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

APLIKASI KEAMANAN *FILE* MENGGUNAKAN ALGORITME KRIPTOGRAFI AES 128 BERBASIS WEB PADA PILAR MEDICAL CENTER

Abiansyah Trista Pandya[1*], Joko Christian Chandra[2]

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

Email: [1*]abiansyahtrista@gmail.com, [2]joko.christian@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan jaringan internet yang sangat membantu manusia untuk bertukar data. Saat bertukar data dan in*form*asi dengan orang lain melalui Internet, transmisi data semakin rentan terhadap serangan penyadapan yang dapat membahayakan integritas data dan bersifat rahasia atau pribadi. Namun pada kenyataannya, pihak-pihak yang tidak bertanggung jawab yang biasa disebut penjahat dunia maya dapat masuk ke dalam banyak kasus pencurian data atau penyadapan data yang sangat rahasia. Pilar Medical Center merupakan perusahaan yang bergerak dibidang kesehatan yang melayani pelayanan medis memiliki *record* pasien yang datanya bersifat rahasia. Saat ini data tersebut masih dalam bentuk *file* biasa yang dapat dibaca pihak yang tidak berwenang. Oleh karena itu Pilar Medical Center perlu meningkatkan keamanan data dengan menerapkan pengamanan kriptografi menggunakan algoritme *Advanced Encryption Standard* 128 (AES 128). Algoritme enkripsi AES telah berhasil digunakan dalam aplikasi keamanan *file* berbasis web di Pilar Medical Center. Waktu yang diperlukan untuk proses enkripsi dan dekripsi sebanding dengan ukuran *file* yang akan diproses (semakin kecil ukuran *file* yang akan diproses, semakin cepat proses enkripsi dan dekripsinya. Begitu pun sebaliknya, semakin besar ukuran *file*, semakin lama pula proses enkripsinya dan dekripsi proses berlangsung). Aplikasi ini telah di uji dengan metode *Blackbox* dan berfungsi penuh untuk data atau dokumen yang bertipe .doc, .docx, .xls, .xlsx, .ppt, .pptx. Pengembangan sistem diperlukan agar tidak hanya dapat menangani dokumen tertulis tetapi juga dokumen gambar, video dan audio. Sistem harus dikembangkan dengan AES192 atau AES258, Hal ini akan mempersulit pihak yang tidak bertanggung jawab untuk mencuri data.

Kata Kunci: kriptografi, aes-128, *cybercrime*, keamanan data, pengamanan data, *advanced encyrption standard*

FILE SECURITY APPLICATION USING WEB-BASED AES128 CRYPTOGRAPHIC ALGORITHM AT PILAR MEDICAL CENTER

Abstract- *The development of the internet network is very helpful for humans to exchange data. When exchanging data and information with others via the Internet, data transmission is increasingly vulnerable to eavesdropping attacks which can compromise data integrity and are confidential or private. But in reality, irresponsible parties who are commonly called cybercriminals can get involved in many cases of data theft or wiretapping of highly confidential data. Pilar Medical Center is a company engaged in the health sector that provides medical services and has patient records whose data is confidential. Currently the data is still in the form of ordinary files that can be read by not many parties. Therefore Pilar Medical Center needs to improve data security by implementing cryptographic security using the Advanced Encryption Standard 128 (AES 128) algorithm. The AES encryption algorithm has been successfully used in a web-based file security application at Pilar Medical Center. The time required for the encryption and decryption process is proportional to the size of the file to be processed (the smaller the file size to be processed, the faster the encryption and decryption process. Vice versa, the larger the file size, the longer the encryption and decryption process will take) . This application has been tested with the Blackbox method and is fully functional for data or documents of type .doc, .docx, .xls, .xlsx, .ppt, .pptx. System development is needed so that it can not only handle written documents but also image, video and audio documents. The system must be developed with AES192 or AES258, this will make it difficult for irresponsible parties to steal data.Keywords: cryptographic,aes-128, cybercrime, file security, advance encyption standard*

Keywords*: cryptography, aes-128, cybercrime, data security, data security, advanced encryption standard*

1. PENDAHULUAN

Pesatnya perkembangan teknologi memberikan pengaruh besar untuk kehidupan manusia. Salah satu perkembangan yang terasa saat ini yaitu jaringan internet. Manusia dapat dengan cepat bertukar in*form*asi maupun

data dengan orang lain melalui internet [1]. Namun, hal ini membuat pengiriman in*form*asi atau data semakin rentan terhadap penyadapan, yang dapat mengubah integritas data. Untuk beberapa tujuan atau keuntungan, seseorang ingin mengirim pesan yang isinya tidak diketahui oleh siapa pun kecuali penerima yang dituju karena isi pesan tersebut bersifat rahasia atau pribadi.

