Pengembangan Sistem Keamanan Data Menggunakan Enkripsi AES-128 Berbasis Web: Studi Kasus pada Aplikasi NetCrypt

Firman Yosef Rangga Neonbeni[1*], Jefriyanto Opat[2], Aloysius Yudha Devan Herianto Opat[3], Julinto Golbertus Soares[4]
[1,2,3,4]Program Studi Teknologi Informasi, Fakultas Pertanian, Sains dan Kesehatan, Universitas Timor, Kefamenanu, Indonesia

E-mail: neonbenijo@gmail.com

ABSTRACT

The rapid advancement of information technology has increased the demand for robust data security systems to prevent unauthorized access to sensitive information. This study aims to design and develop a web-based system capable of performing data encryption and decryption using the Advanced Encryption Standard (AES) algorithm with a 128-bit key length. The application, named NetCrypt, is designed to secure important data by converting original information into an encrypted format, making it unreadable to unauthorized parties. The development process employs the Rapid Application Development (RAD) methodology, which allows for fast and flexible system development through iterative prototyping. Based on the testing results, the system successfully performs encryption and decryption operations and effectively maintains the confidentiality of data from external access. Therefore, NetCrypt has the potential to be an effective data security solution for web applications that require a high level of privacy protection.

Keywords: Data Security, Encryption, AES-128 (Advanced Encryption Standard 128-bit), Web Application, Rapid Application Development.

ABSTRAK

Pesatnya kemajuan teknologi informasi mendorong kebutuhan akan sistem keamanan data yang kuat guna mencegah akses tidak sah terhadap informasi sensitif. Penelitian ini bertujuan untuk merancang dan membangun sebuah sistem berbasis web yang mampu melakukan proses enkripsi dan dekripsi data dengan memanfaatkan algoritma *Advanced Encryption Standard* (AES) berukuran kunci 128-bit. Aplikasi ini dinamakan NetCrypt, yang berfungsi untuk mengamankan data dengan cara mengonversi informasi asli menjadi format terenkripsi, sehingga tidak mudah dipahami oleh pihak yang tidak berkepentingan. Dalam proses pengembangannya, digunakan metode *Rapid Application Development* (RAD) karena pendekatan ini memungkinkan pengembangan sistem secara cepat melalui pembuatan prototipe

Article History
Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

secara berulang dan fleksibel. Berdasarkan hasil pengujian, sistem mampu menjalankan proses enkripsi dan dekripsi secara optimal serta menjaga kerahasiaan data dari akses luar. Oleh karena itu, NetCrypt berpotensi menjadi solusi efektif dalam menjaga keamanan data pada aplikasi web yang membutuhkan perlindungan privasi tinggi.

Kata Kunci: **Keamanan Data, Enkripsi, AES-128, Aplikasi Web, RAD.**

1. PENDAHULUAN

Pengembangan teknologi informasi yang pesat memperkenalkan sejumlah kemudahan dalam menyimpan, memproses, dan menukar data. Pertumbuhan ini juga disertai peningkatan ancaman terhadap keamanan data, terutama pada sistem berbasis web yang terhubung langsung ke jaringan internet. Akses terlarang, pencurian data, dan manipulasi informasi menjadi ancaman nyata yang mengganggu privasi dan integritas data. Dalam konteks serangan terhadap sistem enkripsi, peretas sering kali berusaha menebak atau membongkar kunci enkripsi guna menciptakan algoritma atau kode mereka sendiri untuk membobol sistem. Setelah kunci berhasil dibuka, mereka dapat menyisipkan kode berbahaya ke dalam sistem korban guna memantau aktivitas dan mengakses data secara diam-diam (Febrian et al., 2020).

Salah satu cara paling efektif untuk menjaga kerahasiaan data adalah dengan menggunakan algoritma kriptografi. *Advanced Encryption Standard* (AES) merupakan salah satu algoritma simetris yang banyak digunakan karena tingkat keamanannya yang tinggi dan efisiensinya. Algoritma AES dipilih karena mampu memberikan perlindungan yang andal dalam proses pertukaran informasi. Dalam penelitian ini, dilakukan juga pengujian terhadap file dokumen untuk mengevaluasi kecepatan proses enkripsi dan dekripsi, sehingga dapat diketahui seberapa efisien algoritma ini saat diterapkan dalam konteks aplikasi web. Dalam penelitian ini digunakan varian AES dengan kunci sepanjang 128-bit karena selain aman, juga efisien untuk diterapkan dalam aplikasi web (Prameshwari & Sastra, 2018).

Untuk menjawab kebutuhan akan sistem keamanan data yang handal, dikembangkan sebuah aplikasi web bernama NetCrypt. Aplikasi ini memungkinkan pengguna melakukan proses enkripsi dan dekripsi secara mandiri melalui antarmuka web yang sederhana dan mudah digunakan. Pengembangan aplikasi ini menggunakan metode *Rapid Application Development* (RAD), yang memungkinkan sistem dibangun dalam waktu singkat tanpa mengabaikan kebutuhan pengguna. Metode RAD sendiri merupakan salah satu pendekatan dalam siklus hidup pengembangan sistem (SDLC) yang menekankan proses pembangunan perangkat lunak secara berurutan dan terstruktur, namun dengan durasi pengembangan yang lebih cepat (Bukifan et al., 2025).

