JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

IMPLEMENTASI KRIPTOGRAFI AES-128 MODE CBC UNTUK PENGAMANAN FILE BERBASIS WEB PADA VIA COMPUTER

Danu Febri Andi Prasetyo[1*], Wahyu Pramusinto[2], M. Anif[3], Subandi[4]

[1,2,3,4] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia
email korespondensi: *danuprasetyo746@gmail.com*

(***received***: 01/03/2026, ***revised***: 23/03/2026, ***accepted***: 27/03/2026)

Abstrak

Via Computer merupakan penyedia layanan sewa laptop untuk perusahaan yang mengelola sejumlah data penting seperti data keuangan, data aset, dan kontrak kerja sama sewa yang tidak boleh diakses oleh sembarang pihak. Permasalahannya, berkas-berkas tersebut masih disimpan dalam format .docx, .xlsx, dan .pdf tanpa sistem keamanan berupa enkripsi, sehingga rentan terhadap akses tidak sah dan kebocoran informasi. Penelitian ini mengusulkan pengembangan aplikasi kriptografi berbasis web yang mampu melindungi data digital melalui proses enkripsi dan dekripsi menggunakan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 128-bit dan mode operasi Cipher Block Chaining (CBC), yang dilengkapi validasi kata sandi dan kontrol akses berbasis peran. Aplikasi dibangun menggunakan Next.js, TypeScript, dan PostgreSQL, kemudian diuji menggunakan metode *black box testing*. Hasil pengujian terhadap menunjukkan bahwa berkas yang telah dienkripsi tidak dapat dibuka maupun dibaca, sedangkan proses dekripsi berhasil mengembalikan berkas ke bentuk semula dengan isi dan ukuran yang identik dengan berkas asli, serta waktu proses yang tergolong cepat untuk mendukung kebutuhan operasional perusahaan.

Kata kunci: kriptografi, AES-128, Cipher Block Chaining, keamanan file, aplikasi web

IMPLEMENTATION OF AES-128 CBC MODE CRYPTOGRAPHY FOR WEB-BASED FILE SECURITY AT VIA COMPUTER

Abstract

Via Computer is a company that provides laptop rental services for corporate clients and manages confidential data such as financial records, asset data, and lease agreements that should only be accessible to authorized personnel. However, these files are still stored in .docx, .xlsx, and .pdf formats without any encryption-based security system, making the data vulnerable to unauthorized access and information leakage. This study proposes a web-based cryptography application capable of protecting digital data through encryption and decryption processes using the Advanced Encryption Standard (AES) algorithm with a 128-bit key length and Cipher Block Chaining (CBC) mode, equipped with password validation and role-based access control. The application was built using Next.js, TypeScript, and PostgreSQL, and evaluated using black box testing. Testing on files showed that encrypted files could not be opened or read, while the decryption process successfully restored the files to their original form with identical content and size, and processing time remained fast enough to support the company's daily operational needs.

Keywords: *cryptography, AES-128, Cipher Block Chaining, file security, web application*

1. Pendahuluan

Perkembangan teknologi informasi mendorong hampir seluruh organisasi memanfaatkan sistem digital dalam pengelolaan data, termasuk data yang bersifat rahasia dan sensitif [1]. Perlindungan terhadap data rahasia menjadi prioritas utama agar integritas informasi tetap terjaga dari ancaman pihak yang tidak berwenang, sehingga hanya pihak tertentu yang diperkenankan mengakses dokumen yang bersifat sensitif [2]. Via Computer, sebagai penyedia layanan sewa laptop untuk perusahaan, mengelola sejumlah dokumen penting seperti data keuangan, data aset, dan kontrak kerja sama sewa yang seharusnya hanya dapat diakses oleh pihak yang berwenang.