Pilar Medical Center merupakan perusahaan yang bergerak dibidang kesehatan yang melayani pelayanan medis. Pilar Medical Center didirikan oleh seorang dokter yang bernama Angky Purbo Putrantika. Klinik Pilar Medical Center berlokasi di Pondok Pinang, Kebayoran Lama. Klinik ini memiliki data-data seperti *record* pasien, *invoice,* tagihan lab, dan laporan keuangan yang bersifat rahasia. Saat ini data masih dalam bentuk *file* biasa yang dapat dibaca pihak yang tidak berwenang. Oleh karena itu diperlukan pengamanan *file* menggunakan kriptografi.

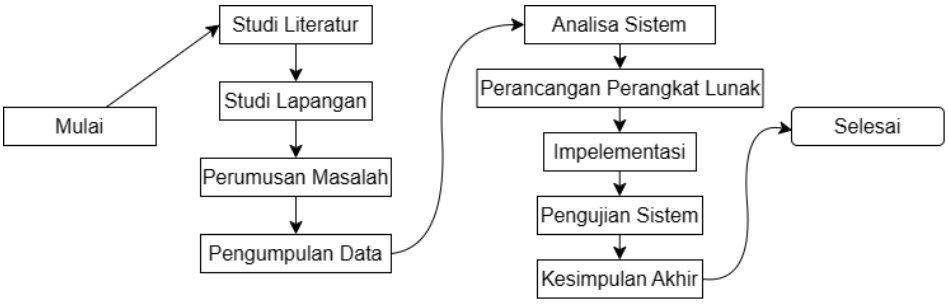
Kriptografi merupakan ilmu untuk merahasiakan *file* dengan menyandikannya ke *form*at yang tidak dapat dibaca. Di kriptografi terdapat dua proses, yang pertama adalah enkripsi. Sedangkan yang kedua adalah dekripsi. Pesan yang belum dienkripsi biasa disebut *plaintext*. Sedangkan pesan yang sudah dienkripsi disebut *chipertext*. Kriptografi juga dibagi menjadi dua jenis kunci. Dua kunci ini adalah kunci simetris dan kunci asimetris. [2]

Algoritme yang digunakan untuk menerapkan pengamanan kriptografi adalah algoritme *advanced encryption* standard atau biasa disebut AES. Algoritme AES adalah blok kode simetris yang menggantikan algoritme *data encryption standard* (DES). Algoritme AES memiliki ukuran blok tetap 128 bit dengan panjang kunci yang berbeda. Kunci AES 128 menggunakan prosedur perulangan yang dikenal sebagai *round*. Ini adalah 10 putaran pola matriks 4x4, setiap pola matriks terdiri dari 1 *byte* atau 8 bit untuk mengenkripsi atau mendekripsi. [3]

2. METODE PENELITIAN

2.1 Metode *Waterfall*

Metode *waterfall* atau metode air terjun adalah salah satu siklus hidup klasik (*Classic life cycle)* dalam pengembangan perangkat lunak. Metode tersebut menggambarkan pendekatan yang sistematis dan berurutan pada pengembangan *software*. Pada Gambar 1 adalah tahapan penelitian. [4]



Gambar 1. Tahapan Penelitian

2.2 Metode *Testing Blackbox*

Blackbox Texting adalah pengujian yang dilakukan untuk mengamati hasil masukan dan keluaran dari perangkat lunak tanpa mempertimbangkan struktur kode dari perangkat lunak. Pengujian ini dilakukan pada akhir pembuatan perangkat lunak untuk menentukan apakah perangkat lunak dapat berfungsi dengan baik. [5]

2.3 Pengumpulan Data

Pada fase ini, pengumpulan data yang diperlukan untuk perancangan sistem. Berikut ini adalah langkah-langkah yang dilakukan: [6]

a. Wawancara dilakukan kepada pihak-pihak terkait. Untuk memperoleh in*form*asi tentang kebutuhan untuk menjalankan sistem pengamanan *file* pada data-data di klinik Pilar Medical Center.
b. Observasi untuk mengumpulkan data dan mengamati tahapan yang terjadi secara langsung di klinik Pilar Medical Center yang akan digunakan sebagai masukan untuk laporan penelitian ini.

2.4 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan keamanan in*form*asi. Bertujuan untuk meningkatkan kepercayaan, integritas data, otentikasi entitas, dan verifikasi keaslian data. Dibutuhkan empat komponen untuk menjalankan kriptografi dengan baik, yaitu: [7]

a. *Plaintext,* merupakan sebuah teks, pesan, data atau in*form*asi yang belum dienkripsi.

