Journal of Artificial Intelligence and Innovative Applications
Vol. 06, No. 4, November 2025
ISSN : 2716-1501 | E-ISSN : 2775-4057
Hal : 114-131

IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK KEAMANAN DATA FILE UJIAN SISWA SMK JAYA BUANA TANGERANG BERBASIS *WEB*

Ahmad Buhori [1], Dani [2]

[1]*Teknik Informatika,. Fakultas Ilmu Komputer, Universitas Pamulang, Jl Raya Puspitek, Buaran, Kec.Pamulang, Kota Tangerang Selatan, Banten 15310*
e-mail: [1] Ahahmadbuhori801@gmail.com, [2] dosen02510@unpam.ac.id

Info Artikel

Riwayat Artikel:

Received oktober 20, 2025
Revised oktober 25, 2025
Accepted november 03, 2025

Abstract *– This study aims to enhance the security of student exam files through the implementation of the Advanced Encryption Standard (AES) within a web-based system. The research method includes requirement analysis and system design using the Waterfall model, implementation of symmetric-key encryption and decryption processes, functional testing, and user evaluation using the PISCES model (Performance, Information, System, Control, Efficiency, Service). The results show that AES effectively protects exam files in .pdf, .docx, and .xlsx formats from potential data leakage, as encrypted files can only be accessed using a valid decryption key. The authentication mechanism also successfully restricts access to authorized users, preventing unauthorized access to exam materials. User evaluation involving 25 teachers out of a total of 34 teachers produced an average score of 87.1%, demonstrating that the system is feasible and effective for secure, centralized, and efficient exam file management. This research further provides a foundation for future development, including cloud-based deployment and expanded support for additional file formats to increase system flexibility.*

Keywords: *AES, Cryptography, Data Security, File Encryption, Web-Based System*

Corresponding Author:
Ahmad Buhori
Email: ahmadbuhori801@gmail.com

Abstrak Indonesia *– Penelitian ini bertujuan untuk meningkatkan keamanan file ujian siswa melalui penerapan algoritma Advanced Encryption Standard (AES) dalam sebuah sistem berbasis web. Metode penelitian meliputi analisis kebutuhan dan perancangan sistem menggunakan model Waterfall, implementasi proses enkripsi dan dekripsi berbasis kunci simetris, pengujian fungsional, serta evaluasi pengguna menggunakan model PISCES (Performance, Information, System, Control, Efficiency, Service). Hasil penelitian menunjukkan bahwa algoritma AES mampu melindungi file ujian berformat .pdf, .docx, dan .xlsx dari potensi kebocoran data karena file hanya dapat diakses menggunakan kunci dekripsi yang sesuai. Mekanisme autentikasi juga berhasil membatasi akses hanya kepada pengguna yang berwenang. Evaluasi pengguna yang melibatkan 25 guru dari total 34 guru memperoleh nilai rata-rata 87,1%, sehingga sistem dinyatakan layak dan efektif untuk mendukung keamanan, pengelolaan, dan penyimpanan file ujian secara terpusat. Penelitian ini juga menjadi dasar bagi pengembangan lebih lanjut, seperti penerapan berbasis cloud dan perluasan dukungan format file agar sistem lebih fleksibel.*

Kata Kunci: *AES, Enkripsi File, Keamanan Data, Kriptografi, Sistem Berbasis Web*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang begitu cepat membawa dampak yang begitu luas terutama dalam hal aspek positif ataupun negatif. Salah satu tantangan besar yang muncul adalah soal akses keamanan data. Kebutuhan untuk melindungi file agar tidak mudah diakses oleh pihak yang tidak berwenang semakin mendesak terutama bagi organisasi, institusi pendidikan, dan perusahaan yang sangat bergantung pada teknologi dan jaringan komunikasi sekarang ini. Teknologi tanpa batas kini telah menjadi bagian yang tidak terpisahkan dari kehidupan manusia modern. Karena hal tersebut mempermudah aktivitas sehari-hari serta mempercepat penyebaran informasi melintasi batas negara dan budaya. Meskipun terdapat banyak kemudahan yang ditawarkan oleh kelebihan dari teknologi modern saat ini. Dalam waktu yang bersamaan pun muncul ancaman baru berupa pencurian data, penyadapan data serta kebocoran informasi yang berpotensi merusak privasi pengguna dan keamanan berbagai pihak.

Ancaman penyadapan data menjadi topik serius yang kini banyak mendapat sorotan di berbagai belahan dunia. Hal ini menunjukkan bahwa kemajuan teknologi tidak selalu berdampak positif bagi penggunanya. Penyadapan semakin menyoroti pentingnya keamanan dalam proses pertukaran informasi terutama karena jaringan komunikasi jarak jauh sering kali tidak sepenuhnya aman dari ancaman penyusupan. Dengan semakin mengalami peningkatan teknologi komputer dan komunikasi yang menjadi akses manusia sehari-hari menunjukkan bahwa kemampuan untuk mendapatkan akses secara ilegal ke data pribadi dan bersifat sensitif pun meningkat, meskipun langkah-langkah pengamanan telah dilakukan.

Pada studi kasus yang dibahas dalam penelitian ini, yaitu SMK Jaya Buana Tangerang dalam mengelola data khususnya file-file soal ujian siswa pun termasuk sangat ketat dan bersifat sangat rahasia. Untuk saat ini, sekolah tersebut menggunakan penyimpanan file yang disimpan dalam sebuah folder dalam komputer dengan format ekstensi .pdf, .docx atau .xlsx berupda draft file dokumen ujian siswa-siswi. Meskipun penggunaan perangkat lunak ini umum, akan tetapi risiko kebocoran data dapat saja terjadi apabila file-file tersebut masih disimpan dalam folder komputer tanpa perlindungan khusus. Siapa pun memiliki peluang kepemilikan akses fisik atau jaringan ke perangkat tersebut yang mengakibatkan dapat mengakses, melihat, menghapusnya bahkan melakukan hal-hal yang dianggap dapat merugikan pihak sekolah dikarenakan mengakses file tersebut penting tanpa izin serta dapat menciptakan risiko kebocoran data yang sangat signifikan.

Untuk mengatasi risiko atau kelemahan yang dihadapi oleh sistem berjalan ini diperlukan teknik perlindungan data yang lebih modern dan salah satunya adalah "kriptografi". Kriptografi menjadi salah satu teknik yang mengamankan data dengan cara mengubah informasi menjadi bentuk yang hanya bisa diakses oleh pihak yang berwenang melalui proses enkripsi dan dekripsi. Enkripsi mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci khusus, sementara dekripsi mengembalikan data ke bentuk aslinya. Kombinasi kedua proses ini menjamin keamanan data dari akses yang tidak sah.

