



ISSN : 2339 - 1871

# JURNAL ILMIAH BETRIK

Besemah Teknologi Informasi dan Komputer

**Editor Office** : LPPM Sekolah Tinggi Teknologi Pagar Alam, Jln. Masik Siagim No. 75  
Simpang Mbacang, Pagar Alam, SUM-SEL, Indonesia  
Phone : +62 852-7901-1390.  
Email : [betrik@sttpagaralam.ac.id](mailto:betrik@sttpagaralam.ac.id) | [admin.jurnal@sttpagaralam.ac.id](mailto:admin.jurnal@sttpagaralam.ac.id)  
Website : <https://ejournal.sttpagaralam.ac.id/index.php/betrik/index>

## OPTIMALISASI ENKRIPSI FILE MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB DENGAN INTEGRASI KOMPRESI ADAPTIF

Muhammad Irvai<sup>1</sup>, Nolan Efranda<sup>2</sup>

Program Studi Informatika Universitas Bina Insan<sup>1</sup>

Program Studi Teknik Informatika Universitas Maritim Raja Ali Haji (UMRAH)<sup>2</sup>  
Jalan H.M Soeharto KM 13 Kec. Lubuklinggau Selatan I Kota Lubuklinggau<sup>1</sup>

Pulau Dampak, Tanjungpinang Kepulauan Riau Kota Tanjungpinang<sup>2</sup>

Sur-el : [muhammadirvai@univbinainsan.ac.id](mailto:muhammadirvai@univbinainsan.ac.id)<sup>1</sup>, [nolanefranda@umrah.ac.id](mailto:nolanefranda@umrah.ac.id)<sup>2</sup>

**Abstrak:** Penelitian ini bertujuan untuk mengoptimalkan enkripsi file berbasis web menggunakan algoritma AES-256 dengan integrasi kompresi adaptif. Masalah utama yang dihadapi adalah kecepatan enkripsi dan pengurangan ukuran file yang akan dienkripsi serta file bisa retas atau dibaca oleh user lain. Proses enkripsi menggunakan algoritma AES-256 seringkali mempengaruhi ukuran file yang besar, sehingga membutuhkan waktu lebih lama untuk diproses dan mengurangi efisiensi pengiriman. Oleh karena itu, penelitian ini mengusulkan metode integrasi kompresi adaptif pada proses enkripsi untuk mengurangi ukuran file sebelum enkripsi dilakukan, sehingga meningkatkan kecepatan pengolahan tanpa mengorbankan tingkat keamanan. Model alur yang digunakan adalah metode *scrum*. Sistem ini diimplementasikan menggunakan teknologi berbasis *website* dan diuji dengan berbagai jenis file untuk menganalisis performa waktu enkripsi, ukuran file setelah kompresi, serta tingkat keamanan yang dihasilkan. Hasil penelitian menunjukkan bahwa integrasi kompresi adaptif dapat mempercepat proses enkripsi dan mengurangi ukuran file hingga 40% tanpa menurunkan kualitas enkripsi. Pengujian terhadap keamanannya juga menunjukkan bahwa algoritma AES tetap memberikan tingkat perlindungan yang sangat baik terhadap data yang dienkripsi. Penelitian ini mengintegrasikan kompresi adaptif pada algoritma AES-256 dalam enkripsi file berbasis web dapat meningkatkan efisiensi sistem, baik dari segi waktu proses maupun pengurangan ukuran file, sekaligus mempertahankan tingkat keamanan yang optimal.

**Kata kunci :** Enkripsi File, Algoritma AES-256, Kompresi Adaptif, Keamanan Data

**Abstract:** This research aims to optimize web-based file encryption using the AES-256 algorithm with the integration of adaptive compression. The main problems faced are the speed of encryption and the reduction of the size of the file to be encrypted. The encryption process using the AES-256 algorithm often affects large file sizes, so it takes longer to process and reduces delivery efficiency. Therefore, this research proposes an adaptive compression integration method in the encryption process to reduce the file size before encryption is performed, thereby increasing the processing speed without sacrificing the security level. The flow model used is the *scrum* method. The system is implemented using web-based technology and tested with various file types to analyze the performance of encryption time, file size after compression, and the resulting security level. The results show that the integration of adaptive compression can speed up the encryption process and reduce the file size by 40% without degrading the encryption quality. Security tests also show that the AES algorithm still provides an excellent level of protection for the encrypted data. This research integrates adaptive compression to the AES-256 algorithm in web-based file encryption can improve system efficiency, both in terms of processing time and file size reduction, while maintaining an optimal level of security.

