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

IMPLEMENTASI ALGORITMA AES-128 UNTUK KEAMANAN FILE DATA KEPENDUDUKAN BERBASIS WEB PADA DESA BOGARES KIDUL

Fikri Prasetyo[1*], Titin Fatimah[2], Mardi Hardjianto[3], Subandi[4]

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

Email: [1*]1811502564@student.budiluhur.ac.id, [2]titin.fatimah@budiluhur.ac.id, [3]mardi.hardjianto@budiluhur.ac.id, [4]subandi@budiluhur.ac.id
(* : corresponding author)

Abstrak- Desa Bogares Kidul mempunyai banyak file dokumen yang disimpan secara sistematis dan terkomputerisasi. File data kependudukan dan file data lainnya tersebut bersifat internal dimana hanya pihak-pihak tertentu saja yang memiliki kewenangan untuk bisa melihat isi file tersebut. Untuk pihakk-pihak yang tidak memiliki kewewngan untuk melihat isi file tersebut dapat menimbulkan kebocoran data, untuk mempertimbangkan hal itu perlu dilakukan pengamanan data yang lebih lanjut. Pada penelitian ini akan mengimplementasikan konsep pengamanan isi file dengan menggunakan algoritma kriptografi. Kriptografi merupakan salah satu solusi atau metode yang bisa melindungi dokumen yang tepat untuk menjaga kerahasiaan dan keaslian dokumen, serta dapat meningkatkan aspek keamanan dokumen atau informasi. Salah satu metode kriptografi untuk mengamankan informasi adalah Advanced Encryption Standard (AES). Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data berbasis web menggunakan bahasa pemrograman PHP dan MySQL sebagai Database Management System dengan mengimplementasikan kriptografi enkripsi pada isi file data dengan menggunakan algoritma Advanced Encryption Standard (AES). Hasil dari pecobaan dua file yang berbeda saat dienkripsi dan dekripsi dengan ukuran yang beda akan mempengaruhi berapa lama waktu enkripsi dan dekripsi. File yang berukuran 50.8066 bytes waktu enkripsinya adalah 3.6311 milisecond dan file yang berukuran 59.6211 bytes waktu enkripnya adalah 6.6399 milisecond. Dari hasil implementasi dapat disimpulkan bahwa algoritma kriptografi AES dapat diimplementasikan dalam menjaga keamanan isi file.

Kata Kunci: Kriptografi, *Advanced Encryption Standard*, AES-128, Keamanan File, Kependudukan.

IMPLEMENTATION OF AES-128 ALGORITHM FOR WEB-BASED POPULATION DATA FILE SECURITY IN BOGARES KIDUL VILLAGE

Abstract- *Desa Bogares Kidul has many document files that are stored systematically and computerized. Population data files and other data files are internal in nature where only certain parties have the authority to be able to view the contents of the file. For parties who do not have the authority to view the contents of the file, it can cause data leakage, to consider this, it is necessary to carry out further data security. In this study, the concept of securing file contents will be implemented using cryptographic algorithms. Cryptography is a solution or method that can protect the right documents to maintain the confidentiality and authenticity of documents, and can improve document or information security aspects. One of the cryptographic methods for securing information is the Advanced Encryption Standard (AES). This study aims to create a web-based data security system using the programming language PHP and MySQL as a Database Management System by implementing cryptographic encryption on the contents of data files using the Advanced Encryption Standard (AES) algorithm. The results of testing two different files when encrypted and decrypted with different sizes will affect how long the encryption and decryption will take. File size 50.8066 bytes encryption time is 3.6311 milisecond and file size 59.6211 bytes encryption time is 6.6399 milisecond. From the implementation results it can be concluded that the AES cryptographic algorithm can be implemented in maintaining the security of file contents..*

Keywords*: Cryptography, Advanced Encryption Standard, AES-128, File Security, Population.*

1. PENDAHULUAN

Teknologi informasi selalu terkait erat dengan semua aspek kehidupan manusia karena komputer dapat memproses dan menyimpan informasi dengan kecepatan yang lebih cepat daripada yang dapat dilakukan oleh pikiran manusia. Komputer dan telekomunikasi telah maju dengan sangat cepat sehingga pengguna dapat menyimpan data secara digital[1]. Bagaimana orang menggunakan teknologi, media, dan komunikasi, serta bagaimana dunia berubah dari waktu ke waktu, dapat berdampak pada kehidupan manusia. Kehidupan manusia dapat dipengaruhi oleh bagaimana orang menggunakan teknologi, media, dan komunikasi, serta bagaimana dunia berkembang dari waktu ke waktu.

