E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi

[1]Saripa

[1 2]Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar, Jl. A.P. Pettarani Kota Makassar, Sulawesi Selatan

Email: saripa2612@gmail.com[1]

Received : 19 Januari 2024
Accepted : 25 Februari 2024
Published : 12 Maret 2024

ABSTRAK

Pada zaman digital yang semakin berkembang ini, keamanan data menjadi semakin penting karena semakin banyak informasi yang disimpan dalam file digital yang rentan terhadap serangan dan akses yang tidak sah. Untuk melindungi privasi dan kerahasiaan informasi pribadi, diperlukan sistem keamanan file yang efektif dan terpercaya. Salah satu cara yang efektif adalah dengan menggunakan algoritma kriptografi seperti *Advanced Encryption Standard* (AES) yang telah digunakan secara luas dalam berbagai aplikasi yang membutuhkan tingkat keamanan yang tinggi. Implementasi sistem keamanan file menggunakan algoritma AES dapat menjadi solusi yang efektif dan terpercaya untuk mengamankan dokumen file pribadi dari serangan dan akses yang tidak sah serta menjaga privasi dan kerahasiaan informasi pribadi. Penelitian ini menggunakan metode Studi Literatur, Perancangan & Analisa, Implementasi, dan Pengujian untuk menganalisis dan mengimplementasikan algoritma AES dengan menggunakan bahasa pemrograman PHP dan database MySQL. Hasil penelitian menunjukkan bahwa algoritma AES dapat menjamin keamanan enam jenis file yang diuji, yaitu gambar, dokumen Word, PDF, Excel, dan PowerPoint. Algoritma AES dapat menjadi pilihan yang efektif untuk mengamankan data dokumen dan gambar secara aman dan andal.

Kata Kunci: Keamanan data, Algoritma AES, Implementasi, Keamanan File.

ABSTRACT

In this growing digital age, data security is becoming increasingly important as more and more information is stored in digital files which are vulnerable to attacks and unauthorized access. To protect the privacy and confidentiality of personal information, an effective and reliable file security system is required. One effective way is to use cryptographic algorithms such as Advanced Encryption Standard (AES) which have been widely used in various applications that require a high level of security. Implementation of a file security system using the AES algorithm can be an effective and reliable solution for securing personal document files from attacks and unauthorized access and maintaining the privacy and confidentiality of personal information. This study uses the method of Literature Study, Design & Analysis, Implementation, and Testing to analyze and implement the AES algorithm using the PHP programming language and MySQL database. The results showed that the AES algorithm can guarantee the security of the six types of files tested, namely images, Word documents, PDF, Excel and PowerPoint. The AES algorithm can be an effective choice for securing document and image data safely and reliably.

Keywords: Data security, AES Algorithm, Implementation, File Security.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

1. PENDAHULUAN

Pada era digital yang semakin maju saat ini, penggunaan teknologi informasi telah membawa kemudahan bagi pengguna dalam menyimpan dan mengakses berbagai jenis informasi, termasuk dokumen file pribadi (Handoyo & Subakti, 2020) . Namun, dengan meningkatnya jumlah informasi yang disimpan dalam format digital, tantangan keamanan data juga semakin kompleks. Keberadaan serangan dan akses yang tidak sah menjadi ancaman serius terhadap kerahasiaan dan privasi informasi pribadi yang disimpan dalam dokumen file tersebut. Oleh karena itu, mengamankan dokumen file pribadi telah menjadi suatu keharusan yang tak terelakkan untuk melindungi integritas dan kerahasiaan informasi yang sangat bernilai.

Dalam era ini, serangan siber semakin canggih dan beragam, termasuk upaya peretasan, pencurian identitas, dan penyebaran malware (Vimy dkk., 2022). Hal ini mengakibatkan risiko kehilangan data sensitif, penyalahgunaan informasi pribadi, dan bahkan ancaman terhadap stabilitas dan keberlanjutan organisasi atau individu. Oleh karena itu, penting untuk memastikan bahwa dokumen file pribadi dilindungi dengan cara yang efektif dan andal. Salah satu solusi yang efektif dalam mengamankan dokumen file pribadi adalah melalui penggunaan algoritma kriptografi, seperti Advanced Encryption Standard (AES) (Pabokory dkk 2016). Algoritma AES telah menjadi standar industri dalam menjaga keamanan data dan telah terbukti kehandalannya dalam berbagai aplikasi kritis, termasuk sistem keamanan militer dan pemerintah.