Berdasarkan uraian di atas, maka penelitian ini bertujuan untuk mengembangkan sistem atau perangkat lunak berbasis kriptografi yang dirancang untuk meningkatkan keamanan data dan informasi dengan berfokus pada perlindungan file-file ujian siswa dan siswi yang bersifat sensitif yang tercetus gagasan serta inovasi pada dunia teknologi dan informasi

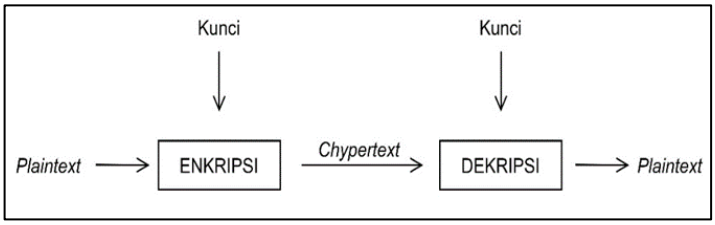
2. PENELITIAN YANG TERKAIT

Pada penjelasan di bawah ini terdapat beberapa penelitian relevan terkait penelitian-penelitian karya ilmiah yang berkaitan erat dengan judul yang diangkat oleh penulis. Penelitian dengan menggunakan acuan pembanding 3 (tiga) jurnal nasional bereputasi. Penelitian relevan bertujuan untuk melihat pembaruan (novelty) dan sisi perbedaan dari penelitian-penelitian sebelumnya. Berdasarkan hasil penelitian bahwa menjaga keamanan, kerahasiaan data-data sekolah, salah satu cara yang dapat digunakan adalah dengan dilakukannya penerapan Algoritma Advanced Encryption Standard (AES), algoritma ini memiliki tingkat keamanan yang tinggi serta menggunakan memori yang sedikit dalam pengoperasianya sehingga tidak membebani proses dan mudah untuk diterapkan. Hasil penelitian yang telah dilakukan dengan menerapkan Algoritma AES menjelaskan bahwa sebelumnya terdapat 2 (dua) kerentanan kategori hight dengan nama serangan XSS, setelah implementasi Algoritma AES maka kerentanan serangan XSS tersebut tidak ditemukan lagi. Berdasarkan hasil yang diperoleh dalam penelitian dapat disimpulkan bahwa Implementasi

Algoritma AES pada token dapat meningkatkan keamanan website dari serangan XSS. Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) Terhadap Serangan Cross Site Scripting (Yendi putra, 2021). Berdasarkan hasil penelitian bahwa setelah dilakukan analisis maka dapat di lihat bahwa algoritma AES dapat mengamankan file dengan berbagai ekstensi, seperti : .doc, .xls, .ppt, .pdf dan juga .png. Hasil dari data yang di enkripsi merupakan kumpulan kombinasi karakter yang tidak dapat dimengerti oleh manusia. Dengan menggunakan kunci yang sama maka hasil Enkripsi dan Dekripsi maka hasilnya akan selalu sama (M.fahri H Damanik, 2022).

Berdasarkan hasil penelitian menunjukkan bahwa implementasi Algoritma kriptografi Advanced Encryption Standard 128 (AES-128) telah berhasil dan digunakan sesuai kebutuhan Apotek, dengan aplikasi ini pihak Apotek dapat menyimpan data obat-obatan di database dengan aman. Karena dengan proses enkripsi, data-data yang disimpan dalam database Apotek tersimpan dengan data berupa kode acak, sekaligus mengamankan informasi data pada Apotek dari pihak yang tidak bertanggung jawab. *(Yudi Wiharto, 2022).*

Dalam praktiknya, kriptografi tidak hanya digunakan dalam komunikasi antar individu, tetapi juga dalam berbagai aplikasi teknologi seperti transaksi keuangan digital, sistem keamanan jaringan, dan perlindungan data pribadi. Teknik-teknik yang digunakan dalam kriptografi terus berkembang seiring dengan pesatnya kemajuan teknologi dan ancaman yang muncul. Proses-proses yang terlibat dalam kriptografi mencakup pengubahan pesan menjadi bentuk yang tidak dapat dimengerti oleh pihak lain, serta pengembalian pesan tersebut ke bentuk aslinya ketika diterima oleh pihak yang berhak. Dengan demikian, kriptografi berperan sangat penting dalam menjaga integritas, kerahasiaan, dan keaslian data yang dipertukarkan di dunia maya. Berikut skema teknik kriptografi diperlihatkan pada Gambar 2.1 Skema Teknik Kriptografi di bawah ini.



Gambar 1. Skema Teknik Kriptografi

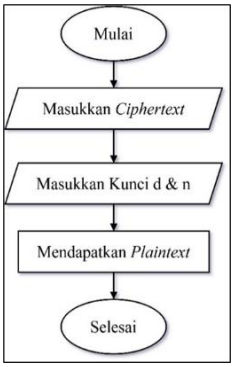
2. Encrypt (Enkripsi)

Encrypt atau dalam bahasa indonesia adalah “Enkripsi” (Suharya & Widia, 2020) yaitu mendeskripsikan suatu proses dimana suatu data teks akan disandikan agar tidak terbaca dengan cara diacak. Enkripsi di lakukan setelah dilakukannya pembangkitan kunci yang akan mendapatkan kunci privat (kunci yang tidak boleh diberitahukan pada orang lain) dan kunci publik (kunci yang boleh diberitahukan pada orang lain). Lalu dilakukanlah pertukaran kunci antara penerima dan pengirim pesan teks, setelah itu maka dilakukan enkripsi teks. Pesan yang akan dienkripsi berupa teks. Bisa dilihat pada Gambar 2.2 di bawah ini, dimana gambar di bawah ini adalah alur kerja dari proses enkripsi. Gambar 2.2 Flowchart Proses Enkripsi

3. Decrypt (Dekripsi)

Decrypt atau dalam bahasa indonesia adalah “Dekripsi” (Sutejo, 2021) merupakan proses mengubah data yang telah dienkripsi (diacak) kembali ke bentuk aslinya, sehingga dapat dipahami atau dibaca. Dekripsi digunakan untuk mengembalikan informasi terenkripsi ke format yang dapat dimengerti oleh manusia atau sistem, menggunakan kunci atau metode yang sesuai. Proses ini merupakan kebalikan dari enkripsi, yang bertujuan untuk melindungi data dari akses yang tidak sah. Proses dekripsi dilakukan pada blok-blok bilangan yang diperoleh dari proses enkripsi sehingga menghasilkan bilangan baru yang apabila diubah kembali kedalam pengkodean ASCII akan menghasilkan karakter yang sama dengan plainteks sebelum dilakukan proses enkripsi. Proses dekripsi menggunakan pasangan kunci privat (d,N). Dalam proses dekripsi, jika kunci privat yang digunakan salah dan berbeda dari yang telah dibangkitkan maka proses dekripsi tidak akan berhasil. Sebelum melakukan dekripsi, user meminta kepada sistem untuk menampilkan data yang dipilih sehingga memanggil perintah tampilkan data maka sistem melakukan

