BETRIK
BESEMAH TEKNOLOGI INFORMASI & KOMPUTER
Editor Office : Pusat Penelitian & Pengabdian Pada Masyarakat (PPPM) ITPA
Phone : 0857-9716-9578
email : betrikitpa@itpa.ac.id
ISSN : 2339 - 1871

Pengamanan Dokumen Digital Berbasis Web dengan Algoritma AES-128 di Lembaga Pendidikan TK

Asep Sapaatullah[1], Mochammad Darip[2]

Sistem Informasi, Ilmu Komputer, Universitas Bina Bangsa, Indonesia[1]
Ilmu Komputer, Ilmu Komputer, Universitas Bina Bangsa, Indonesia[2]
Jl. Raya Serang-Jakarta KM. 03 No. 1B Pakupatan, Kota Serang, Banten
Sur-el : *asepsapaatullah.binabangsa@gmail.com[1], darif.uniba@gmail.com[2]

Penulis Korespondensi : Asep Sapaatullah, asepsapaatullah.binabangsa@gmail.com

Abstrak: Ancaman seperti peretasan, pencurian data, atau penyalahgunaan informasi pribadi menjadi tantangan dan masalah tersendiri yang perlu mendapatkan perhatian khusus, terutama jika melibatkan data sensitif. Hal inilah yang menjadi kekhawatiran yang dihadapi oleh pihak sekolah Taman Kanak-Kanak (TK) Ceria yang berlokasi di Kota Serang. Meski sekolah belum memiliki sistem aplikasi berbasis website, namun sebagian besar dokumen penting, seperti kartu keluarga dan formulir pendaftaran, disimpan dalam format digital pada komputer yang terhubung ke jaringan internet tanpa mekanisme enkripsi dokumen serta perlindungan keamanan yang memadai. Kondisi ini tidak hanya mengancam keamanan data, tetapi juga meningkatkan kekhawatiran akan potensi penyalahgunaan informasi yang dapat merugikan siswa dan keluarganya. Namun untuk bertransformasi ke era digital yang lebih canggih, pihak sekolah masih memiliki kendala, yang salah satu kendalanya adalah keterbatasan sumber daya dan teknologi, sehingga menghambat dalam mengadopsi sistem keamanan berbasis teknologi. Penelitian ini mencoba memberikan rekomendasi bahwa transformasi teknologi dapat dilakukan dengan biaya yang terjangkau tanpa mengorbankan efektivitas dan keamanan. Metode yang digunakan adalah simulasi pengembangan aplikasi berbasis web. Berdasarkan hasil pengujian fungsionalitas utama sistem, aplikasi ini berhasil diimplementasikan sesuai dengan fokus utamanya adalah dalam hal pengamanan data siswa. Selain itu, aplikasi ini mendapat respon positif dari pihak sekolah (pengguna) dengan rata-rata tingkat keberterimaannya sebesar 80.56%. Keberhasilan implementasi sistem ini dapat menjadi langkah awal bagi lembaga pendidikan untuk beradaptasi dengan perkembangan teknologi secara bertahap, sehingga dapat meningkatkan citra dan kepercayaan masyarakat terhadap lembaga tersebut. Penelitian ini juga memberikan gambaran tentang bagaimana institusi pendidikan kecil dapat memanfaatkan teknologi dengan cara yang sederhana dan sesuai kebutuhan.

Kata kunci : Algoritma, AES-128, Dokumen, Kebocoran_Data, Sekolah

Abstract: *Threats such as hacking, data theft, or misuse of personal information are challenges and problems that need special attention, especially if they involve sensitive data. This is a concern faced by the Ceria Kindergarten (TK) school located in Serang City. Although the school does not yet have a website-based application system, most important documents, such as family cards and registration forms, are stored in digital format on computers connected to the internet without adequate document encryption mechanisms and security protection. This condition not only threatens data security, but also raises concerns about the*

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

potential for misuse of information that can harm students and their families. However, to transform into a more sophisticated digital era, the school still has obstacles, one of which is limited resources and technology, which hinders the adoption of a technology-based security system. This study tries to provide recommendations that technological transformation can be carried out at an affordable cost without sacrificing effectiveness and security. The method used is a web-based application development simulation. Based on the results of testing the main functionality of the system, this application was successfully implemented in accordance with its main focus, namely in terms of securing student data. In addition, this application received a positive response from the school (users) with an average acceptance rate of 80.56%. The successful implementation of this system can be an initial step for educational institutions to adapt to technological developments gradually, so that it can improve the image and public trust in the institution. This study also provides an overview of how small educational institutions can utilize technology in a simple and appropriate way.

Keywords: *Algorithm, AES-128, Document, Data Leakage, School*

1. PENDAHULUAN

Beberapa tahun terakhir kasus kejahatan dan korban kejahatan terhadap anak terus meningkat. Menurut data sebaran kasus yang dihimpun oleh KPAI, umumnya kasus tersebut terjadi di daerah perkotaan [1]. Salah satu contohnya adalah pada september 2024 ketika hendak pulang sekolah, seorang anak menjadi korban penculikan di kawasan Ciputat, Tangerang, Banten. Korban yang merupakan siswa sekolah dasar, tertipu oleh pelaku yang mengaku sebagai utusan keluarganya dengan alasan orang tua korban sedang dirawat di rumah sakit [2]. Kejadian ini menggarisbawahi bahwa pelaku kejahatan terhadap anak sering kali melibatkan manipulasi data atau informasi pribadi untuk mendekati korban. Secara tidak langsung, situasi ini mengindikasikan bahwa kasus kejahatan tehadap anak juga terkait dengan lemahnya pengolahan dan perlindungan data pribadi [3].