Algoritma AES (Advanced Encryption Standard) adalah sebuah algoritma kriptografi yang digunakan untuk mengamankan data dengan cara mengenkripsi dan mendekripsi informasi yang disimpan dalam dokumen file .AES didasarkan pada sistem substitusi dan permutasi yang kompleks, yang melibatkan operasi matematika yang rumit. Algoritma ini dirancang untuk memberikan tingkat keamanan yang tinggi dan memiliki tingkat kekuatan kriptografi yang dapat melindungi data dari serangan dan akses yang tidak sah. Pengertian dasar dari algoritma AES adalah melakukan transformasi terhadap blok data dengan menggunakan kunci enkripsi yang sama (Nurnaningsih & Permana, 2018). Proses enkripsi AES melibatkan beberapa tahapan, termasuk substitusi byte, shift row, mix column, dan add round key. Substitusi byte melibatkan penggantian setiap byte data dengan byte lain dari tabel substitusi yang telah ditentukan. Shift row melibatkan pergeseran baris data dalam blok. Mix column melibatkan operasi linier terhadap kolom data dalam blok. Terakhir, add round key melibatkan operasi bitwise XOR antara blok data dengan kunci enkripsi yang sesuai.

Sedangakan pada proses dekripsi AES melibatkan tahapan-tahapan yang merupakan kebalikan dari tahapan enkripsi. Dengan menggunakan kunci dekripsi yang sama, blok data terenkripsi dapat dikembalikan ke bentuk aslinya. AES menggunakan kunci dengan ukuran yang bervariasi, termasuk 128-bit, 192-bit, dan 256-bit, dan jumlah putaran enkripsi yang berbeda tergantung pada ukuran kunci yang digunakan (Ardian & Pramusinto, 2022). Oleh karena itu dengan menggunakan algortma AES dokumen file pribadi dapat dienkripsi sehingga hanya orang yang memiliki kunci enkripsi yang dapat membaca dan membuka file tersebut (Zulma dkk 2022).

Dengan demikian, implementasi sistem keamanan file menggunakan algoritma AES dapat menjadi solusi yang efektif dan terpercaya untuk mengamankan file pribadi dari serangan dan akses yang tidak sah serta menjaga privasi dan kerahasiaan informasi pribadi (Hulu dkk 2020). Keandalan dan keamanan yang ditawarkan oleh algoritma AES menjadikannya pilihan yang tepat dalam mengamankan dokumen file pribadi di era digital yang semakin kompleks dan rentan terhadap ancaman cyber. Dengan menggunakan algoritma AES, pengguna dapat memastikan bahwa data sensitif dan pribadi dalam dokumen file tetap terlindungi dan hanya dapat diakses oleh pihak yang berwenang (Clara, 2020).

2. KAJIAN PUSTAKA

Implementasi Sistem Keamanan File Menggunakan Algoritma AES merupakan sebuah upaya untuk menjaga keamanan dan *privasi* file pribadi dari akses oleh pihak yang tidak berwenang (Muharram dkk 2018). Algoritma AES (*Advanced Encryption Standard*) yang digunakan dalam implementasi sistem ini merupakan salah satu algoritma enkripsi yang paling aman dan banyak digunakan di dunia saat ini (Waluyo dkk 2018). Pada penelitian Implementasi Sistem Keamanan File Menggunakan Algoritma AES bukanlah peneltian pertama kali dilakukan, berikut ini peneltian yang terkait.

Penelitian dengan judul "Implementasi *Advanced Encryption Standard* 128 Sebagai Pengamanan Basis Data Obat obatan Apotek" pada tahun 2022 menjelaskan bahwa Kerahasiaan dan keamanan data merupakan dua hal

penting dalam komunikasi data sebagai upaya menjaga kerahasiaan dan keamanan suatu data. Kriptografi AES 128 bit memiliki ruang kunci 2128 yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack*. Hasil pengujian menunjukkan bahwa nilai dari Algoritma AES berkisar antara 45-60%, dengan nilai tersebut akan membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan (Wiharto & Mufti, 2022). Pengujian enkripsi dilakukan dengan melakukan perbandingan antara perhitungan manual dengan hasil enkripsi pada sistem. Pembuatan sistem ini dilakukan dengan mengumpulkan data, merancang sistem dengan database. Hasil dari pembuatan sistem adalah aplikasi berbasis web yang digunakan dalam kegiatan apoteker atau pegawai apotek untuk menginput dan mengelola data obat

