Jurnal Teknologi Terpadu

https://journal.nurulfikri.ac.id/index.php/jtt
ISSN : 2477-0043 ISSN ONLINE : 2460-7908

KEAMANAN DATA DENGAN ALGORITMA AES 128-BIT DAN BCRYPT DI PT. ANUGRAH LANCAR SUKSES

Rohadi Dwi Junianto[1], Yuni Wibawanti[2], Muhammad Akrom[3]

[1,2,3]Teknik Informatika, Universitas Indraprasta PGRI
Jakarta Selatan, DKI Jakarta, Indonesia 12530
rohadii861@gmail.com, yuniwib206@gmail.com, akromcenos@gmail.com

Abstract

This study aims to design and implement a data security system based on the 128-bit Advanced Encryption Standard (AES) algorithm integrated with BCrypt authentication at PT. Anugrah Lancar Sukses. The research is motivated by the company's practice of distributing internal documents without encryption, which increases the risk of data leakage and misuse. The system was developed using the Waterfall method, comprising requirements analysis, system design, implementation, and testing. The application was implemented as a desktop-based system featuring file encryption and decryption, user authentication, and role-based access control. System evaluation was conducted using Black-Box testing and cryptographic algorithm testing. The results indicate that all core system features functioned correctly with a 100% success rate. AES 128-bit encryption and decryption processes were completed efficiently, with an average processing time of less than one second for various file types, while maintaining data integrity after decryption. In addition, the BCrypt algorithm successfully secured user credentials by generating unique password hashes. These results demonstrate that the proposed system is effective in strengthening internal data protection and supporting information security practices within the organization.

Keywords: *AES 128-bit, BCrypt, Cryptography, Data Security, PT. Anugrah Lancar Sukses*

Abstrak

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan data berbasis algoritma *Advanced Encryption Standard* (AES) 128-bit yang dilengkapi autentikasi BCrypt di PT. Anugrah Lancar Sukses. Latar belakang penelitian ini adalah masih digunakannya distribusi dokumen internal tanpa mekanisme enkripsi, sehingga berisiko terhadap kebocoran dan penyalahgunaan data. Sistem dikembangkan menggunakan metode *Waterfall* yang meliputi tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian. Aplikasi dibangun sebagai aplikasi *desktop* dengan fitur utama enkripsi dan dekripsi *file*, autentikasi pengguna, serta pengelolaan hak akses berbasis peran. Pengujian sistem dilakukan menggunakan metode *Black Box* dan pengujian algoritma kriptografi. Hasil pengujian menunjukkan bahwa seluruh fitur utama sistem berjalan sesuai fungsi dengan tingkat keberhasilan 100%. Proses enkripsi dan dekripsi *file* menggunakan AES 128-bit berhasil dilakukan dengan waktu proses rata-rata kurang dari 1 detik untuk berbagai jenis *file*, serta *file* dapat dikembalikan ke bentuk semula tanpa perubahan isi. Algoritma BCrypt berhasil mengamankan data autentikasi dengan menghasilkan *hash* unik pada setiap proses penyimpanan kata sandi. Berdasarkan hasil tersebut, sistem yang dikembangkan dinilai efektif dalam meningkatkan perlindungan data internal perusahaan serta mendukung penerapan keamanan informasi di lingkungan kerja.

Kata kunci: AES 128-bit, BCrypt, Keamanan Data, Kriptografi, PT. Anugrah Lancar Sukses

1. PENDAHULUAN

Di tengah akselerasi transformasi digital, data telah menjadi aset strategis yang sangat bernilai namun juga rentan terhadap ancaman keamanan. Laporan IBM Security tahun 2025 mencatat bahwa setiap insiden kebocoran data dapat menyebabkan kerugian rata-rata sebesar 4,4 juta dolar [1], menegaskan urgensi penerapan sistem keamanan informasi yang andal, termasuk di perusahaan nasional seperti PT. Anugrah Lancar Sukses. Salah satu pendekatan yang terbukti efektif dalam menjaga kerahasiaan data digital adalah kriptografi, khususnya algoritma *Advanced Encryption Standard* (AES) 128-bit yang dikenal efisien dan tangguh dalam menghadapi ancaman digital. Dapat dikatakan bahwa kriptografi adalah bidang ilmu yang mengajarkan cara menjaga pesan tetap rahasia sehingga tidak dapat dibaca oleh orang yang tidak berkepentingan [2].

Dalam ranah ilmu kriptografi, dikenal sejumlah istilah pokok yang umum digunakan, antara lain *key*, *plaintext*, *ciphertext*, proses enkripsi, serta proses dekripsi [3]. AES

Diterima 11 Agustus 2025, Direvisi 20 Oktober 2025, Diterima untuk publikasi 22 Desember 2025

128-bit menjadi pilihan yang banyak diadopsi dalam berbagai sistem, termasuk oleh perusahaan berskala kecil dan menengah yang tengah beradaptasi ke arah digitalisasi. Karena Algoritma *Advanced Encryption Standard* (AES) menawarkan sejumlah keunggulan dibandingkan algoritma kriptografi lainnya, antara lain tingkat keamanan yang tinggi, efisiensi dalam proses enkripsi dan dekripsi, serta fleksibilitas dalam penerapannya [4].

PT. Anugrah Lancar Sukses, sebagai perusahaan yang bergerak di bidang perdagangan dan pengelolaan properti, masih menghadapi permasalahan serius terkait perlindungan data. Ketika suatu data memiliki nilai penting, maka perlindungan terhadap keamanan dan kerahasiaannya menjadi hal yang tidak bisa diabaikan [5]. Observasi awal menunjukkan bahwa proses penyimpanan dan distribusi dokumen internal masih dilakukan secara manual atau melalui *file* digital terbuka tanpa perlindungan seperti enkripsi atau kata sandi. Dokumen penting seperti laporan keuangan, data konsumen, hingga arsip transaksi disimpan dalam format standar (Word, Excel, PDF) tanpa lapisan keamanan, sehingga rentan terhadap akses ilegal maupun manipulasi oleh pihak yang tidak berwenang, baik dari internal maupun eksternal.

Pemilihan PT. Anugrah Lancar Sukses sebagai objek penelitian didasarkan atas keterbukaan perusahaan terhadap pengembangan sistem keamanan digital serta kesesuaiannya sebagai representasi dari persoalan umum yang dihadapi oleh banyak pelaku usaha lokal. Perusahaan ini memberikan akses dan dukungan penuh terhadap pelaksanaan penelitian, sehingga diharapkan solusi yang dikembangkan dapat menjawab permasalahan aktual sekaligus menjadi rujukan bagi konteks yang lebih luas.

Permasalahan utama yang diidentifikasi dalam penelitian ini mencakup belum digunakannya metode enkripsi digital untuk melindungi dokumen penting, tidak tersedianya sistem keamanan berbasis kriptografi, serta tingginya risiko penyadapan akibat distribusi *file* antar divisi yang dilakukan tanpa enkripsi. Selain itu, rendahnya pemahaman staf terhadap pentingnya keamanan digital memperbesar potensi terjadinya serangan siber. Dalam dunia kriptografi, terdapat dua elemen kunci yang menjadi fondasi utama dalam menjaga kerahasiaan data, yaitu proses enkripsi dan dekripsi. Enkripsi sendiri merupakan tahapan penting dalam pengamanan informasi, di mana data asli (*plaintext*) diubah menjadi format yang tidak dikenali atau disamarkan secara sistematis melalui penerapan algoritma tertentu [6].