Karena itu, penipuan menyebar melalui berbagai saluran komunikasi. Organisasi atau pihak yang tidak bertanggung jawab biasanya terlibat dalam perilaku ini untuk mendapatkan keuntungan dari orang biasa yang tidak

mengetahui ketentuan hukum yang relevan. Di Desa Bogares Kidul Komputer yang digunakan dapat diakses oleh siapa saja, sehingga jika ada orang yang tidak bertanggung jawab mengakses informasi sensitif dan berharga ini, sangat berisiko. Kemungkinan lain adalah unsur-unsur yang dikandungnya dapat berubah sehingga menyebabkan perubahan pada data kependudukan. Ini juga dapat disalahgunakan untuk tujuan yang merugikan pemilik data, yang bisa mengakibatkan hilangnya data secara signifikan. Algoritma kriptografi AES digunakan untuk proses enkripsi dan deskripsi data untuk menangani pencurian, penyalahgunaan, dan kerusakan data. Komponen penting yang saling berhubungan dari sistem keamanan adalah kriptografi.

Enkripsi dan dekripsi adalah dua konsep dasar dalam kriptografi. Enkripsi adalah proses mengenkripsi data agar sulit dipahami atau tidak mungkin dibaca (*Chipertext*). Data yang telah dienkripsi dapat dikembalikan melalui proses dekripsi, yaitu mengembalikan data ke keadaan semula (*Plaintext*) [3]. *National Institute of Standards and Technology* (NIST) menerbitkan algoritma AES pada tahun 2001 sebagai pengganti algoritma DES, yang dianggap ketinggalan zaman dan mudah dibobol. Akibatnya, algoritma AES digunakan sebagai standar untuk melindungi data menggantikan algoritma DES. Cipher blok dengan panjang kunci 128 bit, 192 bit, dan 256 bit adalah algoritma AES. Blok data, juga dikenal sebagai teks biasa, adalah urutan 128 bit yang digunakan algoritme AES untuk mengenkripsi menjadi teks sandi. Jumlah putaran algoritma AES nantinya akan dipengaruhi oleh perbedaan panjang kunci. [6]

Penelitian sebelumnya yang berjudul "Implementasi Pengamanan Data Arsitektur Menggunakan Metode kriptografi Dengan Algoritma Rivest Code 4 (RC4) Pada PT. Naviri Indah. dimana penelitian sebelumnya menggunakan metode RC 4 untuk mengamankan data arsitektur pada PT.Naviri Indah Cemerlang. Pada penelitian saat ini yang berjudul "Implementasi Algoritma AES-128 Untuk Keamanan File data Kependudukan Berbasis Web Di Desa Bogares Kidul" pada penelitian saat ini menggunakan metode algoritma Aes-128 yang dapat mengamankan data kependudukan dan file kependudukan pada Desa Bogares Kidul.

2. METODOLOGI PENELITIAN

2.1 Pengumpulan Data

Metode pengumpulan data yang dilakukan adalah dengan menggunakan tiga metode umum antara lain pengumpulan data dengan observasi, studi literatur dan wawancara [2].

a. Observasi. Observasi langsung merupakan metode untuk mengumpulkan data. Seorang peneliti harus melaksanakan pengamatan ditempat terhadap objek penelitian yang akan diamati dengan menggunakan panca indera sebelum mencatat pengamatan tersebut dalam catatan atau alat perekam lainnya.
b. Studi Literatur. Untuk dapat menerapkan teknik pengumpulan data studi literatur dilakukan pengumpulan jurnal,buku dan paper yang memiliki relevansi dan sesuai dengan yang diperlukan untuk mendukung penelitian. Informasi yang didapatkan berupa data-data referensi, melalui jurnal, buku, ataupun internet.
c. Wawancara. Proses ini dilakukan melalui wawancara atau sesi tanya jawab langsung dengan para pemangku kepentingan yang terlibat dalam pengembangan aplikasi dan program untuk mendapatkan informasi tentang aplikasi dan keamanan yang ada.

