



Sistem Enkripsi Data Menggunakan Algoritma Advanced Encryption Standard (AES) Pada Aplikasi Cloud Storage PT. Gajah Tunggal Tbk.

Muhammad Syidqi Al Badawi^{1*}, Sofyan Mufti Prasetyo²

^{1,2,3} Teknik Informatika, Universitas Pamulang, Jl. Raya Puspitek No. 46 Buaran, Serpong, Kota Tangerang Selatan, Provinsi Banten 15130.

E-mail: muh.syidqialbadawi16@gmail.com¹, sofy004@brin.go.id²,
dosen01809@unpam.ac.id³

ABSTRACT

The rapid development of information and communication technology encourages companies to enhance the security and reliability of digital data management and storage, particularly in cloud-based environments. PT. Gajah Tunggal Tbk, as a large-scale manufacturing company, manages operational data that are critical and confidential, thereby requiring a data security system capable of protecting information from leakage, damage, and unauthorized access. The existing data backup process, which is still performed manually and lacks encryption mechanisms and automated notifications, poses potential security risks and increases the likelihood of human error. Therefore, an information technology-based system is required to secure data through an encryption process before it is stored in cloud storage. This study aims to design and implement a data encryption system using the Advanced Encryption Standard (AES) algorithm in a cloud storage application at PT. Gajah Tunggal Tbk. The AES algorithm was selected because it is a symmetric cryptographic algorithm with a high level of security, efficient processing performance, and has been widely recognized as an international standard for digital data protection. The system development method applied in this research is the Waterfall model, which consists of requirement analysis, system design, implementation, testing, and maintenance stages. Research data were collected through observation, interviews with the IT Support team, and literature study. The results of this study produce a web-based application developed using PHP and MySQL that is capable of performing data encryption and decryption, storing encrypted files in cloud storage, and automatically sending email notifications after the backup process is completed. With the implementation of this system, corporate data security can be improved, the risk of data loss can be minimized, and the backup process becomes safer, more efficient, and monitored in real time.

Keywords: Data Encryption, Advanced Encryption Standard (AES), Cloud Storage, Data Security, Database Backup

Article History

Received: Januari 2026

Reviewed: Januari 2026

Published: Januari 2026

Plagiarism Checker No 235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

**ABSTRAK**

Perkembangan teknologi informasi dan komunikasi mendorong perusahaan untuk meningkatkan keamanan dan keandalan dalam pengelolaan serta penyimpanan data digital, khususnya pada lingkungan penyimpanan berbasis cloud. PT. Gajah Tunggal Tbk sebagai perusahaan manufaktur berskala besar memiliki data operasional yang bersifat penting dan rahasia, sehingga memerlukan sistem pengamanan data yang mampu melindungi informasi dari risiko kebocoran, kerusakan, maupun akses tidak sah. Proses backup data yang masih dilakukan secara manual dan belum dilengkapi dengan mekanisme enkripsi serta notifikasi otomatis berpotensi menimbulkan risiko keamanan dan kesalahan manusia. Oleh karena itu, diperlukan sebuah sistem berbasis teknologi informasi yang mampu mengamankan data melalui proses enkripsi sebelum disimpan ke cloud storage. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem enkripsi data menggunakan algoritma *Advanced Encryption Standard* (AES) pada aplikasi cloud storage di PT. Gajah Tunggal Tbk. Algoritma AES dipilih karena merupakan algoritma kriptografi simetris yang memiliki tingkat keamanan tinggi, efisiensi pemrosesan yang baik, serta telah menjadi standar internasional dalam pengamanan data digital. Metode pengembangan sistem yang digunakan adalah Waterfall, dengan tahapan analisis kebutuhan, perancangan sistem, implementasi, pengujian, serta pemeliharaan. Data penelitian diperoleh melalui observasi, wawancara dengan tim IT Support, dan studi pustaka. Hasil penelitian menghasilkan sebuah aplikasi berbasis web menggunakan PHP dan MySQL yang mampu melakukan enkripsi dan dekripsi data, menyimpan file terenkripsi ke cloud storage, serta mengirimkan notifikasi email secara otomatis setelah proses backup selesai dilakukan. Dengan adanya sistem ini, keamanan data perusahaan dapat ditingkatkan, risiko kehilangan data dapat diminimalkan, serta proses backup menjadi lebih aman, efisien, dan terpantau secara realtime.

Kata Kunci: *Enkripsi Data, Advanced Encryption Standard (AES), Cloud Storage, Keamanan Data, Backup Database*



1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) global telah merevolusi berbagai aspek kehidupan manusia, termasuk dalam hal penyimpanan dan pengelolaan data. Data digital kini menjadi komoditas penting yang mendasari banyak aktivitas, mulai dari pendidikan, bisnis, hingga pemerintahan. Penyimpanan data berbasis *cloud* telah menjadi standar baru karena kemampuannya menyediakan akses yang fleksibel, efisiensi biaya, dan skalabilitas yang tinggi. (Zhang, et al., 2023).