Di era digital, informasi sensitif seperti nama, alamat, atau data keluarga sering kali menjadi celah yang dimanfaatkan oleh pelaku kejahatan untuk merancang strategi manipulasi dan mendekati korban secara lebih meyakinkan. Ancaman seperti peretasan, pencurian data, atau penyalahgunaan informasi pribadi menjadi tantangan dan masalah tersendiri yang perlu mendapatkan perhatian khusus [4], terutama jika melibatkan data sensitif seperti dokumen kartu keluarga atau data anak-anak. Hal inilah yang menjadi kekhawatiran yang dihadapi oleh pihak sekolah Taman Kanak-Kanak (TK) Ceria.

TK Ceria adalah sebuah lembaga pendidikan anak-anak yang terletak di pusat kota Serang Provinsi Banten. Meskipun lembaga pendidikan ini baru berdiri, namun sekolah taman kanak-kanak ini telah berkembang cukup pesat dalam dua tahun terakhir dan menjadi pilihan orang tua dari berbagai kalangan. Seiring perkembangannya, TK Ceria merasa khawatir terhadap penyimpanan data pribadi siswa. Karena sebagian besar dokumen penting, seperti kartu keluarga dan formulir pendaftaran, disimpan dalam format digital pada komputer yang terhubung ke jaringan internet tanpa mekanisme enkripsi dokumen serta perlindungan keamanan yang memadai [5]. Kondisi ini tidak hanya mengancam keamanan data, tetapi juga meningkatkan kekhawatiran akan potensi penyalahgunaan informasi yang dapat merugikan siswa dan keluarganya.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

All author: Asep Sapaatullah, Mochammad Darip

Namun untuk bertransformasi ke era digital yang lebih canggih, pihak sekolah masih memiliki kendala dan pertimbangan beberapa faktor. Salah satu kendalanya adalah keterbatasann sumber daya dan keterbatasan teknologi yang ada, sehingga menghambat mereka (pengelola lembaga/sekolah) dalam mengadopsi sistem keamanan berbasis teknologi. Oleh karena itu, peneliti ingin merekomendasikan dan menunjukkan bahwa transformasi teknologi dapat dilakukan dengan biaya yang terjangkau tanpa mengorbankan efektivitas dan keamanan. Metode yang digunakan dalam penelitian ini adalah simulasi pengembangan aplikasi web berbasis PHP dengan database MySQL, yang diujicobakan melalui server lokal menggunakan XAMPP [6]. Sistem aplikasi ini dirancang untuk memiliki fitur dashboard yang menampilkan informasi pengguna dan jumlah dokumen yang dienkripsi, serta form enkripsi dan dekripsi untuk melindungi file dokumen siswa. Dengan pendekatan ini, penelitian difokuskan pada pengamanan data sebagai langkah awal sebelum pengembangan fitur-fitur tambahan.

Solusi yang direkomendasikan tidak hanya akan memberikan perlindungan terhadap dokumen digital siswa tetapi juga memberikan rasa aman kepada orang tua dan pihak sekolah. Selain itu, keberhasilan implementasi sistem ini dapat menjadi langkah awal bagi lembaga pendidikan ini untuk beradaptasi dengan perkembangan teknologi secara bertahap, sehingga dapat meningkatkan citra dan kepercayaan masyarakat terhadap lembaga tersebut [7]. Penelitian ini juga memberikan gambaran tentang bagaimana institusi pendidikan kecil dapat memanfaatkan teknologi dengan cara yang sederhana dan sesuai kebutuhan.

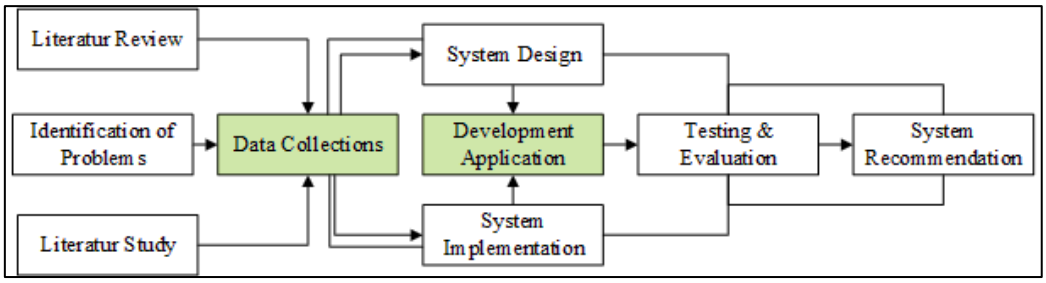
Penelitian mengenai pengamanan data menggunakan algoritma enkripsi sebenarnya telah banyak dilakukan sebelumnya, namun kebanyakan berfokus pada perusahaan besar atau instansi dengan kebutuhan keamanan yang kompleks [8]. Perbedaan utama penelitian ini adalah pendekatan yang lebih sederhana dan spesifik, disesuaikan dengan kebutuhan institusi pendidikan seperti TK Ceria. Fokus utamanya adalah memberikan solusi praktis yang dapat diimplementasikan dengan mudah dan tanpa memerlukan biaya besar. Dengan demikian, penelitian ini tidak hanya menawarkan solusi teknis tetapi juga memberdayakan institusi kecil untuk mengadopsi teknologi secara efektif..