Permasalahannya, Via Computer masih menyimpan dokumen tersebut dalam format .docx, .xlsx, dan .pdf tanpa sistem keamanan berupa enkripsi (*plaintext*), sehingga dokumen rentan terhadap akses

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

tidak sah, penyalinan, maupun pencurian data oleh siapa pun yang memiliki akses ke komputer penyimpanan. Kondisi ini semakin berisiko karena belum tersedia aplikasi keamanan berbasis web yang praktis digunakan untuk melindungi arsip digital perusahaan.

Salah satu teknik yang banyak digunakan untuk melindungi kerahasiaan data adalah kriptografi. Kriptografi memungkinkan data diubah menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak memiliki hak akses melalui proses enkripsi, kemudian dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sesuai.

Penelitian-penelitian sebelumnya telah menerapkan kriptografi untuk mengamankan data, baik pada aplikasi berbasis *desktop* [3] maupun berbasis *mobile* [4], namun kedua pendekatan tersebut memerlukan instalasi dan konfigurasi pada setiap perangkat pengguna. Sebaliknya, aplikasi kriptografi berbasis web memungkinkan pengguna mengakses sistem keamanan cukup melalui peramban tanpa instalasi tambahan [5], [6], sehingga dinilai lebih fleksibel dan sesuai diterapkan pada lingkungan kerja Via Computer.

Berdasarkan permasalahan tersebut, penelitian ini mengimplementasikan pengembangan aplikasi kriptografi berbasis web yang menerapkan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 128-bit dan mode operasi Cipher Block Chaining (CBC). Pemilihan algoritma ini merujuk pada penelitian terdahulu yang menunjukkan bahwa AES memiliki performa enkripsi dan dekripsi yang lebih unggul dibandingkan algoritma simetris lain seperti RC4 [7], sementara mode CBC dinilai efektif menyamarkan pola data sehingga hasil enkripsi lebih sulit dianalisis meskipun data memiliki pola yang berulang [8], [9].

Tujuan penelitian ini adalah merancang dan membangun aplikasi kriptografi berbasis web yang memudahkan pegawai Via Computer mengamankan dokumen tanpa perlu instalasi perangkat lunak tambahan, serta menerapkan algoritma AES-128 mode CBC untuk melindungi data digital dari akses yang tidak berwenang melalui mekanisme enkripsi dan dekripsi berbasis kata sandi. Penelitian ini diharapkan memberikan perlindungan terhadap kerahasiaan isi data digital Via Computer serta menyediakan sarana pengamanan data yang praktis dan efisien melalui *platform* berbasis web.

2. Tinjauan Literatur

Kriptografi merupakan bidang ilmu yang mempelajari cara melindungi informasi dengan mengubah data asli (*plaintext*) menjadi bentuk yang sulit dipahami oleh pihak yang tidak berhak, guna menjaga kerahasiaan, keutuhan, dan keaslian data [10]. Berdasarkan mekanisme kuncinya, kriptografi dibedakan menjadi kriptografi simetris yang menggunakan satu kunci untuk proses enkripsi dan dekripsi, serta kriptografi asimetris yang menggunakan sepasang kunci berbeda. Kriptografi simetris dinilai lebih cepat dan efisien sehingga umum digunakan untuk mengamankan berkas berukuran besar [7].

Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris yang ditetapkan oleh National Institute of Standards and Technology (NIST) sebagai standar enkripsi modern, bekerja pada blok data berukuran 128-bit dengan pilihan panjang kunci 128, 192, atau 256-bit [10]. Varian AES-128 menggunakan 10 putaran transformasi yang terdiri atas tahap SubBytes, ShiftRows, MixColumns, dan AddRoundKey [11], di mana setiap putaran menyamarkan dan menyebarkan data sehingga *ciphertext* yang dihasilkan sulit dianalisis tanpa kunci yang sah [7]. Untuk memperkuat keamanan pada tingkat blok data, penelitian ini menerapkan mode operasi Cipher Block Chaining (CBC), yaitu setiap blok *plaintext* terlebih dahulu dioperasikan XOR dengan blok *ciphertext* hasil enkripsi sebelumnya, atau dengan Initialization Vector (IV) pada blok pertama, sebelum dienkripsi, sehingga perubahan kecil pada satu blok memengaruhi seluruh blok berikutnya dan pola data asli menjadi tersamar [8], [9].

