SISTEM ENKRIPSI FILE DENGAN ID-CARD MENGGUNAKAN LARAVEL

File Encryption System With ID-CARD Using Laravel

Diva Ramadhan[1*], Muhammad Imam Gunawan[2]
[1]*Program Studi Teknik Informatika,* [2]*Politeknik TEDC Bandung*
*Penulis Korespondensi: diparamadhan31@gmail.com

DOI: *https://doi.org/10.58217/ipsikom.v13i2.103*

ABSTRAK

The security of digital data is increasingly critical in today's era of information exchange. Many breaches occur due to weak file protection in web-based systems. This study aims to develop a web-based file encryption system using the Advanced Encryption Standard (AES) algorithm, integrated with ID Card or QR Code authentication to restrict file access. The system was built using the Laravel framework and developed through the Waterfall method, covering stages of analysis, design, implementation, and testing. Key features include automatic file encryption during upload, folder management, and dual authentication. Administrators can manage users, while regular users can only upload and manage personal files. The implementation results show that files were successfully encrypted and access was limited to users with valid authentication. The system improves confidentiality and access control, offering a secure alternative for file storage in environments such as financial institutions.

Keywords: *File Encryption, Advanced Encryption Standard (AES), Laravel, ID Card, Waterfall*

PENDAHULUAN

Perkembangan teknologi informasi berbasis web telah membawa dampak signifikan terhadap pengelolaan data di berbagai sektor, seperti pendidikan, kesehatan, dan keuangan. Pemanfaatan sistem informasi berbasis web memberikan kemudahan akses, efisiensi waktu, dan peningkatan produktivitas dalam pengelolaan data. Namun, di sisi lain, tantangan baru muncul terkait aspek keamanan data. Dokumen digital tanpa perlindungan memadai rentan terhadap kebocoran dan penyalahgunaan. Oleh karena itu, diperlukan sistem pengamanan yang efektif.

Berbagai penelitian terdahulu telah membahas pemanfaatan teknologi web untuk pengembangan sistem informasi. Termasuk di dalamnya adalah pengembangan sistem informasi yang mendukung pertukaran data digital melalui platform berbasis web. (Alif Ramadhan et al., 2023) dalam tinjauan literaturnya mengungkapkan bahwa metode *Waterfall* merupakan pendekatan yang tepat untuk pengembangan sistem informasi berbasis web dengan kebutuhan yang terdefinisi secara jelas, karena alur kerjanya yang sistematis dan terstruktur. Selain itu, penelitian oleh (Alvrahesta et al., 2023) menunjukkan bahwa *framework* Laravel banyak digunakan dalam pengembangan sistem informasi berbasis web karena kemampuannya dalam sejumlah keunggulan termasuk routing yang mudah dan kemampuan dalam pengamanan data digital.

Dari sisi keamanan, beberapa penelitian juga telah menyoroti pentingnya proteksi data (Husain et al., 2024) menyatakan bahwa Laravel memiliki mekanisme keamanan bawaan yang mampu mencegah serangan umum, seperti *SQL Injection* dan *Cross-Site Scripting* (XSS), serta mendukung proses enkripsi data untuk menjaga kerahasiaan informasi. (Ujung et al., 2023) menekankan pentingnya keamanan database untuk melindungi data pribadi pengguna agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Namun demikian, sebagian besar penelitian sebelumnya masih terbatas pada penerapan enkripsi dasar dan belum mengintegrasikan metode autentikasi fisik seperti penggunaan ID Card sebagai lapisan keamanan tambahan.

Berdasarkan studi kasus yang dilakukan di BJB Syariah, khususnya pada Divisi Penyelamatan Penyelesaian Pembiayaan, menunjukkan bahwa pengelolaan file penting masih bergantung pada Cloud Drive dengan pengamanan

standar, di mana file belum dienkripsi secara optimal. Penelitian ini mengembangkan sistem enkripsi file berbasis web menggunakan algoritma AES dan autentikasi ID Card/QR Code sebagai lapisan keamanan tambahan.