2.2 *Advanced Ecryption Standard* (AES)

National Institute of Standards and Technology (NIST) menerbitkan algoritma AES pada tahun 2001 sebagai pengganti algoritma DES, yang dianggap ketinggalan zaman dan mudah dibobol. Akibatnya, algoritma AES digunakan sebagai standar untuk melindungi data menggantikan algoritma DES. Cipher blok dengan panjang kunci 128 bit, 192 bit, dan 256 bit adalah algoritma AES. Blok data, juga dikenal sebagai teks biasa, adalah urutan 128 bit yang digunakan algoritme AES untuk mengenkripsi menjadi teks sandi. Jumlah putaran algoritma AES nantinya akan dipengaruhi oleh perbedaan panjang kunci. [6]

a. Algoritma Enkripsi Aes-128
   Algoritme Enkripsi AES-128 Ringkasan algoritme Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (selain proses pembuatan *addround key*):

1. *AddRoundKey* Melakukan XOR antara state awal (*plaintext*) dengan chipterkey, tahapan ini disebut juga initial round.
2. Putaran sebanyak Nr – 1X. Proses yang dilakukan pada setiap putaran adalah.
   a) SubBytes subtitusi byte dengan menggunakan tabel subtitusi (S-box).
   b) ShiftRows pergeseran baris-baris array state secara wrapping.
   c) MixColumns mengacak data di masing-masing kolom array state.
   d) AddRoundKey melakukan XOR antara state sekarang dengan round key.

b. *Final Round* atau proses untuk putaran terakhir : SubBytes, ShiftRows, AddRoundKey
c. Algoritma Dekripsi AES-128

Proses dekripsi adalah kebalikan dari proses enkripsi, dengan beberapa tahap pemrosesan dan komputasi yang sama. Berikut langkah-langkahnya

1. AddRoundKey : melakukan XOR antara state awal (ciphertext) dengan cipher key. Tahap ini disebut juga initial round.
2. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah.
   a) Inverse InverseShiftRows : pergeseran baris-baris array state secara wrapping kebalikan dari ShiftRows.
   b) InverseSubBytes : subtitusi byte dengan menggunakan tabel invers subtitusi (invers S-box).
   c) AddRoundKey : melakukan XOR antara state sekarang dengan round key.
   d) InverseMixColumns : membalikkan operasi MixColumns.
3. Final round : proses untuk putaran terakhir
   a) InverseShiftRows
   b) InverseSubBytes
   c) AddRoundKeY

2.3 Perancangan Sistem

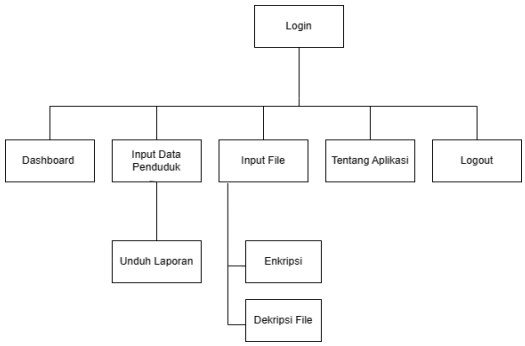
Langkah ini dilakukan untuk mendesain berdasarkan hasil analisis sistem, khususnya perancangan untuk enkripsi dan dekripsi. Selain itu dukungan dan tambahan dibangun ke dalam aplikasi desain antarmuka. Pengembangan sistem dengan metode *Waterfall*. Model harus diselesaikan secara berurutan sebelum melanjutkan ke tahap selanjutnya dan hasil dari setiap tahapan harus didokumentasikan dengan baik

2.4 Rancangan Pengujian

pada proses pengujian ini dilakukan dengan tujuan untuk memverifikasi apakah aplikasi yang dibuat sudah sesuai dengan hasil analisis maupun desain. Apakah aplikasi sudah seperti yang diharapkan. Untuk mengetahui apakah suatu sistem berperilaku seperti yang diharapkan, diperlukan suatu metode pengujian yang merupakan ukuran atau parameter untuk pengujian sistem. Metode pengujian yang digunakan adalah *blackbox*. Ini merupakan teknik yang digunakan untuk menguji aplikasi untuk menemukan bug dan menjalankan eksperimen pada aplikasi fungsional saat *runtime* untuk melihat apakah aplikasi menerima input dan menghasilkan *output* yang diharapkan.[7]

2.5 Rancangan Menu

Pada gambar menunjukan rancangan menu pada aplikasi yang akan dibuat terdiri dari beberapa tampilan yaitu dashboard, input data penduduk, input file, tentang dan bantuan. Di menu input file terdapat pilihan untuk enskripsi file dan dekripsi file.