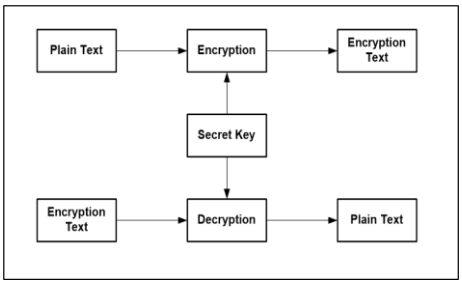
dekripsi dahulu terhadap data (chipertext) yang ada di database sehingga berubah ke bentuk data awal (plaintext) saat di masukkan lalu sistem akan menampilkan data kepada sistem. Bisa dilihat pada Gambar 2.2 di bawah ini.



Gambar 2. Flowchart Proses Dekripsi

4. Algoritma

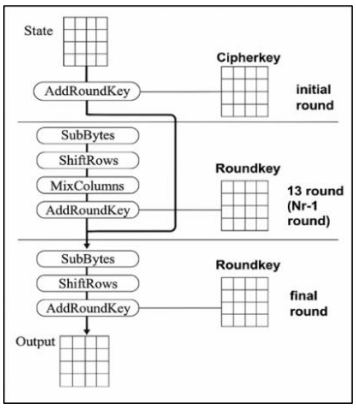
Algoritma simetris disebut juga algoritma kunci rahasia (secret key). Dalam algoritma simetris ini enkripsi dapat dilakukan jika si pengirim informasi dan penerimanya telah sepakat untuk menggunakan metode enkripsi atau kunci rahasia (secret key) enkripsi tertentu. Proses enkripsi dan dekripsi dalam algoritma simetris ini menggunakan satu kunci rahasia (secret key) yang telah disepakati sebelumnya atau menggunakan kunci yang sama (Permana & Nurnaningsih, 2019). Gambar 2.3 Algoritma Simetris.



Gambar 2. Algoritma Simetris

5. Advanced Encryption Standard (AES)

Advanced Encryption Standard, atau umumnya disingkat AES merupakan algoritma cryptographic yang dapat digunkan untuk mengamankan data. AES (Advanced Encryption Standard) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Algoritma AES adalah blok chipertext simetris yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Algoritma AES umumnya menggunakan kunci kriptografi 128, 192, dan 256 bit untuk melakukan enkripsi dan dekripsi data ataupun file (Permana & Nurnaningsih, 2019).



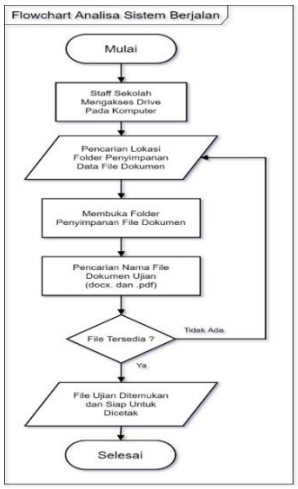
Gambar 3. Ilustrasi Algoritma AES

Selain itu, bagian ini juga dapat memuat kajian teoritis serta *state of the art* yang mendasari penelitian. Apabila diperlukan, kajian teoritis dapat dipisahkan menjadi bagian tersendiri seperti halnya bagian utama lainnya. Sumber rujukan utama sebaiknya berasal dari artikel ilmiah, khususnya jurnal bereputasi, yang diterbitkan dalam kurun waktu maksimal 5 tahun terakhir (kecuali pada kasus tertentu yang memang memerlukan rujukan lebih lama). Dengan demikian, landasan penelitian menjadi lebih kuat, terkini, dan sesuai dengan perkembangan keilmuan.

3. METODE PENELITIAN

1. Analisa Sistem

Analisa sistem menjadi tahapan dari kegiatan mengidentifikasi masalah, mengevaluasi, membuat model serta membuat spesifikasi sistem dengan tujuan untuk merancang pembaruan atau mengembangkan sistem yang telah ada. Analisa sistem secara kesuluruhan sangat perlu dalam penelitian ini untuk dapat mengetahui kelemahan dari sistem yang telah diidentifikasi, baik dari cara kerja sistem maupun pihak pengguna dan semua yang terlibat dalam sistem tersebut, untuk pembuatan sistem informasi baru harus lebih terprogram dan terimplementassi kedalam *database*.



Gambar 5. *Flowchart* Sistem yang Berjalan

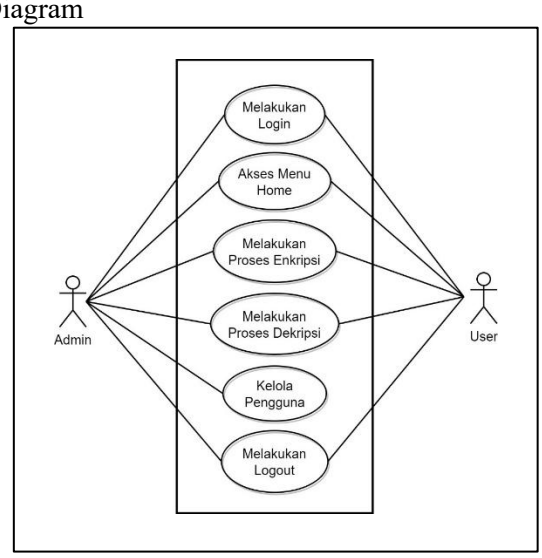
2. Analisa Kebutuhan Pengguna

Tabel 1. Analisa Kebutuhan Pengguna

No.	Kebutuhan Pengguna	Analisa Masalah	Sistem Usulan

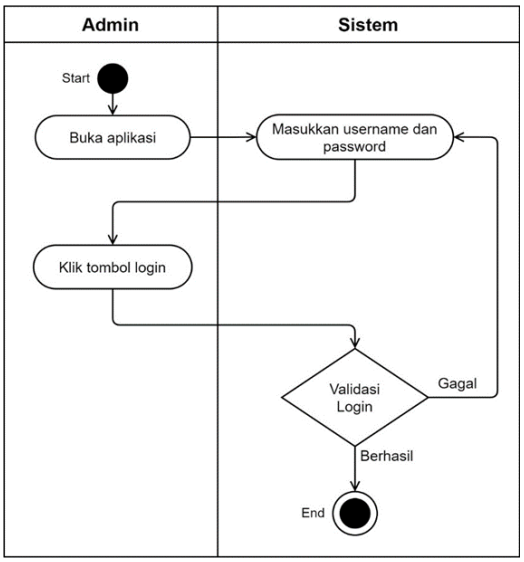
1	Sistem keamanan pengguna	Hak akses terhadap dokumen file ujian.	Dibuatkan sistem yang hanya dapat diakses oleh Admin sistem.
2	Struktur dan kelola file dokumen	Data-data dokumen file ujian masih tercampur dengan file lain pada penyimpanan di komputer.	Dibuatkan *database* sebagai pusat penyimpanan data agar mudah dilacak lokasi penyimpanan.
3	Sistem keamanan dokumen file ujian	Menjaga kerahasiaan data dan dokumen (file) yang bersifat penting agar tidak diketahui pihak yang tidak berkepentingan.	Dibuatkan sistem dengan melakukan penyembunyian file dengan teknik enkripsi file dan dekripsi file agar kerahasiaan file tetap terjaga.

