SENAFTI SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 September 2025 – Jakarta, Indonesia
Volume 4, Nomor 2, September 2025 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KEAMANAN *FILE* BERBASIS *WEB* DENGAN METODE *ADVANCED ENCRYPTION STANDARD* (AES)-256 *COUNTER MODE*

Ahmad Najib Syafi'i[1], Noni Juliasari[2]*

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

Email: [1]2111510299@student.budiluhur.ac.id, [2*]noni.juliasari@budiluhur.ac.id
(* : *corresponding author*)

Abstrak-Penelitian ini bertujuan untuk menerapkan algoritma *Advanced Encryption Standard* (AES) 256-bit dengan mode *Counter* (CTR) sebagai mekanisme pengamanan data di PT Stretchline. Perkembangan teknologi informasi yang semakin pesat membawa dampak besar terhadap sistem pengolahan data di lingkungan perusahaan, termasuk PT. Stretchline yang bergerak di bidang produksi tekstil. Data penting yang dimiliki perusahaan adalah data produksi harian yang digunakan untuk evaluasi dan perencanaan. Namun, data tersebut masih disimpan secara digital tanpa sistem keamanan, sehingga rentan terhadap akses tidak sah, manipulasi, dan kebocoran informasi yang dapat mengganggu jalannya operasional. Berdasarkan permasalahan tersebut, maka pada penelitian ini dilakukan implementasi metode kriptografi dengan menggunakan algoritma *Advanced Encryption Standard* (AES) 256-bit dan *Counter Mode* (CTR) dalam bentuk aplikasi keamanan *file* berbasis *web*. Aplikasi ini menggunakan bahasa pemrograman PHP dan dilengkapi fitur enkripsi, dekripsi, manajemen pengguna, serta autentikasi berbasis pertanyaan keamanan untuk memverifikasi identitas sebelum proses dekripsi dilakukan. Hasil implementasi menunjukkan bahwa sistem mampu menjaga kerahasiaan dan integritas *file* penting secara efektif. Proses enkripsi dan dekripsi berjalan dengan efisien tanpa mengubah ukuran *file* secara signifikan. Berdasarkan pengujian menggunakan metode *black box testing*, seluruh fitur sistem telah berfungsi baik sesuai dengan rancangan, meliputi fitur unggah *file*, enkripsi, verifikasi keamanan, dekripsi, hingga pengunduhan *file* hasil dekripsi. Pada salah satu pengujian, *file* berukuran 12,7969 KB berhasil dienkripsi dalam waktu 0,131 milidetik dan didekripsi kembali dalam waktu 0,67 milidetik, dengan demikian, aplikasi ini mampu menjadi solusi untuk meningkatkan perlindungan data produksi harian dan mencegah penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Penelitian ini juga menyadarkan pentingnya integrasi kriptografi dalam sistem pengolahan data perusahaan yang memiliki informasi sensitif. Penerapan AES 256-bit dengan *mode* CTR memastikan bahwa data yang disimpan terlindungi dari potensi ancaman dan manipulasi. Penggunaan algoritma ini diharapkan dapat memperkuat keamanan. Selain itu, efisiensi proses enkripsi dan dekripsi memastikan bahwa data dapat diproses dengan cepat tanpa mengurangi tingkat keamanannya.