Tujuan dari penelitian ini adalah untuk merancang dan membangun sistem keamanan data berbasis web menggunakan algoritma AES-128, serta menguji efektivitasnya dalam melindungi data dari akses tidak sah. Beberapa penelitian terdahulu yang membahas tentang metode enkripis AES-128, salah satunya menunjukkan bahwa keamanan informasi merupakan aspek penting dalam jaringan internet, sehingga algoritma ini banyak dimanfaatkan untuk melindungi data dari ancaman penyadapan. Implementasinya umumnya diterapkan pada file dokumen seperti PDF, DOC, dan TXT, serta diuji untuk menilai kecepatan proses enkripsi dan dekripsinya

(Prameshwari & Sastra, 2018). Penelitian lain juga menyebutkan bahwa algoritma AES-128 digunakan untuk mengamankan dokumen penting pada PT Gunung Geulis Elok Abadi yang belum memiliki sistem perlindungan data. Pengujian terhadap 20 file menunjukkan bahwa proses enkripsi dan dekripsi dengan algoritma ini memiliki waktu rata-rata masing-masing 12.769 milidetik dan 18.075 milidetik (Ignasius & Shaka Yudha Sakti, 2022). Hasil penelitian lain juga menyebutkan bahwa penerapan algoritma AES-128 terbukti efektif dalam melindungi data, mencegah akses yang tidak sah, serta meningkatkan kepercayaan pengguna terhadap sistem. Melalui proses enkripsi ini, risiko kebocoran informasi dapat ditekan, sehingga keamanan data, seperti pada lingkungan sekolah, menjadi lebih terjaga (Mutiara et al., 2025). Penelitian lain juga menunjukkan bahwa AES-128-CBC berhasil mencegah akses tidak sah karena dokumen yang dienkripsi tetap tidak dapat dibaca tanpa kunci dekripsi yang benar (Fahlevvi et al., 2025).

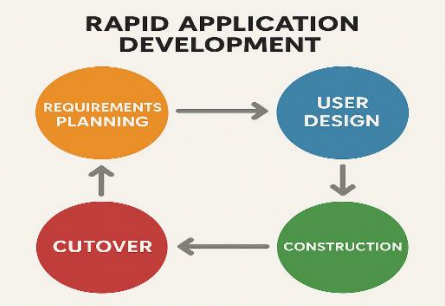
2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan metode *Rapid Application Development* (RAD), yang merupakan salah satu model pengembangan perangkat lunak yang menekankan pada kecepatan, fleksibilitas, dan keterlibatan pengguna secara langsung dalam setiap siklus pengembangan. Metode ini dipilih karena mampu mempercepat proses pengembangan aplikasi dalam waktu yang lebih singkat dibandingkan dengan metode tradisional seperti *Waterfall*, namun tetap mempertahankan kualitas dan relevansi terhadap kebutuhan pengguna (Nurman Hidayat & Kusuma Hati, 2021).

RAD terdiri dari beberapa fase iteratif yang memungkinkan tim pengembang untuk merancang prototipe, mendapatkan umpan balik langsung dari pengguna, dan memperbaiki sistem secara cepat sebelum memasuki tahap implementasi akhir. Dalam konteks pengembangan aplikasi NetCrypt, metode RAD terdiri dari empat tahapan utama sebagai berikut:

1) Perencanaan Kebutuhan

Requirements Planning merupakan tahap awal di mana penulis melakukan studi literatur untuk mengidentifikasi permasalahan yang relevan, khususnya terkait kebutuhan akan keamanan data pada aplikasi web. Setelah permasalahan ditemukan, penulis menganalisis kebutuhan sistem yang akan dikembangkan, yaitu aplikasi enkripsi dan dekripsi data bernama NetCrypt. Proses perencanaan ini mencakup penentuan fitur utama serta pemilihan tools pengembangan, yaitu *Visual Studio Code* sebagai editor dan *XAMPP* sebagai server lokal pendukung.



Gambar 1. Metode RAD

2) Desain Pengguna

Tahap desain sistem dilakukan oleh pengembang sebagai langkah lanjutan setelah perencanaan kebutuhan selesai, dengan tujuan agar sistem yang dikembangkan dapat benar-benar menjawab permasalahan yang telah diidentifikasi sebelumnya. Pada tahap ini, penulis merancang struktur dan alur kerja aplikasi secara menyeluruh agar sesuai dengan fungsi yang diharapkan. Proses perancangan mencakup penyusunan tampilan antarmuka dan pengelompokan fitur-fitur utama yang akan diimplementasikan dalam aplikasi NetCrypt. Beberapa menu inti yang dirancang antara lain menu enkripsi, yang digunakan untuk mengubah data asli menjadi format terenkripsi; menu dekripsi, untuk mengembalikan data terenkripsi ke bentuk semula; serta menu arsip data, yang menampilkan daftar file yang telah melalui proses enkripsi dan dekripsi. Desain ini disusun agar pengguna dapat berinteraksi dengan sistem secara intuitif, efisien, dan aman.

3) Tahap Konstruksi

Tahapan desain yang telah diselesaikan kemudian dilanjutkan ke tahap konstruksi, di mana pengembang mulai membangun sistem sesuai spesifikasi rancangan. Pada tahap ini, penulis mulai membangun aplikasi NetCrypt dengan menulis kode program menggunakan *Visual Studio Code* sebagai editor utama dan *XAMPP* sebagai server lokal untuk menjalankan aplikasi berbasis web. Proses pengembangan difokuskan pada implementasi fitur-fitur utama, seperti enkripsi dan dekripsi data menggunakan algoritma AES-128, serta penyimpanan hasil enkripsi dan dekripsi dalam format yang aman dan terstruktur. Tahap ini bertujuan untuk menghasilkan aplikasi web yang dapat digunakan oleh pengguna untuk mengamankan data penting dari ancaman akses yang tidak sah.