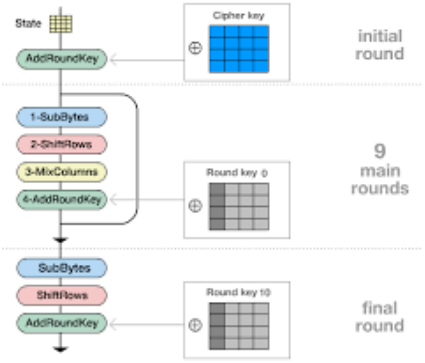
b. *Ciphertext*, merupakan sebuah teks, pesan, data atau in*form*asi yang telah dienkripsi.
c. *Key*, digunakan untuk melakukan enkripsi dan dekripsi pada proses kriptografi.
d. *Encryption decryption algorithm*, merupakan algoritme yang digunakan untuk enkripsi dan dekripsi.

2.5 *Advanced Encryption Standard* (AES)

AES adalah sistem pengkodean blok non-Feistel karena AES memakai komponen yang selalu memiliki panjang blok invers 128 bit. Kunci AES memakai proses yang berulang yang disebut dengan *round*. Proses AES yaitu perubahan terhadap keadaan. Teks sebenarnya dalam blok (128 bit) awalnya diatur sebagai *state*. Enkripsi AES adalah konversi terhadap *state* yang diulangi kedalam beberapa *round*. *State* yang menjadi *output* ronde k menjadi masukan untuk ronde ke-k +1. [8]

2.5.1 Proses Enkripsi AES-128

Pada prosedur awal enkripsi. data di*input* ke dalam *bytes*, dan lalu disalin kedalam *array state* untuk dienkripsi dan dekripsi, hasil *output*nya akan disimpan kedalam *output bytes*. Pada prosedur awal enkripsi, *input* yang telah disalin kedalam *state* akan berubah *AddRoundKey*-nya. lalu *state* akan mengalami *perubahan SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey* secara berulang sebanyak *round* atau putaran. Proses ini dalam algoritme AES disebut *round function*. *Round* yang terakhir, *state* tidak diberikan perubahan *MixColumns*. Pada gambar 2 menjelaskan prosedur awal enkripsi yang memakai algoritme AES-128. [9]



Gambar 2 Proses Enkripsi AES-128

Prosedur enkripsi AES-128 dengan memakai kunci 128 bit adalah sebagai berikut:

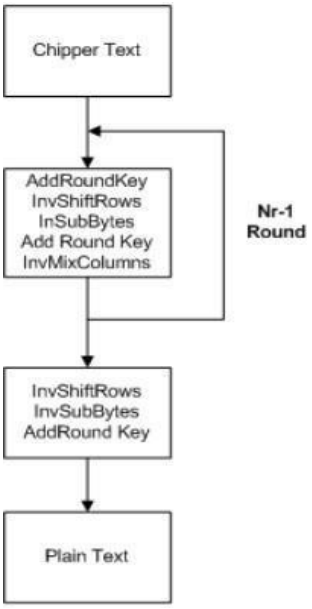
a. *AddRoundKey*: Melakukan *XOR* antara *state* awal (*plaintext*) menggunakan *cipher key*. Pada proses ini disebut juga *initial round.*
b. *Round*: Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   1. *SubBytes:* Substitusi *byte* dengan menggunakan tabel substitusi *(S-box)*
   2. *ShiftRows*: Pergeseran baris-baris *array state* secara *wrapping*
c. *MixColumns*: Mengacak data pada masing-masing kolom *array state* dengan persamaan (1).

$$A(x) = \{03\}x^2 + \{01\}x^2 + \{01\}x^2 + \{02\} \quad (1)$$

d. *AddRoundKey*: Melakukan *XOR* antara *state* sekarang *round key*.
e. *Final Round*: Proses untuk *round* terakhir antara lain *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

2.5.2 Proses Dekripsi AES-128

Konversi *cipher* bisa dilakukan sebaliknya untuk mendapatkan *inverse cipher* yang mudah dimengerti untuk algoritme AES. Konversi *byte* yang mudah dimengerti dari algoritme AES. Dalam proses dekripsi AES, transformasi yang digunakan dalam *inverse cipher* dalam proses dekripsi AES adalah *InvShiftRows, InvSubBytes, InvMixColumns*, dan *AddRoundKey* (Gambar 3). [10]



Gambar 3. Proses Dekripsi AES

a. *InvShiftRows* pada gambar 4 adalah perubahan *byte* yang berbalikan dengan perubahan *ShiftRows*. Pada perubahan *InvShiftRows*, dilakukan pertukaran bit ke kanan sedangkan pada *ShiftRows* dilakukan pertukaran bit ke kiri.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