Sebagai solusi, penelitian ini merancang dan mengembangkan sebuah aplikasi *desktop* yang mengimplementasikan algoritma AES 128-bit untuk proses enkripsi dan dekripsi *file*, serta dilengkapi fitur autentikasi pengguna melalui sistem *login* dan registrasi yang diamankan dengan algoritma BCrypt. Aplikasi ini dibangun menggunakan Java Swing, Karena Java Swing merupakan salah satu pustaka antarmuka grafis (GUI) yang disediakan oleh Java dan memiliki kapabilitas tinggi dalam membangun tampilan aplikasi yang interaktif, intuitif, serta mudah dioperasikan [7]. Kemudian, bahasa pemrograman Java digunakan sebagai dasar dalam pengembangan aplikasi yang berjalan pada platform *mobile* [8].

Laju pertumbuhan era digital yang terus meningkat membuat perusahaan di zaman modern semakin bergantung pada penerapan teknologi dalam setiap aspek kerjanya [9]. Oleh karena itu, untuk menjaga kerahasiaan data digital, *Advanced Encryption Standard* (AES) menjadi salah satu algoritma kriptografi yang paling banyak diterapkan berkat kemampuannya melakukan proses enkripsi dengan cepat serta efisien.

Mengimplementasikan AES pada sistem pengamanan dokumen digital berbasis *desktop*, dengan objek penelitian berupa aplikasi internal perusahaan. Keunggulan penelitian tersebut terletak pada kecepatan proses enkripsi dan kompatibilitas lintas platform. Namun, kelemahannya adalah belum adanya pengamanan pada tahap autentikasi pengguna, sehingga potensi akses tidak sah masih dapat terjadi [10].

Menerapkan AES pada sistem keamanan basis data rumah sakit. Keunggulan yang dicapai adalah integrasi AES dengan protokol SSL/TLS untuk mengamankan data pasien dari serangan *man in the middle* [11]. Meskipun demikian, penelitian tersebut belum menyediakan fitur visualisasi aktivitas yang dapat membantu administrator memantau pola penggunaan sistem secara *real-time*.

Mengeksplorasi pemanfaatan AES dalam aplikasi *cloud storage* untuk sektor pendidikan. Penelitian ini memberikan keuntungan berupa kemudahan akses data secara daring dengan tetap menjaga tingkat keamanan. Akan tetapi, ditemukan kelemahan berupa waktu enkripsi yang meningkat seiring bertambahnya ukuran *file*, yang dapat mengurangi kenyamanan pengguna [12].

Berdasarkan penelitian-penelitian terdahulu, penelitian ini memiliki perbedaan mendasar, yaitu mengintegrasikan AES 128-bit dengan algoritma BCrypt untuk mengamankan autentikasi pengguna. BCrypt dipilih karena memiliki mekanisme *salt* dan *cost factor* yang mampu meningkatkan ketahanan terhadap serangan *brute-force* maupun *rainbow table*. Dengan kombinasi ini, sistem yang dikembangkan tidak hanya menjamin keamanan data melalui enkripsi AES, tetapi juga memperkuat keamanan kredensial pengguna. Selain itu, penelitian ini menambahkan fitur visualisasi aktivitas pengguna menggunakan JFreeChart dan kemampuan ekspor laporan ke PDF melalui *iText*, yang jarang ditemukan pada penelitian terdahulu dan menambah nilai fungsionalitas sistem.

Pengembangan sistem dilakukan menggunakan pendekatan *Waterfall* yang terdiri atas tahapan analisis kebutuhan, desain sistem dan antarmuka, implementasi aplikasi, hingga pengujian fungsionalitas. Evaluasi teknis dilakukan secara

kuantitatif dengan mengukur keberhasilan proses enkripsi-dekripsi, efisiensi waktu pemrosesan, perubahan ukuran *file*, serta efektivitas kontrol akses berbasis peran antara *admin* dan pengguna biasa.

AES merupakan algoritma kriptografi simetris yang diakui secara luas dan digunakan secara intensif dalam berbagai sistem keamanan informasi, dengan tujuan utama untuk melindungi kerahasiaan data melalui proses enkripsi yang kuat dan efisien. Dengan diterapkannya sistem ini, diharapkan PT. Anugrah Lancar Sukses dapat memperoleh peningkatan signifikan dalam perlindungan data internal, sekaligus mendorong kesadaran kolektif mengenai pentingnya keamanan informasi di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan tujuan utama merancang dan mengevaluasi kinerja sistem keamanan *file* digital berbasis algoritma *Advanced Encryption Standard* (AES) 128-bit di PT. Anugrah Lancar Sukses. Metode pengembangan yang diterapkan adalah model *Waterfall*, yang menekankan urutan kerja yang sistematis mulai dari identifikasi masalah, analisis kebutuhan, perancangan, implementasi. Pendekatan ini dinilai sesuai untuk mendukung proses pengembangan aplikasi keamanan data yang terarah dan terstruktur.

2.1 Metode Pengumpulan Data

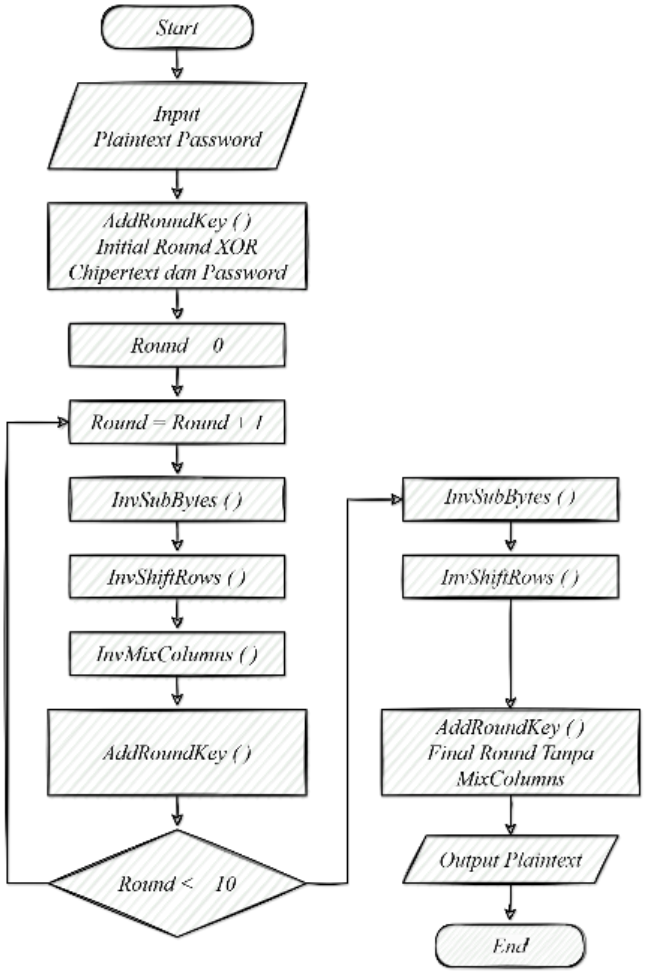
Data yang dibutuhkan untuk membangun sistem ini dikumpulkan dari dua sumber utama. Data primer diperoleh melalui observasi langsung dan wawancara kepada staf internal perusahaan untuk menangkap kondisi nyata serta kebutuhan faktual di lapangan. Sedangkan data sekunder dihimpun dari berbagai literatur seperti jurnal ilmiah, buku referensi, dokumentasi teknis algoritma kriptografi, dan studi terdahulu yang relevan dengan sistem keamanan informasi dan pengembangan aplikasi *desktop*.