Seiring meningkatnya penggunaan *cloud storage*, muncul tantangan serius terkait keamanan dan kerahasiaan data. Data yang dikirim dan disimpan di server *cloud* sangat rentan terhadap kebocoran, pencurian, maupun manipulasi apabila tidak dilindungi dengan sistem keamanan yang memadai. Untuk mengatasi permasalahan tersebut, penerapan sistem enkripsi data menjadi salah satu solusi utama dalam menjaga integritas dan kerahasiaan informasi. Enkripsi bekerja dengan cara mengubah data asli (*plaintext*) menjadi bentuk yang tidak terbaca (*ciphertext*) menggunakan algoritma tertentu, sehingga hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang sah. Menurut (Li, et al., 2021), mekanisme enkripsi berperan penting dalam melindungi data di lingkungan *cloud* agar tidak mudah dieksploitasi oleh pihak yang tidak berwenang. *Advanced Encryption Standard* (AES) merupakan algoritma yang paling efektif digunakan karena memiliki kecepatan tinggi, efisiensi pemrosesan yang baik, serta tingkat keamanan yang kuat terhadap serangan brute force dan eksploitasi data. (Singh, et al., 2022).

PT. Gajah Tunggal Tbk beralamat di Komplek Industri GT, Jl. Gajah Tunggal, Desa Pasir Jaya, Kecamatan Jati Uwung, Tangerang, Banten, merupakan salah satu produsen ban terbesar di Asia Tenggara yang memproduksi berbagai jenis ban untuk mobil penumpang, truk, SUV, industri, hingga sepeda motor, serta produk turunan seperti karet sintetis dan ban dalam. Produk-produknya dipasarkan di dalam negeri dan diekspor ke lebih dari 100 negara di seluruh dunia melalui kemitraan dengan berbagai Original Equipment Manufacturer (OEM). Dalam mendukung operasionalnya yang luas, perusahaan memiliki infrastruktur server komputer yang mengelola data produksi, distribusi, dan karyawan. Server ini menjadi pusat data yang sangat vital sehingga keamanan dan ketersediaan informasi harus selalu terjaga. Untuk mencegah kehilangan data akibat gangguan sistem, tim IT Support rutin melakukan backup database harian sebagai langkah pencegahan terhadap kerusakan perangkat, kesalahan manusia, atau serangan siber. Namun, sistem backup manual yang masih digunakan menyimpan risiko tinggi. Proses salinan data ke media penyimpanan internal seperti hard disk, SSD, atau server cadangan tetap rentan terhadap serangan virus dan malware. Jika media penyimpanan terinfeksi, data hasil backup dapat rusak atau hilang secara permanen.

Pada penelitian ini digunakan algoritma *Advanced Encryption Standard* (AES) sebagai metode utama untuk mengamankan data perusahaan. Algoritma ini dipilih karena memiliki tingkat keamanan tinggi, proses enkripsi yang cepat, serta telah menjadi standar internasional dalam perlindungan data digital. Sistem yang dirancang menerapkan enkripsi database terintegrasi dengan *cloud storage*, di mana setiap file yang akan di-backup dienkripsi terlebih dahulu menggunakan AES sebelum dikirim ke server *cloud*. Setelah proses backup selesai, sistem akan mengirimkan notifikasi email

secara realtime kepada tim IT Support sebagai tanda bahwa data telah terenkripsi dan tersimpan dengan aman. Dengan cara ini, proses backup menjadi lebih aman, efisien, dan transparan, sekaligus meminimalkan risiko kehilangan data akibat serangan malware atau kerusakan perangkat penyimpanan lokal.

Berdasarkan permasalahan yang telah diuraikan, penulis mengajukan judul skripsi “Sistem Enkripsi Data Menggunakan Algoritma Advanced Encryption Standard (AES) pada Aplikasi Cloud Storage PT. Gajah Tunggal Tbk.” Sistem ini dirancang untuk meningkatkan keamanan database melalui enkripsi otomatis dan notifikasi email secara realtime, sehingga proses backup menjadi lebih aman, efisien, dan mampu meminimalkan risiko kehilangan data akibat serangan malware atau kerusakan sistem.

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Metode Pustaka

Pengumpulan data dilakukan dengan menelaah berbagai sumber literatur seperti jurnal ilmiah, buku, artikel, dan penelitian terdahulu yang berkaitan dengan keamanan data, algoritma AES, dan teknologi cloud storage. Metode ini bertujuan untuk memperoleh dasar teori yang kuat dalam perancangan sistem enkripsi data.

2. Wawancara

Wawancara dilakukan secara langsung dengan tim IT Support PT. Gajah Tunggal Tbk untuk memperoleh informasi mengenai mekanisme backup database yang berjalan saat ini, kendala yang sering terjadi, serta kebutuhan sistem yang lebih aman dan efisien. Data hasil wawancara digunakan sebagai acuan dalam perancangan sistem yang diusulkan.