Gambar 1 Rancangan menu

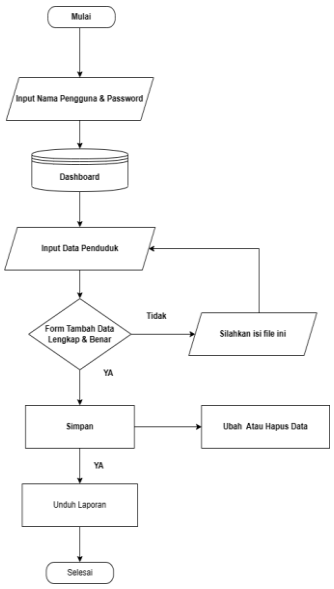
3. HASIL DAN PEMBAHASAN

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*

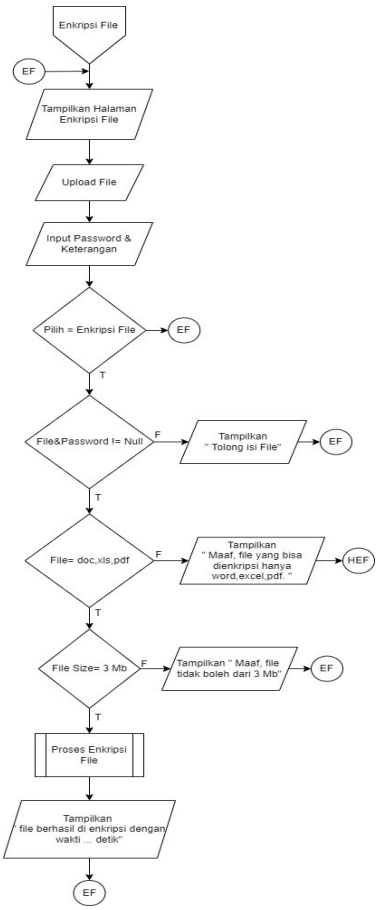
Flowchart merupakan rangkaian dari kejadian yang menjelaskan urutan dari suatu proses kegiatan untuk mencapai tujuan yang diharapkan [8]. Di bawah ini adalah *flowchart* yang digunakan untuk menelusuri proses program pada aplikasi pengamanan file.

a. *Flowchart* Input Data Penduduk
Flowchart ini menjelaskan proses yang terjadi pada tahapan inputan data penduduk.



Gambar 2 *Flowchart* Input Data Penduduk

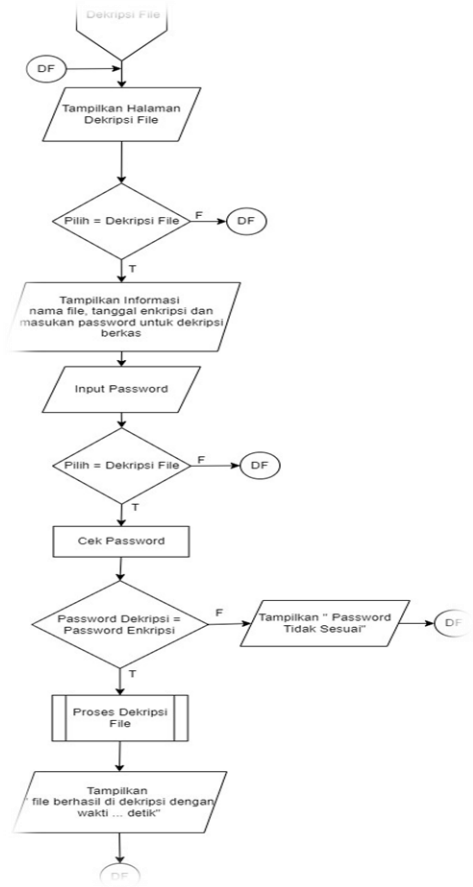
b. *Flowchart* Enkripsi File
Flowchart ini menjelaskan tentang enkripsi file. Saat mengenkripsi file, admin dan anggota harus memasukan kata sandi, setelah itu program akan melanjutkan ke proses enkripsi. Pada Gambar 3 Menunjukkan *Flowchart* Enkripsi.