Berdasarkan hasil analisis dari data yang terkumpul, disusun rancangan sistem dengan fitur-fitur inti, antara lain autentikasi pengguna (*login* dan *register*), proses enkripsi dan dekripsi *file*, manajemen hak akses berbasis peran (*admin* dan *user*), serta tampilan statistik aktivitas dalam bentuk log dan grafik. Seluruh fitur ini dibangun menggunakan kombinasi teknologi, yaitu Java Swing sebagai antarmuka aplikasi, MySQL untuk basis data, NetBeans IDE sebagai lingkungan pengembangan, serta pustaka tambahan seperti jBCrypt, iText, dan JFreeChart.

NetBeans IDE merupakan salah satu platform pengembangan perangkat lunak yang terintegrasi (IDE), dirancang secara khusus untuk mendukung bahasa pemrograman Java. Alat ini memberikan kemudahan dalam membangun aplikasi *desktop* dengan tampilan antarmuka grafis yang interaktif dan menarik [13].

NetBeans dipilih sebagai *Integrated Development Environment* (IDE) karena kemampuannya yang andal dalam mendukung perancangan antarmuka grafis secara visual melalui Java GUI Builder (Matisse). Fitur ini mempermudah proses desain UI tanpa harus menulis seluruh kode secara manual, sehingga lebih efisien dan terstruktur.

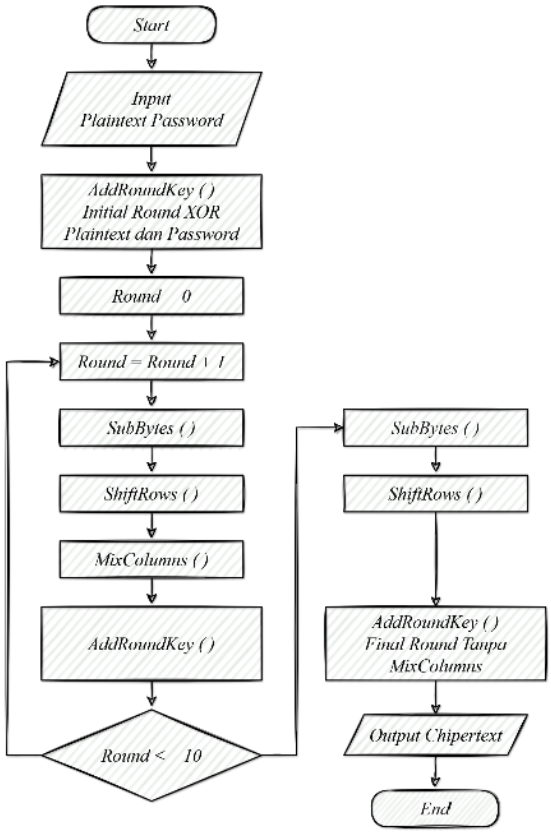
Untuk memperjelas proses kerja sistem, berikut disajikan diagram alur yang menggambarkan bagaimana algoritma AES 128-bit melakukan proses enkripsi data *file* yang diunggah pengguna.



Gambar 1. Enkripsi AES 128-bit

Gambar 1 Enkripsi AES 128-bit ini menunjukkan tahapan-tahapan yang dilakukan sistem dalam mengamankan *file*, mulai dari pembacaan *file*, pembentukan blok data, penerapan kunci AES, hingga menghasilkan *file* terenkripsi.

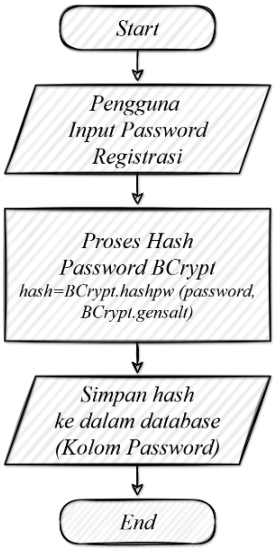
Selanjutnya, Gambar 2 Dekripsi AES 128-bit berikut menjelaskan proses dekripsi, yaitu bagaimana sistem mengembalikan *file* terenkripsi ke bentuk semula menggunakan kunci yang sama.



Gambar 2. Dekripsi AES 128-bit

Diagram ini memperlihatkan proses pembalikan data yang telah dienkripsi, dimulai dari pembacaan *file* terenkripsi, proses *inverse* transformasi kriptografi, hingga menghasilkan *file* asli yang dapat dibaca kembali oleh pengguna.

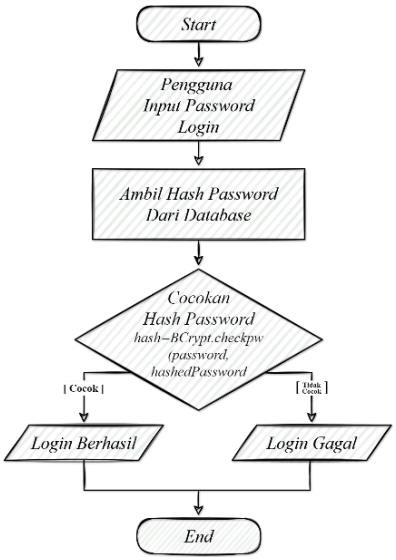
Selain keamanan *file*, sistem juga memperhatikan aspek autentikasi pengguna. Gambar 3 BCrypt Register berikut menunjukkan proses registrasi akun baru yang dilakukan pengguna, lengkap dengan mekanisme *hashing password* sebelum disimpan ke *database*.



Gambar 3. BCrypt *Register*

Flowchart ini menjelaskan bagaimana sistem memverifikasi kredensial pengguna saat *login*. *Password* yang dimasukkan akan dibandingkan dengan *hash* yang tersimpan menggunakan algoritma BCrypt dan *salt* yang dihasilkan secara otomatis.

Sedangkan Gambar 4 BCrypt *Login* di bawah ini menjelaskan alur proses saat pengguna melakukan *login* ke dalam sistem.



Gambar 4. BCrypt *Login*

Gambar ini menjelaskan bagaimana sistem memproses data pengguna baru. *Password* yang dimasukkan tidak disimpan secara langsung, melainkan diproses terlebih dahulu menggunakan *hashing* BCrypt untuk menjaga kerahasiaan.

2.2 Tahapan Penelitian

Tahapan-tahapan dalam penelitian ini dirancang mengikuti pendekatan metodologi *Waterfall*, yang terdiri atas sejumlah langkah berurutan mulai dari perumusan masalah hingga perancangan dan implementasi sistem keamanan data berbasis algoritma AES 128-bit. Setiap tahap disusun secara sistematis untuk mendukung proses pengembangan aplikasi secara menyeluruh dan terarah.

Langkah pertama diawali dengan identifikasi permasalahan di lapangan, yang dilakukan melalui observasi langsung terhadap proses distribusi dokumen internal perusahaan. Hasil dari tahapan ini menunjukkan bahwa sistem pengelolaan *file* di PT. Anugrah Lancar Sukses masih terbuka dan tidak memiliki lapisan keamanan digital. Selanjutnya, dilakukan studi pustaka untuk memperkuat dasar teori dan memastikan bahwa solusi yang dirancang memiliki fondasi ilmiah yang memadai.