Sejumlah penelitian terdahulu telah menerapkan algoritma AES untuk melindungi data dan dokumen digital pada berbagai platform

Penelitian [3], [5], [6] menerapkan AES pada sistem berbasis *desktop* dan web serta menunjukkan bahwa algoritma tersebut efektif menjaga kerahasiaan berkas. Penelitian [7], [8] lebih berfokus pada evaluasi kinerja dan perbandingan algoritma, di mana AES-128 dengan mode CBC terbukti memberikan perlindungan pola data yang lebih baik dibandingkan mode operasi lain. Penelitian [9], [12] menekankan penerapan AES pada pengamanan dokumen digital secara umum, sedangkan

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

penelitian [4], [1] menyoroti pentingnya perlindungan data pribadi di tengah pesatnya adopsi teknologi digital.

Meskipun demikian, sebagian besar penelitian tersebut belum secara khusus menerapkan AES-128 mode CBC pada sistem pengamanan file berbasis web yang digunakan langsung untuk kebutuhan operasional suatu instansi, serta belum ada pembatasan hak akses per pengguna. Kesenjangan inilah yang menjadi dasar pengembangan pada penelitian ini, yaitu membangun sistem kriptografi berbasis web dengan algoritma AES-128 mode CBC yang dilengkapi kontrol akses berbasis peran (*role-based access control*) untuk meningkatkan keamanan dan kerahasiaan data digital pada Via Computer.

3. Metode Penelitian

Data yang digunakan dalam penelitian ini adalah data uji (*dummy*) yang memiliki bentuk dan ciri mirip dengan data operasional Via Computer, yaitu sepuluh berkas dengan format .docx, .xlsx, dan .pdf yang merepresentasikan data keuangan, data aset, dan kontrak sewa, dengan ukuran berkas berkisar antara 30,84 KB hingga 511,81 KB.

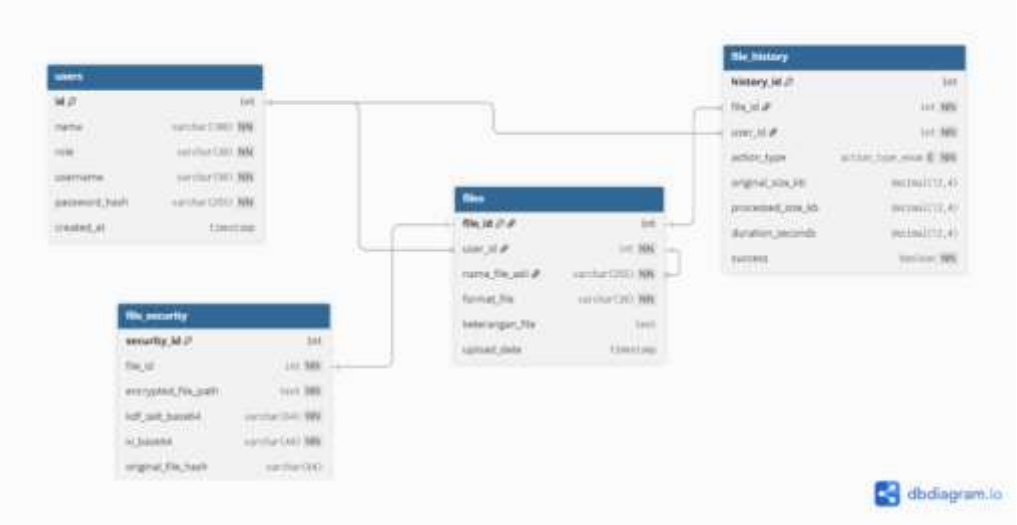
Proses enkripsi diawali dengan pemeriksaan panjang kunci dan Initialization Vector (IV) yang masing-masing harus berukuran 16 *byte* sesuai standar AES-128. Setelah parameter dinyatakan valid, sistem melakukan ekspansi kunci untuk menghasilkan round key dari putaran ke-0 hingga ke-10, kemudian *plaintext* diberi padding PKCS7 agar panjangnya menjadi kelipatan 16 byte. Setiap blok *plaintext* diproses dengan mode CBC: blok pertama dioperasikan XOR dengan IV, sedangkan blok berikutnya dioperasikan XOR dengan *ciphertext* blok sebelumnya, sebelum dienkripsi menggunakan AES-128 sebanyak 10 putaran transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey, sebagaimana diilustrasikan pada Gambar 1. Proses dekripsi dilakukan dengan alur kebalikannya, yaitu ciphertext didekripsi terlebih dahulu menggunakan AES-128, kemudian hasilnya dioperasikan XOR dengan IV atau *ciphertext* blok sebelumnya untuk memperoleh *plaintext* .