Penelitian oleh (Wellem Taju et al., 2024) menunjukkan bahwa integrasi QR Code dan teknologi geolokasi dalam sistem absensi dapat meningkatkan keamanan dan akurasi verifikasi identitas pada sistem berbasis web, sehingga pendekatan autentikasi fisik menjadi semakin relevan.

Framework Laravel dipilih karena mendukung arsitektur MVC, middleware keamanan, serta praktik *secure coding* yang mengikuti standar OWASP (Sismadi et al., 2022). Sistem ini dikembangkan menggunakan pendekatan *Waterfall* melalui tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian. Sistem yang dikembangkan diharapkan dapat meningkatkan keamanan file digital melalui penerapan enkripsi yang kuat serta penggunaan autentikasi dua langkah untuk memperkuat perlindungan akses.

Kontribusi utama dari penelitian ini adalah menggabungkan algoritma enkripsi AES dengan autentikasi berbasis ID Card/QR Code dalam satu sistem web terintegrasi menggunakan Laravel, yang jarang diimplementasikan dalam pendekatan sebelumnya.

Penelitian mengenai keamanan data digital dan sistem informasi berbasis web telah banyak dilakukan dalam beberapa tahun terakhir. Salah satu pendekatan yang umum digunakan adalah penerapan algoritma enkripsi, seperti *Advanced Encryption Standard* (AES), yang terbukti efektif dalam menjaga kerahasiaan data. Penelitian oleh (Handoyo & Subakti, 2020) menunjukkan bahwa AES memiliki tingkat keamanan yang tinggi dan sangat cocok untuk mengamankan file dokumen digital.

Dalam konteks pengembangan sistem informasi berbasis web, framework Laravel banyak dipilih karena menyediakan berbagai fitur keamanan bawaan. (Husain et al., 2024) menyatakan bahwa Laravel memiliki proteksi terhadap serangan umum seperti *SQL Injection* dan *Cross-Site Scripting* (XSS), serta mendukung penerapan enkripsi data. Hal ini menjadikan Laravel sebagai pilihan tepat untuk membangun aplikasi dengan kebutuhan keamanan tingkat lanjut.

Selain enkripsi, autentikasi juga menjadi aspek penting dalam menjaga integritas sistem. (Divva et al., 2022)) meneliti integrasi AES dan autentikasi berbasis token (seperti *password* atau OTP), namun belum mengintegrasikan autentikasi berbasis ID Card atau QR Code. Penelitian ini mencoba mengisi celah tersebut dengan mengombinasikan AES-256 dan autentikasi berbasis ID Card, sehingga sistem memiliki dua lapisan keamanan: logika dan fisik.

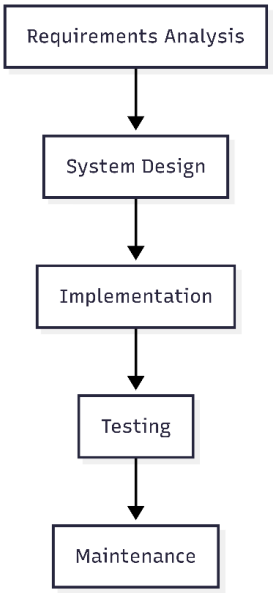
Dari sisi metodologi pengembangan, model *Waterfall* dinilai sesuai untuk proyek yang memiliki kebutuhan jelas sejak awal. (Alif Ramadhan et al., 2023) mengungkapkan bahwa *Waterfall* cocok untuk pengembangan sistem informasi yang terstruktur dan tidak membutuhkan perubahan besar selama proses pengembangan.

Terakhir, (Ujung et al., 2023) menyoroti pentingnya pemeliharaan sistem informasi, terutama yang berkaitan dengan keamanan basis data. Pemeliharaan sistem secara berkala dapat mencegah terjadinya kebocoran data dan memastikan sistem tetap relevan terhadap pembaruan teknologi.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode pengembangan perangkat lunak *System Development Life Cycle* (SDLC) model *Waterfall*. Model ini dipilih karena cocok diterapkan pada proyek dengan kebutuhan sistem yang sudah terdefinisi secara jelas sejak awal dan setiap tahapannya dilakukan secara berurutan.