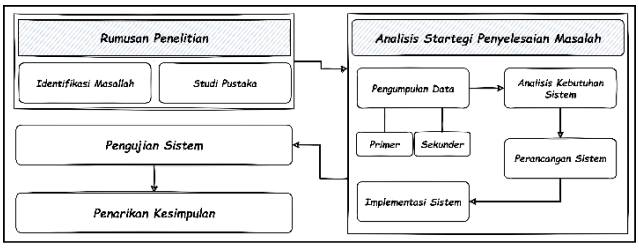
Berdasarkan hasil identifikasi tersebut, data primer dan sekunder dikumpulkan untuk memperoleh gambaran menyeluruh mengenai kondisi dan kebutuhan sistem. Setelah data terkumpul, dilakukan analisis kebutuhan yang menjadi dasar penyusunan fitur-fitur utama aplikasi, di

antaranya *login* dan registrasi, enkripsi dan dekripsi *file*, pengelolaan akses pengguna, serta pelaporan aktivitas sistem.

Tahap berikutnya adalah perancangan sistem, di mana struktur antarmuka, *database*, serta skema kerja algoritma mulai dirancang. Proses ini dilakukan dengan mempertimbangkan aspek keamanan, kemudahan penggunaan, dan efisiensi kinerja sistem. Setelah desain sistem dirasa matang, dilakukan implementasi aplikasi menggunakan Java Swing, didukung pustaka seperti jBCrypt, JFreeChart, dan iText.

Dalam sistem yang dirancang, Java dipilih sebagai salah satu bahasa pemrograman utama yang digunakan. Penguasaan mendalam terhadap Java memegang peranan penting dalam mengarahkan proses pembelajaran teknologi, terutama dalam menghadapi perkembangan kebutuhan industri di masa mendatang [14]. Dengan pemetaan yang tepat, kita dapat menentukan bahasa pemrograman yang paling relevan untuk dipelajari, mengetahui sejauh mana bahasa tersebut didukung dalam berbagai proyek pengembangan perangkat lunak, serta mengidentifikasi keterampilan yang paling strategis dan banyak diminati di pasar kerja saat ini.

Seluruh tahapan dalam penelitian ini divisualisasikan pada Gambar 5 Tahapan Penelitian berikut untuk memperjelas alur kerja sistem secara keseluruhan:



Gambar 5. Tahapan Penelitian

Setelah implementasi selesai, sistem dijalankan dan dievaluasi secara langsung di lingkungan internal PT. Anugrah Lancar Sukses. Dari proses ini diperoleh hasil bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan baik, mengelola hak akses secara efektif, serta menyajikan statistik aktivitas pengguna secara informatif.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil akhir dari proses penelitian dan pengembangan sistem keamanan data berbasis algoritma kriptografi AES 128-bit yang diimplementasikan di lingkungan kerja PT. Anugrah Lancar Sukses. Uji coba dilakukan secara langsung dalam kondisi aktual guna mengamati efektivitas fitur yang dikembangkan, seperti proses enkripsi dekripsi *file*, keamanan *login*, serta antarmuka sistem.

Seluruh hasil yang dipaparkan disusun secara sistematis sesuai tahapan pembangunan sistem, mulai dari pengujian algoritma kriptografi, pemodelan perangkat lunak, tampilan antarmuka pengguna, hingga uji fungsi sistem. Penjabaran hasil ini dilengkapi dengan ilustrasi berupa tabel dan gambar yang bertujuan memperjelas analisis dan interpretasi data.

Pembahasan dalam bagian ini juga menyoroti keberhasilan sistem dalam menjawab rumusan masalah yang telah ditetapkan sebelumnya. Setiap fitur diuji berdasarkan fungsionalitas dan relevansinya terhadap kebutuhan pengguna internal perusahaan.

3.1 Hasil Pengujian Algoritma

Sistem keamanan yang dikembangkan dalam penelitian ini mengandalkan dua algoritma utama, yaitu AES 128-bit untuk proses enkripsi dan dekripsi *file*, serta BCrypt untuk melindungi data autentikasi pengguna. Pengujian terhadap kedua algoritma ini bertujuan untuk mengevaluasi efektivitas dan kestabilan kinerja sistem, sekaligus memastikan bahwa proses pengamanan data berlangsung sesuai dengan spesifikasi yang telah dirancang.

Pengujian pertama dilakukan pada fitur enkripsi dan dekripsi *file* menggunakan AES 128-bit. Enkripsi dalam AES 128-bit berlangsung melalui 10 putaran transformasi, di mana setiap putaran memproses data dalam bentuk biner [15]. Setiap tahapan ini tidak berdiri sendiri, melainkan terhubung erat dengan kunci putaran (*round key*) yang berasal dari ekspansi kunci utama. Dalam setiap putaran, diterapkan empat transformasi inti secara berurutan. Berbagai jenis *file* digunakan dalam pengujian ini guna mengamati waktu proses serta integritas data setelah dilakukan dekripsi.

Proses pengujian dilakukan untuk memastikan seluruh komponen sistem berfungsi sesuai dengan tujuannya. Selain itu, tahap ini juga menjadi langkah penting untuk menilai sejauh mana sistem mampu menjalankan proses enkripsi dan dekripsi dengan akurat serta efisien sesuai rancangan yang telah dibuat.

Tabel 1. Hasil Pengujian Algoritma AES 128-bit

No	Nama *File* Asli	Ukuran *File*	Waktu Enkripsi	Waktu Dekripsi	Hasil Validasi
1	Price_List_Produk_ALS.xlsx	10 kb	0,001 detik	0,001 detik	Berhasil
2	Kontra K_Kerjasama_Vendor.Docx	29,875 kb	0,145 detik	0,520 detik	Berhasil
3	Data_Daftar_Karyawan.PDF	42,550 kb	0,269 detik	0,860 detik	Berhasil

Berdasarkan hasil pengujian pada Tabel 1, algoritma AES 128-bit menunjukkan kinerja yang efisien dalam proses enkripsi dan dekripsi berbagai jenis *file*. Waktu enkripsi berada pada rentang 0,001 hingga 0,269 detik, sedangkan waktu dekripsi berkisar antara 0,001 hingga 0,860 detik, tergantung pada ukuran dan jenis *file* yang diproses. *File* berukuran besar seperti dokumen PDF dengan ukuran 42,550 KB masih dapat diproses dalam waktu kurang dari 1 detik, menunjukkan bahwa sistem memiliki performa yang stabil dan layak digunakan dalam aktivitas operasional perusahaan. Selain itu, seluruh *file* berhasil dikembalikan ke bentuk semula tanpa perubahan isi, sehingga integritas data tetap terjaga setelah proses dekripsi.