a. Rancangan Use Case Diagram



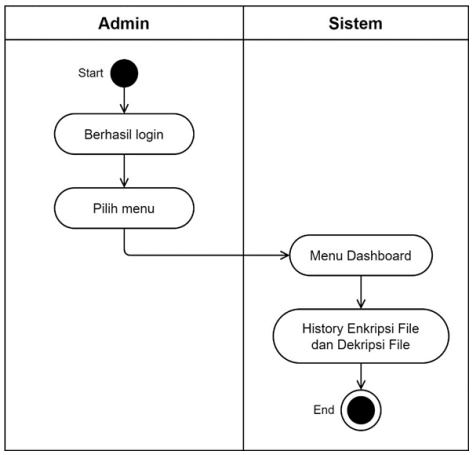
Gambar 6. Use Case Diagram Admin

Pada gambar di atas adalah ilustrasi dari rancangan use case diagram Admin pada aplikasi kriptografi keamanan dokumen file ujian siswa pada SMK Jaya Buana Tangerang terdiri atas 8 case yang terdiri atas: melakukan login, akses menu home, melakukan proses enkripsi, melakukan proses dekripsi, akses menu tentang, akses menu panduan, kelola pengguna dan melakukan logout.



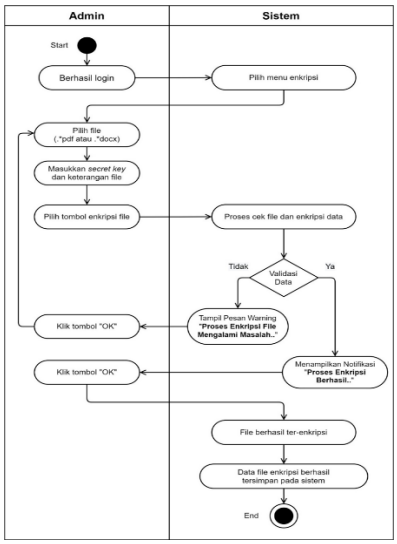
Gambar 7. Activity Diagram Melakukan Login

Pada gambar di atas diperlihatkan rancangan activity diagram pada halaman login Admin. Activity login membutuhkan input username dan password agar dapat mengakses halaman utama sistem atau Home. Proses ini harus melalui validasi apakah data input telah sesuai atau tidak. Jika "Berhasil" berarti pengguna sistem berhasil memasukkan data input *username* dan *password* yang benar. Jika "Gagal" itu berarti pengguna sistem memasukkan data input yang salah. Data input username dan password harus benar keduanya. Apabila hanya *username* yang benar dan *password* yang salah, maka proses login tidak akan berhasil dan akan menampilkan notifikasi peringatan bahwa username dan password yang dimasukkan itu salah.



Gambar 8. Activity Diagram Akses Menu Home

Pada gambar di atas diperlihatkan rancangan activity diagram pada halaman Home menu. Pada tahap ini Admin telah berhasil melakukan proses login yang dilanjutkan ke tahap sistem yang menampilkan tampilan menu home. Tampilan berisikan data terkait jumlah actor user, jumlah file yang terenkripsi dan jumlah file yang terdekripsi. Pada Home terdapat menu navigasi yang terletak pada sisi paling kiri. Ada 3 menu yang disediakan oleh sistem yang dibuat ini yang memudahkan Admin untuk mengelola aplikasi. Menu tersebut terdiri dari: menu home, menu enkripsi dan menu dekripsi.



Gambar 9. Activity Diagram Melakukan Proses Enkripsi

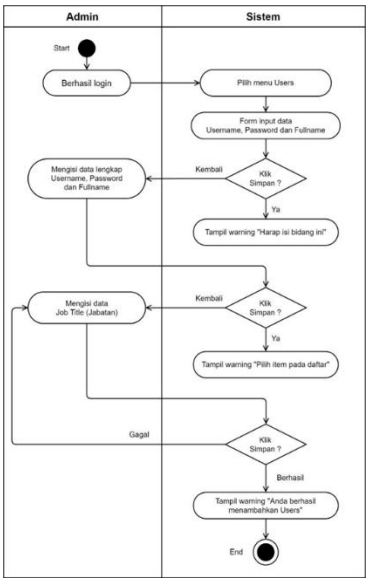
Pada gambar di atas diperlihatkan rancangan activity diagram enkripsi. File yang dapat dienkripsi beberapa file yang berekstensi .docx dan .pdf, dimana sistem file pun akan dicek kembali agar memenuhi syarat dalam proses enkripsi. Apabila file memenuhi syarat dalam tahap proses validasi, maka dinyatakan proses enkripsi berhasil dan sebaliknya apabila proses validasi pada enkripsi tidak memenuhi syarat terhadap file yang tidak mendukung ekstensi .docx dan .pdf, maka akan terjadi proses looping pada sistem program tersebut dan kembali pada tahap sebelumnya. Notifikasi pada halaman sistem ini berupa peringatan yang bertuliskan "Proses Enkripsi File Mengalami Masalah.." yang berarti file tersebut mengalami proses gagal validasi enkripsi dan sebaliknya, "Proses Enkripsi Berhasil.." yang berarti file tersebut telah berhasil melalui proses validasi sehingga file dapat terenkripsi dan tersimpan pada database sistem. Dalam tahap ini perlu untuk memasukkan *secret key* atau kunci rahasia dengan nilai 16 byte yang telah disepakati sebelumnya oleh Admin pada saat proses enkripsi file.