Model *Waterfall* digambarkan seperti aliran air terjun, di mana setiap tahap harus diselesaikan sebelum melanjutkan ke tahap berikutnya. Berikut adalah ilustrasi model *Waterfall* yang digunakan dalam penelitian ini:



Gambar 1. Metode *Waterfall*

Adapun tahapan-tahapan dalam metode Waterfall yang diterapkan pada penelitian ini adalah sebagai berikut:

1) Requirement Analysis

Tahap ini bertujuan untuk mengidentifikasi kebutuhan sistem baik secara fungsional maupun non-fungsional. Proses pengumpulan kebutuhan dilakukan melalui Analisa sistem yang sedang berjalan di BJB Syariah, khususnya pada Divisi Penyelamatan Penyelesaian Pembiayaan.

Pada divisi tersebut, penyimpanan file nasabah saat ini masih mengandalkan *Cloud Drive* dengan pengamanan standar dan autentikasi satu langkah. Untuk meningkatkan keamanan, diperlukan penerapan mekanisme pengamanan tambahan.

Berdasarkan kebutuhan tersebut, dirancanglah sebuah sistem yang mampu mengamankan file dengan enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES). Pemilihan AES didasarkan pada penelitian (Handoyo & Subakti, 2020) yang menunjukkan bahwa algoritma ini memiliki tingkat keamanan yang tinggi dalam melindungi dokumen digital.

Selain itu, sistem ini juga mengintegrasikan metode autentikasi menggunakan ID Card atau QR Code. Pendekatan ini terinspirasi dari penelitian (Divva et al., 2022) yang mengombinasikan AES-256 dengan autentikasi tambahan untuk meningkatkan keamanan data. Penerapan ID Card serta autentikasi dua langkah diharapkan mampu memperkuat perlindungan terhadap data digital secara signifikan.

2) System Design

Pada tahap perancangan sistem, digunakan pendekatan UML (*Unified Modeling Language*) untuk menggambarkan alur proses sistem secara visual.

Peneliti menggunakan *Use Case Diagram* untuk mendeskripsikan interaksi antara aktor dan sistem, serta *Entity Relationship Diagram* (ERD) untuk menggambarkan struktur data dan relasi antar entitas dalam basis data. Menurut (Sastra, 2021), penggunaan UML sangat penting dalam proses perancangan sistem informasi karena dapat mempermudah pemahaman hubungan antar komponen sistem serta memperjelas alur kerja yang akan dibangun.

3) Implementation

Sistem diimplementasikan menggunakan Laravel versi terbaru yang mendukung enkripsi AES-256 dan menyediakan fitur keamanan bawaan. Berdasarkan penelitian yang dilakukan oleh (Husain et al., 2024) Laravel dilengkapi dengan perlindungan bawaan terhadap serangan umum seperti *SQL Injection dan Cross-Site Scripting (XSS),* Hal ini menjadikan Laravel sesuai untuk pengembangan aplikasi yang berfokus pada perlindungan data, termasuk pencegahan serangan *brute force*. Pengembangan sistem dilakukan menggunakan Laravel di komputer berbasis Windows.

4) Testing

Tahap pengujian dilakukan menggunakan metode *Black Box Testing*, yaitu pengujian yang berfokus pada fungsionalitas sistem dengan cara menjalankan sistem melalui beberapa skenario pengujian yang meliputi:

1. Sistem menyediakan fitur registrasi, login, dan secara otomatis menghasilkan ID Card digital bagi pengguna terdaftar.
2. Pengguna dapat melakukan verifikasi identitas dengan dua metode, yaitu melalui akses kamera untuk memindai ID

Card secara langsung atau dengan mengunggah gambar ID Card secara manual serta menampilkan pesan kesalahan jika data tidak valid.
3. Sistem menampilkan daftar folder dan file sesuai identitas pengguna, lengkap dengan informasi jumlahnya, serta memastikan penyimpanan data identitas secara terenkripsi demi menjaga keamanan.
4. Sistem memberikan informasi lengkap mengenai jumlah folder dan file yang dimiliki oleh pengguna, disertai dengan rincian nama dan lokasi penyimpanan.
5. Sistem melakukan validasi terhadap QR Code atau ID Card yang diberikan untuk memastikan data cocok dengan identitas yang tersimpan. Proses ini dilakukan secara otomatis dan real-time.