Tabel 2. Hasil Pengujian Algoritma BCrypt

Username	***Password Input***	**Hasil *Hash* (Ditransformasi)**	**Status Verifikasi**
1_Rohadi	Admin123	$2a$10$EPEzx30kutkFp8jwpOdP3.RCvyMd4wycekP.9rL3mwo...	Berhasil
2_Rohadi	Admin123	$2a$10$EPEzx30kutkFp8jwpOdP3.RCvyMd4wycekP.9rL3mwo...	Berhasil
Hadi	User123	$2a$10$1IJQJKC.H0SsO7A.9kCWs.vTViU6cMDkU1Kmeo8S5bJ...	Berhasil

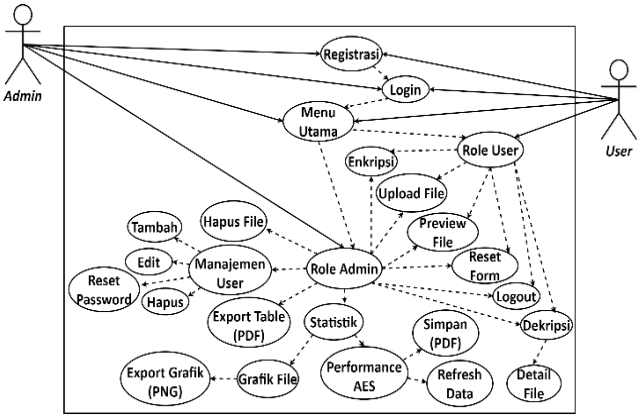
Tabel 2 Hasil Pengujian Algoritma BCrypt memperlihatkan bahwa meskipun *password* yang dimasukkan sama (misalnya "admin123"), hasil *hash* yang dihasilkan selalu berbeda. Hal ini membuktikan bahwa BCrypt bekerja sesuai fungsinya dengan memanfaatkan *salt* untuk mencegah serangan rekonstruksi *password*. Selain itu, proses verifikasi saat *login* juga berjalan lancar, menandakan integrasi algoritma dengan sistem berhasil dilakukan secara tepat.

Dengan pengujian terhadap kedua algoritma tersebut, dapat disimpulkan bahwa sistem berhasil menjalankan fungsi-fungsi keamanan utama secara optimal. AES 128-bit menjamin kerahasiaan *file*, sementara BCrypt memberikan perlindungan yang kuat terhadap data *login* pengguna. Kombinasi keduanya memberikan perlindungan berlapis yang sangat relevan dalam menghadapi ancaman keamanan digital di lingkungan perusahaan.

3.2 Tampilan Antarmuka Aplikasi

Antarmuka pengguna (*user interface*) menjadi elemen penting dalam sebuah aplikasi *desktop*, khususnya untuk mendukung kemudahan penggunaan dan efisiensi operasional. Dalam penelitian ini, antarmuka dirancang menggunakan Java Swing dengan pendekatan desain yang sederhana namun tetap informatif. Tujuan utamanya adalah memastikan bahwa staf internal perusahaan, meskipun tidak memiliki latar belakang teknis, dapat mengoperasikan sistem dengan lancar.

Untuk mendukung proses pengembangan sistem aplikasi yang terstruktur dan terarah, dilakukan tahap pemodelan perangkat lunak sebagai representasi visual dari fungsionalitas serta alur kerja aplikasi yang dikembangkan. Pemodelan pada Gambar 6 *Use Case Diagram* membantu menggambarkan interaksi antara pengguna dan sistem, sekaligus memperjelas struktur internal aplikasi sebelum proses implementasi dilakukan.



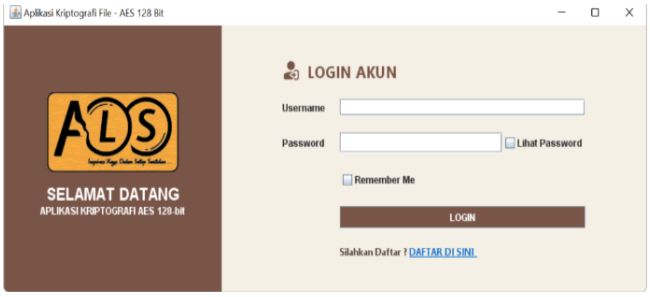
Gambar 6. *Use Case Diagram*

Dalam sebuah sistem, skenario *use case* berperan penting untuk menjelaskan alur interaksi antara aktor dan sistem secara naratif [16]. Penjabaran ini menggambarkan bagaimana peran masing-masing entitas berkontribusi dalam proses sistem. Tak hanya dalam bentuk teks, interaksi tersebut juga divisualisasikan melalui *use case diagram*, sehingga hubungan antar komponen dapat terlihat lebih jelas dan mudah dipahami secara struktural.

Diagram ini menggambarkan hubungan antara aktor (*admin* dan *user*) dengan fitur utama dalam sistem. *Use case* yang ditampilkan mencakup proses *login*, registrasi, unggah *file*, enkripsi, dekripsi, pengunduhan *file*, dan pengelolaan data pengguna.

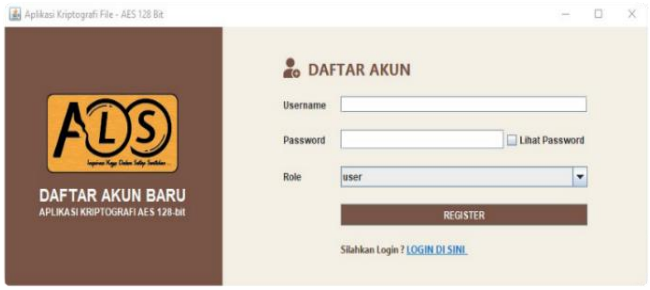
Melalui diagram tersebut dapat dilihat bahwa pengguna biasa (*user*) memiliki akses terbatas hanya pada fitur enkripsi dan dekripsi, sementara *admin* memiliki kontrol penuh terhadap manajemen pengguna dan data. Pendekatan ini memungkinkan sistem untuk membedakan hak akses berdasarkan peran, sehingga keamanan dan keteraturan penggunaan sistem dapat terjaga.

Antarmuka dikembangkan menggunakan Java Swing, yang memungkinkan tampilan *desktop* berbasis GUI dengan elemen visual yang responsif. Berikut disajikan tampilan-tampilan utama dari aplikasi yang dikembangkan, yang mencerminkan alur penggunaan sistem mulai dari autentikasi hingga pemantauan aktivitas.



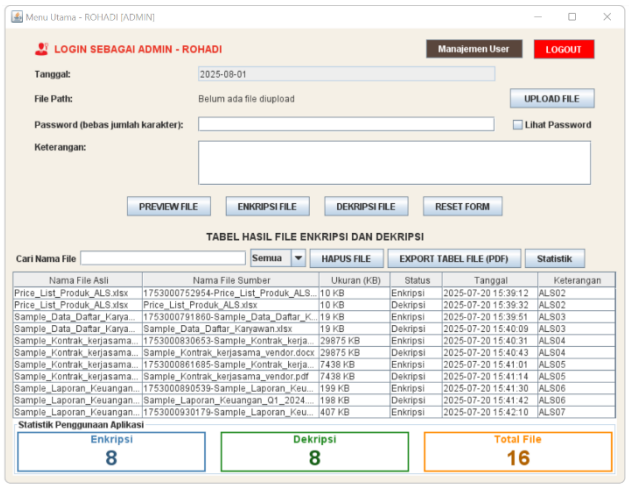
Gambar 7. *Form Login*

Tampilan pada Gambar 7 *Form Login* menunjukkan halaman *form login* yang berfungsi sebagai akses awal ke dalam sistem. Pada tahap ini, pengguna perlu mengisikan nama akun dan kata sandi, yang selanjutnya diverifikasi melalui proses *hashing* dengan memanfaatkan algoritma BCrypt.