Kata Kunci: Kriptografi, AES 256-bit, *Counter Mode*

IMPLEMENTATION OF WEB-BASED FILE SECURITY USING THE ADVANCED ENCRYPTION STANDARD (AES)-256 COUNTER MODE METHOD

Abstract-*This study aims to apply the 256-bit Advanced Encryption Standard (AES) algorithm with Counter (CTR) mode as a data security mechanism at PT. Stretchline. The rapid development of information technology has had a major impact on data processing systems in the corporate environment, including PT. Stretchline, which is engaged in textile production. The company's important data is daily production data used for evaluation and planning. However, this data is still stored digitally without a security system, making it vulnerable to unauthorized access, manipulation, and information leaks that can disrupt operations. Based on these issues, this study implemented a cryptography method using the Advanced Encryption Standard (AES) 256-bit algorithm and Counter Mode (CTR) in the form of a web-based file security application. This application uses the PHP programming language and is equipped with encryption, decryption, user management, and security question-based authentication features to verify identity before the decryption process is carried out. The implementation results show that the system is capable of effectively maintaining the confidentiality and integrity of important files. The encryption and decryption processes run efficiently without significantly changing the file size. Based on testing using the black box testing method, all system features have functioned properly according to the design, including the file upload, encryption, security verification, decryption, and download of decrypted files features. In one test, a 12.7969 KB file was successfully encrypted in 0.131 milliseconds and decrypted in 0.67 milliseconds. Thus, this application can be a solution to improve the protection of daily production data and prevent information misuse by irresponsible parties. This research also highlights the importance of integrating cryptography into data processing systems of companies that handle sensitive information. The application of AES 256-bit with CTR mode ensures that stored data is protected from potential threats and manipulation. The use of this algorithm is expected to strengthen security. In addition, the efficiency of the encryption and decryption process ensures that data can be processed quickly without compromising security.*

Keywords*: Cryptography, AES 256-bit, Counter Mode*

1. PENDAHULUAN

Teknologi informasi dan komunikasi mengalami kemajuan yang cepat, dan memberikan dampak signifikan terhadap operasional perusahaan di berbagai sektor [1]. Kemajuan ini memberikan banyak keuntungan seperti efisiensi kerja, otomatisasi proses, serta peningkatan akurasi dalam pengolahan data. Namun, perkembangan teknologi juga menimbulkan tantangan baru, khususnya dalam aspek keamanan data [2]. Perusahaan yang tidak mengikuti perkembangan sistem keamanan digital berisiko menghadapi pencurian data, perusakan sistem, atau manipulasi informasi yang bisa berdampak pada reputasi dan kelangsungan operasional.

Pentingnya keamanan data dapat terlihat dalam operasional pada perusahaan PT. Stretchline yang bergerak di bidang produksi tekstil. Dalam proses produksinya, perusahaan memiliki data penting dan rahasia berupa data yang mencatat jumlah produksi harian secara rinci. Data ini menjadi acuan penting dalam mengevaluasi kinerja serta merencanakan strategi produksi berikutnya. Permasalahan yang dihadapi adalah data tersebut masih disimpan secara digital tanpa perlindungan keamanan yang memadai, hanya berupa file digital biasa tanpa enkripsi atau kontrol akses yang ketat. Kondisi ini berisiko menimbulkan akses tidak sah, manipulasi, maupun kehilangan data yang dapat mengganggu evaluasi, perencanaan, dan kelangsungan operasional produksi.

Berdasarkan permasalahan tersebut, solusi yang tepat adalah mengimplementasikan sistem keamanan berbasis kriptografi dengan penggunaan metode *Advanced Encryption Standard* (AES) 256-bit dalam *mode Counter* (CTR). Pemilihan algoritma ini didasarkan pada tingginya tingkat keamanannya, kecepatan enkripsi maupun dekripsi yang efisien, serta menghasilkan bentuk enkripsi yang unik dan terjamin keamanannya [3]. Implementasi dalam aplikasi berbasis *web* tidak hanya memberikan perlindungan terhadap data produksi, tetapi juga memudahkan pengguna dalam mengakses serta mengelola data secara aman, transparan, dan efisien melalui berbagai perangkat [4].

2. METODE PENELITIAN

2.1 Data Penelitian

Data penelitian ini merupakan data dalam bentuk format *excel*, *file* ini mencakup catatan hasil produksi PT. Stretchline dalam rentang waktu Januari 2024 – Mei 2024 dan Januari 2025 – Maret 2025, Informasi dalam data merupakan hasil laporan produksi.

2.2 Alur Penerapan Metode

Tahapan dalam alur penerapan metode meliputi proses merumuskan masalah, melakukan studi literatur, mengumpulkan dan menganalisis data, melakukan penyelesaian serta analisis sistem, lalu dilanjutkan dengan perancangan, implementasi, dan pengujian sistem [2]. Jika sistem berjalan tanpa adanya kesalahan, maka proses diteruskan ke tahap penarikan kesimpulan dan penyelesaian. Namun, jika masih terdapat kesalahan, proses akan kembali ke tahap analisis sistem untuk diperbaiki. Alur penerapan metode penelitian berperan sebagai panduan dalam pelaksanaan penelitian agar hasil yang dicapai sesuai dengan tujuan yang telah ditetapkan sebelumnya.