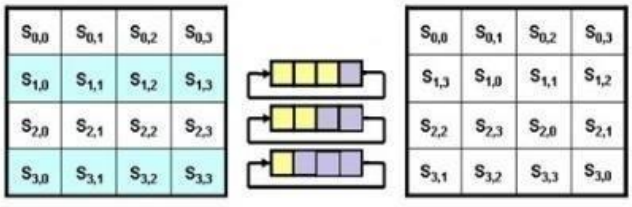
Gambar 4. Proses *InvShiftRows*

b. *InvSubBytes* adakah kebalikan dari trans*form*asi *SubBytes*. Dalam *InvSubBytes* tiap elemen pada *state dipetakan* dengan tabel *Inverse S-Box* seperti gambar 5.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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 5. *Inverse S-Box*

c. *InvMixColumns* pada gambar 6 adalah setiap kolom pada *state* dikalikan dengan *matriks* perkalian didalam AES.

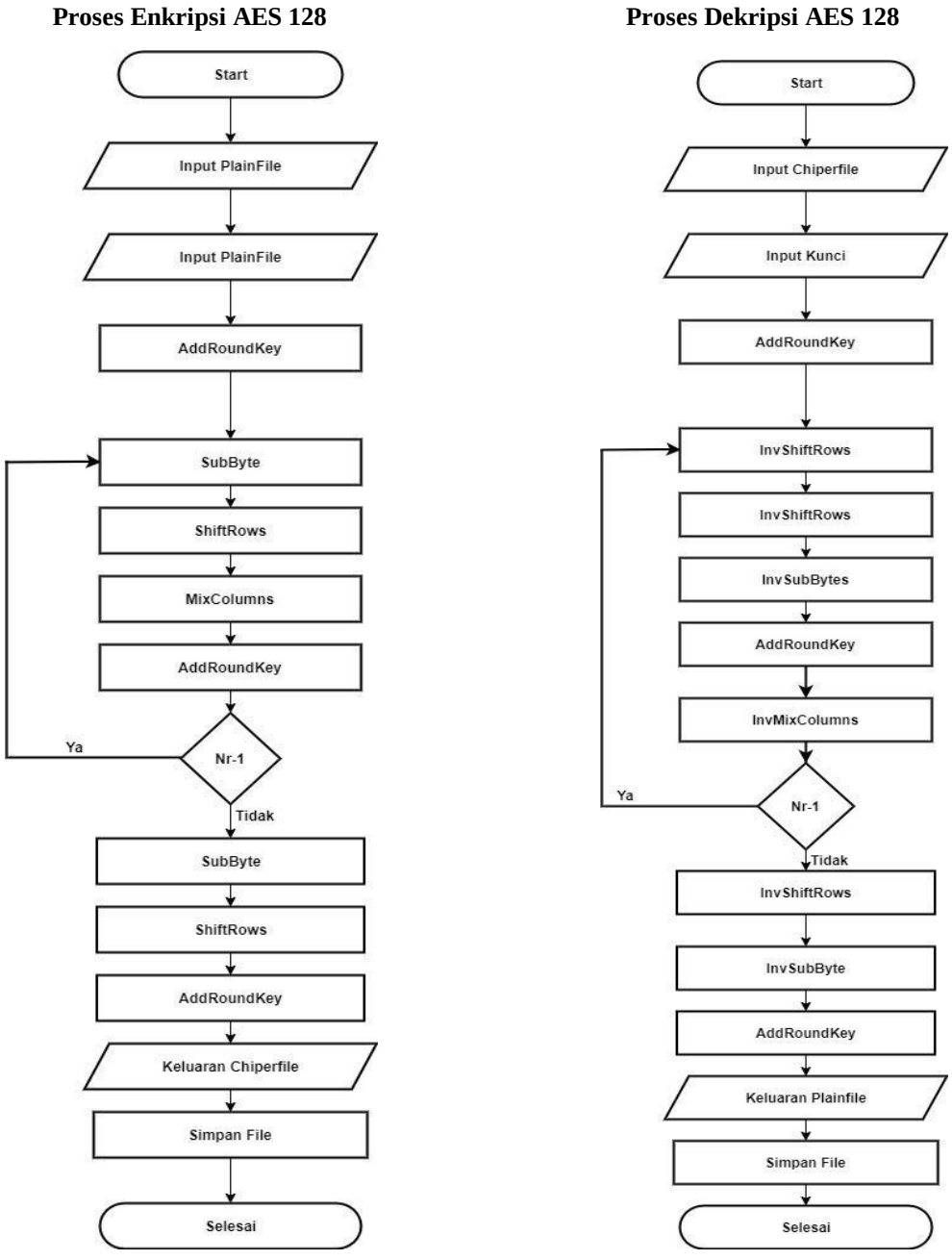


Gambar 6. *InvMixColumn*

3. HASIL DAN PEMBAHASAN

3.1 *Flowchart* Enkripsi dan Dekripsi AES-128

Gambar 7 merupakan *flowchart* yang menjelaskan proses dari enkripsi dan dekripsi dari kriptografi AES 128.