3. Metode Observasi

Peneliti melakukan observasi secara langsung terhadap proses pengelolaan dan backup database di lingkungan kerja PT. Gajah Tunggal Tbk, termasuk sistem penyimpanan yang digunakan dan potensi risiko keamanannya. Hasil observasi ini menjadi dasar dalam menentukan rancangan sistem enkripsi dan notifikasi otomatis yang sesuai dengan kebutuhan perusahaan.

2.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang diterapkan dalam penelitian ini adalah metode Waterfall. Metode ini dipilih karena memiliki alur kerja yang terstruktur dan berurutan, sehingga setiap tahap pengembangan dapat dilakukan secara sistematis dari awal hingga sistem siap digunakan. Dengan pendekatan Waterfall, setiap tahapan harus diselesaikan terlebih dahulu sebelum melanjutkan ke tahap berikutnya agar hasil pengembangan sesuai dengan kebutuhan pengguna.

Adapun penjelasan dari masing-masing tahapan metode Waterfall adalah sebagai berikut:

1. Requirement Analysis (Analisis Kebutuhan)



Tahap ini berfokus pada pengumpulan dan analisis kebutuhan sistem melalui wawancara dan observasi di PT. Gajah Tunggal Tbk, khususnya terkait proses backup data, kebutuhan otomatisasi, serta penerapan enkripsi AES yang terintegrasi dengan cloud storage.

2. System and Software Design (Perancangan Sistem)

Pada tahap ini dilakukan perancangan struktur sistem yang meliputi desain antarmuka, basis data, alur proses enkripsi dan backup, serta perancangan notifikasi email otomatis.

3. Implementation (Penerapan Sistem)

Tahap implementasi merupakan proses penerjemahan rancangan sistem ke dalam bentuk program menggunakan PHP dan MySQL yang terhubung dengan layanan cloud storage.

4. Integration and Testing (Integrasi dan Pengujian Sistem)

Seluruh komponen sistem diintegrasikan dan diuji menggunakan metode Black Box Testing untuk memastikan fungsi enkripsi, penyimpanan cloud, dan notifikasi berjalan dengan baik.

5. Operation and Maintenance (Operasi dan Pemeliharaan)

Pada tahap ini sistem digunakan untuk proses backup data dan dilakukan pemeliharaan secara berkala guna memperbaiki kesalahan serta menyesuaikan sistem dengan kebutuhan pengguna.