2.3 Perumusan Masalah

Tahap ini bertujuan untuk mengidentifikasi permasalahan yang akan dipecahkan dalam penelitian, yakni menjamin keamanan data catatan hasil produksi milik PT. Stretchline yang menjadi bagian penting dalam proses produksi, melalui penerapan algoritma kriptografi *Advanced Encryption Standard* (AES) 256-bit dengan *mode Counter* (CTR) [5].

2.4 Studi Literatur

Pada tahapan ini studi literatur dilakukan dengan membaca dan mempelajari berbagai sumber referensi seperti buku, diktat kuliah, jurnal, serta karya ilmiah yang relevan dengan topik penelitian. Pembahasan pada tahap ini berfokus pada konsep dan perangkat pendukung pembangunan sistem, khususnya yang berkaitan dengan masalah yang akan ditangani, yaitu perlindungan data menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES) 256-bit dalam mode *Counter* (CTR). Dengan adanya tahap ini, penulis dapat memahami dan menggali informasi secara lebih mendalam serta memperoleh landasan teori yang kuat untuk memilih metode yang sesuai dalam menyelesaikan masalah pengamanan data.

2.5 Pengumpulan Data

Tahap pengumpulan data dalam penelitian ini dilakukan melalui beberapa langkah dengan tujuan memperoleh data yang dibutuhkan, sehingga informasi yang terkumpul dapat mendukung pembuatan sistem

sebagai solusi yang tepat. Proses pengumpulan data dilakukan melalui observasi, wawancara, dan metode kepustakaan [4].

2.6 Penyelesaian Masalah

Dalam tahapan analisis masalah, disampaikan bahwa data dan informasi memiliki peranan yang sangat penting dalam mendukung operasional produksi. Menyadari pentingnya aspek kerahasiaan dan keamanan data tersebut, penulis berinisiatif merancang aplikasi berbasis *web* untuk melindungi data penting dari potensi ancaman kebocoran atau manipulasi [6]. Aplikasi ini diharapkan mampu menjadi solusi yang efisien dan efektif dalam menjaga keamanan data agar tidak dapat dicuri atau dimanipulasi oleh pihak yang tidak berwenang.

2.7 Analisis Sistem

Pada tahap analisis data, sistem dirancang dalam penelitian ini mengelompokkan file berdasarkan periode tahun. File di kelompokkan berdasarkan periode tahun mempermudah pengelolaan dan pencarian data sesuai dengan periode tahun produksi.

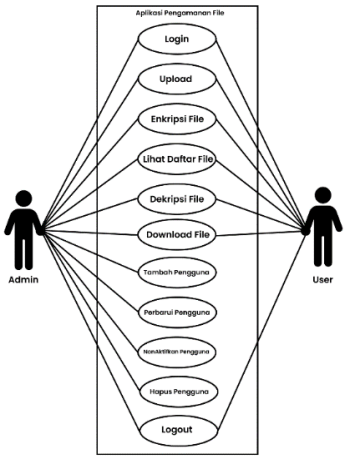
Analisis dilakukan terhadap implementasi algoritma kriptografi *Advanced Encryption Standard* (AES) 256-*bit* dengan *mode Counter* (CTR) [7]. Pada tahap enkripsi, *plaintext* (konten asli *file*) dikonversi menjadi *ciphertext* menggunakan kunci rahasia dan nilai *counter* yang meningkat secara berurutan. *Mode* CTR menghasilkan *keystream* melalui enkripsi blok *counter*, kemudian keystream tersebut digabungkan dengan data asli menggunakan operasi XOR untuk membentuk *ciphertext* [7]. Sementara itu, proses dekripsi dilakukan dengan prinsip serupa, yaitu mengenkripsi *counter* dan melakukan operasi XOR dengan *ciphertext* untuk memperoleh kembali *plaintext* aslinya.