Selanjutnya penelitian tahun pada 2022 dengan judul "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)" dijelaskan bahwa Seiring berjalannya waktu, kemajuan teknologi komputer dan telekomunikasi telah menjadi kebutuhan yang sangat berguna untuk melakukan banyak tugas dengan cepat, tepat, dan akurat. Namun, diyakini bahwa aspek keamanan data penting untuk informasi sensitif, karena juga memiliki efek negatif dari orang yang tidak berwenang menyadap data penting. Enkripsi adalah salah satu solusi atau metode keamanan data terbaik untuk menjaga kerahasiaan dan keandalan data Anda, serta dapat meningkatkan keamanan data atau informasi Anda (Azhari dkk 2022). Tujuan dari penelitian ini adalah untuk mempelajari konsep kriptografi dalam pengamanan data berbasis teks dengan menggunakan algoritma AES. Algoritma AES dipilih karena kemampuannya dalam mengenkripsi dan mendekripsi data dengan berbagai panjang kunci yang berbeda, yaitu 128 bit, 192 bit, dan 256 bit. Panjang kunci yang berbeda ini mempengaruhi jumlah putaran pada algoritma AES. Meskipun teknik pengamanan file dengan menggunakan kriptografi telah banyak diteliti, tampaknya implementasi yang hanya menggunakan algoritma kriptografi telah ditinggalkan dan beralih ke kombinasi asimetris dan simetris. Oleh karena itu, dalam penelitian ini akan dibuat aplikasi untuk mengenkripsi dokumen dan pesan teks dengan menggunakan algoritma AES.

Pada penelitian dengan judul "Penerapan Algoritma *Advanced Encryption Standard* (AES) untuk Keamanan Data Transaksi Pada Sistem *E-Marketplace*" tahun 2022 menjelasakan bahwa belanja secara online menjadi solusi banyak orang untuk melakukan transaksi jual beli. *E-marketplace* merupakan sebuah peluang besar untuk mengatasi terbatasnya akses teknologi informasi dikarenakan modal yang kurang dan tenaga ahli yang tidak memadai. Dalam penggunaannya *e-marketplace* erat kaitannya dengan metode pembayaran online dengan memanfaatkan *payment gateway* untuk mempermudah dalam bertransaksi. Dalam penerapannya, e-marketplace sangat diperlukan pengamanan data mengingat banyak *cybercrime* yang mengincar website dengan lalu lintas pengguna yang tinggi. Fokus penelitian ini adalah membangun sistem *e-marketplace* bibit sriwedari dan menerapkan algoritma kriptografi *Advanced Encryption Standard* (AES) dengan panjang kunci 256 bit untuk melindungi data transaksi pengguna. Tujuan dari penelitian ini adalah menciptakan sebuah sistem *e-marketplace* yang efektif dan efisien dalam menangani proses transaksi jual beli bibit buah dan tanaman di Desa Sriwedari, sambil tetap memperhatikan keamanan data pengguna agar tidak disalahgunakan oleh pihak yang tidak berhak mengaksesnya. Hasil dari penelitian ini adalah data transaksi pembayaran yang tersimpan di dalam database dalam bentuk tersandi (chipertext), yang merupakan hasil dari proses enkripsi data asli yang dimasukkan oleh pengguna (plaintext) (Riyan Andriyanto dkk 2022)

3. METODE PENELITIAN

Metode penelitian digunakan agar penelitian dapat dilakukan sesuai dengan rencana dan tahapan yang telah ditetapkan, sehingga menghasilkan hasil yang diharapkan. Terdapat 4 tahapan yang digunakan yaitu : Pertama, studi literatur. Pada tahap ini, dilakukan tinjauan jurnal, artikel, video youtube dan penelitian yang relevan sebagai referensi dalam melakukan penelitian. Kedua, tahap Perancangan dan Analisis. Pada tahap ini, langkah-langkah yang dilakukan meliputi merancang arsitektur sistem keamanan file berbasis web yang mencakup penggunaan algoritma AES. Selain itu, dilakukan analisis terhadap kebutuhan sistem seperti tipe file yang akan diamankan, metode enkripsi yang akan digunakan, kebutuhan infrastruktur web, dan pengaturan akses pengguna.

Tahap selanjutnya, implementasi. Pada tahap ini, algoritma AES diterapkan dalam pembuatan sistem keamanan. Implementasinya menggunakan bahasa pemrograman PHP. Berikut ini pada gambar 1 menggambarkan bagaimana proses enkrip data menggunakan algoritma Aes.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

```
AES_Encrypt(byte plaintext[4*Nb], byte key[4*Nk], byte ciphertext[4*Nb], word w[Nb*(Nr+1)])
begin
    word state[4,Nb]
    word roundKey[4,Nb]

    // Inisialisasi state dengan plaintext
    for i = 0 to 3 do
        for j = 0 to Nb-1 do
            state[i,j] = plaintext[i + 4*j]
        end for
    end for

    // Inisialisasi round key dengan expanded key
    for i = 0 to 3 do
        for j = 0 to Nb-1 do
            roundKey[i,j] = w[i + 4*j]
        end for
    end for

    // AddRoundKey pada ronde pertama
    AddRoundKey(state, roundKey, 0)

    // Proses ronde 1 hingga Nr-1
    for round = 1 to Nr-1 do
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, roundKey, round)
    end for

    // Proses ronde terakhir (tidak ada MixColumns)
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, roundKey, Nr)

    // Copy state ke ciphertext
    for i = 0 to 3 do
        for j = 0 to Nb-1 do

            ciphertext[i + 4*j] = state[i,j]
        end for
    end for
end
```