Rancangan pada *activity* diagram dekripsi menjelaskan bahwa file yang telah terenkripsi hanya yang dapat didekripsi oleh sistem ini. Pada saat melakukan dekripsi suatu file, lokasi (path) file yang telah dienkripsi harus diketahui oleh aplikasi. Setelah itu akan diminta untuk memasukkan secret key yang sama ketika melakukan proses enkripsi di awal. Data file yang telah didekripsi akan kembali seperti aslinya. Proses dekripsi ini tahap untuk mengembalikan file kedalam bentuk semula dan juga merupakan kebalikan dari proses enkripsi, dimana proses tersebut akan mengembalikan nilai dan struktur bit data pada file kedalam bentuk semula. Proses pengembalian data pada aplikasi keamanan data file ujian yang telah diupload ke sistem aplikasi untuk dienkrip memerlukan *secret key* yang tepat untuk dapat mengubah file menjadi ke bentuk semula. Kesalahan dalam memasukkan kunci pada proses enkripsi akan menyebabkan file menjadi rusak. Berikut rancangan activity proses dekripsi file pada sistem dapat dilihat pada gambar di bawah ini.

Gambar 10. Activity Diagram Melakukan Proses Dekripsi

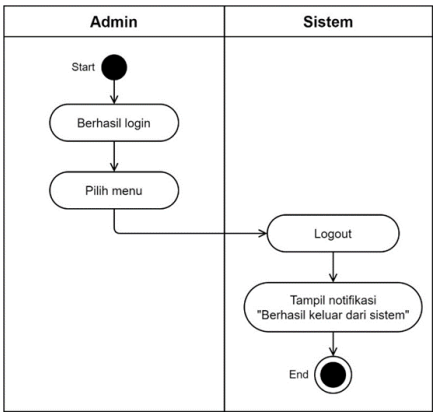
Pada gambar di atas menggambarkan ilustrasi dari rancangan activity diagram dekripsi Pada tahap ini Admin dapat menggunakan hak aksesnya dalam pengelolaan data dokumen file ujian siswa dan siswi yang terdapat dalam sistem. Hak akses yang dimaksudkan adalah Admin dapat melakukan dekripsi file karena mengetahui *secret key* yang sebelumnya telah dibuat sehingga file dapat berhasil terbaca dan dapat digunakan.

b.Rancangan Activity Diagram Melakukan Proses Kelola Pengguna



Gambar 11. Activity Diagram Kelola Pengguna

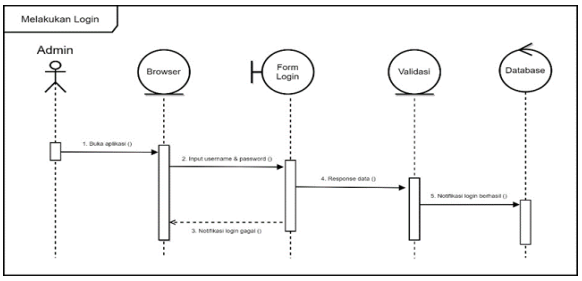
c. Rancangan Activity Diagram Melakukan Proses Logout



Gambar 12. Activity Diagram Melakukan Logout

Pada gambar di atas menggambarkan ilustrasi dari rancangan activity diagram proses logout sistem. Proses ini dapat dikatakan "berhasil" apabila setelah meng-klik tombol logout terdapat notifikasi bertuliskan "Berhasil keluar dari sistem" selanjutnya pengguna akan diarahkan kembali menuju halaman login. *Logout* membantu mencegah pengguna lain mengakses sistem tanpa memverifikasi kredensial pada pengguna aplikasi. Hal ini juga membantu melindungi akses pengguna saat ini atau mencegah tindakan tidak sah pada sesi *login* saat ini dan menjadi peran penting dari salah satu keamanan yang diterapkan oleh aplikasi ini. *Logout* memastikan bahwa akses pengguna dan kredensial pengguna aman setelah sesi login.

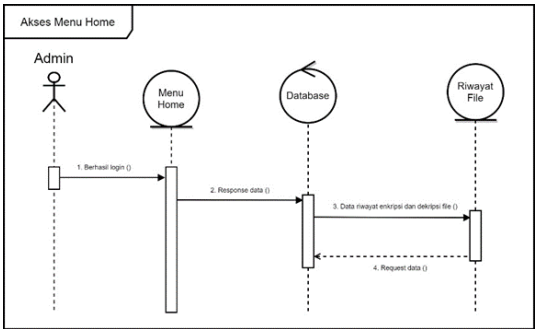
a. Sequence Diagram Login



Gambar 13. Sequence Diagram Melakukan Login

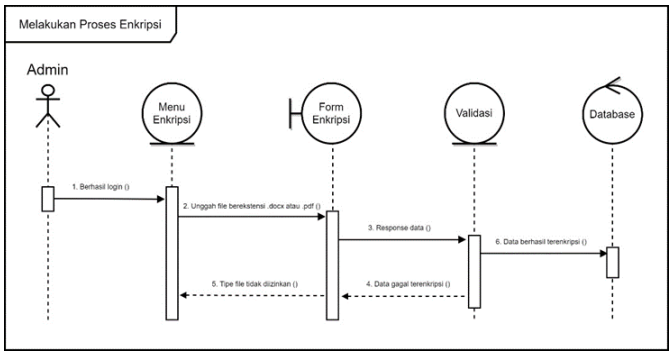
Pada gambar di atas diperlihatkan rancangan sequence diagram pada halaman login. Admin sebagai aktor diharuskan input username dan password agar dapat mengakses halaman utama sistem. Proses ini harus melalui validasi ke database. Jika login berhasil halaman utama akan menampilkan menu berupa tampilan home.

b. Sequence Diagram Home



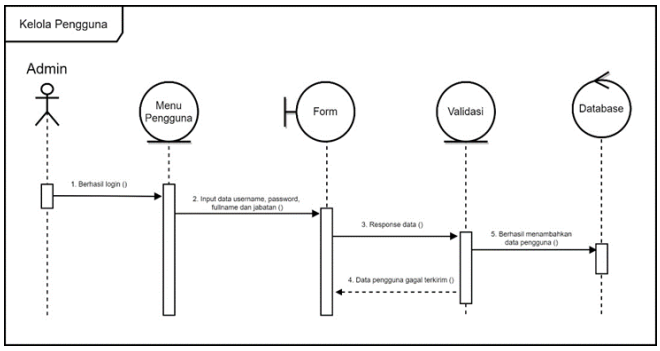
Gambar 14. Sequence Diagram Akses Menu Home

Pada gambar di atas diperlihatkan rancangan sequence diagram home setelah proses login berhasil dilakukan oleh pengguna Admin. Halaman ini menampilkan menu home, enkripsi, dekripsi dan logout.