Pada analisis fitur, penelitian ini merancang sebuah autentikasi pengguna berupa *security question* yang berfungsi sebagai verifikasi identitas pengguna sebelum dapat melakukan dekripsi dan mengunduh file. Fitur ini memuat pertanyaan-pertanyaan pribadi yang hanya diketahui oleh pengguna, sehingga dapat menjadi pengaman tambahan selain penggunaan kunci (*key*). Tujuannya adalah untuk mengatasi kendala pengguna yang mungkin kesulitan mengingat banyak password untuk setiap file yang diamankan. Dalam sistem ini, *security question* tidak menggantikan fungsi kunci enkripsi, melainkan digunakan untuk mengakses kunci yang telah disimpan secara terenkripsi di dalam *database*. Setelah proses verifikasi berhasil, barulah kunci tersebut digunakan untuk menjalankan dekripsi file yang diinginkan.

2.8 Perancangan Perangkat Lunak

Tahap ini merupakan proses perancangan sistem yang disusun berdasarkan hasil analisis yang telah diperoleh sebelumnya, dengan penekanan pada penerapan metode enkripsi dan dekripsi data sebagai bagian inti dari sistem dalam aplikasi. Perancangan dilakukan secara menyeluruh agar pengamanan data dapat berjalan sesuai kebutuhan pengguna. Pada Gambar 1, *use case diagram* menunjukkan interaksi antara dua aktor, yaitu admin dan user, terhadap sistem aplikasi pengamanan file, di mana masing-masing memiliki hak akses fitur sesuai peran dan tanggung jawabnya.

Fitur utama dalam sistem ini mencakup enkripsi *file*, dekripsi *file*, *upload* dan *download file*, yang menjadi bagian inti dari sistem dan dirancang secara menyeluruh untuk memastikan keamanan data berjalan baik dalam sistem aplikasi pengamanan *file* [8]. Selain itu, sistem ini juga dilengkapi fitur kelola user yang berisi fungsi tambah pengguna, perbarui pengguna, nonaktifkan pengguna, dan hapus pengguna, untuk memberikan kendali penuh kepada admin dalam mengatur pengguna yang dapat mengakses sistem aplikasi pengamanan file.



Gambar 1. *Use Case Diagram*

2.9 Implementasi

Pada tahap ini, dilakukan proses implementasi untuk mewujudkan rancangan sistem yang telah dibuat sebelumnya, yakni dengan menerapkan algoritma kriptografi AES 256-bit menggunakan mode CTR ke dalam bahasa pemrograman PHP. Langkah ini bertujuan untuk memastikan mekanisme enkripsi dan dekripsi dapat berfungsi dengan baik [9].

2.10 Kesimpulan

Kesimpulan dari tahap akhir ini menunjukkan bahwa penggunaan metode kriptografi AES 256-bit dalam *mode Counter* CTR berjalan efektif dan sesuai dalam memberikan perlindungan terhadap data catatan produksi milik PT. Stretchline. Berdasarkan hasil implementasinya, penerapan *Advanced Encryption Standard* (AES) 256-*bit* dalam *platform web* dapat mengamankan file secara maksimal sekaligus menjaga kerahasiaan dan keutuhan data [10].

3. HASIL DAN PEMBAHASAN

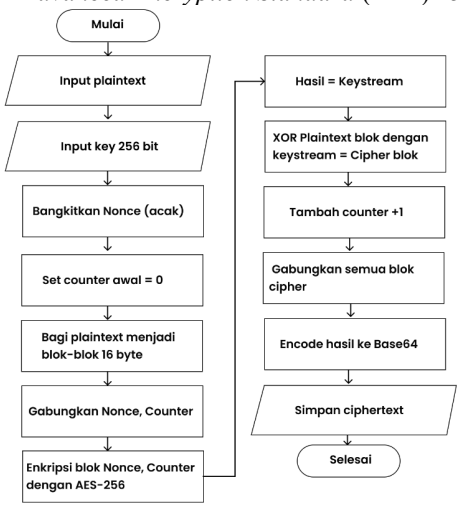
Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1 *Flowchart*

Flowchart merupakan sebuah diagram yang berfungsi untuk menggambarkan tahapan suatu proses secara visual. Diagram ini digunakan untuk menjelaskan langkah-langkah dalam sebuah proses aplikasi. Setiap langkah dalam proses tersebut divisualisasikan menggunakan simbol-simbol tertentu yang memiliki arti khusus. Sementara itu, hubungan atau alur antara satu langkah dengan langkah lainnya ditunjukkan melalui garis atau panah yang menghubungkan simbol-simbol.