5) Maintenance

Pemeliharaan dilakukan secara berkala untuk memastikan sistem tetap aman dan berjalan optimal. Pemeliharaan meliputi:
1. Melakukan pengembangan fitur tambahan sesuai kebutuhan pengguna di masa mendatang.
2. Perbaikan *bug* apabila ditemukan selama penggunaan.
3. Melakukan penambahan kapasitas penyimpanan secara berkala dengan kebutuhan pertumbuhan data pengguna.

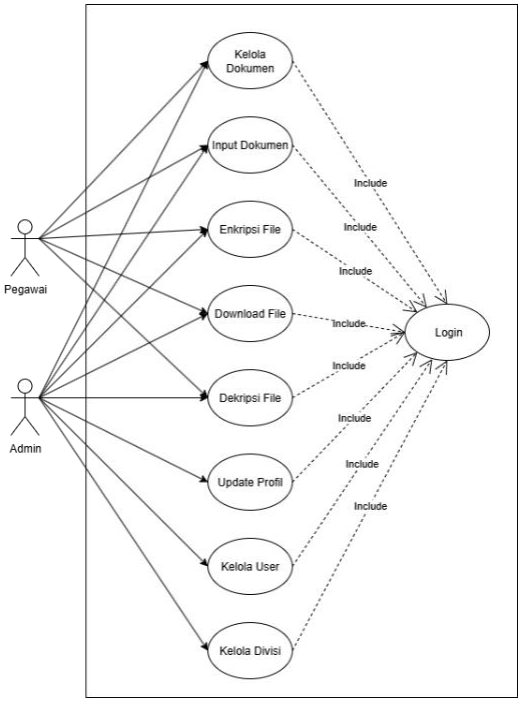
Menurut (Ujung et al., 2023) pemeliharaan rutin pada sistem informasi sangat penting untuk mencegah celah keamanan yang mungkin muncul akibat pembaruan teknologi.

Software Requirement

Berdasarkan hasil analisis dan pengujian yang telah dilakukan di Bank BJB Syariah, sistem yang dikembangkan harus memenuhi beberapa kebutuhan fungsional utama yaitu:
1. Sistem harus menyediakan mekanisme registrasi dan login bagi pengguna untuk membuat akun baru atau masuk ke dalam sistem dengan data yang valid, sehingga pengguna dapat langsung diarahkan ke halaman utama setelah berhasil login.
2. Sistem menyediakan fitur autentikasi melalui kamera atau unggah ID Card, memungkinkan pengguna untuk memverifikasi identitas mereka dengan memindai langsung melalui kamera perangkat atau mengunggah gambar ID Card/QR Code secara manual.
3. Sistem wajib melakukan verifikasi terhadap ID Card atau QR Code yang diunggah atau dipindai, memastikan data sesuai dengan yang tersimpan di sistem, dan menolak akses apabila data tidak valid serta menampilkan pesan kesalahan secara otomatis.
4. Sistem harus menampilkan daftar folder dan file milik pengguna berdasarkan identitas yang telah diverifikasi, dengan memastikan bahwa hanya data milik pengguna yang ditampilkan dan dapat diakses.
5. Sistem wajib menyajikan informasi jumlah folder dan file yang dimiliki oleh pengguna, termasuk rincian nama dan lokasi dari setiap item yang tersedia di dalam sistem.
6. Sistem secara otomatis menghasilkan dan menyediakan ID Card digital bagi setiap pengguna yang telah menyelesaikan proses registrasi, yang dapat digunakan kembali untuk proses login atau autentikasi lanjutan.