Gambar 3. *Flowchart* Enkripsi

c. *Flowchart* Dekripsi *File*

Flowchart ini menjelaskan tentang dekripsi file. Saat mendekripsi file, admin dan anggota harus memasukan kata sandi, setelah itu program akan melanjutkan ke proses selanjutnya yaitu proses dekripsi. Berikut adalah Gambar 4 Menunjukkan Flowchart Dekripsi



Gambar 4. *Flowchart* Dekripsi File

3.2 Algoritma

Bagian ini menampilkan dan menjelaskan algoritma dari *flowchart* sebelumnya. Hanya *source code* yang ditampilkan di bagian ini untuk membuat algoritme lebih mudah dibaca dan dimengerti.

a. Algoritma penduduk. Algoritma ini menjabarkan proses mengisi data pada form data penduduk. Proses dimana data data penduduk ditambahkan.

1	Tampilkan Halaman Beranda
2	*Input* Pilih
3	*If* pilih = *data penduduk*
4	Tampilkan *Form input data penduduk*
5	*Input* data penduduk
6	*If* pilih = simpan
7	*If* file = batal
8	Tampilkan pesan berhasil menambahkan data
9	End if
10	Else if pilih = ubah /*delete*
11	Unduh Laporan
12	End if

b. Algoritma Enkripsi File

```
1   Tampilkan Halaman Beranda
2   Input Pilih
3   If pilih = Enkrip File
4      Tampilkan Form enkripsi
5   Input File
6   Input Password
7   Input Deskripsi/Keterangan
8   if pilih = enkripsi file
9           if File & Password!=null
10             If file = doc,xls,pdf
11                If File Size <= 3mb
12                Proses Enkripsi
13                Tampilkan Pesan “file berhasil”
14  else
15             Tampilkan “Maaf file tidak boleh lebih dari 3MB”
16             End if
17        Else
18             Tampilkan “maaf file yang bisa dienkripsi hanya Word.excel,pdf”
20         End if
21  Else
22       Tampilkan Pesan “Tolong isi File”
23  End if
24  Else If pilih = Beranda
25  Tampilkan Menu Halaman Utama
26  End
```

c. Algoritma Dekripsi *File*

Algoritma ini menjelaskan proses form dekripsi. Proses dimana file di yang telah dienkripsi, dikembalikan seperti semula atau didekripsi.

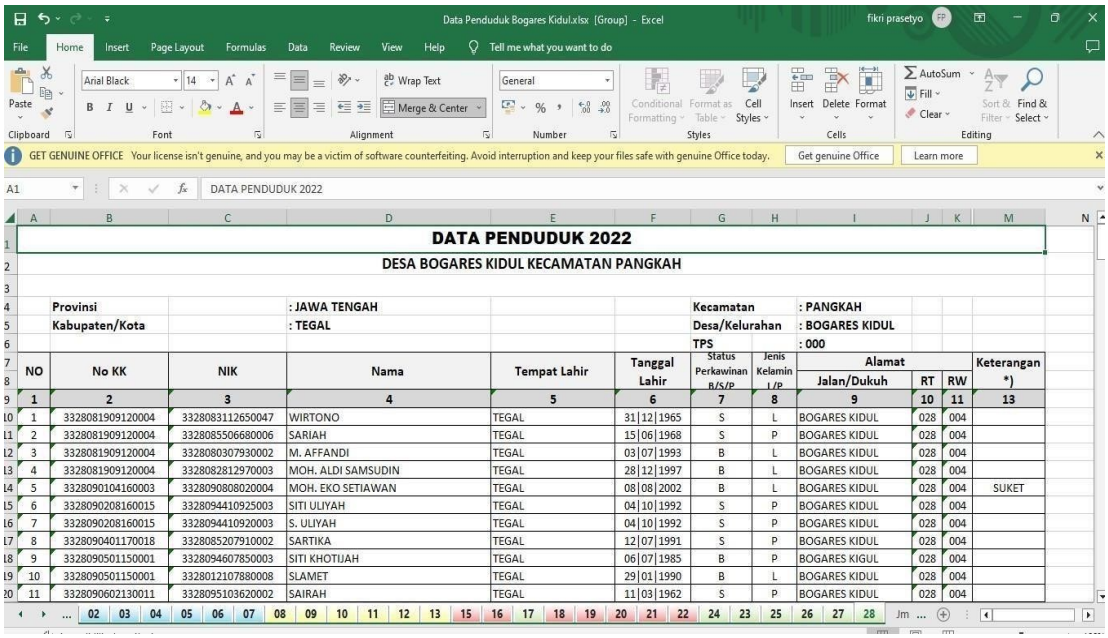
```
1   Tampilkan Halaman Beranda
2   Input Pilih
3   If pilih = Dekripsi
4      Tampilkan Halaman Form Dekripsi
5   If pilih = Dekripsi File
6         Tampilkan Informasi yang akan di dekripsi
7   Input file
8   If pilih = Dekripsi File
9      Periksa Password
10           If password dekripsi = password enkripsi
11     Proses Enkripsi File
12           Tampilkan File Berhasil didekripsi
13      Else Tampilkan Password
14  Salah Else If pilih = Beranda
15       Menampilkan Halaman Beranda
16  End if
17  End if
18  End if
19  End if
```