Gambar 1. Proses Enkripsi AES-128 Mode CBC

Aplikasi dibangun menggunakan bahasa pemrograman TypeScript pada framework Next.js berbasis React, dengan antarmuka pengguna menggunakan Tailwind CSS dan basis data PostgreSQL. Basis data dirancang dengan empat tabel utama, yaitu *users* untuk menyimpan kredensial dan peran pengguna, files untuk metadata berkas yang diunggah, *file_security* untuk menyimpan parameter keamanan seperti jalur berkas terenkripsi, salt, dan IV, serta *file_history* untuk mencatat riwayat setiap

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

proses enkripsi dan dekripsi. Struktur basis data yang digunakan pada aplikasi ini bisa dilihat pada LRS gambar 2.



Gambar 2. Logical Record Structure (LRS)

Sistem menerapkan pembatasan hak akses berbasis peran, yaitu Super Admin yang dapat mengelola akun pengguna selain melakukan enkripsi dan dekripsi, serta Staff yang hanya dapat melakukan enkripsi, dekripsi, dan melihat riwayat aktivitasnya sendiri. Setiap berkas yang dienkripsi hanya dapat didekripsi oleh pengguna yang mengunggah berkas tersebut, sehingga kerahasiaan data antarpengguna tetap terjaga.

Pengujian sistem dilakukan menggunakan metode *black box testing* yang mengevaluasi fungsi sistem berdasarkan *input* dan *output* tanpa melihat struktur kode internal. Pengujian mencakup tujuh skenario, yaitu proses enkripsi berbagai format berkas, proses dekripsi dengan kata sandi benar dan salah, pengujian integritas berkas hasil dekripsi terhadap berkas asli, pengujian hak akses antarpengguna, pengujian fitur kelola pengguna yang hanya dapat diakses Super Admin, serta pengujian kinerja waktu proses enkripsi dan dekripsi terhadap sepuluh berkas uji.

4. Hasil dan Pembahasan

Pengujian proses enkripsi menunjukkan bahwa sistem berhasil mengenkripsi berkas berformat .docx, .xlsx, dan .pdf, serta menolak proses apabila berkas atau kata sandi belum diisi. Pada pengujian dekripsi, sistem berhasil mengembalikan berkas ke bentuk aslinya apabila kata sandi yang dimasukkan sesuai dengan kata sandi saat proses enkripsi, dan menolak proses dekripsi disertai pesan kesalahan apabila kata sandi yang dimasukkan tidak sesuai. Hasil perbandingan antara berkas asli dan berkas hasil dekripsi menunjukkan bahwa isi, format, dan ukuran berkas identik, yang membuktikan bahwa algoritma AES-128 mode CBC tidak menyebabkan kehilangan maupun perubahan data selama proses enkripsi dan dekripsi berlangsung.