System Design

Berikut adalah rancangan interaksi antara user dengan sistem yang digambarkan melalui UML:



Gambar 2. *Use case diagram*

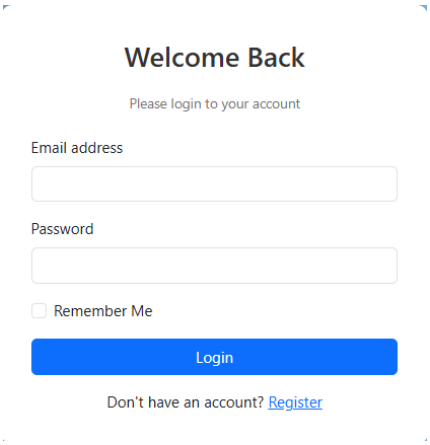
Use Case Diagram di atas menjelaskan fungsi-fungsi utama dalam sistem pengelolaan dokumen digital yang semuanya mengharuskan pengguna untuk melakukan proses login terlebih dahulu. Proses autentikasi ini diwujudkan melalui relasi *include* yang menghubungkan setiap *use case* dengan *use case* login, sehingga login menjadi syarat utama untuk mengakses fitur seperti kelola dokumen, input dokumen, enkripsi dan dekripsi file, download file, update profil, serta pengelolaan user dan divisi.

Gambar 3. *Entity Relationship Diagram*

IMPLEMENTASI

Adapun rancangan interaksi user dengan sistem yang dilakukan melalui UI/UX adalah sebagai berikut:

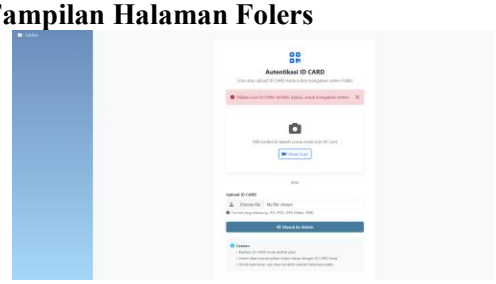
Tampilan Halaman Login



Gambar 4. Tampilan Halaman Login

Gambar 4. Halaman ini berfungsi sebagai gerbang autentikasi pengguna untuk mengakses sistem. Melalui halaman ini, sistem akan memverifikasi pengguna sebelum memberikan akses ke fitur-fitur yang tersedia

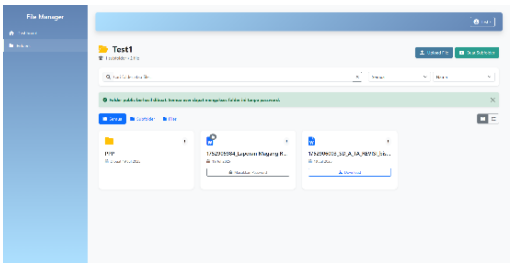
Tampilan Halaman Folers



Gambar 5. Halaman Folders

Gambar 5. Halaman ini memverifikasi identitas pengguna melalui pemindaian QR Code dengan kamera atau unggahan gambar ID Card.Verifikasi ini menjadi tahap autentikasi sebelum pengguna dapat mengakses folder atau file dalam sistem.

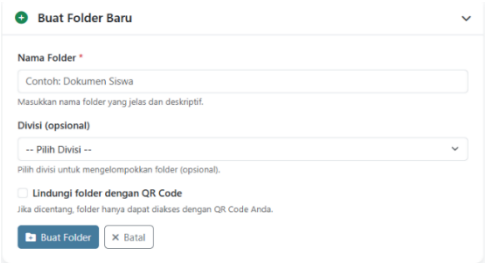
Setelah Verifikasi ID Card



Gambar 6. Halaman Folders Setelah Berhasil Melakukan Pemindaian

Gambar 6. Sistem akan menampilkan daftar folder dan file pengguna setelah ID Card atau QR Code terverifikasi. Pada tahap ini, pengguna dapat mengakses folder untuk membuka, mengunduh, ataupun menambahkan file baru

Halaman Tambah Folders



Gambar 7. Tampilan Halaman Tambah Folder

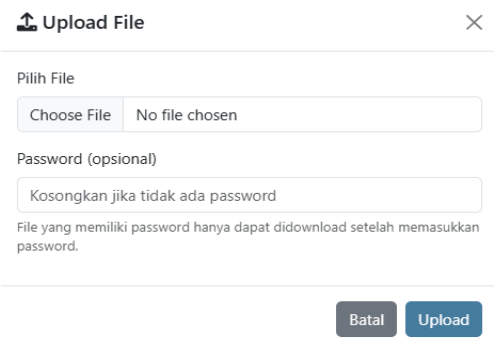
Gambar 7. Halaman ini digunakan untuk membuat folder baru. Pengguna dapat memasukkan nama folder, memilih divisi, dan mengaktifkan opsi perlindungan folder dengan QR Code agar hanya dapat diakses oleh pemilik yang terverifikasi