3.3 Analisis Hasil

Tahapan ini merupakan hasil dari pengujian file asli dengan file terenkripsi menggunakan aplikasi dengan kebutuhan yang telah terpenuhi.

a. Tampilan File Asli

Gambar 5 Menunjukkan tampilan file sebelum di enkripsi. dimana isi file masih bisa dibaca dan normal.



DATA PENDUDUK 2022

DESA BOGARES KIDUL KECAMATAN PANGKAH

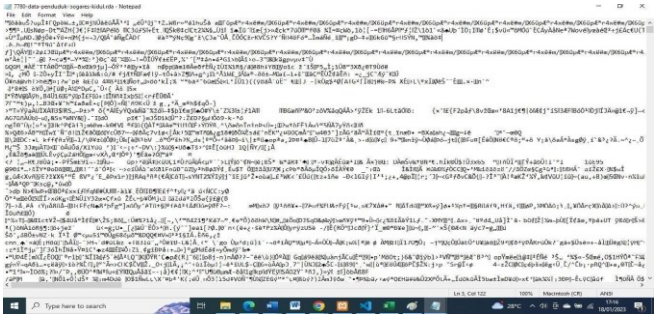
Provinsi	: JAWA TENGAH				Kecamatan	: PANGKAH					
Kabupaten/Kota	: TEGAL				Desa/Kelurahan	: BOGARES KIDUL					
					TPS	: 000					

NO	No KK	NIK	Nama	Tempat Lahir	Tanggal Lahir	Status Perkawinan B/S/P	Jenis Kelamin L/P	Alamat			Keterangan *)
								Jalan/Dukuh	RT	RW	
1	2	3	4	5	6	7	8	9	10	11	13
1	3328081909120004	3328083112650047	WIRTONO	TEGAL	31|12|1965	S	L	BOGARES KIDUL	028	004	
2	3328081909120004	3328085506680006	SARIAH	TEGAL	15|06|1968	S	P	BOGARES KIDUL	028	004	
3	3328081909120004	3328080307930002	M. AFFANDI	TEGAL	03|07|1993	B	L	BOGARES KIDUL	028	004	
4	3328081909120004	3328082812970003	MOH. ALDI SAMSUDIN	TEGAL	28|12|1997	B	L	BOGARES KIDUL	028	004	
5	3328090104160003	3328090808020004	MOH. EKO SETIAWAN	TEGAL	08|08|2002	B	L	BOGARES KIDUL	028	004	SUKET
6	3328090208160015	3328094410925003	SITI ULIYAH	TEGAL	04|10|1992	S	P	BOGARES KIDUL	028	004	
7	3328090208160015	3328094410920003	S. ULIYAH	TEGAL	04|10|1992	S	P	BOGARES KIDUL	028	004	
8	3328090401170018	3328085207910002	SARTIKA	TEGAL	12|07|1991	S	P	BOGARES KIDUL	028	004	
9	3328090501150001	3328094607850003	SITI KHOTIJAH	TEGAL	06|07|1985	B	P	BOGARES KIGUL	028	004	
10	3328090501150001	3328012107880008	SLAMET	TEGAL	29|01|1990	B	L	BOGARES KIDUL	028	004	
11	3328090602130011	3328095103620002	SAIRAH	TEGAL	11|03|1962	S	P	BOGARES KIDUL	028	004	

Gambar 5. Tampilan *File* Asli

b. Tampilan File setelah dienkripsi

Gambar 6 Menunjukkan tampilan file setelah di enkripsi. dimana isi file tidak bisa dibaca dengan normal.



