tanpa melalui perantara dengan melakukan pengumpulan data langsung melalui *informan* yang merupakan karyawan PT. Tumbakmas Niaga Sakti. Data yang diperoleh akan digunakan dalam uji coba pengamanan *file* menggunakan metode *Advanced Ecryption Standard* 128 (AES-128).

2.4 Rancangan Pengujian

Rancangan pengujian yang dilakukan adalah pengujian fungsionalitas untuk memastikan bahwa semua fitur dan fungsionalitas pada aplikasi berjalan dengan baik tanpa adanya kesalahan.

2.5 Rancangan Menu

Pada program ini akan dibuat beberapa halaman yaitu halaman *login* dan halaman *dashboard*, pada *halaman dashboard* terdapat menu enkripsi, dekripsi, admin, dan *logout.*



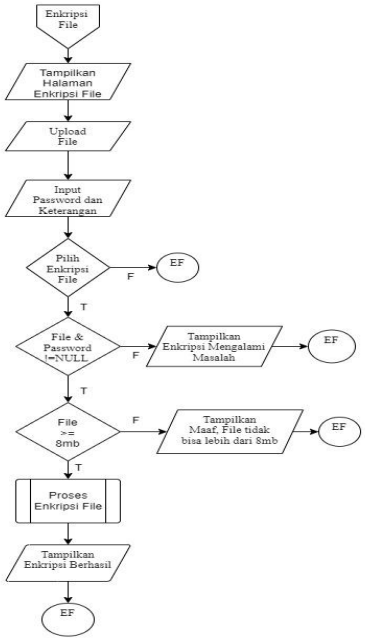
Gambar 4. Rancangan Menu

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1 *Flowchart* Halaman Enkripsi File

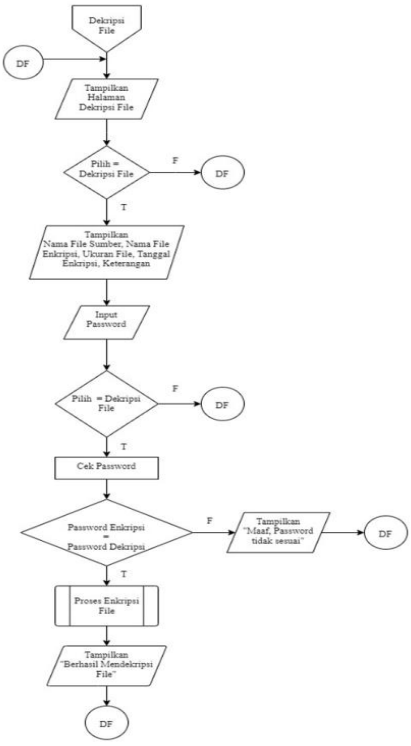
Pada *Flowchart* ini menjelaskan tentang enkripsi *file*, *user* akan melakukan *upload file* yang akan dienkripsi, setelah *file* berhasil di*upload* selanjutnya *input key* untuk melanjutkan proses enkripsi. Berikut gambar 5 menunjukkan *flowchart* halaman enkripsi.



Gambar 5. *Flowchart* Halaman Enkripsi

3.2 *Flowchar*t Halaman Dekripsi *File*

Pada *flowchart* ini merupakan alur proses dekripsi sebuah *fil*e yang telah terenkripsi. Untuk melakukan dekripsi *file* ini, *user* diharuskan untuk *input password* yang sama pada saat melakukan enkripsi. Setelah itu program akan melakukan proses dekripsi, Gambar 6 menujukkan *flowchart* halaman dekripsi.