2. METODOLOGI PENELITIAN

Langkah-langkah penelitian ini dimulai dari tinjauan pustaka sebagai landasan dasar dalam mengimplementasikan algoritma AES-128, yang kemudian dilanjutkan dengan analisis kebutuhan untuk mengidentifikasi permasalahan keamanan data di TK Ceria serta menentukan solusi berbasis teknologi. Selanjutnya, perancangan sistem dilakukan menggunakan diagram UML untuk memodelkan fitur utama, seperti enkripsi dan dekripsi file berbasis algoritma AES-128. Implementasi dalam pengembangan sistem aplikasi berbasis web menggunakan PHP dan MySQL, yang diuji terlebih dahulu pada server lokal dengan XAMPP. Pengujian sistem dilakukan melalui metode black-box untuk memastikan fungsionalitas fitur berjalan sesuai kebutuhan.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

All author: Asep Sapaatullah, Mochammad Darip



Gambar 1. Langkah-Langkah Penelitian

1. Tinjauan Pustaka

Advanced Encryption Standard (AES)-128 merupakan salah satu algoritma enkripsi simetris yang dirancang untuk memberikan tingkat keamanan dengan efisiensi komputasi yang optimal. Algoritma ini menggunakan panjang kunci 128-bit dan proses enkripsi berulang (rounds) sebanyak 10 kali [9]. Hal ini untuk memastikan data yang dienkripsi sulit untuk dipecahkan oleh pihak tidak berwenang. AES-128 diadopsi sebagai standar oleh National Institute of Standards and Technology (NIST) pada tahun 2001 dan telah digunakan secara luas dalam berbagai aplikasi, mulai dari pengamanan data pribadi hingga sistem komunikasi militer.

Berbagai penelitian menunjukkan bahwa AES-128 memiliki keunggulan dalam hal kecepatan proses enkripsi dibandingkan algoritma lainnya seperti Triple DES, sehingga cocok untuk diterapkan dalam lingkungan dengan keterbatasan sumber daya komputasi [10]. Selain itu, tingkat keamanan AES-128 tetap tinggi karena kemampuannya melindungi data dari berbagai jenis serangan kriptografis, seperti serangan brute force [11]. AES-128 menjadi solusi ideal untuk mengamankan dokumen digital sensitif, seperti data siswa atau informasi institusi, terutama pada lembaga pendidikan kecil yang baru beralih ke sistem digital. Adapun proses enkripsi dalam algoritma AES-128 [12] adalah sebagai berikut:

1) Subbytes

   Tahap ini melibatkan transformasi setiap byte dalam matriks state menggunakan tabel substitusi yang dikenal sebagai S-Box. Transformasi ini memetakan setiap elemen dalam matriks state, di mana elemen hasil transformasi dinyatakan sebagai S’[r, c], yaitu elemen pada perpotongan baris dan kolom tabel substitusi. Proses ini bertujuan untuk memperkenalkan non-linearitas pada data, sehingga meningkatkan keamanan terhadap serangan kriptografis..

2) Shiftrows

   Pada tahap ini, dilakukan pergeseran byte di dalam matriks state. Pergeseran tersebut bersifat rotasi, di mana byte paling kiri dipindahkan ke posisi paling kanan, dengan jumlah pergeseran yang bervariasi tergantung barisnya. Baris pertama tidak mengalami pergeseran, sedangkan baris kedua, ketiga, dan seterusnya digeser ke kiri sesuai dengan aturan. Proses ini membantu menyebarkan pengaruh transformasi non-linear antar elemen matriks state.

3) Mixcolumns

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

Tahapan ini mengolah setiap kolom dalam matriks state melalui operasi perkalian polinomial di dalam Galois Field. Proses ini menggunakan operasi modulo untuk mengalikan setiap kolom dengan konstanta matriks tertentu. Tujuan MixColumns adalah mendistribusikan pengaruh setiap bit plaintext dan kunci enkripsi ke seluruh ciphertext, menciptakan efek difusi yang kuat. Matriks yang digunakan untuk proses ini adalah:

[02 03 01 01]

[01 02 03 01]

[01 01 02 03]

[03 01 01 02]

4) AddRoundKey

Dalam tahap ini, setiap elemen matriks state hasil MixColumns dikenakan operasi XOR dengan elemen kunci (round key) yang telah dihasilkan sebelumnya melalui ekspansi kunci. AddRoundKey memastikan bahwa setiap tahap enkripsi dilindungi oleh kunci yang berbeda. Pada putaran terakhir, proses SubBytes, ShiftRows, dan AddRoundKey tetap dilakukan, tetapi MixColumns dihilangkan.

Adapun proses dekripsi dalam algoritma AES-128:

1) AddRoundKey Invers

Dekripsi dimulai dengan proses kebalikan dari AddRoundKey. Byte dalam matriks ciphertext dikenakan operasi XOR dengan round key yang sesuai. Round key yang digunakan dalam proses dekripsi adalah kebalikan dari yang digunakan dalam enkripsi.

2) Inverst SubBytes

Pada tahap ini, elemen matriks state dipetakan kembali menggunakan tabel inverse S-Box. Transformasi ini membalikkan efek non-linearitas yang diperkenalkan oleh SubBytes selama proses enkripsi.

3) Inverst ShiftRows

Proses ini membalikkan pergeseran byte yang dilakukan pada tahap ShiftRows. Byte di setiap baris digeser ke kanan sesuai aturan, mengembalikan elemen matriks state ke posisi semula.

4) Inverst MixColumns

Tahap terakhir dekripsi melibatkan operasi inverse MixColumns, di mana setiap kolom matriks state hasil AddRoundKey Inverse dikalikan dengan matriks berikut:

[0E 0B 0D 09]

[09 0E 0B 0D]

[0D 09 0E 0B]

[0B 0D 09 0E]

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

All author: Asep Sapaatullah, Mochammad Darip

2. Identifikasi Masalah

Langkah kedua dalam penelitian ini adalah mengumpulkan informasi terkait pengelolaan dokumen siswa di TK Ceria, tujuannya untuk memahami permasalahan yang dihadapi oleh lembaga tersebut dalam pengelolaan data siswa yang disimpan dalam file dokumen digital. Pendekatan yang digunakan adalah dengan metode kualitatif melalui wawancara langsung dengan pihak terkait [13]. Selain itu, observasi terhadap sistem penyimpanan dokumen saat ini dilakukan untuk mengidentifikasi celah keamanan yang perlu diatasi. Tabel 1 berikut ini merupakan idnetifikasi masalah yang peneliti rangkum beserta kebutuhan fungsional dan non fungsionalnya.