Gambar 15. Sequence Diagram Melakukan Proses Enkripsi

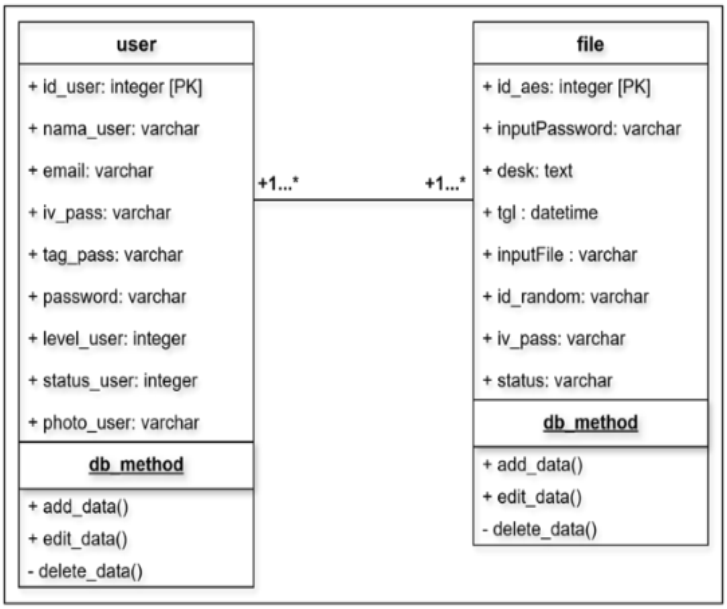
c. Sequence Diagram Kelola Pengguna



Gambar 16. Sequence Diagram Kelola Pengguna

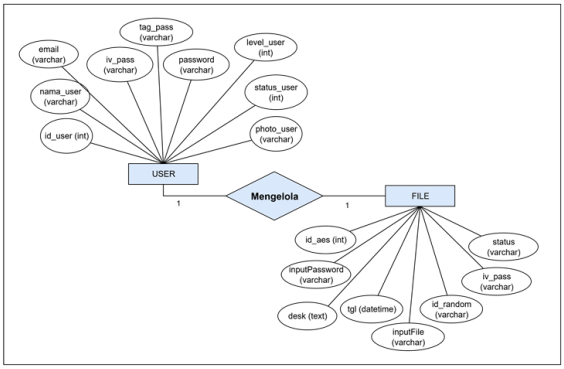
Pada gambar di atas diperlihatkan rancangan sequence diagram pada akses aktor Admin yang berisikan menu form data users. Halaman ini akan menampilkan form input pada halaman aplikasi sistem dan pengguna Admin dapat menambahkan pengguna (users) untuk dapat akses ke aplikasi sistem.

d. Class Diagram



Gambar 17. Class Diagram

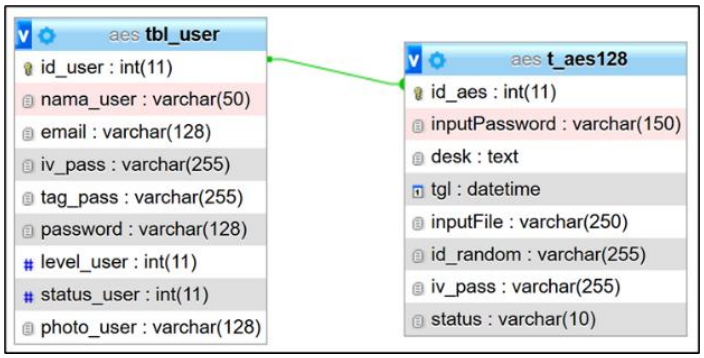
3.Entity Relationship Diagram (ERD)



Gambar 18. Entity Relationship Diagram (ERD)

4. Logical Record Structure (LRS)

LRD dapat dikatakan adalah cara atau teknik untuk menggambarkan basis data berupa relasi antar tabel yang mentransformasikan ERD ke LRS melalui proses kardinalitas.



Gambar 19. Logical Record Structure

Tabel 2. Struktur File Tabel Users

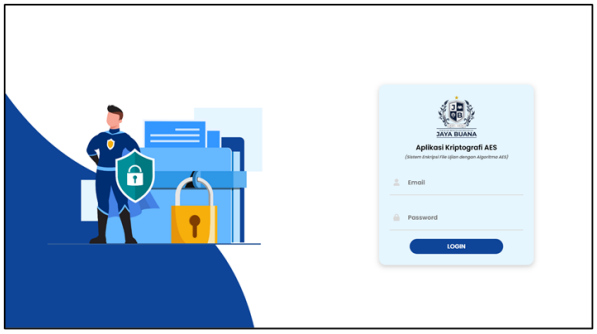
No	Nama *Field*	Tipe Data	*Size*	Keterangan
1	id_user	*int*	11	*Primary Key*
2	nama_user	*varchar*	50	
3	email	*varchar*	128	
4	iv_pass	*varchar*	255	
5	tag_pass	*varchar*	255	
6	level_user	*int*	11	
7	status_user	*int*	11	
8	status_user	*varchar*	128	

4. HASIL DAN PEMBAHASAN

Berikut ini adalah hasil beberapa rancangan program pada usulan sistem yang telah dibuat. Aplikasi sistem ini dijalankan pada lingkungan lokal menggunakan perangkat lunak XAMPP. XAMPP menyediakan berbagai modul tambahan seperti phpMyAdmin untuk pengelolaan basis data dan OpenSSL untuk keamanan, yang memudahkan pengembang dalam mengelola dan mengamankan aplikasi web secara lokal dengan melibatkan browser Chrome saat dijalankan.

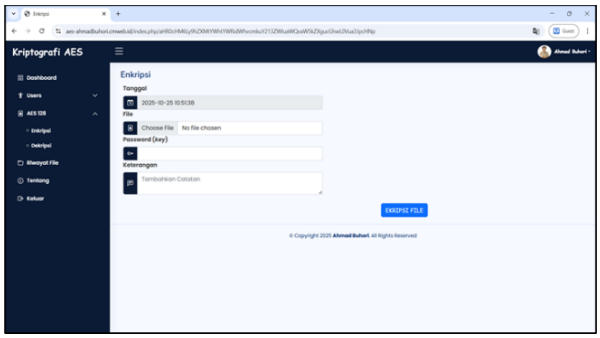
Hasil implementasi dari rancangan aplikasi pada sistem yang dibuat berupa halaman login sebagai awal akses sistem. Halaman login ini dirancang untuk memastikan bahwa hanya pengguna yang terdaftar yang dapat mengakses sistem.

a. Form Login



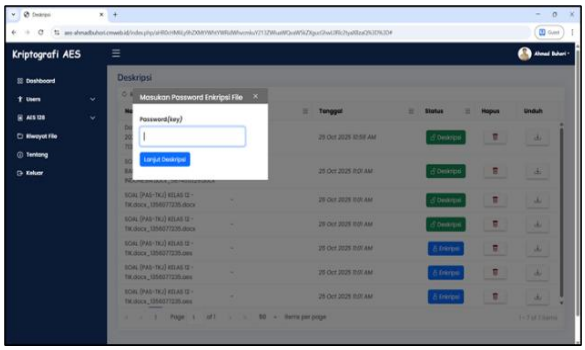
Gambar 20. Halaman Program Login Pengguna

Pada gambar di atas menampilkan sebuah halaman login yang berfungsi sebagai gerbang utama bagi administrator untuk mengakses sistem, dengan menyediakan kolom isian untuk nama pengguna dan kata sandi yang harus diisi. Setelah kredensial yang dimasukkan diverifikasi dan dinyatakan valid, administrator akan diberikan akses ke dashboard utama aplikasi. Desain halaman login yang baik sangat penting untuk memastikan pengalaman pengguna yang optimal dan keamanan sistem yang memadai.