4) Tahap Implementasi

Setelah pengembangan aplikasi NetCrypt selesai, langkah berikutnya adalah implementasi sistem. Pada fase ini, pengembang melakukan pengujian aplikasi untuk memastikan semua fitur, khususnya proses enkripsi dan dekripsi data, berfungsi dengan baik serta mendeteksi adanya kesalahan yang mungkin terjadi selama penggunaan. Penulis menguji aplikasi NetCrypt dengan mengimplementasikannya pada lingkungan server lokal menggunakan *XAMPP*. Pengujian dilakukan menggunakan metode black box testing, yang menitikberatkan pada pemeriksaan fungsi aplikasi tanpa melihat kode sumber, sehingga dapat memastikan setiap fitur seperti menu enkripsi, dekripsi, dan manajemen file berjalan sesuai yang diharapkan serta mengurangi kemungkinan terjadinya kesalahan pada sistem. Selain itu, penulis juga memberikan pelatihan singkat kepada pengguna agar mereka dapat menggunakan aplikasi NetCrypt dengan benar dan aman dalam melindungi data pribadi mereka.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

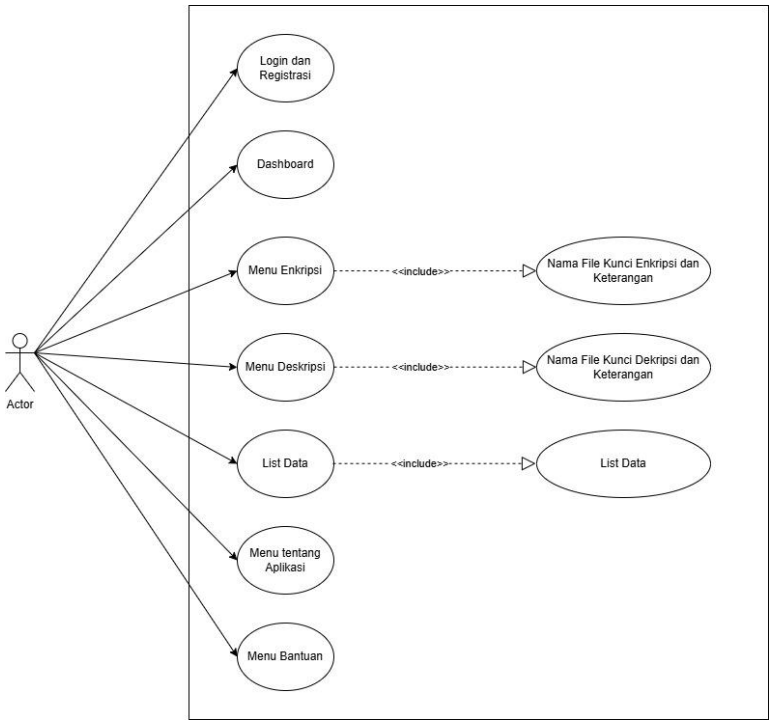
1) *Unified Modelling Language (UML)*

Unified Modelling Language (UML) adalah adalah suatu cara pemodelan visual yang berfungsi sebagai alat bantu dalam mendesain sistem berorientasi objek (Noneng Marthiawati et al., 2024). Dengan menggunakan UML, pengembang mampu memvisualisasikan struktur serta proses dalam sistem lewat berbagai macam diagram, sehingga hubungan antar komponen sistem dapat terlihat dengan lebih jelas dan mudah dipahami (Bukifan et al., 2025). UML membantu dalam menjelaskan dan merancang

sistem, terutama untuk program yang menggunakan cara berpikir berorientasi objek (Siska Narulita et al., 2024). UML juga adalah sebuah teknik pemodelan visual yang berisi diagram-diagram untuk membantu dalam membuat struktur dari sebuah aplikasi.

2) *Use Case Diagram*

Use Case Diagram adalah metode untuk memperlihatkan bagaimana aktor (pengguna) berinteraksi dengan sistem, serta untuk menjelaskan berbagai fungsi yang dimiliki oleh sistem tersebut. Dalam aplikasi bahasa isyarat berbasis Android yang dibuat, use case diagram menampilkan beberapa fitur utama, antara lain:



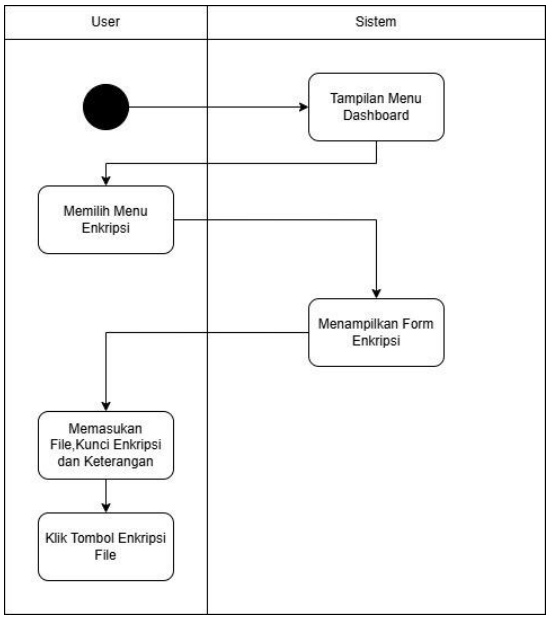
Gambar 2. Use Case Diagram Sistem

3) *Activity Diagram*

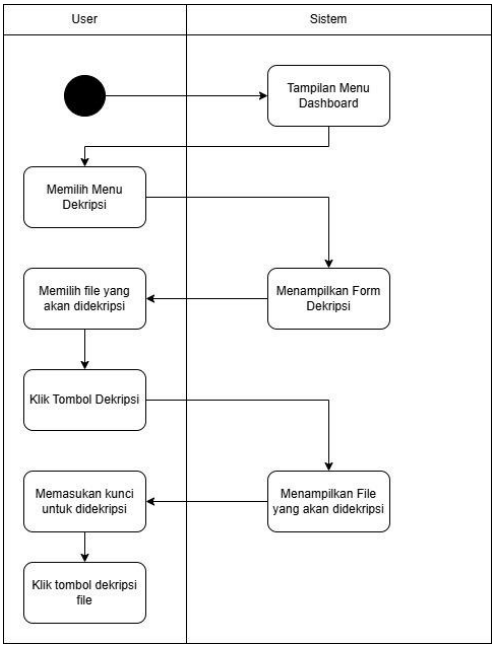
Diagram aktivitas atau *activity diagram* berfungsi sebagai representasi grafis yang memperlihatkan urutan langkah-langkah yang dilakukan oleh pengguna dalam berinteraksi dengan berbagai fitur yang disediakan oleh aplikasi NetCrypt. Diagram ini menyajikan gambaran alur kerja pengguna saat memanfaatkan sistem, khususnya dalam menjalankan proses enkripsi dan dekripsi data. Proses dimulai ketika pengguna membuka tampilan awal aplikasi, yang menyediakan sejumlah pilihan menu utama seperti fitur enkripsi, fitur dekripsi, serta riwayat aktivitas enkripsi dan dekripsi pada list aktivitas.