Gambar 6 Tampilan File Setelah di Enkripsi

3.4 Pengujian

Pengujian ini menunjukkan proses enkripsi untuk Tabel *item* data. Pengujian meliputi *file* asli sebelum enkripsi *filename*, berdasarkan waktu enkripsi (*microtime*). Berikut Tabel 1 adalah hasil proses enkripsi:

a) Tabel Pengujian Proses Enkripsi

Tabel 1. Pengujian File Enkripsi

No	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setelah Di Enkripsi	Keterangan dan Durasi
1	Data PendudukBogares Kidul.xlsx	572 KB	7780-data-penduduk-bogares-kidul.rda	572 kb	Berhasil 3.499985
2	1811502564_tugaspaper_komputasi- awan.pdf	50.2832 KB	1811502564_tugaspaper_komputasi-awan.rda	50.2832 KB	Berhasil 2.5038719
3	1811502564_fikriprasetyo_tugas-paper-komputasi- awan.docx	29.916 KB	1811502564_fikripraspetyo_tugas-paper-komputasi- awan.rda	29.916 KB	Berhasil 3.550053

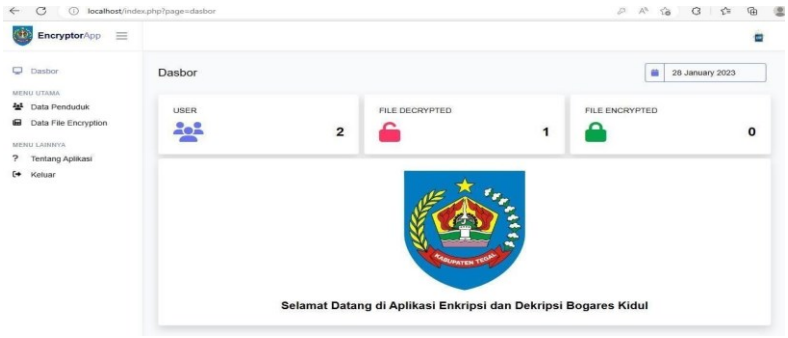
b) Tabel Pengujian Hasil Dekripsi

Tabel 2. Hasil Pengujian File Dekripsi

No	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil dekripsi	Ukuran File Dekripsi	Keterangan dan Durasi
1	7780-data- penduduk-bogares-kidul.rda	572 KB	7780-data-penduduk-bogares- kidul.rda	572 kb	Berhasil 3.499985
2	1811502564_tugaspaper_komputasi-awan.rda	50.2832 KB	1811502564_tug aspaperkomputasi_awan.pdf	50.3 KB	Berhasil 1.2456910610
3	1811502564_fikr iprasetyo_tugas-paper- komputasi- awan.rda	29.916 KB	1811502564_fikr ipraset yo_tugas-paper- komputasi-awan.docx	30 KB	Berhasil 0.7253501415

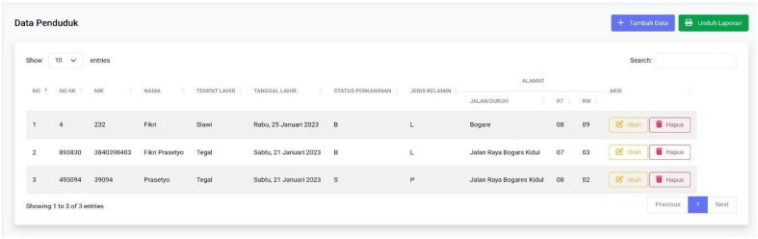
3.5 Tampilan Layar

a) Tampilan *Dashboard*
Terdapat menu data penduduk untuk melakukan input data penduduk dan menu untuk *input* file.