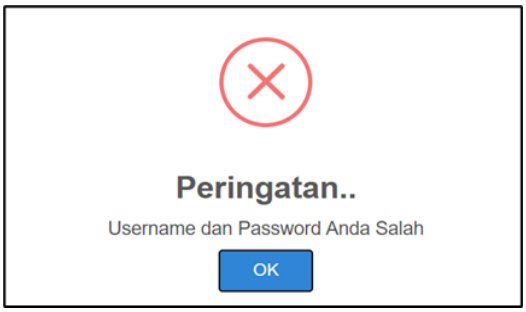
Gambar 21. Form Input Data Enkripsi File

b. Form Input Secret Key Dekripsi File



Gambar 22. *Form Input* Proses Dekripsi *File*

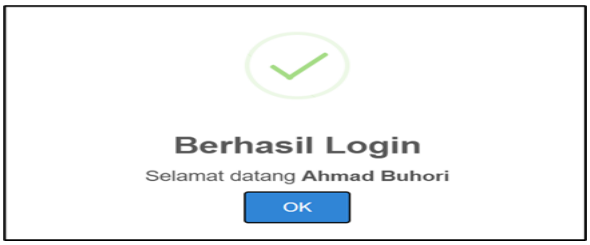
Pada gambar di atas merupakan halaman pada menu dekripsi yang terdapat detail tentang file yang akan dilakukan dekripsi. Pengguna (Admin) membutuhkan *secret key* untuk dapat melihat isi file tersebut. Berikut ini *pseudocode* pada *form input* data file yang akan diproses dekripsi pada aplikasi.



Gambar 23. Proses Login Gagal (Username dan Password Salah)

c. Proses Login Berhasil

Berikut adalah hasil dari implementasi rancangan aplikasi pada sistem yang menggambarkan proses ketika pengguna berhasil login setelah melalui tahap verifikasi data. Proses ini memastikan bahwa hanya pengguna yang memiliki kredensial valid yang dapat mengakses sistem dan menggunakan fitur yang tersedia. Untuk notifikasi pada sistem hasil proses pada saat pengguna berhasil melakukan login dapat dilihat pada Gambar 4.5 di bawah ini.

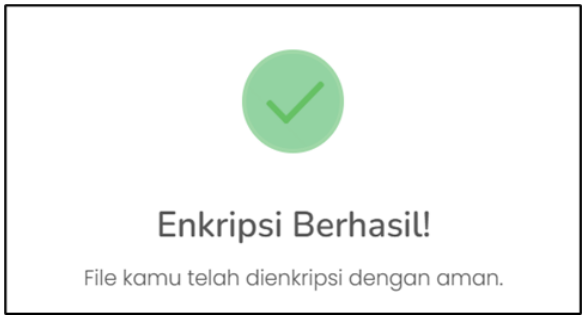


Gambar 24. Notifikasi Login Berhasil

d. Proses Enkripsi Gagal (Bukan File Word dan PDF)

Gambar 25. Proses Enkripsi Gagal (Bukan File Word dan PDF)

e. Proses Enkripsi File Berhasil



Gambar 26. Proses Enkripsi File Berhasil

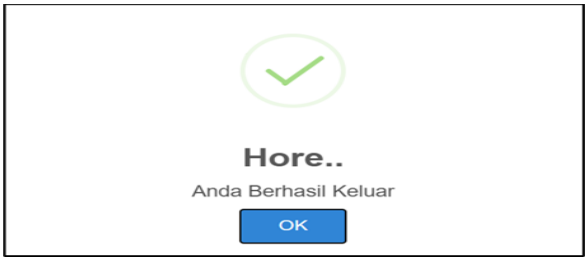
f. Proses Dekripsi Berhasil

Gambar 27. Notifikasi Proses Dekripsi Berhasil

g. Proses Dekripsi Gagal

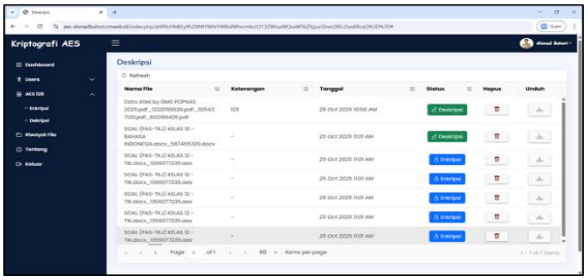
Gambar 28. Notifikasi Proses Dekripsi Gagal

h. Proses Logout Berhasil



Gambar 29. Notifikasi Logout Berhasil

Output Sistem Penyimpanan Hasil Enkripsi File

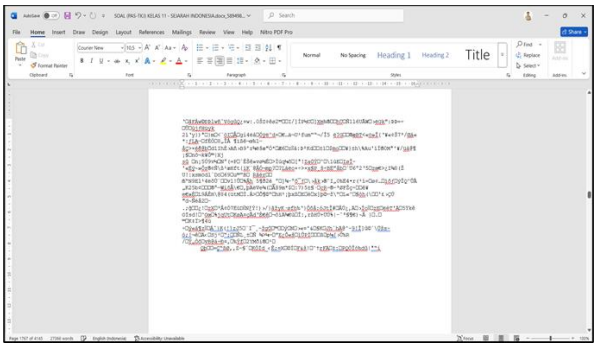


Gambar 30. Output Penyimpanan Hasil Enkripsi File

a. Output Hasil Proses Enkripsi File Pada Dokumen (Open Notepad)

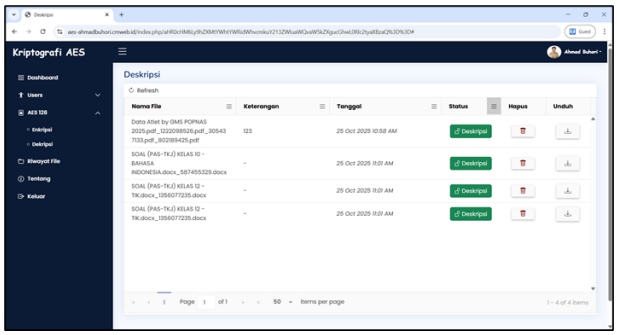
Gambar 31. Output Hasil Enkripsi File Pada Dokumen (Open Notepad)

b. Output Hasil Proses Enkripsi File Pada Dokumen (Open Word)