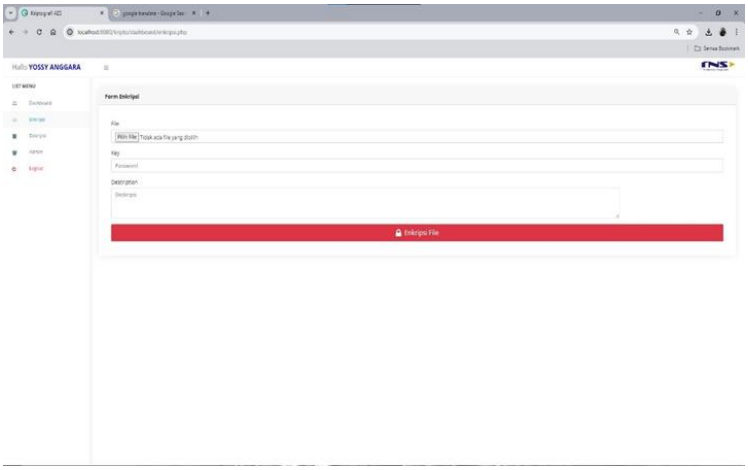
Gambar 6. *Flowchart* Halaman Dekripsi

3.3 Pengujian Program

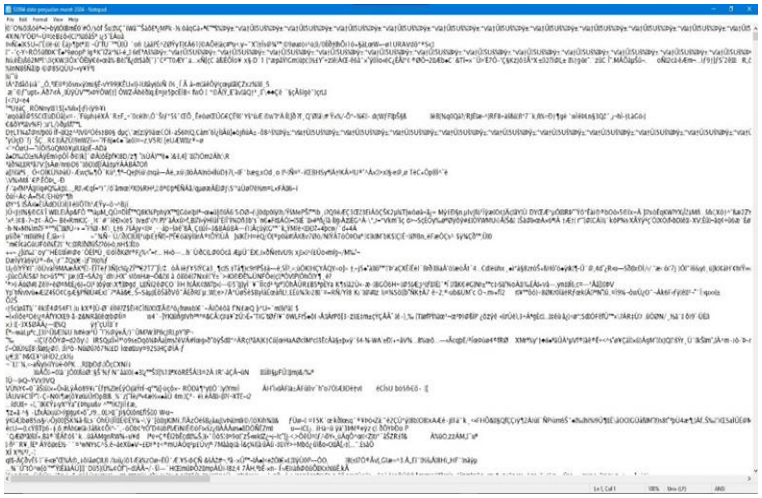
Pada tahap ini dilakukan pengujian program terhadap aplikasi yang telah selesai dibuat. Pengujian meliputi proses enkripsi dan dekripsi untuk mengetahui keberhasilan *file* yang dienkripsi berdasarkan ukuran *file* serta mengukur kecepatan *file* saat melakukan proses enkripsi maupun proses dekripsi.

3.4 Proses Enkripsi

Untuk melakukan proses enkripsi, pengguna harus *login* terlebih dahulu. Setelah berhasil *login* kemudian pilih menu Enkripsi, tampilan menu Enkripsi dapat dilihat pada gambar 7. Langkah selanjutnya pilih *file* yang ingin dienkripsi, jika sudah pilih lalu masukkan *password* sebagai kunci untuk melakukan enkripsi, masukkan keterangan jika diperlukan. Setelah semua telah diisi lalu pilih *button* Enkripsi *file*, proses enkripsi berlangsung jika berhasil akan muncul *pop up* "Enkripsi Berhasil". *File* yang berhasil dienkripsi untuk isi *file* tidak dapat dibaca, dapat dilihat pada gambar 8.