Setelah pengguna memilih menu enkripsi data, sistem akan menampilkan antarmuka untuk memasukkan data yang ingin diamankan dalam bentuk file. Sistem kemudian memproses data tersebut menggunakan algoritma AES-128, dan hasil enkripsi ditampilkan kepada pengguna dalam format terenkripsi. Selanjutnya, pengguna dapat berpindah ke menu dekripsi data. Pada menu ini, pengguna memasukkan data terenkripsi beserta kunci yang sesuai, lalu sistem memprosesnya dan menampilkan hasil dekripsi berupa informasi asli yang dapat dibaca kembali oleh pengguna. Setelah pengguna menyelesaikan proses pada menu enkripsi dan dekripsi, mereka dapat meninjau kembali

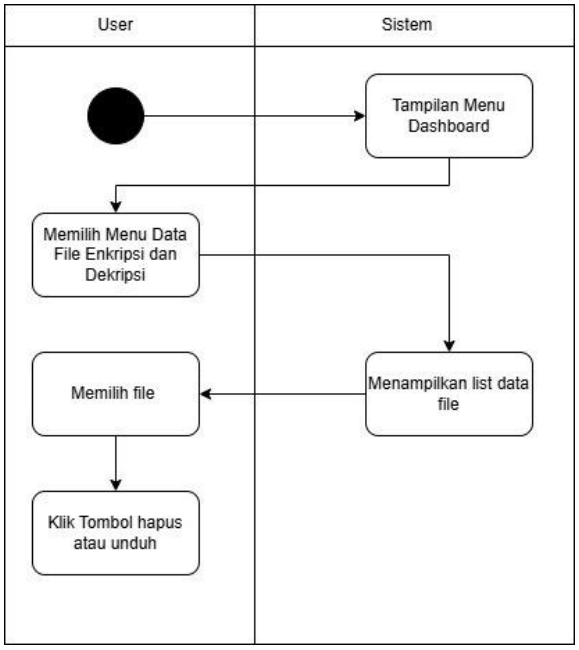
seluruh aktivitas yang telah dilakukan melalui menu list data. Pada tahap ini, pengguna memilih opsi list data dari menu utama, dan sistem akan menampilkan daftar atau list data dari file yang sudah dienkripsi maupun didekripsi. Informasi ini ditujukan untuk membantu pengguna dalam melakukan pemantauan dan validasi terhadap setiap tindakan pengamanan data yang dilakukan. Dengan demikian, sistem memberikan kontrol lebih kepada pengguna terhadap data yang telah diproses. *Activity diagram* ini menggambarkan urutan logis dari interaksi pengguna dengan sistem, yang menjadi dasar penting dalam proses perancangan dan implementasi fitur-fitur keamanan pada aplikasi NetCrypt berbasis web.



Gambar 3. Diagram Aktivitas Menu Enkripsi



Gambar 4. Diagram Aktivitas Menu Dekripsi

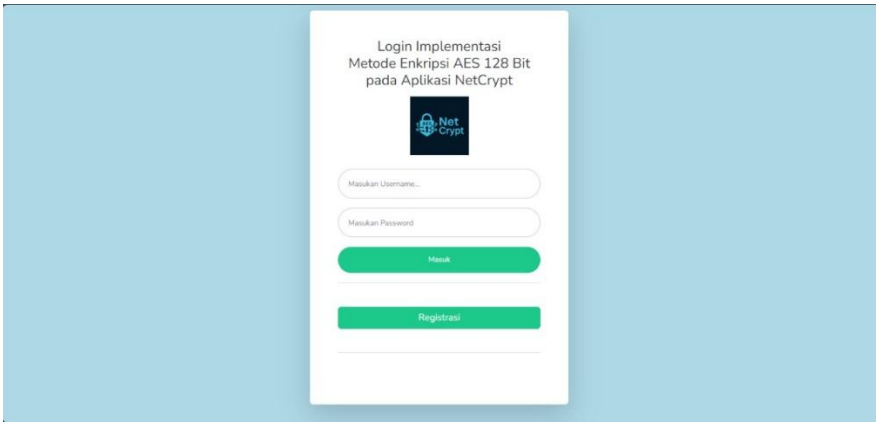


Gambar 5. Diagram Aktivitas Menu List Data

3.2 IMPLEMENTASI

1) *Login* dan Registrasi

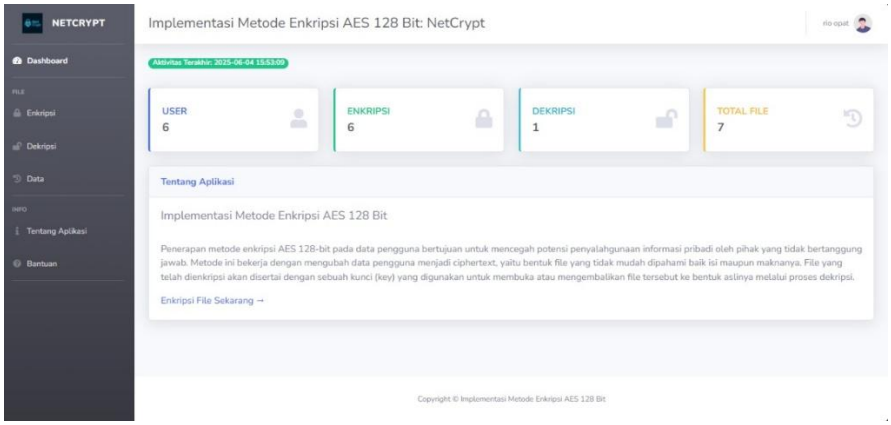
Halaman *login* dan registrasi merupakan tampilan awal yang diakses oleh pengguna saat pertama kali menggunakan website ini. Pengguna yang belum memiliki akun diwajibkan untuk melakukan proses registrasi terlebih dahulu. Setelah memiliki akun, pengguna dapat masuk ke dalam sistem dengan memasukkan nama pengguna dan kata sandi yang telah didaftarkan. Tampilan *login* dan registrasi ditunjukkan pada Gambar 6.