Pengujian hak akses menunjukkan bahwa berkas yang dienkripsi oleh seorang pegawai hanya dapat dilihat dan didekripsi oleh akun pegawai tersebut, sedangkan akun pegawai lain baik dengan peran Staff maupun Super Admin tidak dapat mengakses berkas tersebut. Pengujian fitur kelola pengguna menunjukkan bahwa menu tersebut hanya dapat diakses oleh peran Super Admin, sementara peran Staff tidak dapat melihat maupun mengakses menu tersebut. Seluruh skenario pengujian *black box testing* yang mencakup 13 kasus uji dinyatakan berhasil, sebagaimana dirangkum pada Tabel 1.

Tabel 1. Ringkasan Hasil Pengujian Black Box Testing

No	Skenario Pengujian	Hasil
1	Enkripsi berkas .docx, .xlsx, dan .pdf	Berhasil; berkas menjadi ciphertext berekstensi .enc

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

No	Skenario Pengujian	Hasil
2	Enkripsi tanpa berkas / tanpa kata sandi	Berhasil ditolak dengan pesan kesalahan
3	Dekripsi dengan kata sandi benar	Berhasil; berkas kembali ke bentuk asli
4	Dekripsi dengan kata sandi salah	Berhasil ditolak; dekripsi gagal
5	Integritas berkas asli vs. hasil dekripsi	Isi, format, dan ukuran berkas identik
6	Hak akses antarpengguna	Berkas hanya dapat diakses oleh pengunggah
7	Menu kelola pengguna	Hanya dapat diakses oleh peran Super Admin
8	Tambah, reset, dan hapus akun pengguna	Seluruh fungsi berjalan sesuai harapan

Pengujian kinerja terhadap sepuluh berkas uji dengan ukuran 30,84 KB hingga 511,81 KB menunjukkan bahwa waktu proses enkripsi berkisar antara 0,028 hingga 0,716 detik, sedangkan waktu proses dekripsi berkisar antara 0,066 hingga 1,289 detik, sebagaimana disajikan pada Tabel 2. Hasil ini menunjukkan bahwa waktu proses meningkat seiring bertambahnya ukuran berkas, namun secara keseluruhan waktu pemrosesan masih tergolong cepat untuk kebutuhan operasional sehari-hari. Waktu dekripsi secara konsisten sedikit lebih lama dibandingkan waktu enkripsi, yang disebabkan oleh proses tambahan berupa pembacaan parameter keamanan (IV dan *salt*) serta validasi integritas berkas melalui hash sebelum data dikembalikan ke bentuk asli.

Tabel 2. Hasil Pengujian Kinerja Proses Enkripsi dan Dekripsi

No	Format	Ukuran (KB)	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	.xlsx	511,81	0,716	1,289
2	.xlsx	354,16	0,425	1,131
3	.xlsx	30,84	0,028	0,066
4	.pdf	56,21	0,070	0,176
5	.pdf	56,85	0,105	0,137
6	.docx	121,05	0,102	0,501
7	.docx	121,84	0,135	0,325
8	.pdf	53,55	0,047	0,122
9	.pdf	43,37	0,054	0,105
10	.pdf	42,17	0,061	0,109

Untuk menggunakan ini user harus melakukan login menggunakan username dan password untuk menggunakan aplikasi ini. Tampilan halaman login bisa dilihat pada gambar 3.

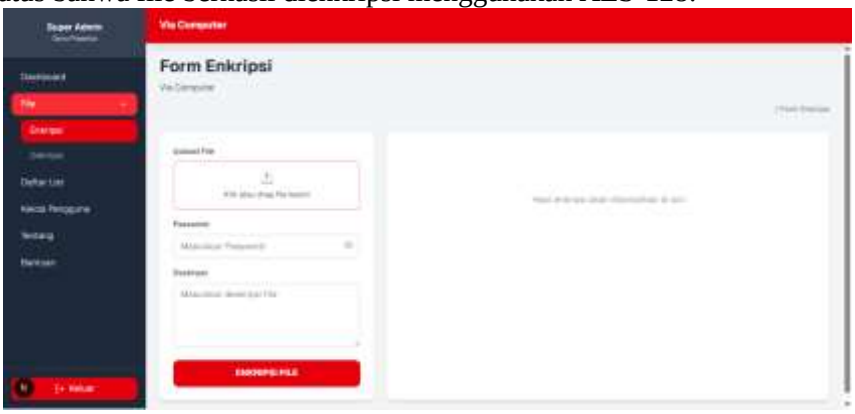
Gambar 3. Tampilan Halaman Login

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)