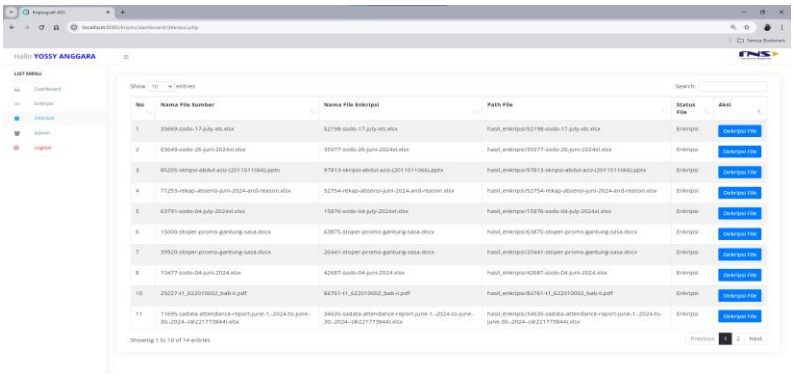
Gambar 7. Halaman Form Enkripsi



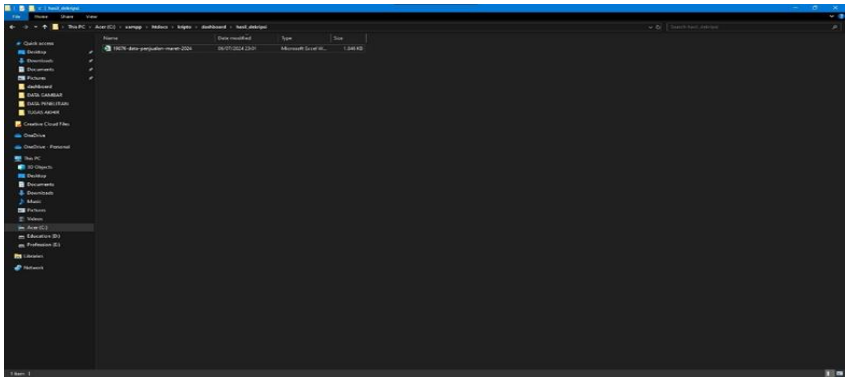
Gambar 8. Hasil Enkripsi File

3.5 Proses Dekripsi

Setelah proses enkripsi berhasil dilakukan, selanjutnya adalah melakukan pengujian untuk mengembalikan keaslian *file* yang telah terenkripsi yaitu dengan melakukan dekripsi *file*. Untuk melakukan dekripsi *file* langkah pertama yang harus dilakukan adalah pilih menu dekripsi maka akan muncul halaman *form* dekripsi yang dapat dilihat pada gambar 9. Pada halaman *form* dekripsi terdapat *list file* dengan status Enkripsi, dengan memilih *button* Dekripsi *File* pada kolom aksi maka akan ditampilkan detail *file* yang akan didekripsi. Langkah selanjutnya masukkan *password*, perlu diingat untuk melakukan dekripsi, *password* ynag dimasukkan harus sama saat melakukan enkripsi. Terakhir pilih *button Decrypt File*, jika berhasil akan muncul *pop up* "Berhasil dekripsi file". Pada gambar 10 menujukkan *file* hasil dekripsi.



Gambar 9. Halaman Form Dekripsi



Gambar 10. File Hasil Dekripsi

3.6 Hasil Pengujian Enkripsi dan Dekripsi File

Berikut ini hasil uji coba yang dijalankan pada aplikasi Enkripsi dan Dekripsi AES-128 dengan tujuan untuk mengetahui berhasil atau tidaknya hasil yang diperoleh. Pada Tabel 1 menggambarkan pencapaian dari pengujian Enkripsi yang dilakukan melalui aplikasi Enkripsi dan Dekripsi AES-128.

Tabel 1. Tabel Hasil Pengujian Enkripsi

No	Nama *file* Asli	Nama *File* Enkripsi	Ukuran *file* Enkripsi	Status Enkripsi	Waktu
1	15523-sodo-04-july-2024xl.xlsx	63612-sodo-04-july-2024xl.xlsx	1851.31 KB	BERHASIL	0.29s
2	33910-stopper-jsm-171123-sat.docx	53793-stopper-jsm-171123-sat.docx	47.6533 KB	BERHASIL	0.28s
3	57896-sales-brief-mtc-sasa,-hpi,-msbi-nka,-mti---jan-24.xlsx	77211-sales-brief-mtc-sasa,-hpi,-msbi-nka,-mti---jan-24.xlsx	696.115 KB	BERHASIL	0.59s
4	83513-riview---cirebon-juli-2024.pptx	86646-riview---cirebon-juli-2024.pptx	1148.4 KB	BERHASIL	0.39s
5	20801-program-consumer-promo-msbi-agustus-2024-only-mm-2024-(1).xlsx	3160-program-consumer-promo-msbi-agustus-2024-only-mm-2024-(1).xlsx	840.322 KB	BERHASIL	0.38s
6	40222-report-closing-mtc-mei-2024-yossy-anggara.xlsx	47186-report-closing-mtc-mei-2024-yossy-anggara.xlsx	76.8506 KB	BERHASIL	0.14s
7	58657-09.-key-performance-indicator-(kpi)-2020---2023.pptx	17885-09.-key-performance-indicator-(kpi)-2020---2023.pptx	2100.35 KB	BERHASIL	0.51s
8	35693-pkm-red-karpet.txt	3682-pkm-red-karpet.txt	2.03809 KB	BERHASIL	0.27s
9	1848-data-penjualan-juli-2024.txt	55038-data-penjualan-juli-2024.txt	0.03808 5 KB	BERHASIL	0.40s
10	15363-stoper-promo-gantung-sasa.docx	16768-stoper-promo-gantung-sasa.docx	18.6074 KB	BERHASIL	0.20s

Pada tabel 1 sudah berhasil melakukan uji coba enkripsi dan tahap selanjutnya akan dilakukan uji coba dekripsi untuk mengembalikan *file* yang sudah terenkripsi menjadi *file* asli yang utuh tanpa ada kekurangan pada isi *file*. Hasil dekripsi dapat dilihat pada Tabel 2.