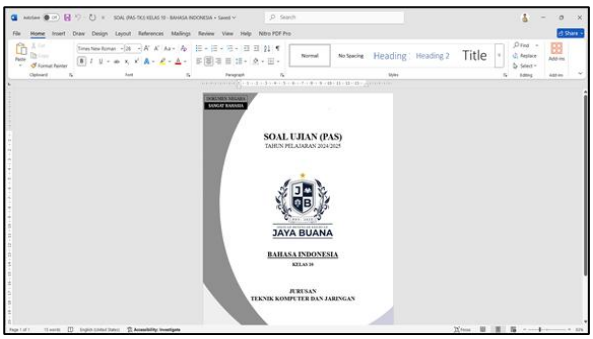
Gambar 32. Output Hasil Enkripsi File Pada Dokumen (Open Word)

c. Output Penyimpanan Hasil Dekripsi File



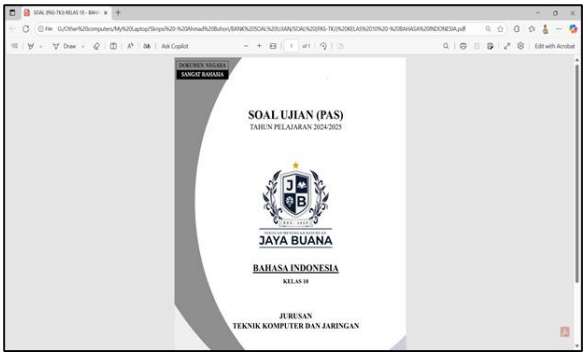
Gambar 33. Output Penyimpanan Hasil Dekripsi File

d. Output Hasil Proses Dekripsi (File Word)



Gambar 34. Output Hasil Proses Dekripsi (File Word)

e. Output Hasil Proses Dekripsi (File Pdf)



Gambar 35. Output Hasil Proses Dekripsi (File PDF)

5. KESIMPULAN

Penerapan algoritma Advanced Encryption Standard (AES) pada sistem berbasis web mampu meningkatkan keamanan file ujian siswa melalui proses enkripsi dan dekripsi yang memanfaatkan kunci simetris secara efektif. Pengembangan sistem menggunakan model Waterfall memberikan alur kerja yang terstruktur mulai dari analisis, perancangan, implementasi, hingga pengujian, sehingga menghasilkan sistem yang stabil dan sesuai dengan kebutuhan pengguna. Hasil implementasi menunjukkan bahwa enkripsi AES mampu melindungi file dengan format .pdf, .docx, dan .xlsx dari akses tidak sah serta meminimalkan risiko kebocoran data. Evaluasi pengguna menggunakan model PISCES yang melibatkan 25 guru dari total 34 guru memperoleh nilai rata-rata 87,1%, yang menandakan bahwa sistem dinilai layak, mudah digunakan, dan efektif sebagai media pengelolaan file ujian secara terpusat. Penelitian ini juga membuka peluang untuk pengembangan lebih lanjut, seperti integrasi berbasis cloud, penyempurnaan fitur manajemen file, serta penambahan dukungan format dokumen lainnya agar sistem lebih fleksibel dan adaptif terhadap kebutuhan pengguna di masa mendatang.

DAFTAR PUSTAKA

[1] Afiifah, K., Azzahra, Z. F., & Anggoro, A. D. (2022). Analisis Teknik Entity Relationship Diagram dalam Perancangan Database: Sebuah Literature Review. Intech, 3(1), 18–22.
[2] Alhamidi, L. A. (2022). Pengaruh Teaching Factory Dan Leadership Terhadap Kinerja Civitas Akademik Sekolah Menengah Kejuruan. Jurnal Pendidikan Manajemen Perkantoran, 7(1), 1–15.
[3] Audrilia, M., & Budiman, A. (2020). Perancangan Sistem Informasi Manajemen Bengkel Berbasis Web (Studi Kasus : Bengkel Anugrah). Jurnal Madani : Ilmu Pengetahuan, Teknologi, Dan Humaniora, 3(1), 1–12.
[4] Darwi, M., Islamiyah, & Jundillah, M. L. (2023). Penerapan Metode PIECES Framework Sebagai Analisis Tingkat Kepuasan Mahasiswa Dalam Penggunaan Sistem Informasi Akademik. Adopsi Teknologi Dan Sistem Informasi (ATASI), 2(1), 59–70.
[5] Dwi Putri, Y., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. JIKO (Jurnal Informatika Dan Komputer), 2
[6] Farid, H., Yusup, D., & Carudin. (2022). Analisis Usability Pada Aplikasi Momby Spa Menggunakan Metode Usability Testing. Jurnal Ilmiah Wahana Pendidikan, 8(14), 155–163.
[7] Kafa, N. A., & Sakti, D. V. S. Y. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. Jurnal Ticom: Technology of Information and Communication, 12(2), 50-55.
[8] Permana, A. A., & Nurnaningsih, D. (2019). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES). Jurnal Teknik Informatika, 11(2), 177–186.
[9] Rangkuti, A. Z. F., & Fahmi, H. (2020). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 3(2), 170–175.
[10] Regita, M., Risdiana, A., & Arifin, A. K. (2022). Perancangan Aplikasi Sistem Manajemen Penjualan Berbasis Java Netbeans Pada Toko Apara Jaya Perkasa Depok. Jurnal Riset Dan Aplikasi Mahasiswa Informatika (JRAMI), 03(02), 322–329.
[11] Sari, E. P., Wahyuni, A., & Narti. (2019). Sistem Informasi Sekolah Berbasis Web. Indonesian Journal on Software Engineering (IJSE), 5(1), 87–94.

[12] Suharya, Y., & Widia, H. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay. Jurnal Informatika (Computing), 07(01), 20–29.
[13] Sutejo. (2021). Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. INTECOMS: Journal of Information Technology and Computer Science, 4(1), 104–114.
[14] Widyawan, D., & Imelda. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode AES -128 Berbasis Web Di Komite. SKANIKA, 4(1), 15–22
[15] Wijaya, Y. D., & Astuti, M. W. (2021). Pengujian Blackbox Sistem Informasi Penilaian Kinerja Karyawan PT. INKA (Persero) Berbasis Equivalence Partitions. Jurnal Digital Teknologi Informasi, 4(1), 22–26.