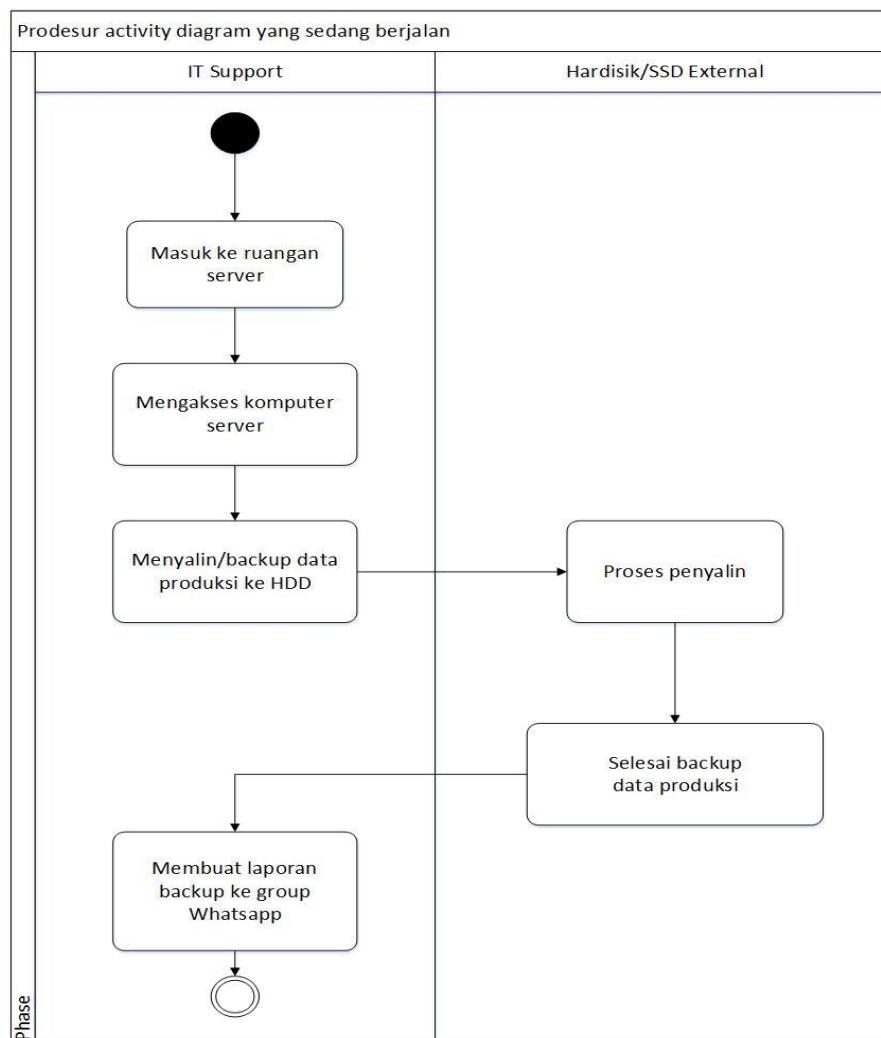
3. HASIL DAN PEMBAHASAN

3.1 Analisa Sistem

Tahap analisa sistem dilakukan setelah perencanaan awal dan sebelum proses perancangan sistem dimulai. Analisa ini bertujuan untuk memahami kondisi sistem yang berjalan, termasuk alur proses, fungsi sistem, serta permasalahan yang dihadapi. Tahap analisa memiliki peran penting dalam pengembangan sistem, karena hasil analisa menjadi dasar dalam menentukan rancangan sistem agar sesuai dengan kebutuhan dan tujuan yang diharapkan.

3.2 Analisa Sistem Berjalan

Analisis sistem berjalan dilakukan untuk menilai proses backup data yang saat ini digunakan di PT. Gajah Tunggal Tbk. Sistem masih bersifat manual dengan menyalin data ke media lokal seperti hard disk atau server cadangan, sehingga rawan terhadap serangan malware, kesalahan pengguna, dan kerusakan perangkat. Selain itu, belum terdapat mekanisme enkripsi otomatis maupun notifikasi realtime yang menjamin keamanan data. Oleh karena itu, diperlukan sistem baru yang mampu menerapkan enkripsi menggunakan algoritma Advanced Encryption Standard (AES) sebelum data dikirim ke cloud storage, guna meningkatkan keamanan serta efisiensi proses backup.

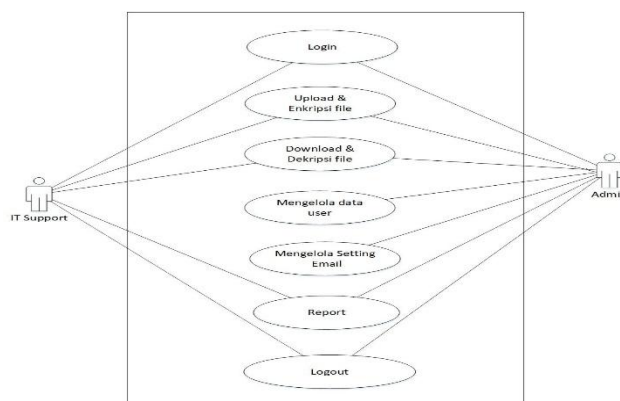


Gambar 3.1 Activity Diagram Sedang Berjalan

3.1 Desain

3.1.1 Use Case Diagram

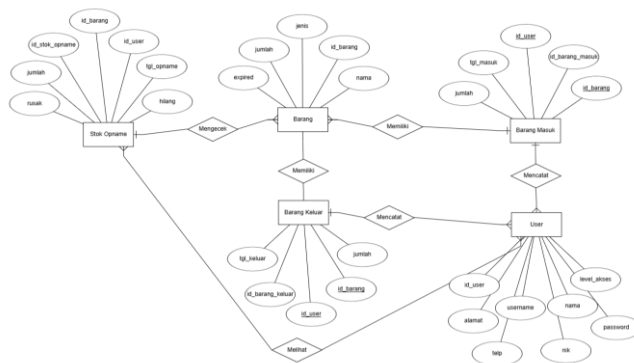
Use Case Diagram adalah satu jenis dari diagram UML (Unified Modelling Language) yang menggambarkan hubungan interaksi antara sistem dan aktor Use case diagram digunakan untuk menunjukkan peran aktor serta interaksi yang terjadi antara aktor dan sistem. Diagram ini menggambarkan fungsi-fungsi yang disediakan oleh sistem serta pihak yang berhak mengakses fungsi tersebut. Use case diagram pada sistem yang diusulkan dirancang untuk menjelaskan alur interaksi pengguna dengan sistem secara menyeluruh...