Tabel 2. Tabel Hasil Pengujian Dekripsi

No	Nama file Enkripsi	Nama File Dekripsi	Ukuran file Dekripsi	Status Enkripsi	Waktu
1	63612-sodo-04-july-2024xl.xlsx	15523-sodo-04-july-2024xl.xlsx	1851.31 KB	BERHASIL	0.15s
2	53793-stopper-jsm-171123-sat.docx	33910-stopper-jsm-171123-sat.docx	47.6533 KB	BERHASIL	0.37s
3	77211-sales-brief-mtc-sasa,-hpi,-msbi-nka,-mti---jan-24.xlsx	57896-sales-brief-mtc-sasa,-hpi,-msbi-nka,-mti---jan-24.xlsx	696.115 KB	BERHASIL	0.29s
4	86646-riview---cirebon-juli-2024.pptx	83513-riview---cirebon-juli-2024.pptx	1148.4 KB	BERHASIL	0.3s
5	3160-program-consumer-promo-msbi-agustus-2024-only-mm-2024-(1).xlsx	20801-program-consumer-promo-msbi-agustus-2024-only-mm-2024-(1).xlsx	840.322 KB	BERHASIL	0.4s

6	47186-report-closing-mtc-mei-2024-yossy-anggara.xlsx	40222-report-closing-mtc-mei-2024-yossy-anggara.xlsx	76.8506 KB	BERHASIL	0.17s
7	17885-09.-key-performance-indicator-(kpi)-2020---2023.pptx	58657-09.-key-performance-indicator-(kpi)-2020---2023.pptx	2100.35 KB	BERHASIL	0.28s
8	3682-pkm-red-karpet.txt	35693-pkm-red-karpet.txt	2.03809 KB	BERHASIL	0.5s
9	55038-data-penjualan-juli-2024.txt	1848-data-penjualan-juli-2024.txt	0.038085 KB	BERHASIL	0.10s
10	16768-stoper-promo-gantung-sasa.docx	15363-stoper-promo-gantung-sasa.docx	18.6074 KB	BERHASIL	0.15s

4. KESIMPULAN

Setelah semua uji coba dilakukan pada aplikasi berbasis *web* dapat disimpulkan bahwa implementasi metode AES-128 untuk keamanan data penjualan PT. Tumbakmas Niaga Sakti memberikan solusi keamanan yang efektif untuk mengurangi risiko kerugian finansial dan reputasi kebocoran data yang dapat menyebabkan menurunya persentase penjualan yang sebelumnya sudah meningkat. Aplikasi ini dapat melakukan enkripsi dan dekripsi *file* dengan ukuran *file* dibawah 8 mb dan ekstensi *file* seperti *.doc, .docx, .xls, .xlss, .ppt, .pptx.* Dari hasil *file* yang dienkripsi dan didekripsi untuk integritas data dan ukuran *file* asli dengan *file* hasil enkripsi atau dekripsi masih sama, tidak mengalami perubahan. Berdasarkan dari hasil kesimpulan, diperlukan adanya saran untuk pengembangan lebih lanjut agar dapat meningkatkan kinerja aplikasi ini. Untuk pengembangan selanjutnya diharapkan dapat melakukan enktipsi *file* dengan ukuran *file* lebih besar dari 8 mb. Pada aplikasi ini kecepatan enkripsi berdasarkan besar kecilnya ukuran *file*. Disarankan jika proses enkripsi terlalu lama, maka akan muncul pemberitahuan apakah masih ingin melanjutkan untuk menyelesaikan prosesnya atau dibatalkan.

DAFTAR PUSTAKA

[1] A. P. R. Tarigan, P. S. Ramadhan, and K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)," *Jurnal Cyber Tech*, vol. 5, no. 1, pp. 26–35, 2023.

[2] 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. 163–171, 2022.

[3] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM: Jurnal Riset Komputer*, vol. 7, no. 1, pp. 182–193, 2020.

[4] W. Rista Maya, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," Jurnal SAINTIKOM: *Jurnal Sains Manajemen Informatika dan Komputer*, vol. 21, no. 1, pp. 1–9, 2022.

[5] N. Wa. Hidayatulloh, et al, "Mengenal Advanced Encryption Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," vol. 3, no. 1, pp. 1–10, 2023.

[6] Z. Basim and Painem, "Implementasi Kriptografi Algoritma Rc4 Dan 3des Dan Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 3, no. 4, pp. 54-60, 2020.

[7] D. Widyawan and Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 4, no. 1, pp. 15–22, 2021.

[8] A. E. Putri, A. Kartikadewi, and L. A. A. 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," *AISM: Applied Information System and Management*, vol. 3, no. 2, pp. 69–78, 2020.

[9] M. Faisal Nu'man and R. R. Santika, "Implementasi Algoritme AES 128 Berbasis Web Dalam Proyek Pembangunan Perumahan Anggana Sentul PT. Adhi Karya," *Prosiding SENAFTI Ke-3 September*, 2023, pp. 206-213.

[10] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia," *SKANIKA: Sistem Komputer dan Teknik Informatika* , vol. 4, no. 1, pp. 66–71, 2021.