Gambar 6. Tampilan *Login* dan Registrasi

2) Menu Utama (*Dashboard*)

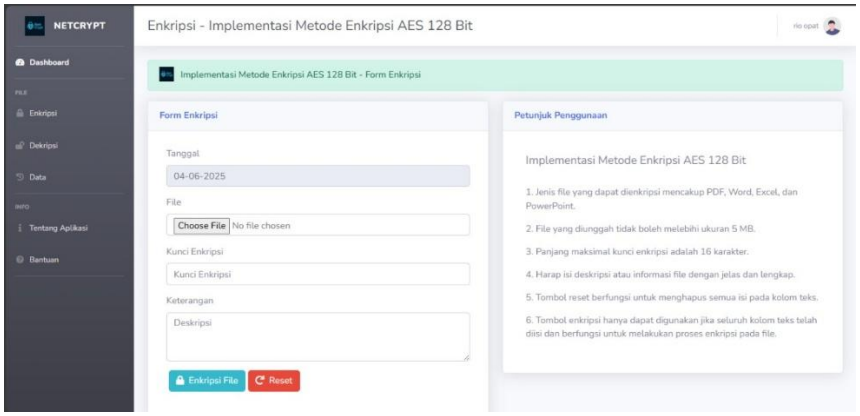
Tampilan utama dari aplikasi NetCrypt adalah *dashboard* yang menyajikan informasi umum mengenai aplikasi, termasuk jumlah pengguna yang telah menggunakan aplikasi ini, serta total data yang telah dienkripsi dan didekripsi. Pada bagian samping (*sidebar*), terdapat dua menu utama, yaitu File dan Info. Menu File terdiri atas submenu Enkripsi, Dekripsi, dan Data (daftar data), sedangkan menu Info memuat submenu Tentang Aplikasi dan Bantuan. Pengguna dapat memilih submenu Enkripsi untuk memulai proses enkripsi, submenu Dekripsi untuk mendekripsi data, serta submenu Data untuk melihat daftar data yang telah diproses. Tampilan *dashboard* aplikasi ditampilkan pada Gambar 7.



Gambar 7. Tampilan Menu Utama (*Dashboard*)

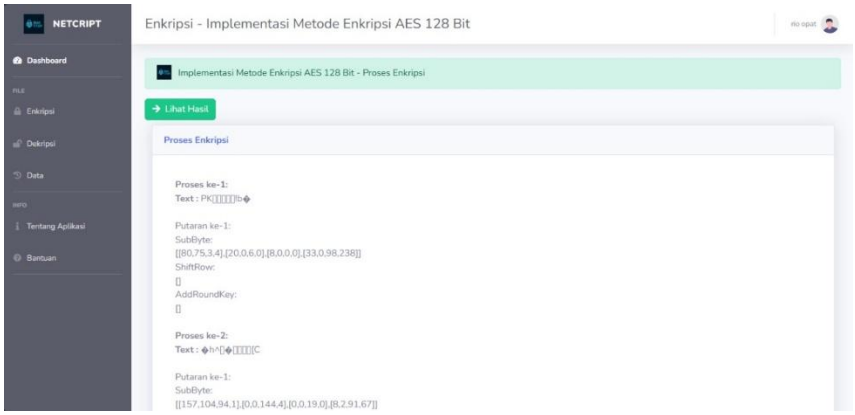
3) Tampilan Halaman Menu Enkripsi

Menu Enkripsi menyediakan sebuah formulir yang terdiri atas beberapa komponen, yaitu tanggal proses enkripsi, file yang akan dipilih untuk dienkripsi, kunci enkripsi yang wajib diisi oleh pengguna sebagai syarat agar file tidak dapat diakses oleh pihak yang tidak berwenang, serta keterangan mengenai file tersebut. Di sisi kanan formulir, terdapat petunjuk penggunaan yang dapat dibaca oleh pengguna sebelum memulai proses enkripsi, guna memastikan bahwa data dienkripsi dengan benar. Tampilan menu Enkripsi ditunjukkan pada Gambar 8.



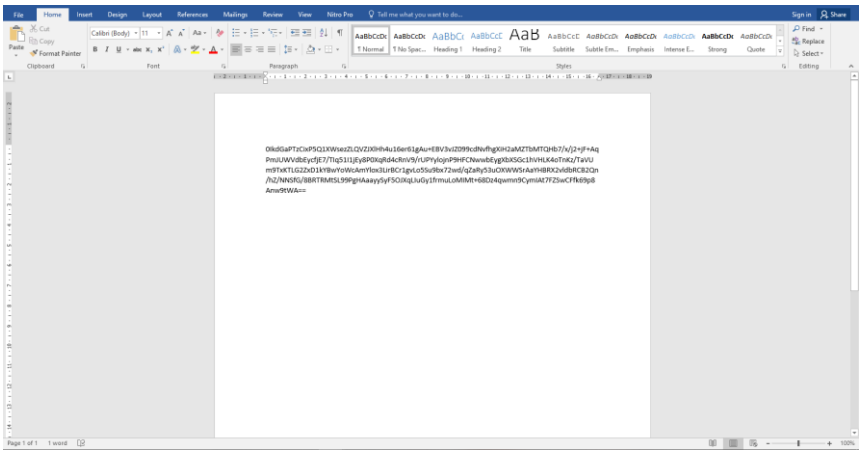
Gambar 8. Tampilan Halaman Menu Enkripsi