Gambar 4 menunjukkan halaman dashboard untuk pengguna dengan *role* Super Admin yang tampil setelah sistem berhasil memverifikasi *role* saat login. Antarmuka ini menampilkan statistik jumlah pengguna dan total aktivitas enkripsi serta dekripsi di sistem. Di sisi kiri terdapat menu navigasi yang memungkinkan Super Admin mengawasi lalu lintas sistem dan mengakses fitur khusus seperti "Kelola Pengguna" agar keamanan dan pengelolaan data tetap terjaga dan berada di bawah pengawasan pihak yang berwenang.

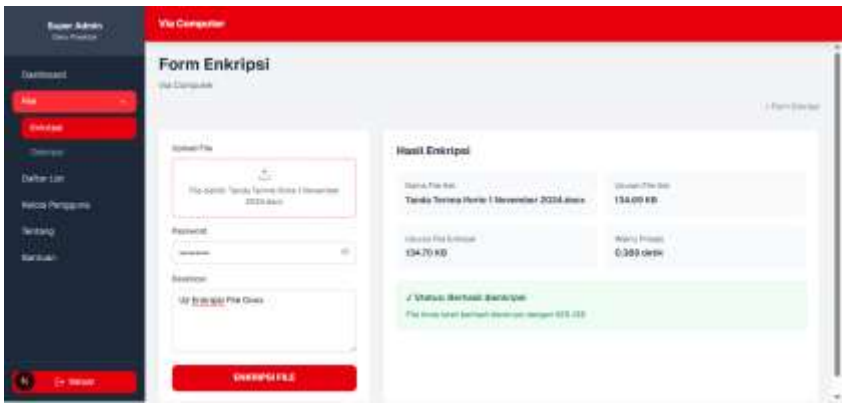
Gambar 4. Tampilan dashboard

Pada tampilan layar halaman enkripsi pada gambar 5 yang terdiri dari fitur seperti file, *password*, dan kolom deskripsi.. Setelah super admin memilih file, mengisi *password*, dan menekan tombol Enkripsi File, sistem memproses data dan menampilkan informasi seperti pada gambar 6 yaitu menampilkan hasil enkripsi, meliputi nama file asli, ukuran file sebelum dan sesudah enkripsi, waktu proses, serta status bahwa file berhasil dienkripsi menggunakan AES-128.



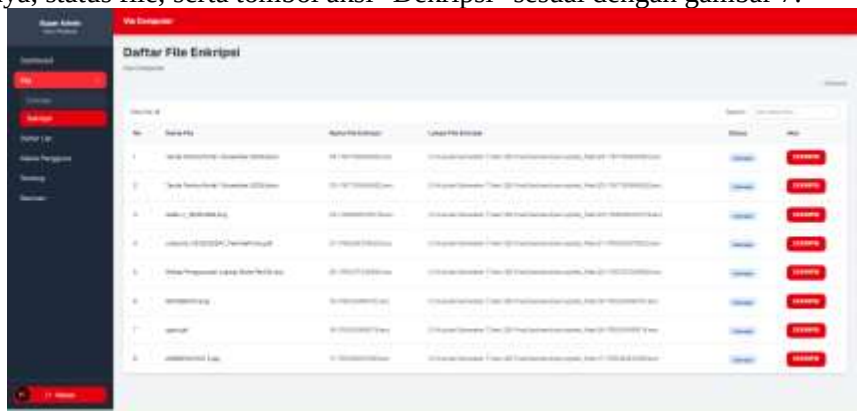
Gambar 5. Tampilan halaman enkripsi

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)