Tabel 1. Kebutuhan Fungsional dan Non Fungsional Sistem

Identifikasi Masalah	Kebutuhan Fungsional	Kebutuhan Non Fungsional
TK Ceria belum memiliki sistem pengelolaan dokumen data siswa.	Membangun sebuah sistem yang dirancang dapat melakukan penyimpanan dan pengelolaan dokumen siswa secara digital.	Sistem aplikasi yang dirancang harus memiliki kecepatan akses yang cukup tinggi dan dapat dioperasikan dengan baik di perangkat komputer dengan spesifikasi standar.
Keamanan data dokumen digital	Rancangan sistem harus menerapkan algoritma enkripsi (AES-128) guna melindungi dokumen penting (seperti formulir data siswa, kartu keluarga) dari akses tidak sah.	Sistem harus mampu mengenkripsi dan mendekripsi file dengan waktu proses yang cepat tanpa mengurangi kinerja aplikasi.
Belum memiliki sistem aplikasi berbasis website.	Pengembangan aplikasi web untuk menyediakan akses yang lebih mudah dan terorganisir bagi pihak sekolah dan orang tua siswa.	Aplikasi web harus memiliki tampilan yang user-friendly dan responsif agar mudah digunakan oleh pihak sekolah maupun orang tua siswa, terutama yang belum berpengalaman dengan teknologi.
Ketergantungan pada pengambilan data fisik	Sistem yang memungkinkan pihak sekolah untuk menyimpan dan mengakses data siswa secara digital dan aman.	Sistem harus dapat diakses dengan mudah melalui jaringan lokal atau internet dengan downtime minimal, serta memiliki backup data yang aman.
Risiko keamanan terkait akses data oleh pihak tidak berkepentingan	Pembatasan akses ke dokumen digital hanya kepada pengguna yang berwenang.	Keamanan data harus terjamin dengan enkripsi yang kuat dan sistem akses berbasis peran (role-based access control).

3. Studi Literatur

Untuk tahapan studi literatur ini, peneliti menggunakan metode eksploratif untuk mengkaji berbagai referensi terkait algoritma enkripsi AES-128 dan studi implementasi keamanan data di institusi pendidikan [14]. Studi literatur ini juga mencakup analisis kebutuhan teknologi yang sederhana namun efektif untuk institusi kecil dengan anggaran terbatas.

4. Perancangan Sistem

Dalam tahap ini, desain sistem aplikasi web dibuat dengan fitur utama yang dirancang meliputi dashboard, form enkripsi dan dekripsi dokumen, serta struktur data untuk mendukung pengelolaan file. Arsitektur sistem berbasis PHP dengan database MySQL. Pendekatan yang digunakan dalam pengembangan sistem ini mengikuti SDLC (Software Development Life Cycle), yang meliputi

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

tahapan perencanaan, analisis, desain, pengembangan, pengujian, dan implementasi secara terstruktur [15]. Diagram UML digunakan untuk memodelkan sistem secara terstruktur, seperti diagram use case, activity, dan class untuk menggambarkan alur kerja, hubungan antar elemen, dan interaksi pengguna dengan sistem [16]. Struktur database dirancang untuk mendukung fitur utama seperti enkripsi dan dekripsi dokumen, dengan mempertimbangkan efisiensi penyimpanan dan keamanan data.

5. **Implementasi Sistem**

   Proses implementasi dilakukan dengan metode pengembangan iteratif [17]. Sistem prototipe dikembangkan menggunakan PHP untuk backend, MySQL untuk database, dan XAMPP sebagai server lokal. Fokus pada tahap ini adalah memastikan bahwa algoritma AES-128 dapat diintegrasikan secara mulus ke dalam aplikasi untuk proses enkripsi dan dekripsi dokumen.

6. **Pengujian Sistem**

   Metode black-box testing diterapkan untuk mengevaluasi fungsionalitas dan keamanan sistem tanpa mempertimbangkan struktur internal aplikasi [18]. Pengujian ini berfokus pada keluaran yang dihasilkan oleh sistem berdasarkan input yang diberikan. Uji coba meliputi validasi terhadap algoritma enkripsi untuk memastikan dokumen terenkripsi dengan benar. Selian itu, metode evaluasi kualitatif dan kuantitatif digunakan untuk mengumpulkan feedback dari pihak sekolah. Hasil pengujian dianalisis untuk menyempurnakan prototipe sebelum implementasi lebih lanjut [19].

7. **Rekomendasi Sistem**

   Hasil evaluasi dianalisis untuk menyusun rekomendasi penerapan sistem. Proses ini juga mencakup perencanaan pengembangan [20].

3. HASIL DAN PEMBAHASAN

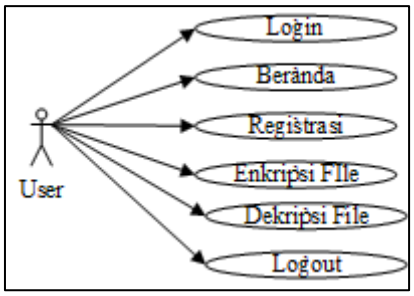
3.1 Perancangan Sistem

Dalam perancangan sistem yang dilakukan adalah dengan memodelkan alur kerja menggunakan diagram UML yang meliputi use case, activity, dan class diagram untuk memastikan struktur sistem terdefinisi dengan baik.