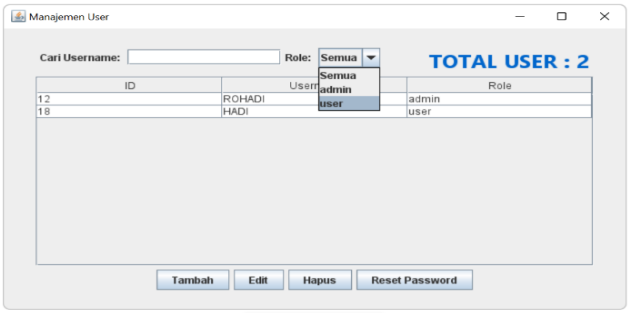
Gambar 8. *Form Register*

Tampilan pada Gambar 8 *Form Register* digunakan pengguna sebagai proses untuk pembuatan akun baru. *Input* kata sandi akan langsung diolah menggunakan BCrypt sebelum disimpan di basis data, memastikan keamanan data autentikasi sejak awal.



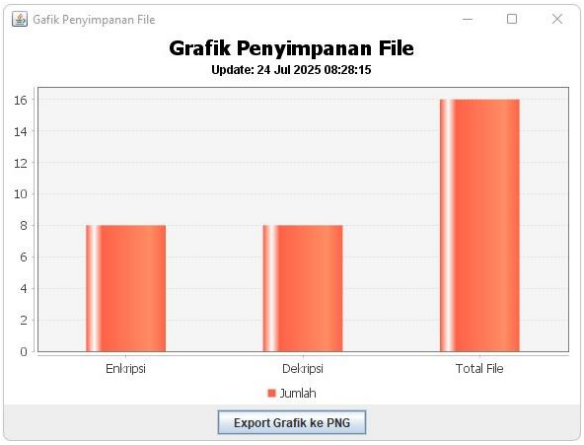
Gambar 9. Menu Navigasi Utama

Tampilan pada Gambar 9 Menu Navigasi Utama merupakan menu navigasi utama yang mengarahkan pengguna ke berbagai fitur seperti enkripsi, dekripsi, manajemen akun, dan pelaporan. Antarmuka disusun agar setiap fungsi dapat diakses dengan mudah.



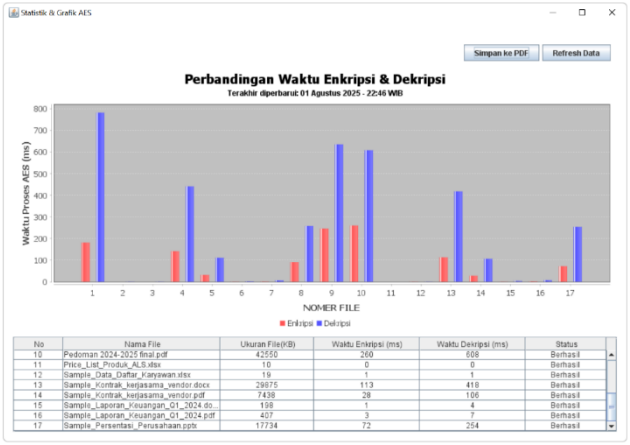
Gambar 10. Manajemen Akun Pengguna

Tampilan pada Gambar 10 Manajemen Akun Pengguna untuk mengatur seluruh data pengguna yang terdaftar dalam sistem. Melalui antarmuka ini, administrator dapat melakukan pencarian berdasarkan nama pengguna atau peran (*role*), seperti *admin* dan *user*, sehingga proses pengelolaan akun menjadi lebih terarah. Selain itu, fitur seperti Tambah, Edit, Hapus, dan *Reset Password* turut mempermudah pengendalian akses serta menjaga keamanan sistem agar tetap konsisten dan terkendali.



Gambar 11. Visualisasi Statistik Penyimpanan *File*

Antarmuka pada Gambar 11 Visualisasi Statistik Penyimpanan *File* menyajikan informasi tentang aktivitas penyimpanan *file* dalam bentuk statistik. Data yang ditampilkan mencakup jumlah *file* terenkripsi dan didekripsi oleh masing-masing pengguna.



Gambar 12. Grafik Evaluasi Performa Sistem

Grafik pada Gambar 12 Grafik Evaluasi Performa Sistem digunakan untuk mengevaluasi performa sistem dalam bentuk visual. Data ditampilkan dalam bentuk diagram batang dan garis, mencerminkan jumlah transaksi enkripsi dan dekripsi dalam kurun waktu tertentu.

Seluruh tampilan antarmuka dirancang untuk mendukung tujuan utama sistem, yaitu meningkatkan keamanan dan efisiensi kerja dalam pengelolaan data penting perusahaan. Desain yang intuitif diharapkan dapat membantu pengguna dalam menjalankan tugas tanpa hambatan, sekaligus meminimalkan risiko kesalahan manusia.

3.3 Hasil Pengujian Aplikasi

Pengujian aplikasi dilakukan guna memastikan seluruh fitur dapat berjalan sebagaimana mestinya sesuai kebutuhan pengguna internal perusahaan. Pengujian dilakukan secara lokal pada lingkungan kerja PT. Anugrah Lancar Sukses, dan difokuskan pada aspek fungsional, kemudahan penggunaan, serta ketahanan sistem terhadap kemungkinan kesalahan pengguna.

Pengujian dilakukan pada empat aspek utama: (1) fungsi utama sistem seperti *login*, enkripsi, dekripsi, dan manajemen akun; (2) pembatasan hak akses berdasarkan peran pengguna (*admin* dan *user*); (3) efektivitas algoritma BCrypt dalam mengamankan data autentikasi; serta (4) proses enkripsi dan dekripsi *file* menggunakan algoritma AES 128-bit.

Setiap pengujian disusun berdasarkan skenario yang merepresentasikan aktivitas nyata pengguna di lapangan, dan hasilnya dicatat secara sistematis dalam bentuk tabel. Data yang diperoleh dari pengujian ini menjadi dasar evaluasi keberhasilan implementasi sistem, sekaligus mendukung kesimpulan akhir dalam penelitian ini.

3.3.1 Pengujian Fungsionalitas Sistem

Pengujian ini difokuskan untuk memastikan bahwa seluruh fitur utama pada aplikasi, seperti *login*, registrasi, unggah *file*, enkripsi, dekripsi, *logout*, dan fitur lainnya, telah berjalan sesuai dengan alur logika dan kebutuhan pengguna yang telah dirancang sebelumnya. Seluruh fungsi diuji menggunakan metode *Black Box*, yang berfokus pada masukan dan keluaran dari sistem. *Black Box* merupakan metode pengujian perangkat lunak yang berfokus pada fungsi sistem tanpa memperhatikan alur kontrol program. Pendekatan ini menitikberatkan pada informasi domain yang diuji untuk memastikan fungsi berjalan sesuai spesifikasi. Umumnya, proses pengujian ini dilakukan oleh tim internal pengembang [17].