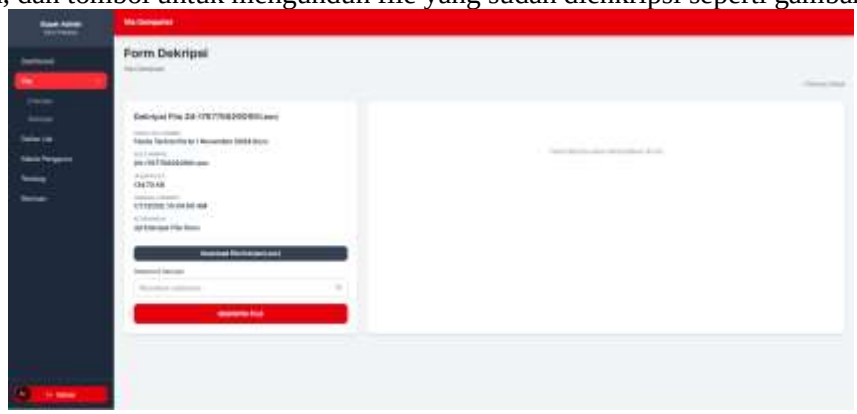
Gambar 6. Tampilan halaman hasil enkripsi

Di tampilan layar halaman dekripsi menampilkan daftar file yang sudah dienkripsi, sistem menampilkan semua file lengkap dengan nama file asli, nama file yang sudah dienkripsi, tempat penyimpanannya, status file, serta tombol aksi "Dekripsi" sesuai dengan gambar 7.



Gambar 7. Tampilan halaman daftar file enkripsi

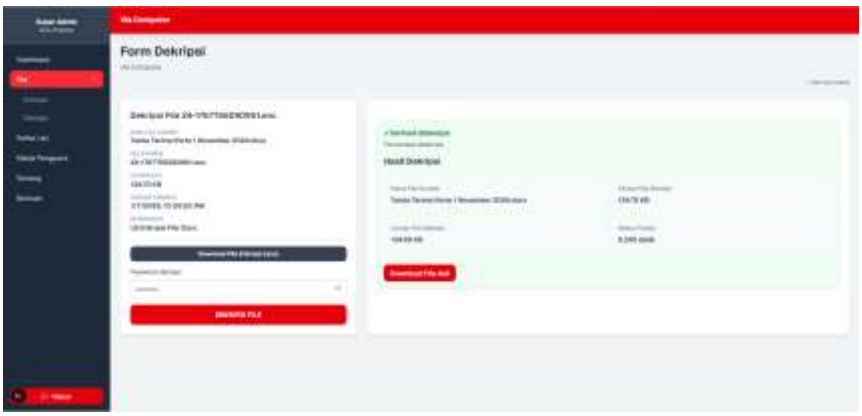
Saat pengguna mengklik tombol aksi “Dekripsi“, sistem akan membuka halaman Form Dekripsi yang menampilkan informasi detail tentang file yang sudah dienkripsi, seperti nama asli file, ukuran file, tanggal upload, dan tombol untuk mengunduh file yang sudah dienkripsi seperti gambar 8.



Gambar 8. Tampilan halaman form dekripsi

Selanjutnya, pengguna diminta memasukkan *password* yang sama dengan password yang digunakan saat proses enkripsi. Jika *password* yang dimasukkan benar, sistem akan memulai proses dekripsi, menampilkan informasi hasil dekripsi, ukuran file setelah didekripsi, durasi proses, serta memberikan tombol untuk mengunduh kembali file aslinya seperti gambar 9.