1. **Use Case Diagram**

   Use case diagram adalah representasi visual yang menggambarkan interaksi antara pengguna (aktor) dan sistem untuk menyelesaikan tugas-tugas tertentu khususnya dalam hal pengamanan data siswa. Diagram ini menunjukkan hubungan antara aktor dan berbagai fungsi yang disediakan oleh sistem yang biasa kita disebut use case. Selian itu, use case diagram akan dapat membantu dalam memetakan kebutuhan pengguna terhadap fitur yang akan dikembangkan nantinya, sehingga pengembang dapat memahami alur kerja dan memastikan sistem memenuhi tujuan pengguna.

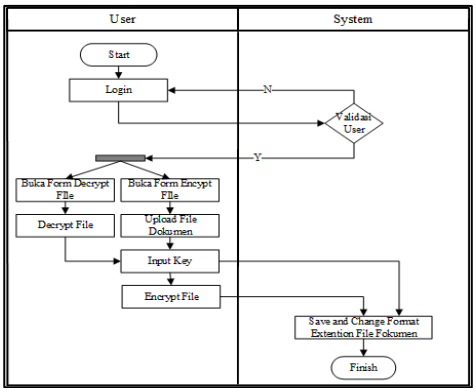
Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025



Gambar 2. Use Case Diagram

2. Activity Diagram

Activity diagram digunakan untuk memodelkan alur proses atau aktivitas dalam sistem secara dinamis. Diagram ini menggambarkan urutan langkah-langkah atau tindakan yang dilakukan oleh pengguna dan sistem untuk mencapai suatu tujuan tertentu. Setiap aktivitas dalam diagram direpresentasikan dengan node, sedangkan alur kerja antar aktivitas dihubungkan oleh panah yang menunjukkan urutan atau aliran proses. Activity diagram membantu dalam menggambarkan proses secara terperinci, termasuk percabangan keputusan, paralelisme, dan kondisi akhir. Diagram ini sangat berguna dalam merancang logika alur kerja sistem, memvalidasi skenario penggunaan, dan mengidentifikasi potensi efisiensi atau hambatan dalam proses sistem. Gambar 2 berikut ini merupakan model pengamanan data di TK Ceria yang peneliti usulkan.

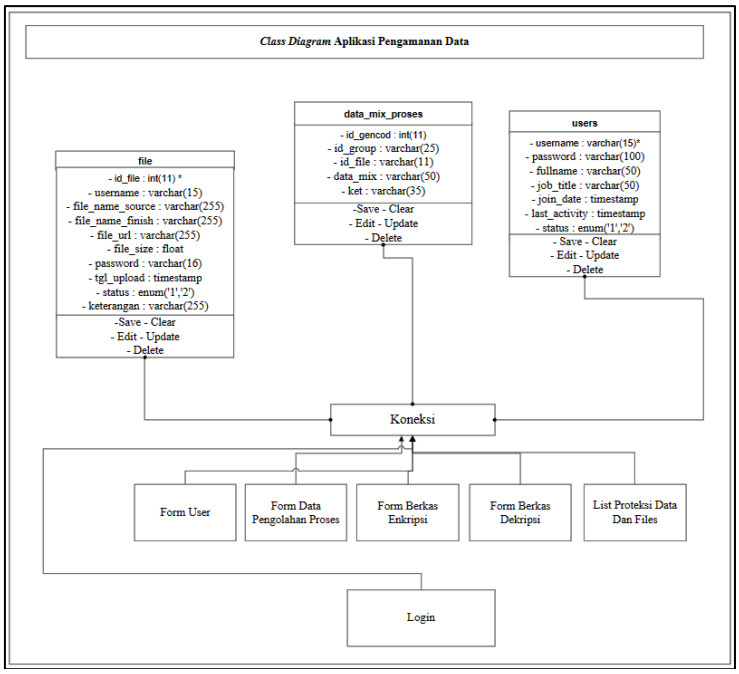


Gambar 3. Activity Diagram

3. Class Diagram

Class diagram adalah salah satu diagram dalam UML yang digunakan untuk memodelkan struktur statis dari sistem. Diagram ini menunjukkan kelas-kelas dalam sistem beserta atribut, metode, dan hubungan di antara kelas-kelas tersebut, seperti asosiasi, generalisasi, dan agregasi. Class diagram membantu pengembang memahami bagaimana data dan fungsi terorganisasi dalam sistem, sehingga mempermudah proses desain dan implementasi. Melalui representasi visual ini, pengembang dapat memetakan interaksi antara kelas, memastikan bahwa struktur sistem mendukung fungsionalitas yang dirancang. Diagram ini juga berfungsi sebagai dokumentasi untuk referensi selama siklus pengembangan perangkat lunak.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025



Gambar 4. Class Diagram

3.2 Implementasi Sistem

Implementasi sistem dilakukan dengan membangun aplikasi web menggunakan PHP yang di-hosting pada server lokal menggunakan XAMPP, dengan fokus pada pengintegrasian algoritma enkripsi dan antarmuka pengguna dengan fitur utama seperti enkripsi dan dekripsi dokumen berbasis algoritma AES-128 yang didukung database MySQL.

1. Menu Login

   Menu Login memungkinkan pengguna, seperti admin sekolah, untuk mengakses aplikasi setelah melakukan autentikasi dengan memasukkan username dan password. Setelah berhasil login, pengguna diarahkan ke use case dashboard.