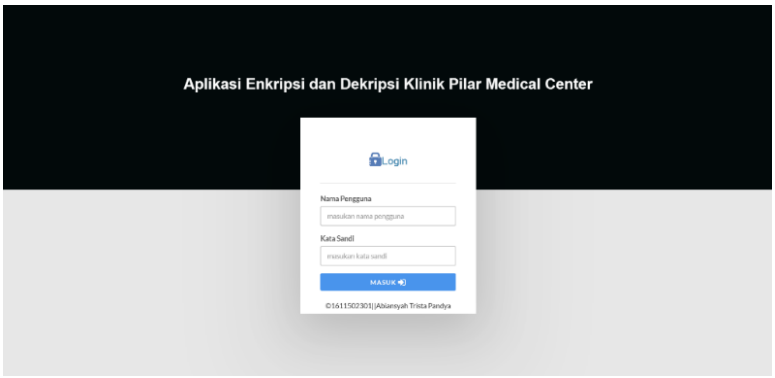


Gambar 7. *Flowchart* Enkripsi AES-128

3.2 Tampilan Layar

3.2.1 Tampilan Layar Halaman *Login*

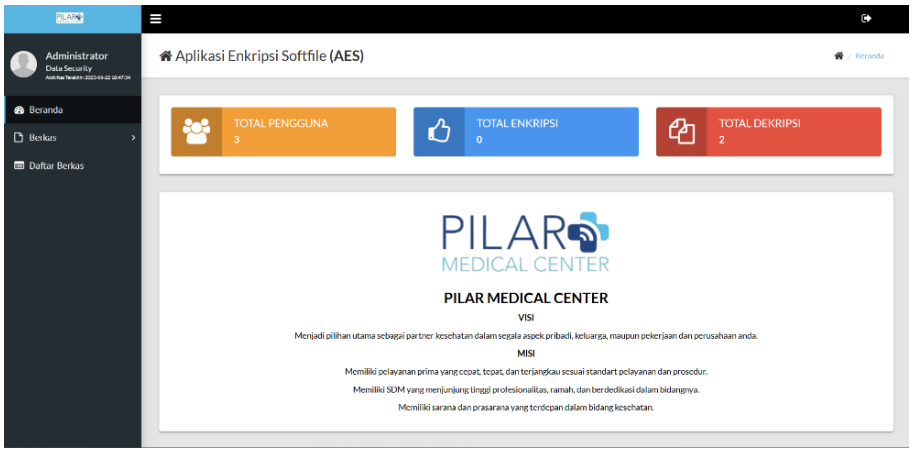
Tampilan layar *login* ditampilkan di gambar 8.



Gambar 8. Tampilan Layar Halaman *Login*

3.2.2 Tampilan Layar Halaman *Dashboard*

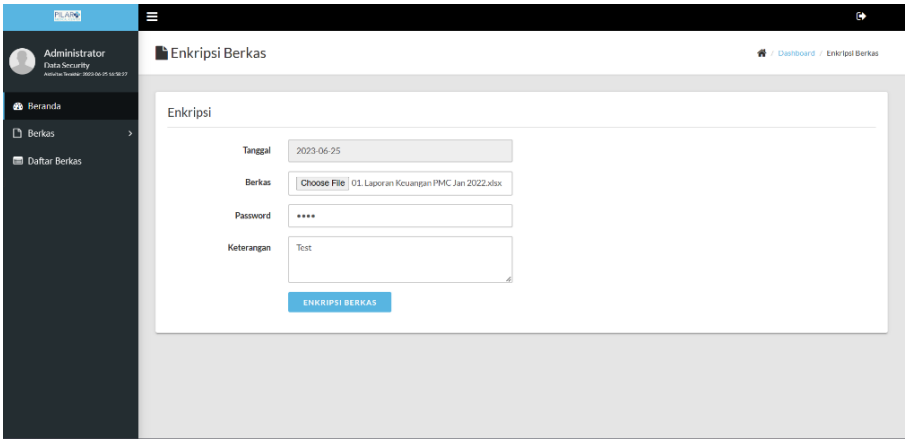
Tampilan Layar halaman *Dashboard* akan ditampilkan di gambar 9.