Setelah pengguna memilih file yang akan dienkripsi, memasukkan kunci enkripsi, serta menambahkan keterangan, pengguna dapat menekan tombol Enkripsi File untuk melanjutkan proses, atau menekan tombol Reset apabila ingin membatalkan proses dan mengisi ulang formulir enkripsi. Saat tombol Enkripsi File ditekan, sistem akan memulai proses enkripsi secara bertahap, dimulai dari proses pertama hingga selesai, dengan menggunakan metode enkripsi AES 128-bit. Proses enkripsi ditampilkan pada Gambar 9. Setelah proses selesai, pengguna dapat memilih opsi Lihat Hasil untuk diarahkan secara otomatis ke menu *List* Data.



Gambar 9. Tampilan Proses Enkripsi

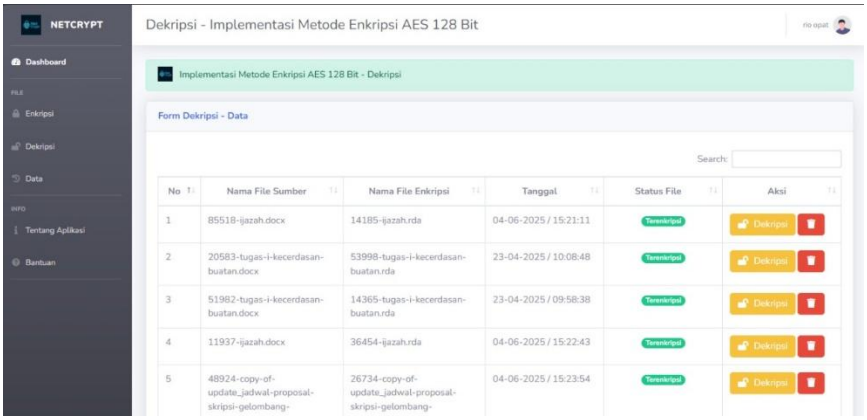
Pada gambar 10 akan diperlihatkan contoh hasil dari file yang sudah di enkripsi



Gambar 10. Hasil File Yang Telah di Enkripsi

4) Tampilan Halaman Menu Dekripsi

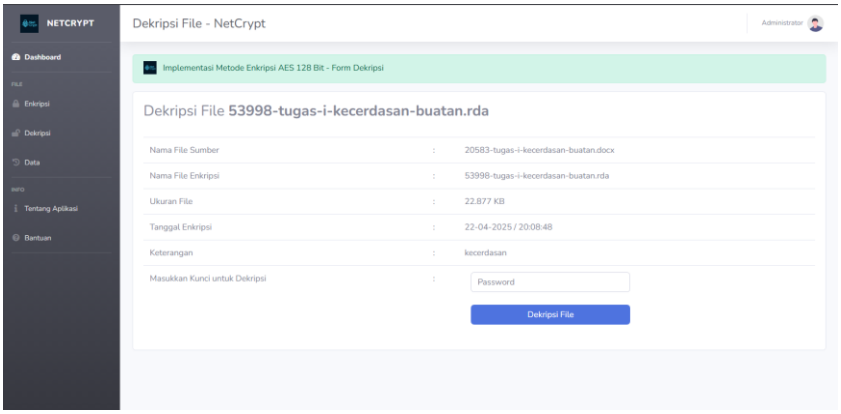
Pada menu Dekripsi, pengguna akan disajikan formulir yang berisi tabel yang memuat informasi mengenai nama file sumber, nama file hasil enkripsi, tanggal, status file, serta kolom aksi yang berisi pilihan untuk melakukan dekripsi atau menghapus file. Tampilan menu Dekripsi dapat dilihat pada Gambar 11.



Gambar 11. Tampilan Halaman Menu Dekripsi

Pengguna dapat memilih aksi dekripsi untuk mendekripsi file yang diinginkan dan secara otomatis akan diarahkan ke halaman formulir dekripsi. Pada formulir tersebut, ditampilkan

informasi berupa nama file sumber, nama file hasil enkripsi, ukuran file, tanggal enkripsi, serta keterangan terkait. Untuk melanjutkan proses dekripsi, pengguna harus memasukkan kunci dekripsi kemudian menekan tombol Dekripsi File. Proses dekripsi ditampilkan pada Gambar 12.

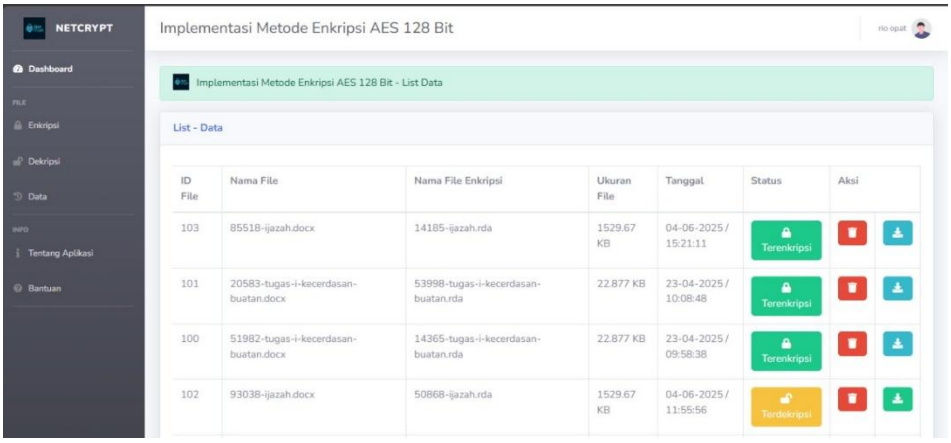


Gambar 12. Tampilan *Form* Proses Dekripsi

Ketika pengguna sudah mendekripsi file yang dipilih, maka akan langsung diarahkan pada menu list data