Halaman Detail Folders

Gambar 8. Tampilan Detail Folder

Gambar 8. Halaman ini menampilkan isi dari folder yang dipilih. Pengguna dapat melihat daftar file di dalam folder, mengunggah file baru, serta mengunduh atau menghapus file yang sudah ada sesuai dengan hak akses yang dimiliki

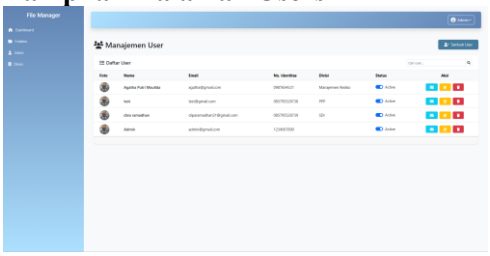
Tampilan Halaman Input Dokumen



Gambar 9. Halaman Input Dokumen

Gambar 9. Halaman ini digunakan untuk mengunggah file ke dalam folder. Pengguna dapat memilih file yang akan diunggah dan menambahkan kata sandi opsional untuk melindungi file. File yang diberi kata sandi hanya dapat diunduh setelah pengguna memasukkan kata sandi yang benar.

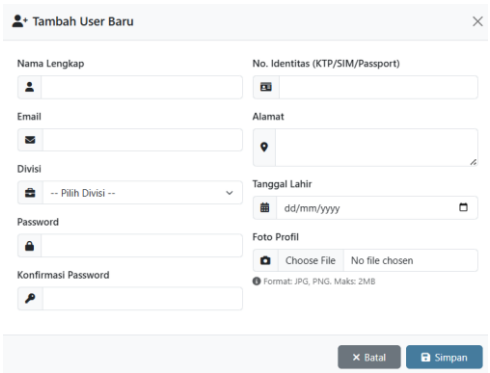
Tampilan Halaman Users



Gambar 10. Halaman User

Gambar 10. Halaman ini hanya dapat diakses oleh admin untuk mengelola data pengguna. Admin dapat melihat daftar pengguna, termasuk informasi nama, email, nomor telepon, divisi, dan status akun. Selain itu, admin memiliki kontrol penuh untuk mengedit, menonaktifkan, atau menghapus akun pengguna sesuai kebutuhan.

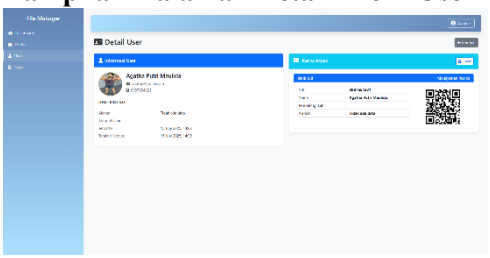
Tampilan Halaman Tambah User



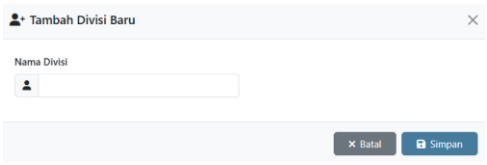
Gambar 11. Tampilan Halaman Tambah User

Gambar 11. Halaman ini digunakan oleh admin untuk menambahkan pengguna baru ke dalam sistem. Admin dapat mengisi data lengkap seperti nama, nomor identitas (KTP/SIM/Passport), email, alamat, divisi, tanggal lahir, password (beserta konfirmasi), serta mengunggah foto profil. Setelah semua data terisi, admin dapat menyimpan data untuk menambahkan pengguna baru.