Gambar 97. Tampilan Layar Halaman *Dashboard*

3.2.3 Tampilan Layar Halaman Enkripsi Berkas

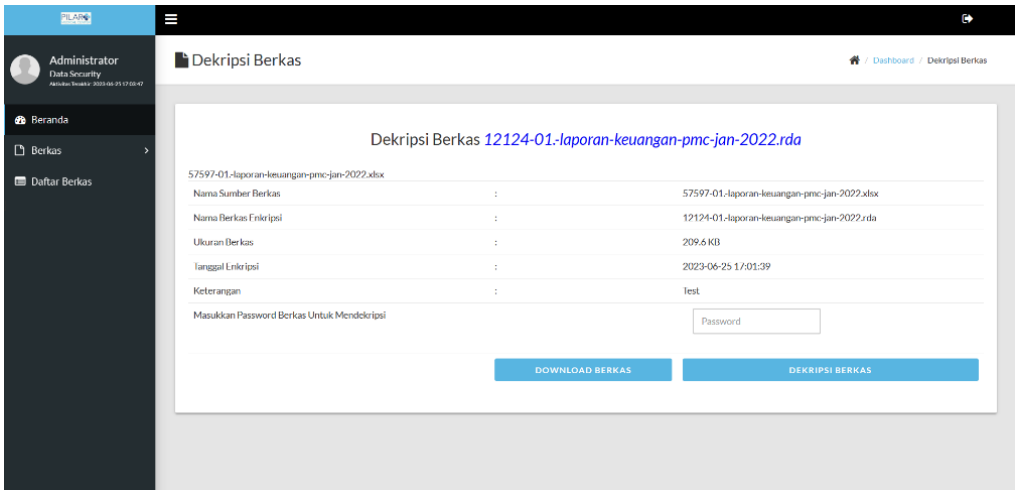
Tampilan layar halaman enkripsi berkas akan ditampilkan di gambar 10.



Gambar 8. Tampilan Layar Halaman Enkripsi Berkas

3.2.4 Tampilan Layar Halaman Dekripsi Berkas

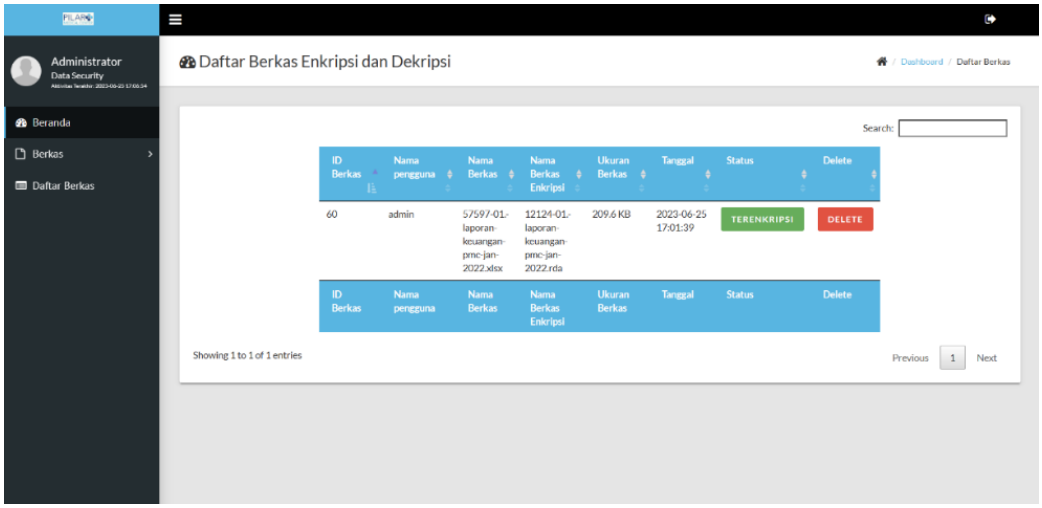
Tampilan layar halaman dekripsi berkas akan ditampilkan di gambar 11.



Gambar 9. Tampilan Layar Halaman Dekripsi Berkas

3.2.5 Tampilan Layar Halaman Daftar Berkas

Tampilan layar menu berkas akan ditampilkan di gambar 12.



Gambar 102. Tampilan Layar Halaman Daftar Berkas

3.3 Pengujian

3.3.1 Pengujian Rancangan Program

Table 1 merupakan hasil rancangan pengujian dari program yang telah dibuat.