Gambar 3.2 Use Case Diagram

3.1.2 Entity-Relationship Diagram (ERD)

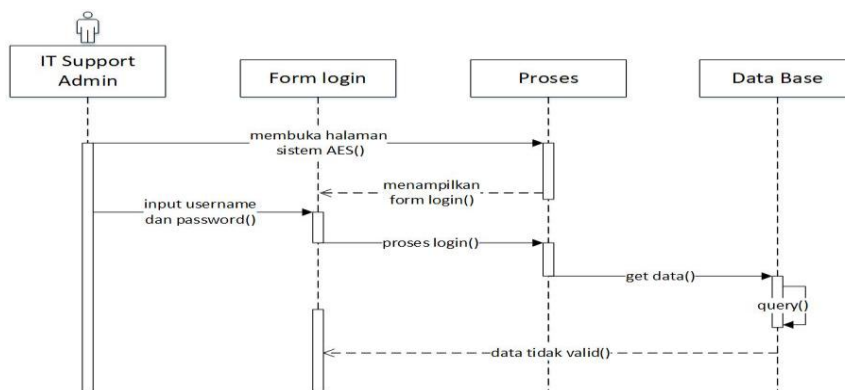
Diagram Entity-Relationship (ERD) metode pemodelan penelitian yang menggunakan diagram untuk menunjukkan informasi tentang atribut entitas yang berfungsi untuk menghubungkan hubungan satu sama lain dengan entitas lainnya.



Gambar 3.3 Entity-Relationship Diagram (ERD)

3.1.3 Sequence Diagram

Sequence diagram salah satu jenis diagram di UML (Unified Modeling Language) yang digunakan untuk menggambarkan interaksi antar objek dalam sebuah sistem berdasarkan urutan waktu.