Gambar 1. Logo PISCES

Kemudian pada gambar 2 menggambarkan bagaimana proses deksripsi algoritma AES untuk mengembalikan data file ke bentuk semula setelah proses enkripsi.

```
AES_Decrypt(byte ciphertext[4*Nb], byte key[4*Nk], byte plaintext[4*Nb], word w[Nb*(Nr+1)])
begin
    word state[4,Nb]
    word roundKey[4,Nb]

    // Inisialisasi state dengan ciphertext
    for i = 0 to 3 do
        for j = 0 to Nb-1 do
            state[i,j] = ciphertext[i + 4*j]
        end for
    end for

    // Inisialisasi round key dengan expanded key
    for i = 0 to 3 do
        for j = 0 to Nb-1 do
            roundKey[i,j] = w[i + 4*j]
        end for
    end for

    // AddRoundKey pada ronde terakhir
    AddRoundKey(state, roundKey, Nr)

    // Proses ronde Nr-1 hingga 1
    for round = Nr-1 downto 1 do
        InvShiftRows(state)
        InvSubBytes(state)
        AddRoundKey(state, roundKey, round)
        InvMixColumns(state)
    end for

    // Proses ronde pertama (tidak ada InvMixColumns)
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, roundKey, 0)

    // Copy state ke plaintext
    for i = 0 to 3 do
        for j = 0 to Nb-1 do
            plaintext[i + 4*j] = state[i,j]
        end for
    end for
end
```

Gambar 2. Pseudocode Proses Dekripsi

Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi (Pabokory dkk 2016). Algoritma AES merupakan algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit (Saputra & Kusumaningsih, 2018). Perbedaan dari ketiga urutan

tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat digambarkan dalam bentuk tabel 3 diawah ini.

Tabel 3. Algoritma Aes

AES (Bits)	Panjang Kunci (NK Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (Nr)
AES – 128	4	4	10
AES – 192	6	4	12
AES- 256	8	4	14

Pada Tabel 3 di atas dijelaskan mengenai tipe dari algoritma AES dengan panjang kunci, Panjang blok dan jumlah putaran yang berbeda-beda. Kemudian terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi (Wibowo dkk 2022). Informasi lebih lanjut dapat dilihat pada tabel 4 dibawah ini.

Tabel 4. Proses enkripisi dan dekripsi

	Enkripsi		Dekripsi	
AES	***SubBytes***	menukar isi dari byte dengan menggunakan tabel substitusi.	***InvShiftRows***	Melakukan pergeseran bit ke kanan pada setiap blok baris
	ShiftRow	Proses pergeseran blok per baris pada state array.	***InvSubBytes***	setiap elemen pada state dipetakan dengan tabel Inverse S-Box.
	MixColumn,	proses mengalikan blok data (pengacakan) di masing-masing state array.	***InvMixColumn***	setiap kolom dalam state dikalikan dengan matriks AES.
	AddRoundKey	mengombinasikan state array dan round key dengan hubungan XOR.	***AddRoundKey***	mengombinasikan state array dan round key dengan hubungan XOR.

Tahap terakhir dalam metode penelitian adalah tahap Pengujian. Pada tahap ini, dilakukan pengujian terhadap sistem keamanan file berbasis web yang telah diimplementasikan. Dalam pengujian, terdapat dua langkah yang dilakukan. Pertama, dilakukan Pengujian Fungsi Enkripsi dan Dekripsi. Pengujian ini bertujuan untuk memastikan bahwa fungsi enkripsi dan dekripsi berjalan dengan benar dan menghasilkan hasil yang sesuai dan akurat. Selanjutnya, dilakukan Pengujian Fungsionalitas Sistem secara keseluruhan. Pengujian ini mencakup pengujian terhadap seluruh fungsionalitas sistem, termasuk antarmuka pengguna, fitur login, pengunggahan file, enkripsi dan dekripsi file, serta penyimpanan file di database. Tujuannya adalah memastikan bahwa semua fitur berfungsi sesuai dengan yang diharapkan dan berjalan tanpa ada masalah. Dengan melakukan pengujian secara menyeluruh, dapat dipastikan bahwa sistem keamanan file berbasis web telah diuji dengan baik dan siap digunakan untuk menjaga keamanan file dalam lingkungan web.