3.1.1 *Flowchart* Enkripsi

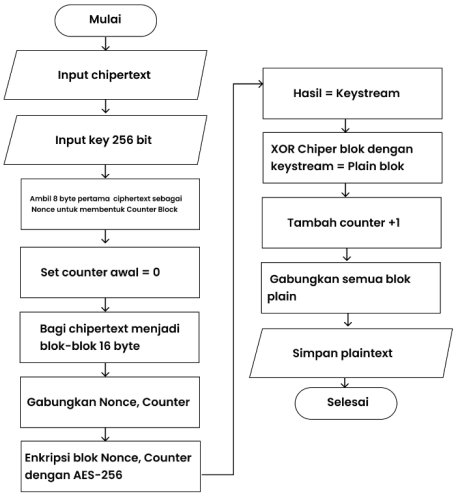
Pada gambar 2 *flowchart* enkripsi menampilkan tahapan proses enkripsi pada aplikasi pengamanan *file*, yang menggambarkan tahapan dari proses *Advanced Encryption Standard* (AES) 256-bit dengan *Counter mode* (CTR).



Gambar 2. *Flowchart* Enkripsi

3.1.2 *Flowchart* Dekripsi

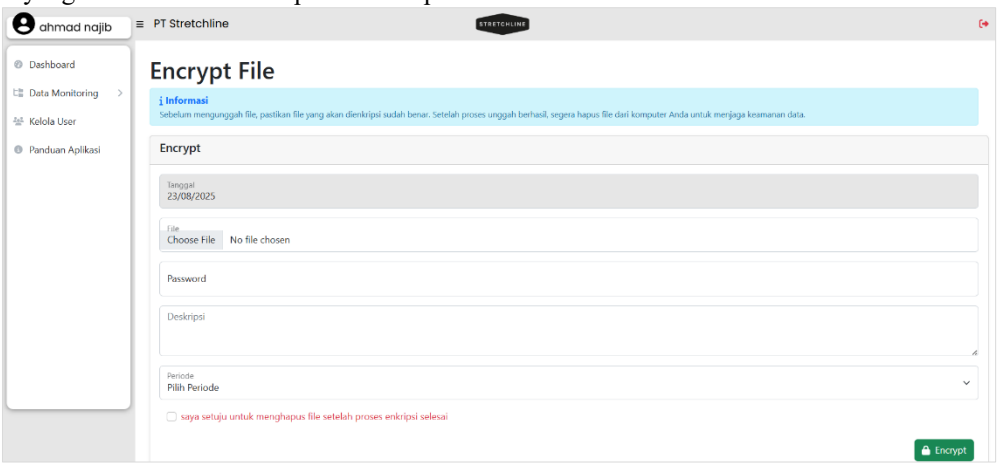
Pada gambar 3. *Flowchart* Dekripsi menampilkan tahapan proses enkripsi pada aplikasi pengamanan file, yang menggambarkan tahapan dari proses *Advanced Encryption Standard* (AES) 256-*bit* dengan *Counter mode* (CTR).



Gambar 3. *Flowchart* Dekripsi

3.2 Tampilan Layar Enkripsi *File*

Pada Gambar 4 tampilan layar halaman *encrypt file* merupakan tampilan halaman *encrypt file* pada aplikasi. Antarmuka ini muncul ketika pengguna memilih menu enkripsi, dengan fungsi utama untuk mengunggah *file*. Pada halaman ini tersedia *field* untuk *upload file*, *password*, deskripsi, *dropdown* periode, serta *checkbox* persetujuan yang harus diisi sebelum proses enkripsi dilakukan.