Gambar 1.4 Sequence Diagram

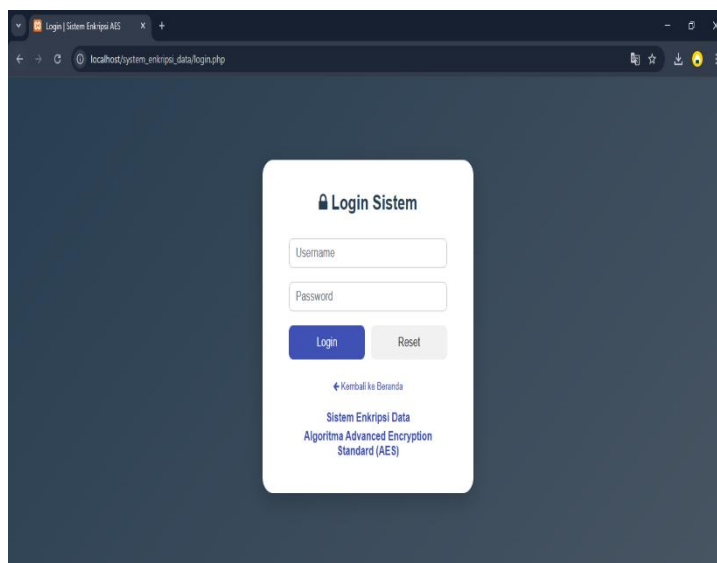
3.2 Implementasi Sistem

3.2.1 Halaman Utama



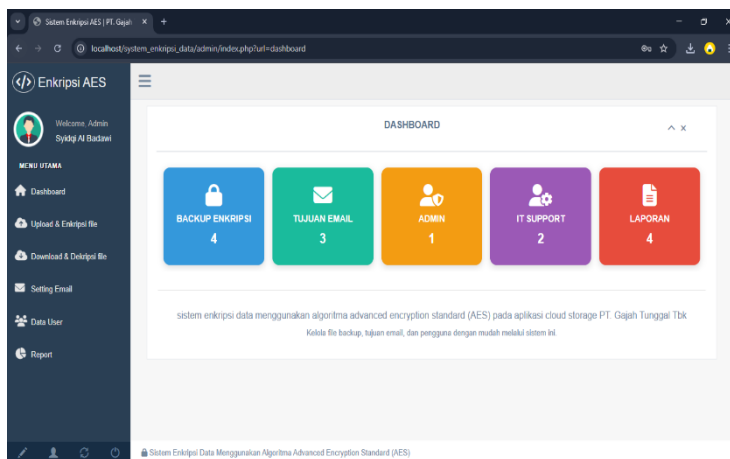
Gambar 3.5 Halaman Utama

3.2.2 Halaman Login



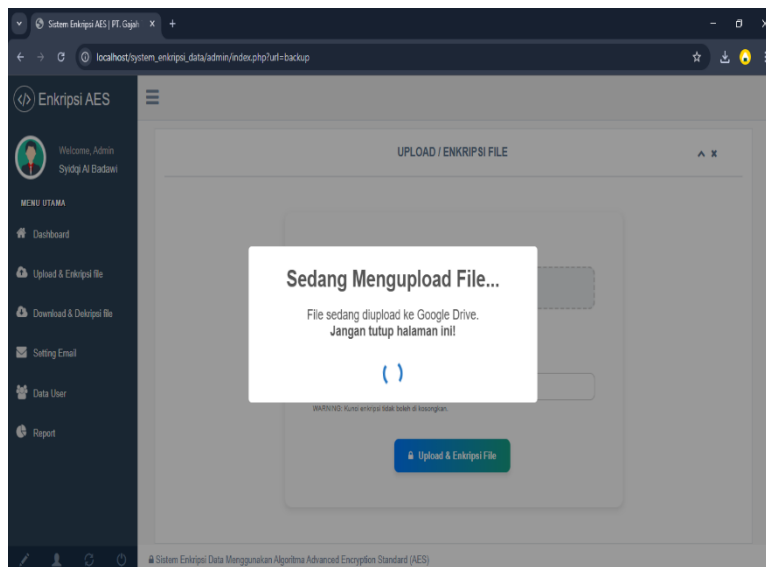
Gambar 3.6 Halaman Login

3.2.3 Halaman Dashboard



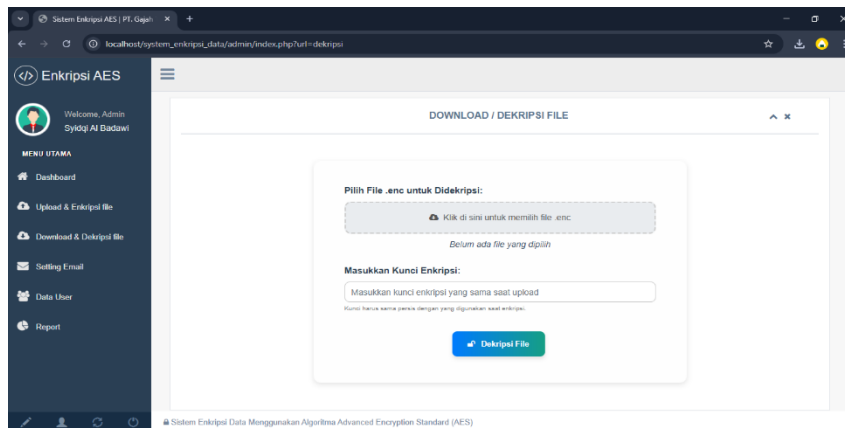
Gambar 3.7 Halaman Dashbaord

3.2.4 Halaman Upload Dan Enkripsi File



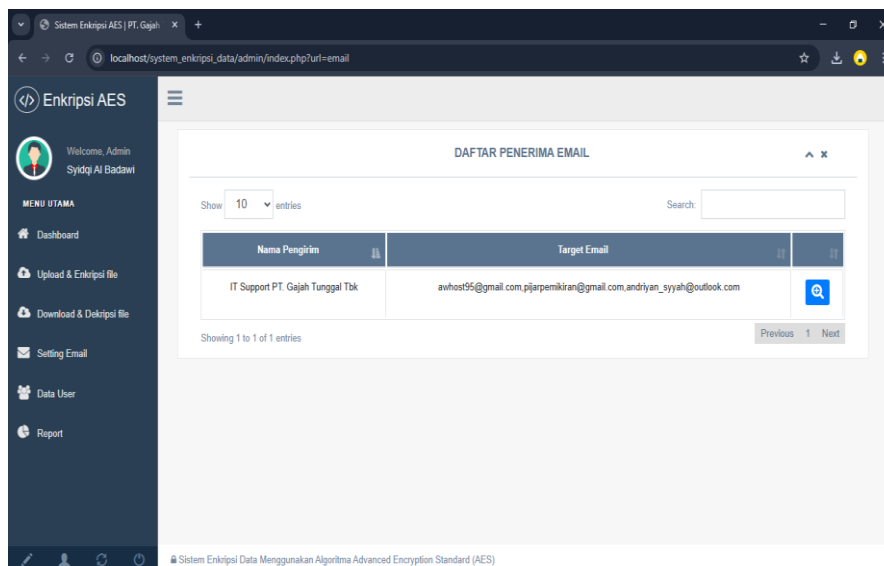
Gambar 3.8 Halaman Upload Dan Enkripsi File

3.2.5 Halaman Download Dan Dekripsi File



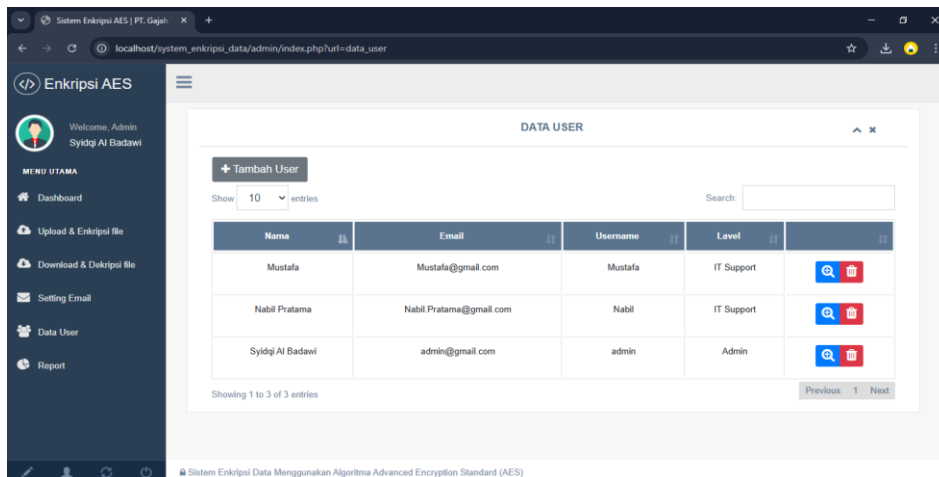
Gambar 3.9 Halaman Download Dan Dekripsi File