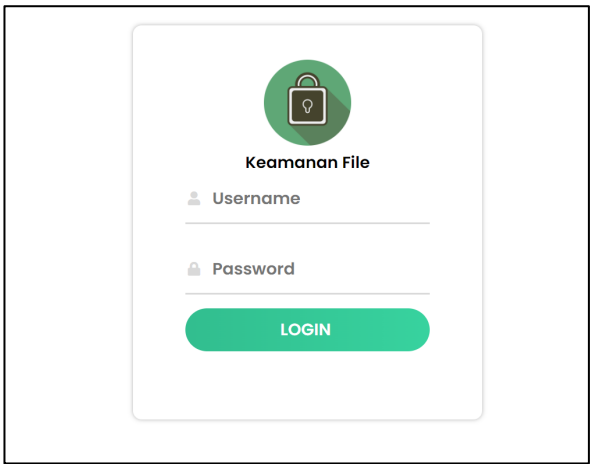
4. HASIL DAN PEMBAHASAN

Setelah melakukan perancangan terhadap sistem yang dibangun serta melakukan analisa kebutuhan dari sistem yang akan dibangun, berikut ini hasil implementasi

4.1 Tampilan Login

Pada tahap awal akses oleh pengguna, tampilan login akan muncul yang terdiri dari dua bentuk yaitu form username dan form password. Untuk dapat masuk ke dalam sistem ini, pengguna harus memasukkan

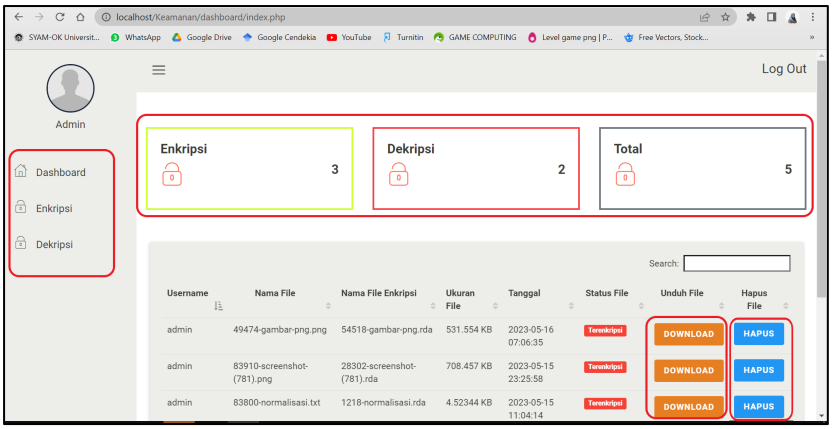
username dan password yang telah terdaftar dengan benar. Tampilan login yang dimaksud dapat dilihat pada gambar 5 dibawah ini.



Gambar 7. Tampilan Login

4.2 Tampilan Dashboard

Pada gambar 6 merupakan halaman dashboard terdapat 3 menu Form yaitu form Enkripsi, form Dekripsi, dan form Dashboard itu sendiri. Didalam menu dashboard terdapat beberapa fitur yang dapat menampilkan jumlah file enkripsi, jumlah file dekripsi dan tabel yang berisi daftar file yang telah dilakukan enkripsi dan dekripsi serta memiliki tombol download dan hapus file baik itu file yang telah terenkripsi maupun file terdekripsi.

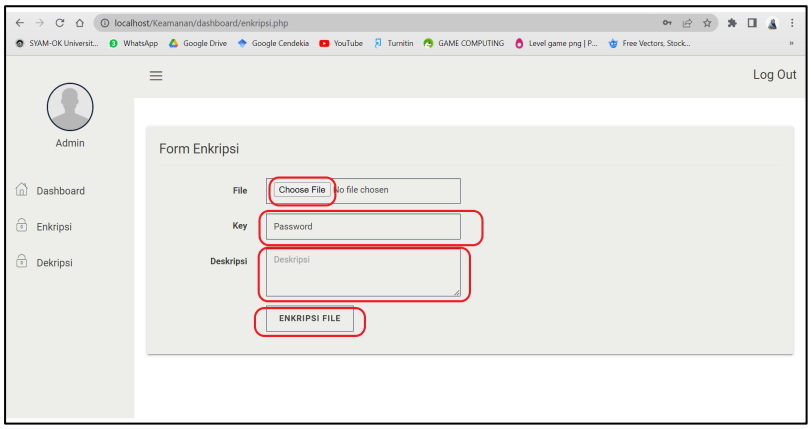


Gambar 6. Tampilan Dashboard

4.3 Tampilan Menu enkripsi

Pada tampilan menu enkripsi memiliki beberapa elemen dapat dilihat pada gambar 7, di antaranya adalah tombol "*choose file*", kolom teks password, dan kolom teks dekripsi. Kolom "*choose file*" berguna untuk memilih file yang akan dienkripsi. Kolom teks password digunakan untuk memasukkan kata sandi atau kunci untuk file yang akan dienkripsi, sedangkan kolom teks dekripsi berguna untuk memberikan informasi mengenai file yang telah dienkripsi. Kemudian tombol enkripsi untuk melakukan proses enkripsi.