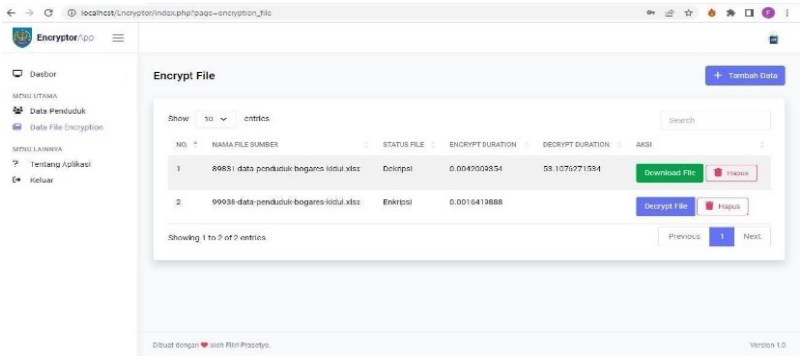
Gambar 7. Tampilan File Layar Dasboard

b) Tampilan Input Data Penduduk
Melakukan proses input data, pilih menu data penduduk, lalu klik tombol Tambah data. Terdapat pada Gambar 7.



Gambar 8. Tampilan Layar Input Data Penduduk

c) Tampilan layar enkripsi fle



Gambar 9. Tampilan Layar Input *File* Enkripsi

4. Kesimpulan

Dengan dibuatnya aplikasi untuk pengamanan data kependudukan menggunakan metode AES-128, maka dapat kesimpulan yaitu aplikasi dapat mengenkripsi file dengan format docx,xlxs,txt dan pdf, algoritma AES-128 dapat diterapkan pada aplikasi keamanan data kependudukan di Desa BogaresKidul, File yang berukuran kecil akan lebih cepat durasi waktu enkripsi dan dekripsinya, Aplikasi dapat mengamankan file data kependudukan. Pada penelitian selanjutnya sebaiknya aplikasi dapat mengenkripsi dalam bentuk gambar, suara dan video, sebaiknya menerapkan 2 metode dalam 1 aplikasi, untuk perkembangan selanjutnya di harapkan setelah data di-*input* laporan bisa di-*download* bukan hanya dalam bentuk PDF dan Excel.

DAFTAR PUSTAKA

[1] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 54–60, 2020.

[2] K. T. Rukmana and P. F. Ariyani, "Penerapan Algoritma Aes-128 Untuk Pengamanan File Pada Smk Pgri 31 Legok Application of Aes-128 Algoritma for File Security At Smk Pgri 31 Legok," *Senafti*, no. September, pp. 327–336, 2022.

[3] M. A. Sutejo and M. Hardjianto, "Pengamanan File Pendaftaran Siswa Baru Menggunakan Metode Algoritme Rc4 Di Tk Nurul Irfan Security of New Student Registration Files Using the Rc4 Algorithm Method in Tk Nurul Irfan," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, vol. 4, no. September, pp. 394–401, 2022.

[4] U. Ungkawa, D. Rosmala, and H. Fauzi, "Penerapan Advance Encryption Standart dalam Pengamanan Elektronik Voting," *J. Inf. Technol.*, vol. 3, no. 1, pp. 17–23, 2021, doi: 10.47292/joint.v3i1.51.

[5] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[6] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

[7] R. Riski, D. Andika, and S. Mulyati, "Penerapan Algoritma Aes-128 Untuk Aplikasi Pengarsipan Dokumen Berbasis Web Pada Pt Studio Inovasi Teknologi Application of Aes-128 Algorithm for Web-Based Document Archiving Application At Pt Studio Inovasi Teknologi," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 411–420, 2022.

[8] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 02, no. 01, pp. 31–42, 2020, doi: 10.54367/kakifikom.v2i1.666.

[9] D. Romadhan and F. Ferdiansyah, "Implementasi Keamanan Database Menggunakan Kriptografi Rc4 Pada Sistem Milik Pt. Torop Sumber Makmur," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 368–376, 2022.

[10] Sri Handriana Dewi Hastuti, "Pentingnya Pemanfaatan Data Kependudukan Di Era Digital," *Tek. Teknol. Inf. dan Multimed.*, vol. 1, no. 1, pp. 18–21, 2020, doi: 10.46764/teknimedia.v1i1.9.