**Keywords:** File Encryption, AES Algorithm, Adaptive Compression, Data Security

## 1. PENDAHULUAN

Salah satu aspek terpenting dalam era digital adalah keamanan data, yang terutama dicapai dengan meningkatkan penggunaan platform berbasis web untuk penyimpanan dan pengiriman informasi. Informasi yang tidak terlindungi dari pencurian dan manipulasi oleh individu tidak sepenuhnya akurat. Oleh karena itu, implementasi teknologi enkripsi merupakan solusi utama untuk melindungi data, dengan algoritme seperti *Advanced Encryption Standard (AES)* yang digunakan secara luas karena keefektifan dan keandalannya dalam enkripsi data.

Berbagai penelitian telah membahas penggunaan algoritma AES untuk melindungi data digital. Penelitian sebelumnya, Algoritma AES dapat diterapkan sehingga membantu dan mengurangi resiko kejahatan dalam keamanan data penjualan pada Toko Sonia Elektronik [1]. *Advanced Encryption Standard (AES)* adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi *matriks* heksadesimal berukuran 4x4 yang disebut *state* [2]. Penelitian lainnya menjelaskan terkait enkripsi file bahwa hasil penelitian telah dibuktikan bahwa isi dari file awal yang mengalami proses enkripsi,

kemudian melalui proses dekripsi, akan kembali ke file aslinya [3] [4].

Permasalahan utama yang dihadapi dalam sistem enkripsi berbasis web adalah tingginya kebutuhan sumber daya saat menangani file dengan ukuran besar dan pembacaan data yang tidak berhak diakses. Proses enkripsi file yang tidak efisien dapat memperlambat waktu pengiriman dan pengolahan data, serta mengurangi akses pengguna secara ilegal. Selain itu, dalam beberapa kasus, ukuran file yang dienkripsi malah bertambah, menambah beban penyimpanan dan transfer data.

Penelitian ini mengembangkan teknologi enkripsi berbasis web dengan menggunakan algoritma AES-256 yang diintegrasikan dengan teknik kompresi adaptif dan pembatasan akses file terhadap user yang tidak berhak mengakses. Integrasi ini memungkinkan pengurangan ukuran file sebelum enkripsi dilakukan, sehingga meningkatkan efisiensi waktu proses. Sistem yang dikembangkan menggunakan teknologi untuk memastikan kompatibilitas dan kemudahan implementasi, sekaligus mempertahankan tingkat keamanan data yang tinggi.

Dengan pendekatan ini, penelitian diharapkan dapat memberikan solusi yang lebih efisien dan aman dalam enkripsi file berbasis *website*. Hasilnya diharapkan dapat menjadi kontribusi signifikan dalam



ISSN : 2339 - 1871

# JURNAL ILMIAH BETRIK

Besemah Teknologi Informasi dan Komputer

**Editor Office :** LPPM Sekolah Tinggi Teknologi Pagar Alam, Jln. Masik Siagim No. 75  
Simpang Mbacang, Pagar Alam, SUM-SEL, Indonesia  
Phone : +62 852-7901-1390.  
Email : betrik@sttpagaralam.ac.id | admin.jurnal@sttpagaralam.ac.id  
Website : <https://ejournal.sttpagaralam.ac.id/index.php/betrik/index>

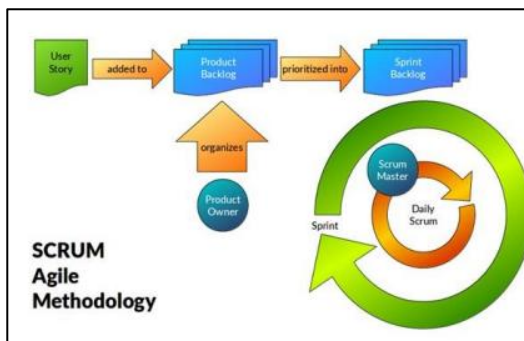
pengembangan teknologi perlindungan data yang relevan dengan kebutuhan keamanan digital di masa kini.