3.2.6 Halaman Settingan Email



Gambar 3.10 Halaman Settingan Email

3.2.7 Halaman Data User



Gambar 3.11 Halaman Data User

3.3 Testing

Berdasarkan tabel dibawah, seluruh fitur utama berjalan dengan baik tanpa error signifikan.

Table 1 Testing

No	Skenario Uji	Harapan Sistem	Hasil Uji	Kesimpulan
1	Membuka aplikasi	Sistem menampilkan halaman login	Berhasil	Diterima
2	Mengisi username dan password	Input diterima dan diproses oleh sistem	Berhasil	Diterima
3	Menekan tombol Login	Jika data salah muncul pesan error, jika benar diarahkan ke dashboard	Berhasil	Diterima
4	Menekan tombol Logout	Sistem mengakhiri sesi dan kembali ke halaman login	Berhasil	Diterima

4. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan terhadap Sistem Enkripsi Data Menggunakan Algoritma Advanced Encryption Standard (AES) pada Aplikasi Cloud Storage PT. Gajah Tunggal Tbk, maka diperoleh beberapa kesimpulan sebagai berikut:

- Dengan adanya sistem enkripsi data dapat mengotomatiskan proses backup database agar lebih efisien dan meminimalkan potensi kesalahan human error.



Saran

Berdasarkan hasil implementasi dan pengujian terhadap Sistem Enkripsi Data Menggunakan Algoritma Advanced Encryption Standard (AES) pada Aplikasi Cloud Storage PT. Gajah Tunggal Tbk, penulis menyadari bahwa sistem yang dikembangkan masih memiliki sejumlah keterbatasan yang dapat ditingkatkan pada penelitian maupun pengembangan berikutnya. Oleh karena itu, beberapa saran yang dapat diberikan adalah sebagai berikut:

- a. Sistem perlu dioptimalkan agar proses enkripsi dan dekripsi berjalan lebih cepat untuk file berukuran besar.
- b. Disarankan menambah pilihan layanan cloud storage lain sebagai alternatif selain Google Drive.
- c. Fitur notifikasi email perlu ditingkatkan dengan log status pengiriman yang lebih detail.
- d. Pengelolaan kunci enkripsi sebaiknya dibuat lebih aman, misalnya dengan enkripsi ganda atau penyimpanan terproteksi.
- e. Perlu ditambahkan fitur audit aktivitas agar setiap proses enkripsi, upload, dan dekripsi dapat tercatat secara rinci.
- f. Sistem dapat dikembangkan dalam versi mobile atau desktop untuk meningkatkan fleksibilitas pengguna.
- g. Diperlukan peningkatan tampilan antarmuka agar lebih responsif pada berbagai ukuran layar.
- h. Sistem sebaiknya memiliki fitur pengecekan otomatis terhadap file yang rusak sebelum diproses.
- i. Perlu ditambahkan opsi restore otomatis untuk mempermudah pemulihan data dari cloud.
- j. Keamanan akses pengguna dapat ditingkatkan dengan menambahkan autentikasi dua faktor (2FA).
- k. Fitur manajemen user sebaiknya dilengkapi dengan pengelompokan hak akses yang lebih beragam.
- l. Disarankan menambahkan fitur backup terjadwal otomatis tanpa perlu input manual dari pengguna.
- m. Sistem perlu menyediakan dashboard monitoring yang menampilkan grafik aktivitas backup harian.
- n. Dokumentasi sistem dan panduan penggunaan perlu disusun lebih lengkap untuk pengguna baru.

DAFTAR PUSTAKA

- Adlani, M. Adharis, & Putra, Ricky Eka. "Pengamanan Mnemonic Phrase Menggunakan Modified Advanced Encryption Standard." *Journal of Informatics and Computer Science (JINACS)*, 3.04 (2022): 425-434.
- Alfani, Mhd. Reza, Mhd. Furqan, & Nasution, Yusuf Ramadhan. "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (DSA) dan Advanced Encryption Standard (AES)." *Journal of Science and Social Research*, 7.1 (2024): 301-306.