Tampilan Halaman Detail Profil User

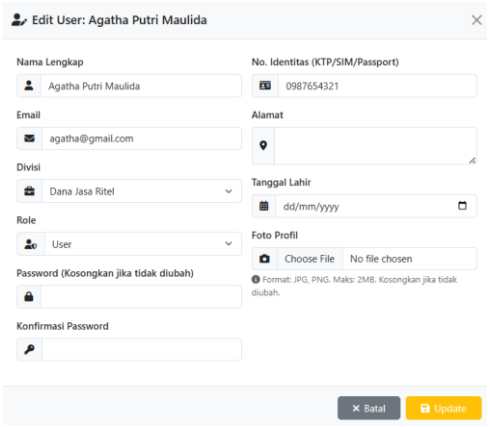


Gambar 12. Halaman Detail Profil User



Gambar 12. Halaman ini menampilkan informasi lengkap mengenai profil pengguna, termasuk foto profil, nama lengkap, email, nomor identitas, dan data pribadi lainnya. Selain itu, tersedia juga kartu akses dalam bentuk QR Code yang dapat digunakan untuk autentikasi dan akses ke dalam sistem

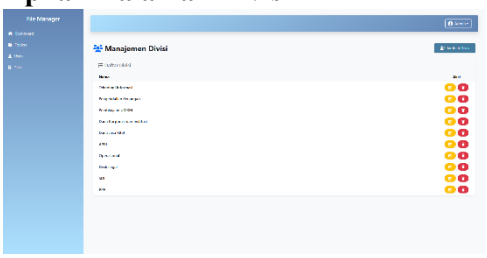
Tampilan Halaman Edit User



Gambar 13. Halaman Edit User

Gambar 13. Halaman ini digunakan untuk memperbarui data pengguna yang sudah terdaftar. Admin dapat mengubah informasi seperti nama lengkap, nomor identitas, email, alamat, divisi, role pengguna, tanggal lahir, serta mengganti foto profil. *Password* hanya perlu diisi jika ingin diperbarui, sedangkan jika tidak diubah, kolomnya dapat dikosongkan.

Tampilan Halaman Divisi



Gambar 14. Tampilan Halaman Divisi

Gambar 14. Halaman ini berfungsi untuk mengelola data divisi yang ada dalam sistem. Admin dapat melihat daftar divisi, menambah divisi baru, mengedit nama divisi, atau menghapus divisi yang sudah tidak diperlukan. Fitur ini membantu pengelompokan folder atau file berdasarkan divisi untuk memudahkan manajemen data.

Tampilan Tambah Divisi

Gambar 15. Tampilan Tambah Divisi

Gambar 15. Halaman ini digunakan oleh admin untuk menambahkan divisi baru ke dalam sistem. Admin hanya perlu memasukkan nama divisi yang sesuai, kemudian menyimpannya. Fitur ini berguna untuk memperbarui struktur organisasi agar folder atau file dapat dikelompokkan sesuai dengan divisi terkait.

Tampilan Halaman Divisi

Tampilan Edit Divisi

Gambar 16. Tampilan Edit Divisi

Gambar 16. Halaman ini digunakan oleh admin untuk memperbarui atau mengubah nama divisi yang sudah ada di dalam sistem. Fitur ini memudahkan pengelolaan divisi agar tetap sesuai dengan perubahan struktur organisasi atau penyesuaian nama divisi di instansi terkait.

TESTING

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fitur dan fungsi yang telah diimplementasikan pada sistem berjalan sesuai dengan kebutuhan yang telah ditetapkan. Metode pengujian yang

digunakan adalah *Black Box Testing*, yang berfokus pada pengujian fungsionalitas. Tabel berikut menunjukkan skenario pengujian:

Tabel 1. Tabel Pengujian

No	Fitur yang diuji	Hasil yang Diharapkan	Kesimpulan
1	Registrasi dan Login	Sistem menyimpan akun baru dan mengarahkan pengguna ke halaman utama setelah login	Valid
2	Akses Kamera atau Unggah ID Card	Sistem menampilkan tampilan untuk upload file gambar ID atau buka kamera	Valid
3	Verifikasi ID Card	Sistem membaca QR dan memverifikasi identitas pengguna	Valid
4	Validasi QR Code atau ID Card	Sistem menolak akses dan menampilkan pesan error	Valid
5	Menampilkan folder & file sesuai identitas	Sistem hanya menampilkan file/folder milik pengguna terkait	Valid
6	Menampilkan jumlah folder dan file	Sistem menampilkan total jumlah folder dan file milik pengguna	Valid
7	Menyediakan ID Card untuk pengguna	Sistem men-generate dan memberikan ID Card dalam format QR code	Valid