Gambar 4. Tampilan Layar Halaman *Encrypt File*

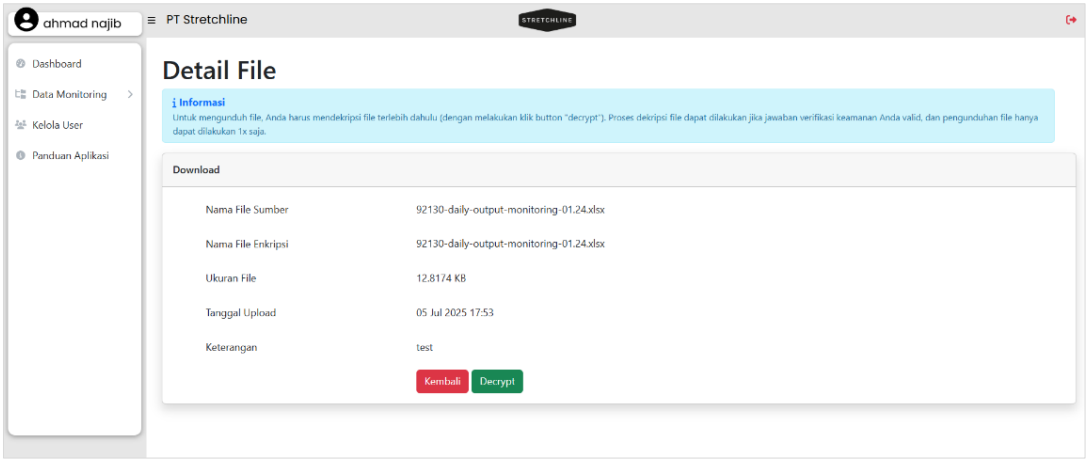
Halaman *Encrypt File* memungkinkan pengguna melakukan proses unggah sekaligus enkripsi file. Proses diawali dengan pengisian *file*, *password*, deskripsi, periode, dan persetujuan melalui *checkbox*, kemudian dilanjutkan dengan menekan tombol *upload*. Sistem akan memverifikasi persetujuan, memeriksa format serta ukuran *file*, dan apabila sesuai, sistem menjalankan tahapan enkripsi yang meliputi enkripsi kunci (*key*), pembacaan *file*, proses enkripsi, hingga penyimpanan file beserta kunci yang telah terenkripsi ke dalam *database*.

3.3 Tampilan Layar Dekripsi File

Proses dekripsi *file* pada aplikasi dilakukan dengan beberapa tahapan, mulai dari halaman *detail file, pop up* verifikasi keamanan, dan halaman *download file.*

3.3.1 Tampilan Layar *Detail File*

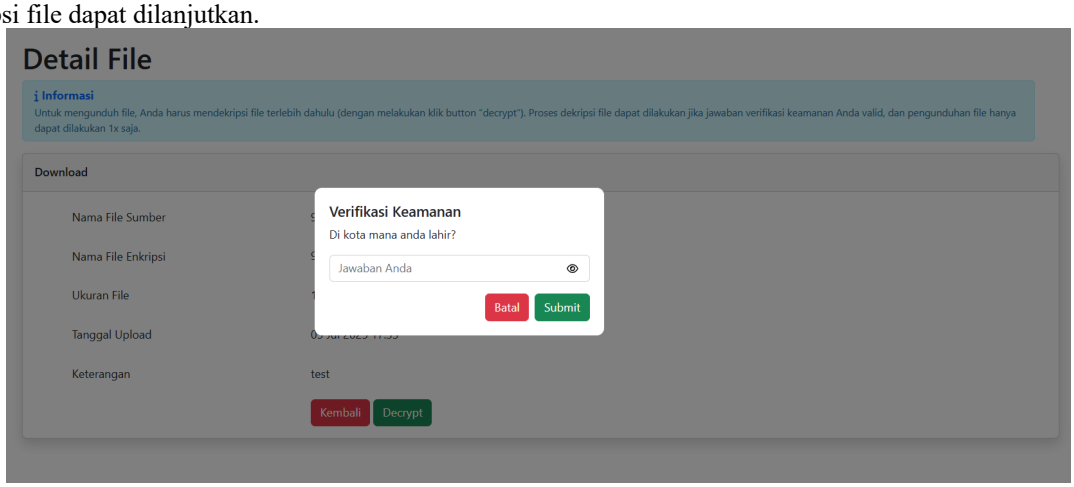
Pada Gambar 5 tampilan layar halaman *detail file* merupakan tampilan halaman *detail file* pada aplikasi. Halaman ini muncul ketika pengguna menekan tombol *Detail* pada halaman *View*. Melalui tampilan tersebut, pengguna dapat melakukan proses dekripsi file dengan memilih tombol *Decrypt*.