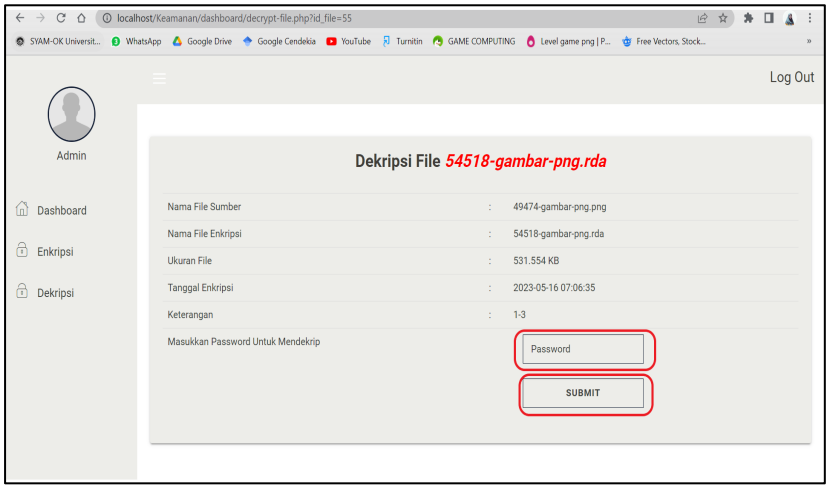
PISCES
Progressive Information, Security, Computer, and Embedded System
E-ISSN: 2986-7258
P-ISSN : 2986-724X
PISCES Volume 02 Nomor 01 Maret 2024



Gambar 7. Tampilan Fom Menu Enkripsi

4.4 Tampilan Menu dekripsi

Pada gambar 8 merupakan tampilan menu dekripsi, terdapat teks yang menampilkan informasi mengenai file, sebuah kolom teks untuk memasukkan kata sandi yang sesuai dengan password enkripsi, serta sebuah tombol untuk melakukan proses dekripsi pada file tersebut.



Gambar 8. Tampilan Form Menu Dekripsi

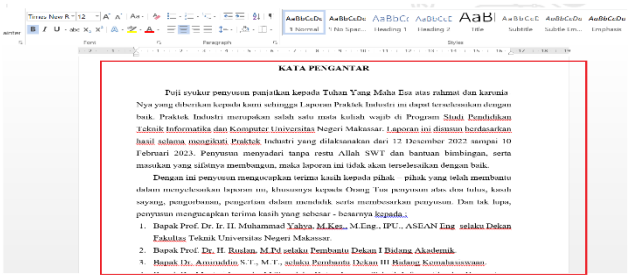
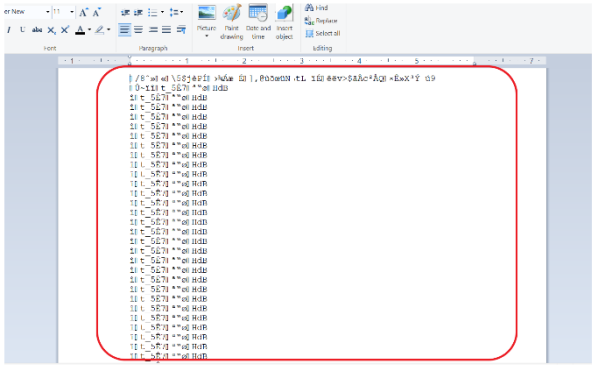
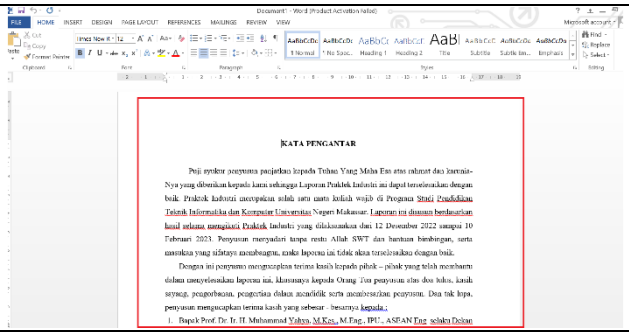
4.5 Uji Sistem pada File

Enkripsi adalah proses yang mengubah teks biasa menjadi sandi atau teks rahasia (Purnomo dkk 2022). Hal ini bertujuan untuk menjaga kerahasiaan data atau pesan agar tidak dapat dimengerti oleh pihak yang tidak berwenang. Sebelum melakukan proses enkripsi, diperlukan analisis isi file untuk memastikan bahwa file tersebut memenuhi syarat untuk dienkripsi. Sebelumnya telah dilakukan uji coba pada semua ekstensi file untuk memastikan kemampuan program dalam melakukan enkripsi. Namun, sebagai contoh, pada uji sistem ini hanya menampilkan dua hasil dari uji coba tersebut, yaitu dokumen dengan ekstensi Word dan gambar dengan ekstensi JPG.