Tabel 1. Hasil Pengujian Rancangan *File*

No	Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
1.	*User* mengisi *form login*	Tampil halaman menu *Dashboard*	Sesuai harapan
2.	*User* memilih submenu berkas Enkripsi	Tampil halaman submenu enkripsi	Sesuai harapan
3.	*User* memilih sub Menu berkas dekripsi	Tampil halaman submenu dekripsi	Sesuai harapan
4.	Memasukkan *file* dan menekan tombol untukdienkripsi atau didekripsi	Tampil halaman hasil proses enkripsi atau dekripsi berkas	Sesuai harapan

5.	Men*download file* yang sudah terenkripsi dan terdekripsi	Berhasil men*download* berkas	Sesuai harapan
6.	*User* memilih submenu daftar berkas	Tampil halaman daftar berkas yang sudah terenkripsi dan yang belum terenkripsi atau tampil halaman hapus Berkas	Sesuai harapan
7.	*User* menekan Hapus Berkas	Tampil halaman berkas Terhapus	Sesuai harapan
8.	*User* menekan tombol *logout*	Tampil kembali ke halaman *login*	Sesuai harapan

3.3.2 Pengujian Hasil Enkripsi *File*

Tabel 2 merupakan hasil dari uji *file* asli yang sudah melewati prosedur enkripsi

Tabel 2. Hasil Pengujian Enkripsi *File*

No.	Nama Asli *File*	Ukuran *File* Asli (KB)	Nama *File*Setelah Dienkripsi	Ukuran *File* Setelah Dienkripsi (KB)	Waktu (detik)	Kinerja Enkripsi (KB per detik)
1.	01. Laporan Keuangan PMC Jan 2022.xlsx	210kb	31551-01.-laporan-keuangan-pmc-jan-2022.rda	209.9kb	3,4dtk	61,73 KB/s
2.	02. Laporan Keuangan PMC Feb 2022.xlsx	467kb	58228-02.-laporan-keuangan-pmc-feb-2022.rda	446.739kb	6,2dtk	0,16 KB/s
3.	03. Laporan keuangan PMC Mar 2022.xlsx	339kb	99783-03.-laporan-keuangan-pmc-mar-2022.rda	338.3kb	6,4dtk	51,85 KB/s
4.	2022 MEDIS – KWM 0291.pdf	232kb	11683-2022-medis---kwm-0291.rda	12.9961kb	5,6dtk	2,32 KB/s
5.	2022 MEDIS – KWM 0311.pdf	232kb	66174-2022-medis---kwm-0311.rda	231.89kb	5,9dtk	39,30 KB/s
6.	2022 MEDIS – KWM 0482.pdf	231kb	75873-2022-medis---kwm-0482.rda	230.193kb	5,7dtk	40,38 KB/s
7.	2022 MEDIS – INV 0977.pdf	367kb	80350-2022-medis---inv-0977.rda	381.206kb	10,1dtk	37,74 KB/s
8.	2022 MEDIS – INV 0978.pdf	367kb	74096-2022-medis---inv-0978.rda	366.559kb	8,9dtk	41,18 KB/s
9.	2022 MEDIS – INV 0979.pdf	382kb	21756-2022-medis---inv-0979.rda	381.206kb	9,6dtk	39,70 KB/s
10.	11. Kalgen November 2022.pdf	1.959kb	7217-11.-kalgen-november-2022.rda	1958.53kb	50,1dtk	26,99 KB/s
11.	0112 INV KLINIK PILAR MEDICAL CENTER – 11145.pdf	1.848kb	74779-0122-inv-klinik-pilar-medical-centre---11145.rda	1847.91kb	45,4dtk	40,70 KB/s

3.3.3 Pengujian Hasil Dekripsi *File*

Tabel 3 merupakan hasil uji *file* dekripsi yang sebelumnya sudah dienkripsi terlebih dahulu.

Tabel 3. Hasil Pengujian Dekripsi *File*

No.	Nama *File* Enkripsi	Ukuran Setelah Dienkripsi (Per KB)	Nama *File* Dekripsi	UkuranSetelah Didekripsi (Per KB)	Waktu Per (Detik)	Kinerja Dekripsi (KB Per Detik)