Gambar 5. Tampilan Layar Halaman *Detail File*

3.3.2 Tampilan *Pop Up* Verifikasi Keamanan

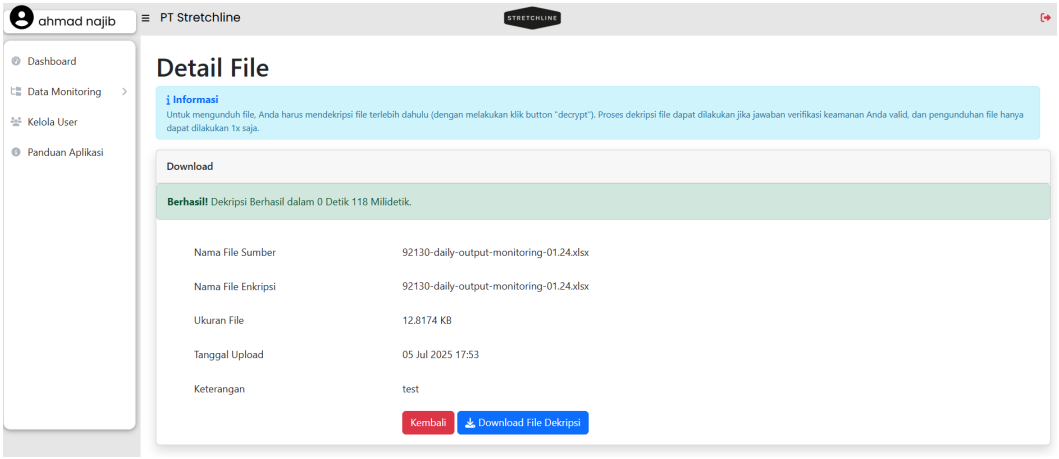
Pada Gambar 6 tampilan *pop up* verifikasi keamanan merupakan tampilan *pop up* verifikasi keamanan pada aplikasi. Tampilan ini muncul setelah pengguna menekan tombol *Decrypt*. Pada tahap ini, sistem menampilkan *pop-up* verifikasi yang mewajibkan pengguna memasukkan jawaban keamanan dengan benar sebelum proses dekripsi file dapat dilanjutkan.



Gambar 6. Tampilan Layar Verifikasi Keamanan

3.3.3 Tampilan Layar *Download File*

Pada Gambar 7 tampilan layar *download file* menampilkan tampilan layar halaman *download file* pada aplikasi. Halaman ini muncul setelah pengguna berhasil menyelesaikan proses dekripsi. Pada tampilan tersebut, sistem memberikan notifikasi bahwa dekripsi berhasil, dan pengguna dapat menekan tombol *Download File* untuk mengunduh berkas yang telah terdekripsi.



Gambar 7. Tampilan Layar *Download File*

3.4 Hasil Pengujian Enkripsi

Pengujian Enkripsi telah dilakukan untuk memastikan bahwa proses enkripsi berjalan dengan baik dan sesuai. Hasil dari pengujian enkripsi terdapat pada Table 1 hasil pengujian enkripsi.

Tabel 1. Hasil Pengujian Enkripsi

Nama *File*	Ukuran *File* Terenkripsi	Ukuran *File* Asli	Waktu Enkripsi (Milidetik)	Hasil
Daily Output Monitoring 01.23.xlsx	17,0898 Kb	12,7969 Kb	0,131	Berhasil
Daily Output Monitoring 02.23.xlsx	17,0703 Kb	12,7617 Kb	0,113	Berhasil
Daily Output Monitoring 03.23.xlsx	17,2500 Kb	12,9297 Kb	0,130	Berhasil
Daily Output Monitoring 04.23.xlsx	16,5820 Kb	12,4297 Kb	0,133	Berhasil
Daily Output Monitoring 05.23.xlsx	16,8906 Kb	12,6563 Kb	0,134	Berhasil
Daily Output Monitoring 01.24.xlsx	17,1055 Kb	12,8164 Kb	0,129	Berhasil
Daily Output Monitoring 02.24.xlsx	16,6484 Kb	12,4766 Kb	0,126	Berhasil

3.5 Hasil Pengujian Dekripsi

Pengujian Dekripsi telah dilakukan guna memastikan proses dekripsi berjalan dengan sesuai. Hasil dari pengujian dekripsi terdapat pada Table 2 hasil pengujian dekripsi.