a. File Dokumen Ekstensi Docx

Pada Tabel 9 terdapat contoh file dokumen sebelum dan setelah melalui proses enkripsi. File awal dengan ekstensi .docx berisi teks yang ingin diamankan menggunakan sistem keamanan yang diimplementasikan. Melalui proses enkripsi menggunakan kunci yang sesuai, file tersebut berubah menjadi bentuk terenkripsi. Selain itu, proses enkripsi juga memiliki bentuk dekripsi yang sesuai, di mana file terenkripsi dapat dikembalikan ke bentuk aslinya menggunakan kunci enkripsi yang sama. Gambar tersebut memberikan gambaran tentang hasil dekripsi dari file terenkripsi setelah melalui proses yang sesuai dengan sistem keamanan yang diterapkan.

Tabel 9. Hasil enkripsi dan dekripsi pada file ekstensi docx

Gambar	Keterangan
	File Asli
	Hasil enkripsi
	Hasil dekripsi

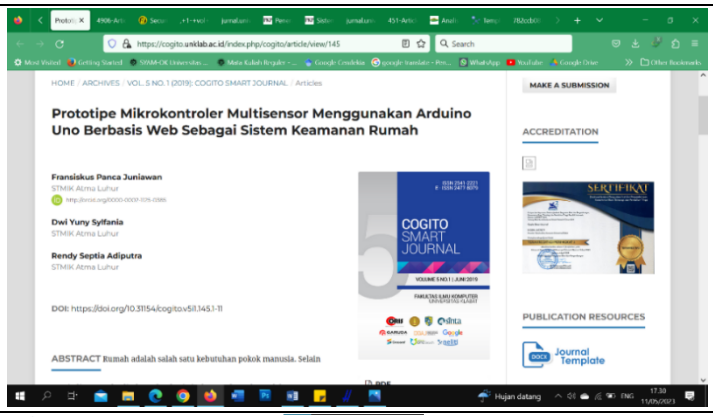
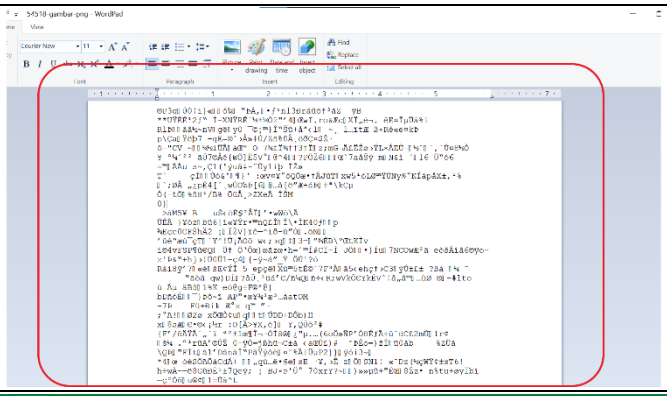
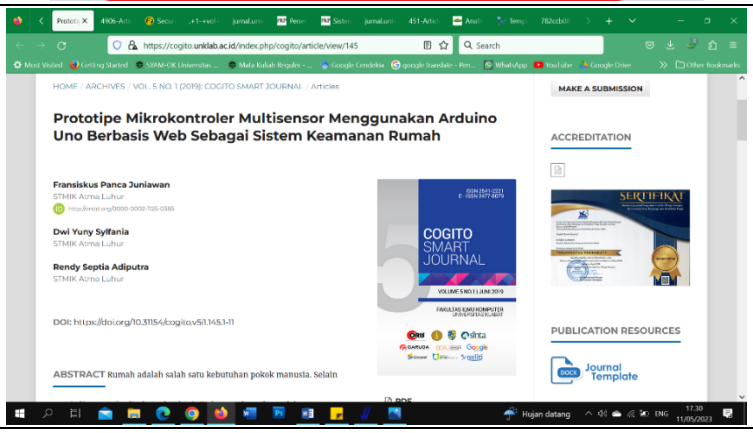
b. Gambar dengan Ekstensi PNG

Pada tabe 10 yang ditampilkan, terlihat contoh file gambar dalam format PNG sebelum dan setelah melalui proses enkripsi serta dekripsi. Gambar pertama menunjukkan file gambar sebelum enkripsi, yang kemudian diubah menjadi bentuk terenkripsi menggunakan algoritma AES. Gambar kedua menampilkan file gambar selama proses enkripsi, di mana informasi dalam gambar tidak dapat terbaca tanpa kunci enkripsi yang sesuai. Gambar ketiga menunjukkan file gambar setelah melalui proses dekripsi, di mana file terenkripsi berhasil dikembalikan ke bentuk aslinya menggunakan kunci enkripsi yang sama. Hal ini memungkinkan akses dan pemahaman informasi dalam gambar oleh pihak yang berwenang.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

Tabel 10. Hasil enkripsi dan dekripsi pada file ekstensi png

Gambar	Keterangan
	File Asli
	Hasil enkripsi
	Hasil dekripsi

5. KESIMPULAN DAN SARAN

Algoritma AES merupakan metode yang efektif dalam mengamankan data dokumen dan gambar. Penelitian ini menjawab permasalahan mengenai keamanan data digital yang semakin penting dalam era informasi saat ini. Melalui proses enkripsi dan dekripsi, algoritma AES mampu menjaga kerahasiaan dan integritas informasi yang terdapat dalam berbagai jenis file, termasuk gambar, Word, PDF, Excel, dan PowerPoint.