Tabel 3. Hasil Pengujian Fungsional Sistem

Fitur	Skenario Uji	Hasil yang Diharapkan	Hasil Aktual	Status
Registrasi	Mengisi data dengan benar kemudian menekan tombol "Daftar"	Akun baru berhasil dibuat dan tersimpan	*Form* berhasil dikirim, akun aktif terbentuk	Lulus
Login	Memasukkan *username* dan *password* yang valid	Pengguna berhasil masuk ke dalam sistem	Sistem menampilkan halaman utama aplikasi	Lulus
Menu Utama	Berpindah antar menu setelah berhasil *login*	Fitur utama sistem muncul sesuai navigasi	Seluruh tombol menu berfungsi dan responsif	Lulus
Upload File	Memilih *file* dari perangkat lalu menekan tombol "*upload file*"	*File* tampil pada daftar *file* di sistem	*File* berhasil diunggah dan ditampilkan	Lulus
Enkripsi	Menekan tombol "Enkripsi" setelah *file* diunggah	*File* tersimpan dalam format terenkripsi	*File* berubah ke bentuk terenkripsi	Lulus
Preview File	Memilih *file* dan menekan tombol "*Preview*"	Isi *file* tampil dalam area teks yang tersedia	Konten *file* terbaca dengan baik	Lulus
Dekripsi	Memilih *file* terenkripsi lalu klik tombol "Dekripsi"	*File* asli muncul kembali seperti semula	*File* berhasil dikembalikan ke bentuk awal	Lulus
Reset Form	Menekan tombol "*Reset*" pada *form* pendaftaran atau unggah *file*	Formulir kembali dalam kondisi kosong	Semua isian dalam *form* berhasil dibersihkan	Lulus
Logout	Menekan tombol *logout* pada tampilan utama	Sistem kembali ke halaman *login* awal	Pengguna dialihkan ke *form login*	Lulus

Hasil pengujian fungsionalitas sistem yang disajikan pada Tabel 3 menunjukkan bahwa seluruh fitur utama, meliputi registrasi, *login*, unggah *file*, enkripsi, dekripsi, serta manajemen navigasi, berhasil dijalankan sesuai dengan skenario pengujian. Dari seluruh skenario yang diuji, sistem mencapai tingkat keberhasilan 100% tanpa ditemukan kegagalan fungsi. Hal ini menunjukkan bahwa implementasi sistem telah memenuhi kebutuhan fungsional pengguna serta berjalan stabil pada lingkungan internal perusahaan.

3.3.2 Pengujian Hak Akses (*Role-based Access Control*)

Pengujian hak akses berbasis peran menunjukkan bahwa mekanisme *role-based access control* telah diterapkan secara efektif. Seluruh skenario pengujian untuk peran *admin* dan *user* menghasilkan status lulus, di mana *admin* memiliki akses penuh terhadap fitur manajemen dan pelaporan, sementara *user* dibatasi hanya pada fungsi enkripsi dan dekripsi. Pemisahan hak akses ini berperan penting dalam mencegah akses tidak sah dan meningkatkan keamanan sistem secara keseluruhan.

a) Pengujian Hak Akses untuk *Admin*

Pengujian memverifikasi bahwa pengguna dengan peran *admin* memiliki keleluasaan penuh terhadap fitur-fitur yang berkaitan dengan pengelolaan sistem dan analisis data statistik. Detail hasil pengujian disajikan melalui Tabel 4 Hasil Pengujian Hak Akses (*Admin*) berikut:

Tabel 4. Hasil Pengujian Hak Akses (*Admin*)

Fitur	Skenario Uji	Hasil yang Diharapkan	Hasil Aktual	Status
Manajemen *User*	*Admin* mengakses menu manajemen pengguna	Halaman manajemen berhasil ditampilkan	Tampil	Lulus
Hapus *File*	*Admin* memilih *file* lalu menekan tombol hapus	*File* berhasil dihapus dari sistem	*File* terhapus	Lulus
Export Table (PDF)	*Admin* menekan tombol "Export" pada halaman data	*File* PDF tersimpan dengan sukses	Berhasil	Lulus
Grafik Penyimpanan *File*	*Admin* membuka Statistik > Penyimpanan *File*	Grafik ditampilkan sesuai data	Grafik muncul	Lulus

b) Pengujian Hak Akses untuk *User*

Pengujian pada bagian ini bertujuan untuk memastikan bahwa *user* biasa tidak dapat mengakses fitur-fitur yang dikhususkan untuk *admin*, sehingga mencegah tindakan yang tidak sesuai dengan peran yang diberikan. Detail hasil pengujian disajikan melalui Tabel 5 Hasil Pengujian Hak Akses (*User*) berikut:

Tabel 5. Hasil Pengujian Hak Akses (*User*)

Fitur	Skenario Uji	Hasil yang Diharapkan	Hasil Aktual	Status
Manajemen *User*	*User* mencoba mengakses menu manajemen pengguna	Akses ditolak / fitur tidak tersedia	Ditolak	Lulus
Hapus *File*	*User* menekan tombol hapus *file*	Akses ditolak / fitur tidak tersedia	Ditolak	Lulus
Export Table (PDF)	*User* mencoba klik tombol *export*	Akses ditolak / fitur tidak tersedia	Ditolak	Lulus
Grafik Penyimpanan *File*	*User* mengakses menu statistik	Akses ditolak / fitur tidak tersedia	Ditolak	Lulus

3.3.3 Pengujian Keamanan *Password* (BCrypt)

Pengujian ini dilakukan untuk memastikan bahwa *password* pengguna tidak disimpan dalam bentuk asli, melainkan telah di-*hash* menggunakan algoritma BCrypt. *Salt* ini berperan penting dalam meningkatkan keamanan kata sandi, karena menambahkan kompleksitas tambahan yang membuat teknik serangan *brute force* menjadi jauh lebih sulit untuk menembusnya [18].

Hasil uji menunjukkan bahwa sistem berhasil melakukan *hashing* serta verifikasi *login* tanpa menyimpan data *plaintext*. Rincian pengujian ditampilkan pada Tabel 6 Hasil Pengujian Keamanan *Password* berikut:

Tabel 6. Hasil Pengujian Keamanan *Password*

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	Registrasi dengan *password* baru	*Password* tersimpan sebagai *hash* BCrypt	*Hash* terenkripsi muncul	Lulus
2	*Login* dengan *password* yang sesuai	Sistem cocokkan *input* dengan *hash*	*Login* berhasil	Lulus
3	Cek *database* pada kolom *password*	Tidak ditemukan *password* asli (*plaintext*)	*Hash* terenkripsi	Lulus

3.3.4 Pengujian Enkripsi dan Dekripsi (AES 128-bit)

Pengujian ini bertujuan untuk mengevaluasi sejauh mana proses enkripsi dan dekripsi mampu menjaga keutuhan data. Pengujian dilakukan dengan cara mengenkripsi sebuah *file*, kemudian mendekripsinya kembali guna memastikan bahwa isi *file* tidak mengalami perubahan atau kerusakan. Berdasarkan hasil pengujian, *file* yang telah dienkripsi tidak dapat dibuka atau dibaca secara langsung karena telah berubah menjadi format tidak terbaca. Sementara itu, setelah proses dekripsi dilakukan, *file* berhasil dikembalikan ke bentuk semula dengan struktur dan isi yang identik seperti sebelum dienkripsi.

Tahapan ini menguji apakah proses enkripsi-dekripsi *file* berjalan dengan waktu yang efisien dan data dapat dikembalikan ke bentuk awal tanpa perubahan atau kerusakan *file*. Rincian hasil pengujian disajikan pada Tabel 7 Hasil Pengujian Enkripsi dan Dekripsi (AES 128-bit) berikut:

Tabel 7. Hasil Pengujian Enkripsi dan Dekripsi (AES 128-bit)

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	Mengunggah *file* lalu melakukan enkripsi	*File* terenkripsi tidak dapat dibuka secara langsung	*File* berubah menjadi karakter acak	Lulus
2	Melakukan dekripsi terhadap *file* yang terenkripsi	*File* kembali ke bentuk asli tanpa kerusakan	*File* berhasil dikembalikan utuh	Lulus
3	Membuka *file* hasil enkripsi tanpa aplikasi sistem	*File* tidak terbaca oleh Notepad maupun editor teks biasa	Karakter tidak dikenali oleh sistem	Lulus

Hasil menunjukkan bahwa *file* berhasil dienkripsi dan didekripsi dengan waktu proses yang cepat dan hasil validasi yang tepat, menandakan algoritma AES 128-bit terintegrasi secara efektif ke dalam sistem.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan *file* berbasis algoritma AES 128-bit yang dilengkapi autentikasi BCrypt di PT. Anugrah Lancar Sukses. Sistem yang dikembangkan mampu mengamankan dokumen internal perusahaan melalui proses enkripsi dan dekripsi *file* serta pengelolaan hak akses berbasis peran antara *admin* dan *user*.