5) Tampilan Halaman Menu *List* Data

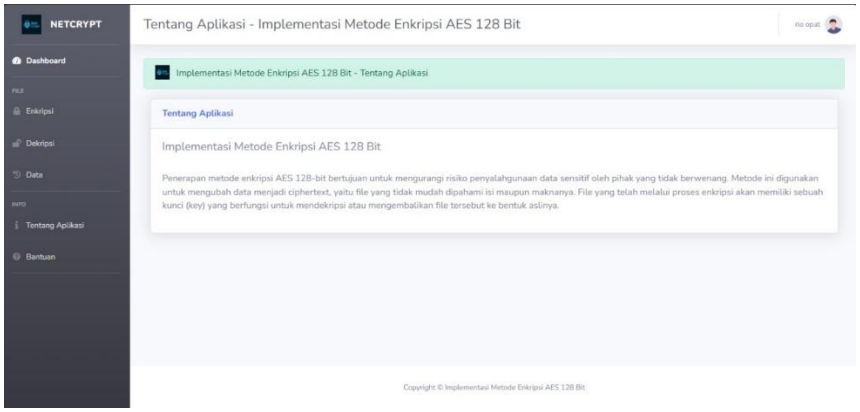
Menu *List* Data berfungsi untuk menampilkan daftar file yang telah melalui proses enkripsi maupun dekripsi. Pada Gambar 13, menu ini memperlihatkan tabel yang memuat informasi seperti *ID* file, nama file asli, nama file hasil enkripsi, ukuran file, tanggal, serta status file yang menunjukkan apakah file tersebut dalam keadaan terenkripsi atau terdekripsi. Status file ditandai dengan warna hijau untuk file yang terenkripsi dan warna kuning untuk file yang terdekripsi. Selain itu, terdapat kolom aksi yang memungkinkan pengguna untuk menghapus atau mengunduh file yang tersedia.



Gambar 13. Tampilan Menu *List* Data

6) Tampilan Halaman Menu Tentang Aplikasi

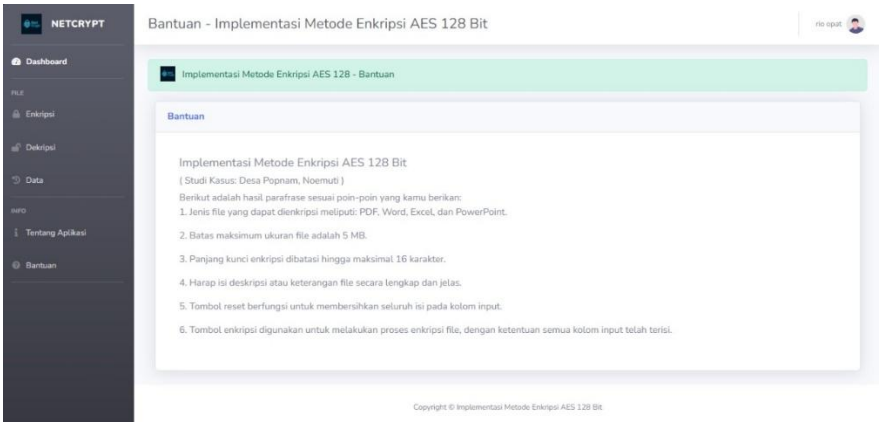
Aplikasi NetCrypt juga menyediakan menu Tentang Aplikasi yang memuat informasi mengenai aplikasi serta tujuan pembuatan aplikasi tersebut.



Gambar 14. Tampilan Halaman Menu Tentang Aplikasi

7) Tampilan Halaman Menu Bantuan

Menu terakhir pada aplikasi NetCrypt adalah menu Bantuan, yang dapat diakses oleh pengguna yang mengalami kesulitan dalam menggunakan aplikasi ini.



Gambar 15. Tampilan Halaman Menu Bantuan

3.3 PEMBAHASAN

Pengembangan aplikasi website NetCrypt ini menggunakan metode *Rapid Application Development* (RAD) serta menerapkan algoritma *Advanced Encryption Standard* (AES) dengan kunci 128 bit guna mempermudah proses enkripsi sekaligus mengurangi risiko penyalahgunaan data sensitif oleh pihak yang tidak berwenang. Pemilihan metode RAD dilakukan karena dianggap efektif dalam mempercepat proses pengembangan sistem tanpa mengurangi kualitas hasilnya (Hariyanto et al., 2021). Aplikasi web ini memiliki dua fitur utama, yaitu enkripsi dan dekripsi file, yang disusun dalam beberapa menu berbasis sidebar. Menu-menu tersebut meliputi tampilan utama (dashboard) yang menampilkan informasi mengenai aplikasi, serta menu enkripsi file yang dirancang dengan antarmuka sesederhana mungkin agar pengguna dapat dengan mudah mengenkripsi file mereka.

Dalam proses enkripsi, pengguna diwajibkan mengisi beberapa informasi yang dibutuhkan, seperti keterangan file dan kunci enkripsi. Setelah itu, pengguna dapat melakukan enkripsi file serta melihat dan mengunduh file yang telah terenkripsi. Selain itu, terdapat menu dekripsi yang berisi daftar file yang sebelumnya telah dienkripsi. Pengguna dapat memilih file yang akan didekripsi dengan menekan tombol dekripsi pada kolom aksi, kemudian memasukkan kunci dekripsi yang sama dengan yang digunakan saat enkripsi. Apabila kunci enkripsi yang dimasukkan salah, proses dekripsi tidak dapat dilakukan. Menu tambahan dalam aplikasi ini

adalah menu tentang aplikasi dan menu bantuan, yang keduanya dirancang agar mudah dipahami oleh pengguna.