- Andriyanto, Muhammad Riyan, Pristi Sukmasetya, & Penulis Korespondensi, E. "Penerapan Algoritma Advanced Encryption Standard (AES) untuk Keamanan Data Transaksi pada Sistem E-Marketplace." *Journal of Computer System and Informatics (JoSYC)*, 4.1 (2022): 179-187.
- Bibiola, Fimianti, Toibah Umi Kalsum, & Hendri Alamsyah. "Penerapan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File pada Aplikasi Berbasis Web." *Jurnal Surya Energy*, 8.1 (2023): 35-51.
- Cristy, Niolinda, & Fristi Riandari. "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan." *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, 4.2 (2021): 75-85.
- Fahlevvi, Mohammad Rezza, Dhita Satria Aprilliana Putra, & Wahyu Ariandi. "Algoritma AES128-CBC untuk Enkripsi dan Dekripsi Berkas Dokumen PT. Adiarta Muzizat." *Journal of Innovation and Future Technology (IFTECH)*, 7.1 (2025): 166-176.
- Ferdiansyah, Ferdiansyah. "Penggunaan QR Code Berbasis Kriptografi Advanced Encryption Standard (AES) untuk Administrasi Rekam Medis." *Jurnal Syntax Admiration*, 2.10 (2021): 1870-1884.
- Hermawati, Fefiana Diny, et al. "Keamanan E-Voting di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advanced Encryption Standard)." *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, 2.2 (2023): 45-56.
- Irawan, Brikitha Olivia Putri Irine, et al. "Implementasi Kriptografi pada Keamanan Data Menggunakan Algoritma Advanced Encryption Standard (AES)." *Jurnal Simantec*, 11.2 (2023): 167-174.
- Kafa, Nizamuddin Aulia, & Dolly Virgian Shaka Yudha Sakti. "Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria." *Jurnal Ticom*, 12.2 (2024): 50-55.
- Kaur, G., & Singh, R. "Analysis of Modern IDEs for Web Development Productivity: A Comparative Study of Visual Studio Code and Sublime Text." *International Journal of Computer Applications*, 184(12) (2022): 25-32.
- Khoirudin, Nurfauzan Humam, & Windarto, Windarto. "Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web." *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, 4.1 (2024): 62-71.
- Li, J., & Wang, P. "Secure and Scalable Cloud Storage Framework with Data Synchronization." *Journal of Cloud Computing Research*, 10(3) (2022): 201-212.
- Lingga, Teguh Wijaya, Oris Krianto Sulaiman, & Khairuddin Nasution. "Advanced Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data pada Aplikasi E-Pariwisata." *Sudo Jurnal Teknik Informatika*, 3.4 (2024): 201-216.
- Muchamad, Reski Mulud, Asriyanik Asriyanik, & Agung Pambudi. "Implementasi Algoritma Advanced Encryption Standard (AES) untuk Mengenkripsi Datastore pada Aplikasi Berbasis Android." *Jurnal Mnemonic*, 6.1 (2023): 55-64.
- Oktaviani, Selli, Fahrizal Rizky, & Indra Gunawan. "Analisis Keamanan Data dengan Menggunakan Kriptografi Modern Algoritma Advanced Encryption Standard (AES)." *Jurnal Media Informatika*, 4.2 (2023): 97-101.
- Pujiono, Imam Prayogo, Eko Hari Rachmawanto, & Dicky Anggriawan Nugroho. "The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images." *Journal of Applied Intelligent System*, 8.1 (2023): 69-80.
- Putra, Yendi, Y. Yuhandri, & Sumijan. "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Serangan Cross Site Scripting." *Jurnal Sistim Informasi dan Teknologi*, (2021): 56-63.



- Putri, A. Eka, Aghistina Kartikadewi, & LA Abdul Rosyid. "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang." *Applied Information System Management*, 3.2 (2021): 69-78.
- Putranto, Reynaldo Dwi. "Analisa dan Perancangan Sistem Keamanan File dengan Advanced Encryption Standard (AES) Berbasis Website." *Jurnal Informatika MULTI*, 1.6 (2023): 601-611.
- Rahman, M., Singh, A., & Patel, R. "Enhancing Cloud Data Confidentiality Using AES-Based Hybrid Cryptosystem." *Journal of Cloud Computing and Security*, 12(1) (2023): 88-97.
- Ramadhani, Tarisa Auliya, Adi Fajaryanto Cobantoro, & Sugianti. "Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem Registrasi Pasien." *Jurnal Informatika Polinema*, 10.4 (2024): 521-526.
- Sianipar, Josua Syahputra, Nurcahyo Budi Nugroho, & Ita Mariami. "Pengamanan Data Gaji Karyawan dengan Menggunakan Metode Advanced Encryption Standard (AES)." *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, 3.1 (2024): 35-45.
- Zhang, L., Huang, X., & Liu, Y. "Cloud Storage Systems: Architecture, Security Challenges, and Future Directions." *IEEE Access*, 9 (2021): 134521-134534.
- Zulkarnain, Aliffia Nurrohmah, et al. "Analisis Proses Enkripsi Algoritma Kriptografi Modern Advanced Encryption Standard (AES)." *Jurnal Adijaya Multidisiplin*, 1.02 (2023): 380-387.