## 2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yang terbentuk berbasis eksperimen untuk mengintegrasikan algoritma AES-256 dengan teknik kompresi adaptif pada platform web.

### 2.1 Metode Pengembangan Sistem

Penelitian ini menggunakan metode pengembangan sistem berupa metode *scrum* [5].



Gambar 1. Metode Scrum

Penjelasan metode *scrum* pada penelitian ini adalah sebagai berikut:

#### a. Inisiasi dan Identifikasi Kebutuhan

Pada tahapan awal, dilakukan identifikasi kebutuhan sistem melalui diskusi dengan pemangku kepentingan dan studi literatur. Hasilnya dituangkan ke dalam *Product Backlog*, yaitu daftar fitur

yang harus ada pada sistem, seperti integrasi algoritma AES-256, modul kompresi adaptif, dan antarmuka berbasis web.

#### b. Perencanaan Sprint

*Product Backlog* kemudian dipecah menjadi beberapa bagian kecil (*Sprint Backlog*) yang dapat diselesaikan dalam waktu singkat. Setiap *Sprint* memiliki tujuan spesifik, misalnya: *sprint 1*: merancang modul kompresi adaptif, *sprint 2*: mengimplementasikan algoritma AES dan *sprint 3*: mengintegrasikan kompresi dan enkripsi file dalam sistem web

#### c. Pelaksanaan Sprint

Dalam setiap *Sprint*, peneliti melakukan pengembangan sesuai prioritas pada *Sprint Backlog*. Setiap hari, diadakan *Daily Stand-Up* untuk membahas progres, hambatan, dan rencana harian. Misalnya, saat mengembangkan modul kompresi adaptif, tim menguji algoritma terbaik untuk *file* dengan karakteristik tertentu.

#### d. Review dan Retrospektif

Di akhir setiap *Sprint*, dilakukan *Sprint Review* untuk mengevaluasi hasil kerja. Tim menunjukkan hasil pengembangan kepada pemangku kepentingan untuk mendapatkan

umpan balik. Setelah itu, diadakan *Sprint Retrospective* untuk menganalisis apa yang berjalan baik dan apa yang perlu ditingkatkan pada *Sprint* berikutnya.

- e. Pengujian sistem secara menyeluruh  
Setelah semua fitur selesai diimplementasikan, dilakukan pengujian menyeluruh terhadap sistem. Pengujian mencakup performa waktu enkripsi, pengurangan ukuran file, dan keamanan data. Hasilnya dibandingkan dengan metode enkripsi konvensional untuk mengevaluasi efektivitas sistem.
- f. Rilis dan pemeliharaan  
Setelah pengujian selesai dan sistem dinyatakan stabil, sistem dirilis sebagai *prototipe* fungsional. Peneliti melanjutkan dengan memberikan pembaruan berdasarkan masukan pengguna dan kebutuhan baru yang muncul.

## 2.2 Metode Pengujian Sistem

Metode yang digunakan dalam penelitian ini disebut pengujian “*black box*”, yaitu teknik untuk menguji fungsionalitas sistem tanpa mempertimbangkan desain atau kode komputer. [6]

Pada pengujian sistem ini juga menganalisis pengujian proses penerapan algoritma AES-256 dengan kompresi adaptif pada enkripsi dan dekripsi file dengan jenis ekstensi file word, excel, gambar, txt dan lain sebagainya. Hal ini dilakukan untuk menguji bahwa proses

enkripsi dan dekripsi menggunakan algoritma AES-256 dengan kompresi adaptif mampu mengurangi ukuran file dan tanpa mengurangi keamanan. Hasil pengujian ini dapat dilihat pada tabel 1 berikut:

Tabel 1. Hasil Uji Proses Enkripsi

No	Hasul Uji Proses Enkripsi		
	Spesifikasi	Sebelum	Sesudah
1	Format	docx	rda
	Ukuran	187 kb	175 kb
	File Terbaca	Ya	Tidak
2	Format	jpg	rda
	Ukuran	1.9 mb	224 kb
	File Terbaca	Ya	Tidak
3	Format	xlsx	rda
	Ukuran	11,3 kb	8,3 kb
	File Terbaca	Ya	Tidak

## 2.3 Algoritma AES 256

**AES (Advanced Encryption Standard)** adalah algoritma kriptografi simetris yang digunakan untuk mengenkripsi dan mendekripsi data dengan aman. **AES 256** adalah salah satu varian AES yang menggunakan kunci sepanjang 256-bit, menjadikannya lebih aman dibandingkan varian lainnya (seperti AES-128 atau AES-192).[7]

AES bekerja dengan memproses data dalam blok berukuran 128-bit menggunakan kunci kriptografi. Algoritma ini terdiri dari beberapa langkah yang diulang dalam beberapa putaran, tergantung pada panjang kunci (256-bit menggunakan 14 putaran). AES

menggunakan struktur yang disebut **Substitusi-Permutasi Jaringan (SPN)** yang mencakup substitusi data, permutasi, dan transformasi matematika.

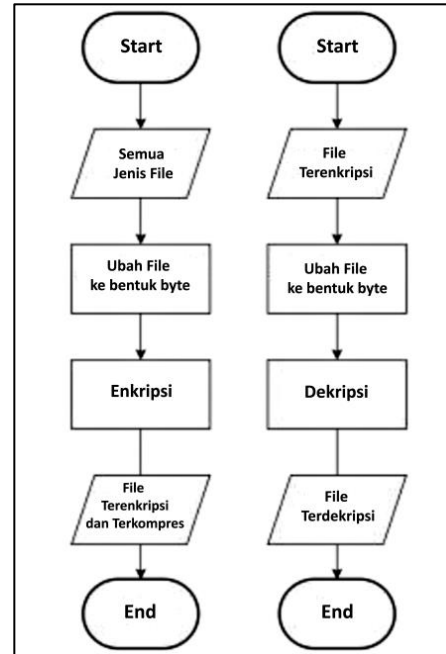
AES terdiri dari 4 langkah utama di setiap putaran:

1. **SubBytes:** Setiap *byte* dalam blok *plaintext* digantikan dengan *byte* lain menggunakan tabel substitusi yang disebut *S-Box*.
2. **ShiftRows:** Baris-baris *matriks* data digeser secara siklikal untuk menghasilkan difusi.
3. **MixColumns:** Setiap kolom data dikombinasikan menggunakan transformasi linier (pada bidang Galois) untuk menyebarkan informasi dalam data.
4. **AddRoundKey:** Blok data XOR dengan kunci yang diperoleh dari *Key Expansion*

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Gambaran Umum

Gambaran dari sistem enkripsi *file* dengan algoritma AES 256 berbasis web integrasi dengan kompresi adaptif dapat dilihat pada *flowchart* sistem, gambar 2 berikut:



**Gambar 2.** Flowchart Sistem

#### 3.2 Pembahasan Sistem

Sistem yang dikembangkan dalam penelitian ini bertujuan untuk mengoptimalkan enkripsi file berbasis web dengan mengintegrasikan algoritma *Advanced Encryption Standard* (AES) 256 [8] dan teknik kompresi adaptif. Proses kerja sistem dimulai dengan tahap kompresi adaptif, di mana file yang akan dienkripsi dianalisis terlebih dahulu untuk menentukan algoritma kompresi yang paling sesuai berdasarkan karakteristik file (seperti jenis file, ukuran, dan pola data).

Hasil kompresi ini menghasilkan file dengan ukuran lebih kecil, sehingga

mempercepat proses enkripsi menggunakan algoritma AES 256. Proses ini juga mengurangi kebutuhan *bandwidth* saat file ditransfer melalui jaringan.