Gambar 5. Menu Login

2. Menu Utama (Dashboard)

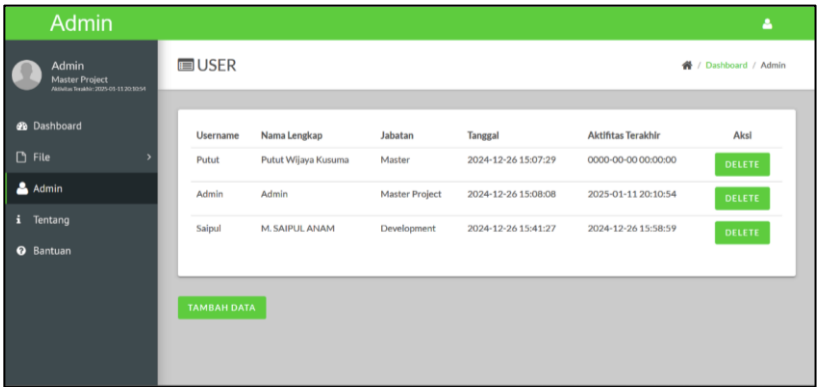
   Selain sebagai halaman utama sistem, menu dashboard juga yang menyediakan ringkasan informasi, seperti jumlah file yang dienkripsi dan dekripsi, serta informasi pengguna aktif.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

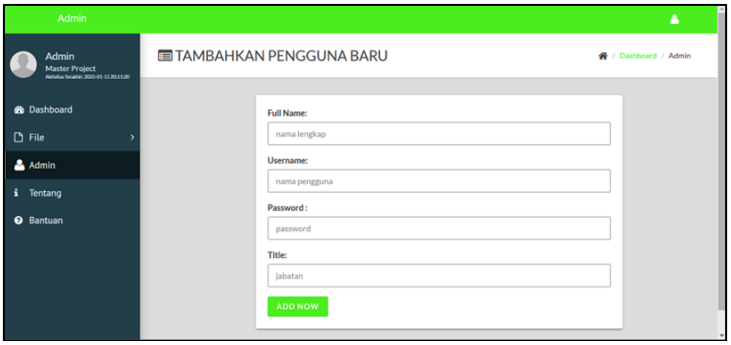
Gambar 6. Menu Utama

3. Menu Informasi Data User

Menu informasi pengguna menyediakan data terkait pengguna yang telah terdaftar dalam sistem. Disamping itu pengguna yang aktif dapat memungkinkan melakukan pendaftaran akun baru untuk admin tambahan dengan validasi data pengguna untuk menjaga keamanan akses. Setelah pendaftaran berhasil, akun baru tersebut akan ditambahkan ke dalam daftar informasi pengguna, sehingga dapat langsung digunakan sesuai kebutuhan operasional.



Gambar 7. Menu DataUser



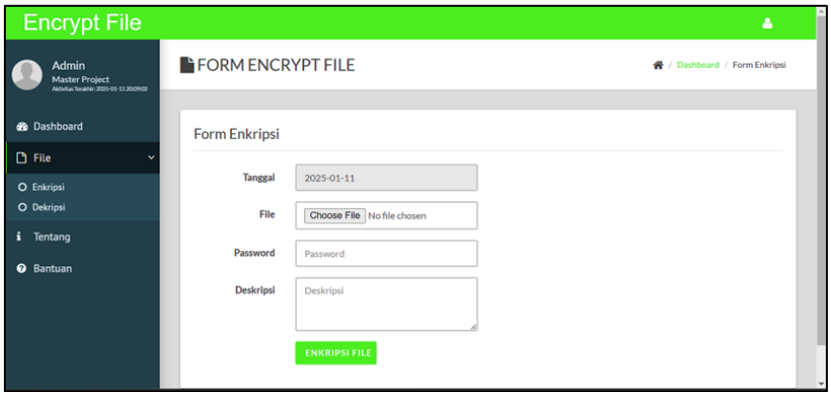
Gambar 8. Menu Tambah User

4. Menu Enkripsi File

Menu utama enkripsi file memungkinkan admin memilih dokumen dari perangkat penyimpanan komputer untuk dienkripsi menggunakan algoritma AES-128. Setelah proses enkripsi, sistem akan

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

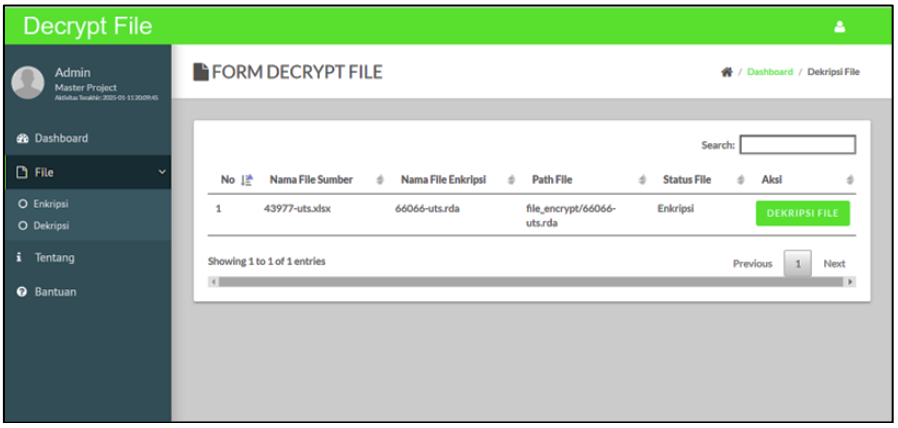
menghasilkan file yang telah dienkripsi dan menyimpannya kembali ke ruang penyimpanan komputer dengan format yang aman dan tidak dapat dibaca tanpa proses dekripsi menggunakan kunci yang sesuai.



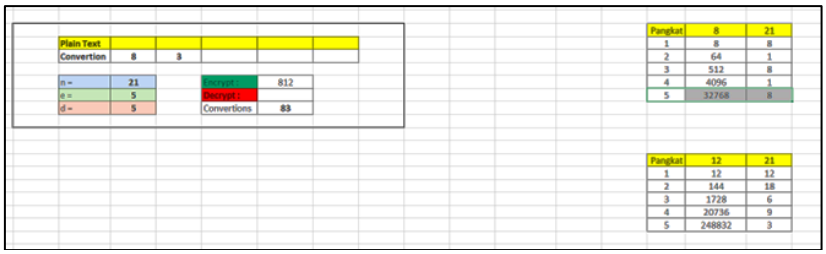
Gambar 9. Halaman Enkripsi

5. Dekripsi File

Menu utama dekripsi file memungkinkan pengguna untuk mengakses kembali dokumen dalam format asli dengan memasukkan file terenkripsi dan kunci enkripsi yang sesuai. Pada menu ini terdapat informasi sumber file, nama file yang di enkripsi.