1.	31551-01.-laporan-keuangan-pmc-jan-2022.rda	209.9kb	47415-01.-laporan-keuangan-pmc-jan-2022	209.9kb	3dtk	61,73 KB/s
2.	58228-02.-laporan-keuangan-pmc-feb-2022.rda	446.739kb	2332-02.-laporan-keuangan-pmc-feb-2022	446.739kb	6,2dtk	0,16 KB/s
3.	99783-03.-laporan-keuangan-pmc-mar-2022.rda	338.3kb	89254-03.-laporan-keuangan-pmc-mar-2022	338.3kb	6,4dtk	51,85 KB/s
4.	11683-2022-medis---kwm-0291.rda	12.9961kb	8405-2022-medis---kwm-0291	12.9961kb	5,6dtk	2,32 KB/s
5.	66174-2022-medis---kwm-0311.rda	231.89kb	63911-2022-medis---kwm-0311	231.89kb	5,9dtk	39,30 KB/s
6.	75873-2022-medis---kwm-0482.rda	230.193kb	89006-2022-medis---kwm-0482	230.193kb	5,7dtk	40,38 KB/s
7.	80350-2022-medis---inv-0977.rda	381.206kb	32309-2022-medis---inv-0977	381.206kb	10,1dtk	37,74 KB/s
8.	74096-2022-medis---inv-0978.rda	366.559kb	54987-2022-medis---inv-0978	366.559kb	8,9dtk	41,18 KB/s
9.	21756-2022-medis---inv-0979.rda	381.206kb	37306-2022-medis---inv-0979	381.206kb	9,6dtk	39,70 KB/s
10.	7217-11.-kalgen-november-2022.rda	1958.53kb	1353-11.-kalgen-november-2022	1958.53kb	50,1dtk	26,99 KB/s
11.	74779-0122-inv-klinik-pilar-medical-centre---11145.rda	1847.91kb	17215-0122-inv-klinik-pilar-medical-centre---11145	1847.91kb	45,4dtk	40,70 KB/s

4. KESIMPULAN

Berdasarkan analisis yang sudah dilakukan terhadap permasalahan dari program aplikasi yang sudah dibuat, maka dapat ditarik kesimpulan sebagai berikut:

a. Algoritme kriptografi AES berhasil diimplementasikan menggunakan metodologi *Waterfall* pada aplikasi pengamanan *file* berbasis web pada klinik Pilar Medical Center.
b. Waktu yang dibutuhkan untuk enkripsi dan dekripsi sebanding dengan ukuran *file* yang melewati proses enkripsi dan dekripsi (semakin kecil ukuran *file* yang diproses, semakin cepat proses enkripsi dan dekripsinya, semakin besar ukuran *file*nya, semakin lama proses enkripsi dan dekripsinya).
c. Sistem keamanan *file* ini telah diuji dengan metode *Blackbox* dan berfungsi penuh untuk dokumen yang berekstensi .doc, .docx, .xls, .xlsx., .ppt, .pptx, .pdf.

DAFTAR PUSTAKA

[1] D. Setiawan, "Dampak Perkembangan Teknologi Infomasi dan Komunikasi Terhadap Budaya," *Simbolika*, vol. IV, pp. 62-72, 2018.

[2] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan," *Jurnal Pendidikan Sains dan Komputer,* vol. II, pp. 163-171, 2022.

[3] H. Wijaya, "IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN URL (UNI*FORM* RESOURCE LOCATOR) DARI SQL INJECTION," *Akademika Jurnal,* vol. 17, pp. 8-13, 2020.

[4] Guntoro, "Badoystudio," 15 June 2023. [Online]. Available: https://badoystudio.com/metode-waterfall/.

[5] Y. D. Wijaya and M. W. Astuti, "PENGUJIAN BLACKBOX SISTEM IN*FORM*ASI PENILAIAN KINERJA KARYAWAN PT INKA (PERSERO) BERBASIS EQUIVALENCE PARTITIONS," *Jurnal Digital Teknologi Informasi,* vol. IV, pp. 22-26, 2021.

[6] I. B. Pujaastawa, "TEKNIK WAWANCARA DAN OBSERVASI UNTUK PENGUMPULAN BAHAN IN*FORM*ASI," UNIVERSITAS UDAYANA, Bali, 2016.

[7] F. N. Pabokory, I. F. Astuti and A. H. Kridalaksana, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI *FILE* DOKUMEN, DAN *FILE* DOKUMEN MENGGUNAKAN ALGORITME ADVANCE ENCRYPTION STANDARD," *Jurnal Informatika Mulawarman,* vol. X, pp. 20-31, 2015.

[8] A. Rahmatulloh, Y. Permanasari and E. Harahap, "Kriptografi Advance Encryption Standard (AES) Untuk Penyandian *File* Dokumen," *Jurnal Matematika UNISBA,* vol. XV, pp. 7-14, 2016.

[9] A. Prameshwari and N. P. Sastra, "Implementasi Algoritme Advance Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi *File* Dokumen," *Jurnal Eksplora Informatika,* vol. VIII, pp. 52-58, 2018.

[10] V. Yuniati, G. Indriyanta and A. Rachmat, "ENKRIPSI DAN DEKRIPSI DENGAN ALGORITME AES 256 UNTUK SEMUA JENIS *FILE*," *Jurnal Informatika,* vol. V, pp. 22-31, 2019.