JURNAL TELEMATIKA MKOM
Volume 18, Nomor 1, Maret, 2026
Halaman 19-27
ISSN: 2527-9033 (*online*), 2085-725X (cetak)



Gambar 9. Tampilan halaman dekripsi berhasil

5. Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa aplikasi kriptografi berbasis web dengan algoritma AES-128 mode CBC berhasil dikembangkan menggunakan Next.js, TypeScript, dan PostgreSQL, serta mampu membantu pegawai Via Computer mengamankan berkas .docx, .xlsx, dan .pdf. Algoritma AES-128 mode CBC terbukti efektif menyamarkan data digital sehingga berkas yang telah dienkripsi tidak dapat dibaca oleh pihak yang tidak berwenang, sementara proses dekripsi mampu mengembalikan berkas ke bentuk asli dengan isi dan ukuran yang identik. Mekanisme validasi kata sandi dan Initialization Vector yang berbeda pada setiap proses enkripsi, dikombinasikan dengan kontrol akses berbasis peran, memastikan hanya pegawai pengunggah berkas yang dapat mendekripsi berkas miliknya sendiri. Hasil pengujian *black box testing* menunjukkan seluruh fitur utama sistem berjalan sesuai dengan yang diharapkan, dan hasil pengujian kinerja menunjukkan bahwa waktu proses enkripsi dan dekripsi masih tergolong cepat untuk mendukung kebutuhan operasional Via Computer sehari-hari.

Daftar Pustaka

[1] T. A. Berutu, D. L. R. Sigalingging, G. K. V. Simanjuntak, and F. Siburian, "Pengaruh Teknologi Digital terhadap Perkembangan Bisnis Modern," *Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi*, vol. 2, no. 3, pp. 358–370, 2024.

[2] A. Faisal and N. Yulian Yusuf, "Tinjauan Yuridis Tindak Pidana Penyalahgunaan Data Pribadi pada Kasus Kredit Fiktif," *Jurnal Sultra Review*, vol. 6, no. 2, 2024.

[3] Y. J. El Anwar, R. Habibi, and N. Riza, "Penerapan Metode Kriptografi AES untuk Mengamankan File Dokumen," *Jurnal Tekno Insentif*, vol. 16, no. 2, pp. 92–104, 2022.

[4] R. Milafebina, I. Putra Lesmana, and M. R. Syailendra, "Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerce di Indonesia," *Jurnal Teknologi dan Manajemen*, 2024.

[5] I. Priambudi, "Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 6, no. 1, p. 22, 2023.

[6] F. N. Syahrani and W. Pramusinto, "Implementasi Algoritma Kriptografi AES 128 dan Vigenere Cipher pada Coffee Shop NgoPi dengan Aplikasi Berbasis Web," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), vol. 3, no. 2, p. 74, Sep. 2024.

[7] R. N. Fitriana and Djuniadi, "Analisis Perbandingan Algoritma AES dan RC4 pada Enkripsi dan Dekripsi Data Teks Berbasis CrypTool 2," *Systemic: Information System and Informatics Journal*, vol. 7, no. 2, pp. 1–7, 2022.

[8] G. Putra Riatma, B. Satya Dian Nugraha, and A. Nur Rahmanto, "Performance Evaluation and the Impact of File Size on Various AES Encryption Modes," *Journal of Telecommunication Network*, vol. 15, no. 2, 2025.

[9] F. M. Kaaffah, N. Nugroho, D. Nurnaningsih, and H. Harriansyah, "Sistem Enkripsi Dokumen Digital Melalui Kombinasi AES-128 dan Hashing SHA-256 Berbasis Salt," *Jurnal Ilmiah FIFO*, vol. 17, no. 1, p. 78, 2025.

[10] A. Suranta, D. Virgian, and S. Y. Sakti, "Penerapan Algoritma AES (Advanced Encryption Standard) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 1, pp. 1–10, 2022.

[11] M. A. Jayana, D. Rafael, and A. A. Rahman, "Implementasi Pengamanan Data Pengarsipan dengan Metode Algoritma Kriptografi AES: Studi Kasus pada Bank BJB KCP Pasteur Bandung," n.d.

[12] A. Rahayu, G. Abdillah, and H. Ashaury, "Pengamanan Menggunakan Algoritma AES (Advanced Encryption Standard) dan BCrypt (Blowfish Crypt) pada File Dokumen," *Jurnal Mahasiswa Teknik Informatika*, vol. 8, no. 6, 2024.