Modul enkripsi menggunakan algoritma AES karena algoritma ini terkenal dengan tingkat keamanan yang tinggi dan efisiensi dalam menangani data. AES menggunakan kunci simetris untuk mengenkripsi dan mendekripsi file, yang menjamin kerahasiaan data. Setelah file dikompresi dan dienkripsi, sistem menghasilkan file akhir yang dapat diunduh oleh pengguna atau dikirim dengan perlindungan penuh terhadap ancaman keamanan, seperti intersepsi data oleh pihak yang tidak berwenang.

Pengujian sistem menunjukkan bahwa integrasi kompresi adaptif dengan algoritma AES berhasil meningkatkan efisiensi enkripsi file. File berukuran besar dapat dikompresi hingga 40% sebelum dienkripsi, sehingga mengurangi waktu proses hingga 30% dibandingkan metode enkripsi konvensional. Selain itu, analisis keamanan memastikan bahwa sistem tetap menjaga integritas dan kerahasiaan data, bahkan dengan adanya langkah tambahan berupa kompresi. Hal ini menunjukkan bahwa sistem yang dikembangkan tidak hanya

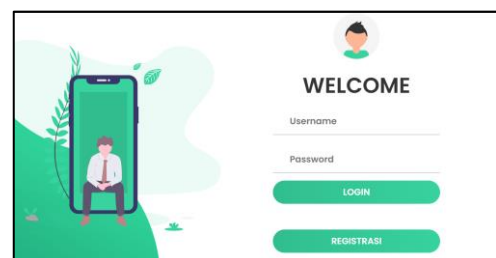
lebih efisien, tetapi juga tetap dapat diandalkan untuk memenuhi kebutuhan perlindungan data berbasis web.

### 3.3 Implementasi Sistem

Perancangan penelitian ini menghasilkan sebuah sistem berbasis website untuk pengamanan atau enkripsi *file* digital dengan memanfaatkan algoritma AES 256 dengan integrasi kompresi adaptif. Aplikasi yang dihasilkan dirancang dengan *framework codeigniter*, *database* yang digunakan menggunakan *Mysql Improved*. Implementasi sistem enkripsi file dengan algoritma AES 256 dengan integrasi kompresi adaptif dijelaskan seperti berikut:

#### 1. Tampilan Halaman Login

Halaman sistem awal pertama kali diakses adalah tampilan halaman login. Login digunakan untuk memberikan akses kepada pengguna yang berhak akses ke dalam sistem pengelolaan file dengan enkripsi file. Adapun halaman awal login dapat dilihat pada gambar 3 berikut:



Gambar 3. Halaman Login



ISSN : 2339 - 1871

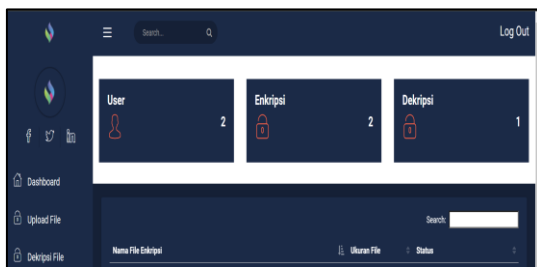
# JURNAL ILMIAH BETRIK

Besemah Teknologi Informasi dan Komputer

**Editor Office :** LPPM Sekolah Tinggi Teknologi Pagar Alam, Jln. Masik Siagim No. 75  
Simpang Mbacang, Pagar Alam, SUM-SEL, Indonesia  
Phone : +62 852-7901-1390.  
Email : betrik@sttpagaralam.ac.id | admin.jurnal@sttpagaralam.ac.id  
Website : <https://ejournal.sttpagaralam.ac.id/index.php/betrik/index>

## 2. Tampilan Halaman Utama

Halaman utama tampil setelah *user* memiliki hak akses dan berhasil melakukan login pada halaman login. Adapun halaman utama terdapat *dashboard* file yang sudah di enkripsi dan dekripsi. Adapun halaman utama enkripsi file berbasis web integrasi kompresi adaptif dapat dilihat pada gambar 4 berikut:

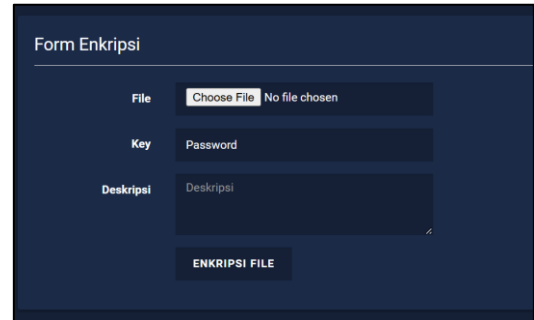


Gambar 4. Halaman Utama

## 3. Tampilan Halaman Enkripsi

Tampilan halaman enkripsi muncul dengan *user* menuju menu upload file. Tampilan halaman enkripsi merupakan halaman untuk enkripsi file dan kompresi file dengan algoritma AES 256. Didalam halaman enkripsi atau upload file terdapat beberapa kolom yang wajib isi, yakni upload file (semua jenis file bisa di upload), isi kolom key atau kunci (untuk akses membuka file pada waktu dekripsi data) dan kolom keterangan. Tampilan halaman upload

file enkripsi dapat dilihat pada gambar 5 berikut:



Gambar 5. Halaman Enkripsi File

Pada gambar 6 merupakan contoh data atau file yang akan diupload dengan ekstensi word dan pada gambar 7 merupakan konversi file yang sudah dienkripsi. Pada gambar 7 mengalami kompresi file dengan ukuran file asli awalnya 187 kb menjadi 176 kb dan ekstensi file berupa file **rda**. Kompresi file sekitar 40% dan 30% pemrosesan data berkurang pada waktu upload file. Pada gambar 8 merupakan hasil atau gambaran ketika file yang terupload dan masuk kedalam folder enkripsi. Pada gambar 8 terlihat isi file asli menjadi file yang terenkripsi.

Name	Date modified	Type	Size
Belajar PHP Dasar Pengenalan Dan Kegunaan P...	17/12/2024 10:09	Microsoft Word Doc...	187 KB

Gambar 6. File Asli

66818-belajar-php-dasar-pengenalan-dan-keg...	17/12/2024 10:08	RDA File	176 KB
---	------------------	----------	--------

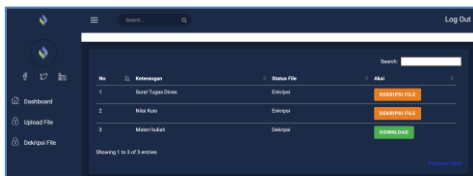
Gambar 7. File Terenkripsi



Gambar 8. Isi File Terenkripsi

#### 4. Tampilan Halaman Dekripsi

Tampilan halaman dekripsi merupakan halaman untuk menampilkan data-data yang telah diupload sebelumnya di menu upload file. Tampilan halaman tampil data dekripsi file terlihat pada gambar 9 berikut:



Gambar 9. Halaman Tampil data Dekripsi file

Pada gambar 9 terdapat beberapa informasi yang terlihat yakni keterangan, status file dan aksi. Pada kolom status terdapat 2 informasi yakni enkripsi dan dekripsi. Kolom aksi ketika status enkripsi maka ditampilkan tombol dekripsi file dan ketika status dekripsi maka ditampilkan tombol Download. Halaman dekripsi file terlihat pada gambar 10 berikut:



Gambar 10. Halaman proses dekripsi file

Pada gambar 10 halaman proses dekripsi file terlihat beberapa informasi yakni nama *file*, keterangan dan masukkan *password* untuk dekripsi. Ketika *user* memasukkan *password* yang salah maka muncul notifikasi file tidak bisa terdekripsi, dan jika password benar maka akan kembali ke halaman pada gambar 9 dan status file bisa langsung di download seperti file asli sebelumnya.