Hasil penelitian menunjukkan bahwa algoritma AES dapat mengenkripsi file sehingga berubah menjadi bentuk yang tidak dapat dibaca, menjaga data dari akses yang tidak sah. Proses dekripsi menggunakan kunci yang sama memungkinkan pengembalian file ke bentuk aslinya. Dalam uji coba yang dilakukan, algoritma AES berhasil melindungi kelima jenis file tersebut dengan baik. Berdasarkan temuan penelitian ini, disarankan adanya

penelitian lanjutan untuk lebih menyempurnakan penggunaan algoritma AES dalam mengamankan data. Penelitian selanjutnya dapat fokus pada peningkatan kecepatan proses enkripsi dan dekripsi, terutama untuk file dengan ukuran yang lebih besar. Selain itu, penting juga untuk melibatkan jenis file lainnya dalam uji coba, sehingga dapat memperluas pemahaman tentang keandalan algoritma AES dalam berbagai konteks penggunaan. Selain itu, penelitian selanjutnya dapat mempertimbangkan penggunaan kombinasi algoritma enkripsi untuk meningkatkan tingkat keamanan data. Pengembangan teknik enkripsi yang lebih canggih dan penambahan lapisan keamanan tambahan juga dapat menjadi fokus penelitian yang berpotensi memberikan hasil yang lebih baik.

REFERENSI

Ardian, M. T., & Pramusinto, W. (2022). *Pengamanan Database Perpustakaan Dengan Algoritma Aes-128 Pada Sma Waskito Library Database Security With Aes-128 Algorithm on*. *September*, 248–257.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Clara, L. (2020). Implementasi Metode Algoritma Aes Pada Perlindungan Data Sistem Login. *Skripsi*, *2017*(1), 1–9. http://eprints.kwikkiangie.ac.id/914/

Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes). *Jurnal SITECH : Sistem Informasi dan Teknologi*, *3*(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

Hulu, D., Nadeak, B., & Aripin, S. (2020). Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. *KOMIK (Konferensi ...*, *4*, 78–86. https://doi.org/10.30865/komik.v4i1.2590

Muharram, F., Azis, H., & Manga, A. R. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). *Proc. of the Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, *3*(2), 112–115.

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *Jurnal Teknik Informatika*, *11*(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Purnomo, H. D., Sembiring, I., No, J. D., Sidorejo, K., Salatiga, K., & Tengah, J. (2022). *Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks*. *2*(1).

Riyan Andriyanto, M., Sukmasetya, P., & Penulis Korespondensi, E. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of Computer System and Informatics (JoSYC)*, *4*(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

Saputra, D., & Kusumaningsih, D. (2018). Implementasi Keamanan Database Menggunakan Algoritma Aes-192 Pada Pt Gurita Lintas Samudera Berbasis Android. *Jurnal Skanika*, *1*(`Vol 1 No 3 (2018): Jurnal SKANIKA Juli 2018), 884–888. http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2501

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal ...*, *6*(1), 2319–2327. http://journal.upy.ac.id/index.php/pkn/article/view/2989

Waluyo, S., Ferdiansyah, & firman. (2018). Sistem Keamanan Management File Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus : Tabitha Indonesia. *Seminar Nasional Teknologi Informasi Universitas Ibn Khaldun Bogor*, 639.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

Wibowo, Y. A., Nugroho, N. B., & Andika, B. (2022). Penerapan Algoritma AES 128 Bit Untuk Keamanan Data Peminjaman Senjata Api Pada DENPOM I/5 Medan. *Jurnal Cyber Tech*, *10*(10). https://ojs.trigunadharma.ac.id/index.php/jct/article/view/1747

Wiharto, Y., & Mufti. (2022). Implementasi Advanced Encryption Standard 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek. *Jurnal Teknik Informatika dan Sistem Informasi*, *8*(2), 335–350. https://doi.org/10.28932/jutisi.v8i2.4817

Zulma, G. D. M., Seta, H. B., & Yuniati, T. (2022). Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan File Dokumen. *Informatik : Jurnal Ilmu Komputer*, *18*(2), 163. https://doi.org/10.52958/iftk.v18i2.4667