Hasil dari aplikasi web ini berupa file yang telah dienkripsi menggunakan metode AES-128, di mana isi file tersebut diubah menjadi kode-kode khusus sehingga data tidak dapat diakses secara bebas oleh pihak yang tidak berwenang. Selain itu, file yang telah terenkripsi dapat didekripsi kembali oleh pengguna untuk memperoleh isi asli dari file tersebut.

Keterbatasan dari aplikasi web ini adalah belum mendukung proses enkripsi dan dekripsi untuk gambar atau foto. Oleh karena itu, penelitian selanjutnya diharapkan dapat memperhatikan aspek tersebut serta menambahkan penjelasan lebih rinci mengenai proses enkripsi agar lebih mudah dipahami oleh pengguna. Meskipun demikian, aplikasi web ini telah berhasil mencapai tujuan penelitian, yaitu merancang dan membangun sistem keamanan data berbasis web dengan algoritma AES-128 serta menguji efektivitasnya dalam melindungi data dari akses yang tidak sah. Implementasi metode *Rapid Application Development* (RAD) dan algoritma AES-128 menjadi keunggulan utama aplikasi ini, di mana metode RAD memungkinkan pengembangan sistem yang cepat dan efisien, sedangkan algoritma AES-128 mempercepat proses enkripsi dan dekripsi. Dengan pengembangan lebih lanjut, aplikasi web ini berpotensi memberikan solusi yang lebih optimal dalam menjaga keamanan data setiap individu.

KESIMPULAN

Aplikasi website NetCrypt berhasil dikembangkan dengan memanfaatkan metode *Rapid Application Development* (RAD) serta algoritma *Advanced Encryption Standard* (AES-128 Bit). Pemilihan metode RAD didasarkan pada kemampuannya dalam mempercepat proses pengembangan sistem tanpa mengorbankan kualitas, sementara penggunaan algoritma AES-128 Bit menjamin proses enkripsi dan dekripsi data berlangsung dengan cepat dan aman. Aplikasi ini menghadirkan dua fitur utama, yaitu enkripsi dan dekripsi file, yang disajikan dalam antarmuka yang sederhana agar memudahkan pengguna dalam penggunaannya. Hasil dari aplikasi ini adalah file yang telah berhasil dienkripsi sehingga isi file tersebut tidak dapat diakses secara bebas dan hanya dapat dibuka kembali dengan menggunakan kunci dekripsi yang valid. Aplikasi ini telah berhasil memenuhi tujuan penelitian, yaitu merancang dan mengembangkan sistem keamanan data berbasis web serta menguji efektivitasnya dalam melindungi data dari akses yang tidak sah. Pada penelitian selanjutnya, diharapkan aplikasi ini dapat dikembangkan lebih lanjut untuk mendukung proses enkripsi dan dekripsi file dalam format gambar atau foto, serta dilengkapi dengan penjelasan yang lebih detail mengenai mekanisme enkripsi agar memudahkan pemahaman pengguna.

DAFTAR PUSTAKA

Bukifan, P., Rema, Y., Risald, & Baso, B. (2025). Implementasi Metode Rapid Application Development dalam Pembuatan Aplikasi Bahasa Isyarat Bagi Penyandang Tunarungu. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *9*(June), 585–594.

Fahlevvi, M. R., Putra, D. S. A., & Ariandi, W. (2025). ALGORITMA AES128-CBC (ADVANCED ENCRYPTION STANDARD) UNTUK ENKRIPSI DAN DEKRIPSI BERKAS DOKUMEN PT. ADIARTA MUZIZAT. *Jurnal Innovation and Future Technology (IFTECH*, *7*(1), 166–176.

Febrian, R., Fauzi, A., Hidayat, T. M., Ardian, R., & Saputra, A. S. (2020). Pentingnya Keamanan Data dalam Intelijen Bisnis. *Jurnal Sistem Informasi*, *2*(1), 41–49.

https://ejournal.unibba.ac.id/index.php/j-sika/article/view/381/319

Hariyanto, D., Sastra, R., Putri, F. E., Informasi, S., Kota, K., Komputer, T., Informasi, S., Informatika, B. S., & Pusat, J. (2021). Implementasi Metode Rapid Application Development Pada Sistem Informasi Perpustakaan. *Jurnal Al-Ilmi*, *13*(1), 110–117.

Ignasius, A., & Shaka Yudha Sakti, D. V. (2022). Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi. *Skanika*, *5*(1), 1–10. https://doi.org/10.36080/skanika.v5i1.2118

Mutiara, T. T., Widagdo, B. W., Studi, P., & Informatika, T. (2025). *IMPLEMENTASI APLIKASI ENKRIPSI DATA MENGGUNAKAN ALGORITMA AES 128 UNTUK MENINGKATKAN KEAMANAN*. *3*(1), 16–26.

Noneng Marthiawati, Kevin Kurniawansyah, Hafiz Nugraha, & Fiqa Khairunnisa. (2024). Pelatihan Pembuatan UML (Unified Modelling Language) Menggunakan Aplikasi Draw.io Pada Prodi Sistem Informasi Universitas Muhammadiyah Jambi. *Transformasi Masyarakat : Jurnal Inovasi Sosial Dan Pengabdian*, *1*(2), 25–33. https://doi.org/10.62383/transformasi.v1i2.109

Nurman Hidayat, & Kusuma Hati. (2021). Penerapan Metode Rapid Application Development (RAD) dalam Rancang Bangun Sistem Informasi Rapor Online (SIRALINE). *Jurnal Sistem Informasi STMIK Antar Bangsa*, *10*(1), 8–17. https://doi.org/10.51998/jsi.v10i1.352

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Siska Narulita, Ahmad Nugroho, & M. Zakki Abdillah. (2024). Diagram Unified Modelling Language (UML) untuk Perancangan Sistem Informasi Manajemen Penelitian dan Pengabdian Masyarakat (SIMLITABMAS). *Bridge : Jurnal Publikasi Sistem Informasi Dan Telekomunikasi*, *2*(3), 244–256. https://doi.org/10.62951/bridge.v2i3.174