Tabel 2. Tabel Pengujian Rata-rata

No	Ukuran File	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	100kb	0,95	1,05
2	500kb	1,04	1,15
3	1mb	1,09	1,20
4	10mb	2,01	1,26

KESIMPULAN

Berdasarkan hasil penelitian dan pengembangan sistem enkripsi file berbasis web, dapat disimpulkan bahwa sistem ini berhasil meningkatkan keamanan penyimpanan file melalui penerapan algoritma *Advanced Encryption Standard* (AES). Sistem mampu membatasi akses file Sistem berhasil membatasi akses file hanya untuk pengguna yang memiliki kunci dekripsi. *Framework* Laravel digunakan untuk membangun fitur pengelolaan folder dan file yang diamankan dengan kata sandi serta enkripsi AES.

Selain itu, penerapan autentikasi tambahan menggunakan ID Card atau QR Code terbukti efektif dalam membatasi akses folder hanya untuk pengguna yang memiliki identitas valid, sehingga menambahkan lapisan keamanan fisik dan digital secara bersamaan. Pengujian menggunakan metode *Black Box Testing* menunjukkan bahwa seluruh fitur utama, seperti unggah, enkripsi, dekripsi, autentikasi ID Card, pengunduhan file terenkripsi, dan penghapusan file telah berjalan sesuai dengan spesifikasi.

Kontribusi utama dari sistem ini adalah integrasi antara enkripsi AES dan autentikasi berbasis ID Card dalam satu platform web, yang belum banyak diimplementasikan dalam sistem penyimpanan file konvensional. Pendekatan ini menawarkan solusi keamanan berlapis (*layered security*) yang memadukan proteksi logis dan fisik untuk mengurangi risiko kebocoran data. Dengan demikian, sistem ini dapat menjadi alternatif penyimpanan file yang lebih aman dibandingkan layanan *cloud* umum yang cenderung rentan terhadap akses tidak sah.

DAFTAR PUSTAKA

Alif Ramadhan, J., Tresya Haniva, D., & Suharso, A. (2023). Systematic Literature Review Penggunaan Metodologi Pengembangan Sistem Informasi Waterfall, Agile, dan Hybrid. In *Journal Information Engineering and Educational Technology* (Vol. 07).

Alvrahesta, A., Pertiwi Windasari, I., Budi Prasetijo, A., Windasari, I. P., Prasetijo, A. B., & Bangun Sistem Informasi Penerimaan, R. (2023). Rancang Bangun Sistem Informasi Penerimaan Beasiswa Sariraya Co. Ltd. Menggunakan Framework Laravel dan Bootstrap How to cite: A. *Jurnal Teknik Komputer*, *2*(1), 1–10. https://doi.org/10.14710/jtk.v2i1.37723

Divva, G., Zulma, M., Seta, H. B., & Yuniati, T. (2022). *Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen*.

Handoyo, J., & Subakti, Y. M. (2020). *Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES)*. http://www.jurnal.umk.ac.id/sitech

Husain, S. M., Azhari, L., Aksani, M. L., & Saputra, S. A. (2024). Analisis dan Implementasi Fitur Keamanan Aplikasi Pada Framework Laravel. *JIKA (Jurnal Informatika)*, *8*(3), 281. https://doi.org/10.31000/jika.v8i3.11198

Sastra, R. (2021). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Penggajian. *Jurnal Teknik Komputer AMIK BSI*, *7*(1). https://doi.org/10.31294/jtk.v4i2

Sismadi, W., Agung Martono, B., & Widyastuti, T. (2022). Comparative Analysis of Codeigniter, Laravel and Ktupad Frameworks: Case Study Online Exam Applications-Sismadi et al. *Indonesian Journal of Applied Research (IJAR)*, *3*(3), 207–219. https://doi.org/10.30997/ijar.v3i3.236

Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44. http://jurnal.unidha.ac.id/index.php/jteksis

Wellem Taju, S., Putra Mamahit, Y., & Andrew Pongantung, J. (2024). Implementing QR code and Geolocation Technologies for the Student Attendance System. *COGITO Smart Journal*, *10*(1).