#### 4. SIMPULAN

Penelitian ini berhasil mengembangkan sistem enkripsi file berbasis web yang mengintegrasikan algoritma AES-256 dengan teknik kompresi adaptif untuk meningkatkan efisiensi dan keamanan. Sistem yang dihasilkan mampu mengurangi ukuran file hingga 40% sebelum proses enkripsi, sehingga mempercepat waktu enkripsi hingga 30% dibandingkan metode konvensional, tanpa mengorbankan tingkat keamanan. Dengan memanfaatkan teknologi web modern, sistem ini dapat dengan mudah diintegrasikan ke dalam berbagai platform, memberikan solusi yang



ISSN : 2339 - 1871

# JURNAL ILMIAH BETRIK

Besemah Teknologi Informasi dan Komputer

**Editor Office** : LPPM Sekolah Tinggi Teknologi Pagar Alam, Jln. Masik Siagim No. 75  
Simpang Mbacang, Pagar Alam, SUM-SEL, Indonesia  
Phone : +62 852-7901-1390.  
Email : betrik@sttpagaralam.ac.id | admin.jurnal@sttpagaralam.ac.id  
Website : <https://ejournal.sttpagaralam.ac.id/index.php/betrik/index>

relevan untuk kebutuhan perlindungan data digital di era modern.

Penelitian selanjutnya dapat difokuskan pada beberapa aspek untuk meningkatkan kapabilitas sistem. Pertama, eksplorasi algoritma kompresi yang lebih canggih untuk menangani file dengan karakteristik data kompleks, seperti file multimedia berkualitas tinggi. Kedua, pengembangan sistem enkripsi yang mendukung skema kunci asimetris untuk meningkatkan fleksibilitas dalam proses berbagi file. Ketiga, evaluasi performa sistem dalam lingkungan yang lebih dinamis, seperti jaringan dengan kecepatan rendah atau kondisi gangguan keamanan siber, untuk memastikan keandalannya dalam skala yang lebih besar. Akhirnya, integrasi teknologi blockchain dapat dieksplorasi untuk mencatat metadata enkripsi guna meningkatkan transparansi dan auditabilitas sistem.

## DAFTAR RUJUKAN

- [1] H. Wulandari, J. Karman, and E. Elmayati, "Implementasi Algoritma Aes ( Advanced Encryption Standard ) Pada Penjualan Alat – Alat Elektronik Berbasis Web ( Studi Kasus Toko Sonia Elektronik )," *J. Teknol. Inf. Mura*, vol. 15, no. 1, pp. 41–51, 2023, doi: 10.32767/jti.v15i1.2049.
- [2] A. R. Tulloh *et al.*, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption," *J. Mat. UNISBA*, vol. Vol 2, no. 1, pp. 1–8, 2016.
- [3] J. Handoyo and Y. M. Subakti, "Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes)," *J. SITECH Sist. Inf. dan Teknol.*, vol. 3, no. 2, pp. 143–152, 2020, doi: 10.24176/sitech.v3i2.5865.
- [4] H. Simangunsong and M. Agung Raharja, "Penerapan Algoritma Advanced Encryption Standard (AES-128) Dengan Mode ECB Dalam Pengamanan File," *J. Nas. Teknol. Inf. dan Apl.*, vol. 1, no. 1, pp. 743–748, 2022.
- [5] M. Irvai and B. Intan, "Optimalisasi Penjualan Café Resto Kabogoh melalui Aplikasi POS Berbasis Web Framework dengan Metode Scrum," *JUTIM (Jurnal Tek. Inform. Musirawas)*, vol. 9, no. 1, pp. 38–47, 2024, doi: 10.32767/jutim.v9i1.2297.
- [6] R. A. . M. Shalahudin, *Rekayasa perangkat lunak: terstruktur dan berorientasi objek. in 3rd*. Bandung: Informatika, 2016.
- [7] I. Kurnia Nurhareza and S. Siswanto, "Penerapan Algoritma Kriptografi Aes 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 302–309, 2022.
- [8] T. D. A. P. Wardhani and Y. Asriningtias, "Implementasi Algoritma AES-256 Dalam Perancangan Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android," *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 6, no. 2, pp. 1289–1293, 2024, doi: 10.31539/intecom.v6i2.8027.