Tabel 2. Hasil Pengujian Dekripsi

Nama *File*	Ukuran *File* Dekripsi	Ukuran *File* Asli	Waktu Dekripsi (Milidetik)	Hasil
Daily Output Monitoring 01.23.xlsx	12,7969 Kb	12,7969 Kb	0,67	Berhasil
Daily Output Monitoring 02.23.xlsx	12,7617 Kb	12,7617 Kb	0,67	Berhasil
Daily Output Monitoring 03.23.xlsx	12,9297 Kb	12,9297 Kb	0,74	Berhasil
Daily Output Monitoring 04.23.xlsx	12,4297 Kb	12,4297 Kb	0,68	Berhasil
Daily Output Monitoring 05.23.xlsx	12,6563 Kb	12,6563 Kb	0,72	Berhasil
Daily Output Monitoring 01.24.xlsx	12,8164 Kb	12,8164 Kb	0,67	Berhasil
Daily Output Monitoring 02.24.xlsx	12,4766 Kb	12,4766 Kb	0,65	Berhasil

4. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang dilakukan pada *data daily output monitoring* di PT Stretchline, dapat disimpulkan bahwa penerapan algoritma AES 256-bit dengan *mode Counter* (CTR) berjalan sesuai dengan tujuan awal penelitian. Sistem yang dibangun mampu mengamankan data dengan menjaga kerahasiaan serta mencegah akses tidak sah, sementara proses enkripsi dan dekripsi terbukti efektif dalam melindungi data secara optimal. Selain itu, aplikasi berbasis *web* yang dikembangkan mendukung berbagai format *file* umum dengan batas ukuran 10 MB, serta dilengkapi verifikasi pertanyaan keamanan yang memudahkan pengguna tanpa mengurangi tingkat perlindungan.

DAFTAR PUSTAKA

[1] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[2] H. Saputra Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Dokumen Pada Pt Varnion Technology Semesta," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 149–158, 2022.

[3] M. A. Saputra and P. F. Ariyani, "Implementasi Algoritma Kriptografi Advance Encryption Standard Dengan Counter Mode Untuk Implementations Of Advanced Encryption Standard Cryptography Algorithm With Counter Mode To Secure," vol. 2, no. September, pp. 314–323, 2023.

[4] R. Febrianto and S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-256) Untuk Mengamankan Database Penilaian Karyawan Pada KJPP NDR," *Bit (Fakultas Teknol. Inf. Univ. Budi Luhur)*, vol. 20, no. 1, p. 44, 2023, doi: 10.36080/bit.v20i1.2223.

[5] I. Jaka Prayudha, Saniman, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[6] N. A. kafa Kafa and D. V. S. Y. Sakti, "View of Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria.pdf," 2024.

[7] M. A. Saputra and P. F. Ariyani, "Implementasi Algoritma Kriptografi Advance Encryption Standard Dengan Counter Mode Untuk Implementations of Advanced Encryption Standard Cryptography Algorithm With Counter Mode To Secure," *Senafti*, vol. 2, no. September, pp. 314–323, 2023.

[8] D. A. Aldianto and A. W. Wibowo, "Tampilan IMPLEMENTASI KRIPTOGRAFI DENGAN AES 256 DAN MD 5 UNTUK MENGAMANKAN DATA DI PT. EBDESK TEKNOLOGI.pdf," 2023.

[9] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 1, no. 02, pp. 108–114, 2021, doi: 10.30998/jrkt.v1i02.4096.

[10] A. Aprizald, M. A. Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *JEKIN - J. Tek. Inform.*, vol. 2, no. 2, pp. 85–95, 2023, doi: 10.58794/jekin.v2i2.225.