Hasil pengujian menunjukkan bahwa seluruh fitur utama sistem berfungsi dengan tingkat keberhasilan 100%. Proses enkripsi dan dekripsi *file* menggunakan AES 128-bit dapat dilakukan secara efisien dengan waktu pemrosesan kurang dari 1 detik untuk berbagai jenis *file*, serta mampu menjaga integritas data setelah proses dekripsi. Selain itu, penerapan algoritma BCrypt berhasil meningkatkan keamanan autentikasi dengan memastikan bahwa kata sandi pengguna tidak disimpan dalam bentuk asli.

Dengan demikian, sistem yang dikembangkan dinilai efektif dalam meningkatkan perlindungan data internal perusahaan dan mendukung penerapan keamanan informasi di lingkungan kerja. Untuk pengembangan selanjutnya, sistem ini masih dapat ditingkatkan dengan pengujian performa pada skala data yang lebih besar serta pengembangan ke platform berbasis web atau *mobile*.

Ucapan Terima Kasih

Ucapan terima kasih juga disampaikan kepada PT. Anugrah Lancar Sukses yang telah bersedia menjadi mitra dalam pelaksanaan penelitian ini, serta kepada seluruh pihak yang telah memberikan dukungan, bantuan, maupun kontribusi dalam bentuk apa pun hingga penelitian ini dapat terselesaikan dengan baik.

DAFTAR PUSTAKA

[1] IBM, "Laporan Biaya Pelanggaran Data 2024." Accessed: Aug. 07, 2025. [Online]. Available: https://www.ibm.com/id-id/reports/data-breach

[2] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, Jul. 2018, doi: 10.54914/jtt.v4i1.110.

[3] D. Pradeka, "Implementasi Aplikasi Kriptografi Berbasis Android Menggunakan Metode Subtitusi dan Permutasi," *In Search – Informatic, Science, Entrepreneur, Applied Art, Research, Humanism*, vol. 18, no. 2580–3239, pp. 161–168, Apr. 2019, Accessed: Jun. 14, 2025. [Online]. Available: http://repository.unibi.ac.id/id/eprint/158

[4] B. L. Ananya, V. Nikhitha, S. Arjun, and N. C. Gowda, "Survey of applications, advantages, and comparisons of AES encryption algorithm with other standards," *International Journal of Computational Learning & Intelligence, 2023*, vol. 2, pp. 87–98, Apr. 2023, doi: https://doi.org/10.5281/zenodo.7921019.

[5] Mukhtar and Harun, *Kriptografi untuk Keamanan Data*, 1st ed. Yogyakarta: Deepublish, 2018. Accessed: Jun. 12, 2025. [Online]. Available: https://harumanja.wordpress.com/wp-content/uploads/2019/02/harun-mukhtar-buku-sample.pdf

[6] Rosdiana, "Sekuritas Sistem Dengan Kriptografi," *Al-Khwarizmi: Jurnal Pendidikan Matematika dan Ilmu Pengetahuan Alam*, vol. 3, no. 1, pp. 21–32, Sep. 2018, doi: 10.24256/jpmipa.v3i1.216.

[7] F. Ramadhana, V. R. Ana, V. A. Aprilyan, M. F. Akbar, P. H. Nadia, and F. A. Akbar, "Aplikasi Manajemen Perpustakaan Menggunakan Java Swing," *Jurnal Ilmiah Teknologi Informasi dan Robotika*, vol. 5, no. 1, pp. 9–19, Jun. 2023, doi: 10.33005/jifti.v5i1.176.

[8] S. Usman, J. Jeffry, and F. Aziz, "Pengembangan Absensi berbasis Mobile Aplikasi pada Badan Kepegawaian dan Pengembangan Sumber Daya Manusia Kabupaten Bone," *Jurnal Teknologi Terpadu*, vol. 7, no. 2, pp. 108–112, Dec. 2021, doi: 10.54914/jtt.v7i2.437.

[9] R. Maulana, A. Voutama, and T. Ridwan, "Analisis Sentimen Ulasan Aplikasi MyPertamina pada Google Play Store menggunakan Algoritma NBC," *Jurnal Teknologi Terpadu*, vol. 9, no. 1, pp. 42–48, Jul. 2023, doi: 10.54914/jtt.v9i1.609.

[10] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *Journal of Computer System and Informatics (JoSYC)*, vol. 4, pp. 179–187, Nov. 2022, doi: 10.47065/josyc.v4i1.2451.

[11] I. M. A. Bhaskara, M. P. A. Ariawan, I. B. A. Peling, and I. P. A. Prayudha, "Studi Literatur: Analisa Perbandingan Teori Tentang Tingkat Keamanan Antar Algoritma Simetris," *Jurnal Bangkit Indonesia*, vol. 13, no. 1, pp. 40–45, Mar. 2024, doi: 10.52771/bangkitindonesia.v13i1.278.

[12] A. Hermawan, M. Novianto Anggoro, D. Lozera Devi, and A. Faroqi, "Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (AI) terhadap Keamanan Data di Indonesia," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI)*, no. ISSN (Online) 2828-786X, pp. 581–591, Sep. 2023, doi: https://doi.org/10.33005/sitasi.v3i1.363.

[13] A. Anggraini, A. Sayuti, A. Dwiyono, and Q. Ilahi, "Implementasi Aplikasi Netbeans untuk Pengolahan Data Barang pada Percetakan Duta Yuzaka Permai ," *Jurnal Surya Informatika*, vol. 15, no. 1, pp. 9–14, May 2025, doi: 10.48144/suryainformatika.v15i1.2068.

[14] B. Haryanto, A. Ardiansyah, and M. Kurniasih, "Pengenalan Database NoSQL dan Perbandingannya dengan Database Relasional," *Jurnal IPSIKOM*, vol. 12, no. 1, p. 2024, Jun. 2024, doi: https://doi.org/10.58217/ipsikom.v12i1.272.

[15] T. S. Shazhaq *et al.*, "Analisa Penyandian File Dokumen Kriptografi Menggunakan Advanced Encryption Standard (AES)," *Jurnal Kendali Teknik dan Sains*, vol. 1, no. 2, pp. 103–115, Apr. 2023, doi: 10.59581/jkts-widyakarya.v1i2.314.

[16] T. A. Kurniawan, "Pemodelan Use Case (UML): Evaluasi Terhadap beberapa Kesalahan dalam Praktik," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 1, pp. 77–86, Mar. 2018, doi: 10.25126/jtiik.201851610.

[17] M. R. Fiqryansyah dan I. Hermawan, "Rancang Bangun Aplikasi Website Percetakan Printop Pada Modul Costumer Dan Editor Dengan Metode Pengembangan Waterfall ", *j. teknologi terpadu*, vol. 6, no. 2, hlm. 72–78, Des 2020.

[18] T. P. Batubara, S. Efendi, and E. B. Nababan, "Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force," *J. Phys*, p. 12129, 2021, doi: 10.1088/1742-6596/1811/1/012129.