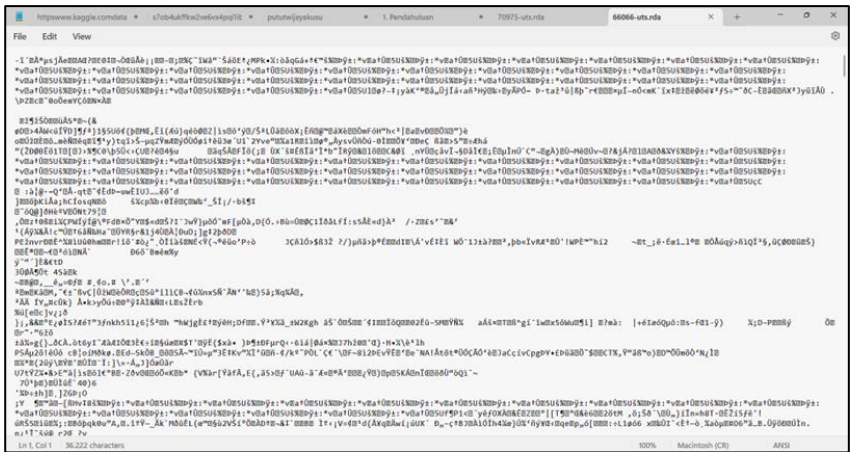


Gambar 10. Halaman Dekripsi



Gambar 11. Contoh File yang Akan Dienkripsi

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025



Gambar 12. Contoh File yang Telah Dienkripsi

3.3 Pengujian

1. Pengujian Blackbox

Pengujian sistem dilakukan melalui pendekatan black-box testing untuk mengevaluasi fungsionalitas utama, seperti validitas proses enkripsi dan dekripsi, keamanan data, serta kompatibilitas sistem terhadap berbagai jenis dokumen, guna memastikan bahwa aplikasi berjalan sesuai dengan spesifikasi yang dirancang.

Tabel 2. Hasil Pengujian Blackbox

Fitur yang Diuji	Skenario Pengujian	Input	Ekspetasi Hasil	Hasil Uji
Login	Admin memasukkan username dan password dengan yang benar	Username: admin, Password: 12345	Sistem menampilkan dashboard setelah login berhasil	Berhasil
	Admin memasukkan username dan password dengan yang salah	Username: admin, Password: salah123	Sistem menampilkan pesan error "Username atau password salah"	Berhasil
Dashboard	Admin mengakses dashboard setelah login	-	Sistem menampilkan menu utama, informasi jumlah file yang terenkripsi, dan nama pengguna	Berhasil
Enkripsi File	Admin mengunggah dokumen untuk dienkripsi	File dokumen (.docx, .pdf,. xlsx, .ppt)	Sistem menghasilkan file terenkripsi dengan format aman (.enc)	Berhasil
	Admin mengunggah file dengan format yang tidak didukung	File gambar (.jpg, .png)	Sistem menampilkan pesan error "Format file tidak didukung"	Berhasil
Dekripsi File	Admin membuka file terenkripsi dan memasukkan kunci enkripsi yang benar	File terenkripsi (.enc), kunci yang valid	Sistem mengembalikan file ke bentuk aslinya (misal: .docx, .pdf)	Berhasil
	Admin menghapus file yang terenkripsi di path penyimpanan dan	-	Sistem menampilkan pesan error "File Tidak Ada, dekripsi gagal"	Berhasil

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

	kemudian membukanya pada sistem			
Registrasi Pengguna	Admin menambahkan pengguna baru dengan data yang valid	Informasi pengguna baru	Sistem berhasil menambahkan akun pengguna baru ke database	Berhasil
	Admin menambahkan pengguna dengan username yang sudah ada	Username yang sudah terdaftar	Sistem menampilkan pesan error "Username sudah digunakan"	Berhasil
Logout	Admin melakukan logout	-	Sistem mengakhiri sesi dan mengarahkan admin ke halaman login	Berhasil

2. Pengujian Usability

Metode kualitatif dilakukan melalui wawancara langsung, sedangkan metode kuantitatif melibatkan survei dengan skala penilaian untuk mengukur tingkat kepuasan dan pemahaman terhadap prototipe yang telah diuji. Berikut tabel hasil feedback dari pihak sekolah TK Ceria mengenai tingkat kepuasan dengan pendekatan usability user test.

$$\%\boldsymbol{SkorAktual} = \frac{\boldsymbol{skoraktual}}{\boldsymbol{skorideal}}\boldsymbol{x100} \quad \text{..... (b)}$$

Tabel 3. Hasil Pengujian Usaility User

	Jawaban			
Aspek	Jumlah Instrument	Setuju	Netral	Tidak Setuju
Ease of Use	6	94.44%	5.56%	0.00%
Satisfaction and Perceived Secuirity	2	83.33%	16.67%	0.00%
Visual and Information Clarity	3	77.78%	16.67%	0.00%
Performance	1	66.67%	16.67%	16.67%
Rata-rata	-	80.56%	15.28%	4.17%

Berdasarkan hasil evaluasi di atas, rata-rata tingkat keberterimaan sebesar 80.56%, terutama pada aspek kemudahan penggunaan yang mencapai 94.44%, meskipun aspek performa (66.67%) dan kejelasan visual (77.78%). Untuk pengembangannya, disarankan untuk meningkatkan performa sistem melalui optimasi kode, memperbaiki kejelasan visual dengan desain yang lebih menarik dan informatif, serta menambahkan fitur keamanan yang lebih kuat guna meningkatkan rasa aman pengguna sistem.

4. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan dengan fokus utamanya pada pengamanan data siswa, aplikasi ini berhasil dalam mengimplementasikan fungsionalitas utamanya. Dan mendapatkan respons positif secara keseluruhan dengan rata-rata tingkat keberterimaan sebesar 80.56%. Aspek Ease of Use (Kemudahan Penggunaan) mencatat tingkat persetujuan tertinggi (94.44%), menunjukkan mayoritas responden merasa sistem ini mudah digunakan. Sementara itu, aspek Satisfaction and Perceived Security (Kepuasan dan Keamanan yang Dirasakan) dinilai cukup baik dengan tingkat persetujuan sebesar 83.33%.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

Namun pada aspek Performance (Performa) dengan tingkat persetujuan terendah (66.67%) dan tingkat ketidaksetujuan tertinggi (16.67%). Selain itu, aspek Visual and Information Clarity (Kejelasan Visual dan Informasi) dengan tingkat persetujuan sebesar 77.78% mengindikasikan bahwa perlunya pengembangan lebih lanjut untuk bagian ini. Secara keseluruhan, sistem aplikasi ini telah diterima dengan baik, tetapi optimalisasi lebih lanjut pada aspek performa dan kejelasan visual perlu dilakukan untuk meningkatkan pengalaman pengguna secara keseluruhan.

DAFTAR RUJUKAN

[1] "SIMFONI-PPA," https://kekerasan.kemenpppa.go.id/ringkasan. Accessed: Jan. 16, 2025. [Online]. Available: https://kekerasan.kemenpppa.go.id/ringkasan

[2] M. Iqbal, "Polisi Tangkap Pelaku Penculikan dan Pelecehan Seksual Terhadap Anak di Ciputat," https://www.tempo.co/hukum/polisi-tangkap-pelaku-penculikan-dan-pelecehan-seksual-terhadap-anak-di-ciputat-4510. Accessed: Jan. 15, 2025. [Online]. Available: https://www.tempo.co/hukum/polisi-tangkap-pelaku-penculikan-dan-pelecehan-seksual-terhadap-anak-di-ciputat-4510

[3] H. Puspita Sari, M. Aji Nilamsari, D. Dimas Fajarian Sitorus, and Y. Widagdo Harimurti, "Efektivitas Hukum Perlindungan Data Pribadi Terhadap Kejahatan Siber di Indonesia," *PT. Media Akademik Publisher*, vol. 2, no. 11, pp. 1–26, Nov. 2024, doi: 10.62281.

[4] D. Aprilia Rismasari and I. Wikartika, "Sosialisasi Meningkatkan Kesadaran Masyarakat Dalam Mencegah Kebocoran Data Nasabah Perbankan Digital Melalui Pesan Phishing di Era Digitalisasi," *Pengabdian dan Edukasi Sekolah (Jubaedah)*, vol. 5, no. 1, pp. 41–50, Apr. 2025, doi: 10.46306/jub.v5i1.

[5] M. Sudirman *et al.*, "Menganalisis Penanganan Kebocoran Data Pengguna Facebook Dalam Konteks Manajemen Sekuriti," *Portofolio: Jurnal Manajemen Bisnis*, vol. 3, no. 3, pp. 255–268, Jul. 2024.

[6] J. Rahmad Mulia, A. Afif, and K. H. Manurung, "Aplikasi Simulasi Prediksi Obat Pemakaian Kronis Dengan Metode Monte Carlo," *Jurnal Sistem Informasi dan Sistem Komputer*, vol. 10, no. 1, pp. 60–71, Jan. 2025, doi: 10.51717/simkom.v10i1.734.

[7] A. Winarto, E. Mahmud, and A. Muadin, "Manajemen Humas dalam Membangun Citra Lembaga: Studi Multisitus di STAI Sangatta dan STIPER Sangatta Kutai Timur," *Sustainable Jurnal Kajian Mutu Pendidikan*, vol. 6, no. 1, pp. 159–169, Jun. 2023, doi: 10.32923/kjmp.v6i1.3355.

[8] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]*, vol. 4, no. 2, pp. 75–85, Sep. 2021.

[9] Aprizaldi, M. Arief Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *Jurnal Teknik Informatika (JEKIN)*, vol. 2, no. 2, pp. 86–95, 2022.

[10] H. Fiji Ardiansyah and N. Juliasari, "Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 30 Agustus 2023-Jakarta," Jakarta: https://senafti.budiluhur.ac.id/index.php/senafti/index, Aug. 2023, pp. 260–268. [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index

[11] M. Akbar, "Implementasi Algoritma Advanced Encrytion Standard (AES) untuk Pengamanan Citra Digital," *Jurnal Ilmu Komputer: Revolusioner*, vol. 8, no. 12, pp. 28–32, 2024.

[12] H. Amanda Sagala, "Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data," *Journal Global Tecnology Computer*, vol. 2, no. 2, pp. 75–86, 2023.

[13] M. Darip and H. Hamdan, "Dokumen Perancangan Perangkat Lunak Pelayanan Laboratorium UPTD Dinas Lingkungan Hidup Kota Serang," *Jurnal Ilmiah Media Sisfo*, vol. 18, no. 2, pp. 150–165, Oct. 2024, doi: 10.33998/mediasisfo.2024.18.2.1701.

[14] F. Arisanti, J. Sulthon Habiby, and A. Muttaqin, "Penggunaan Teknologi Augmented Dengan Pendekatan Studi Eksploratif Reality DAlam Pembelajaran Anak Usia Dini," *JOECES Journal of Early Childhood Education Studies*, vol. 4, no. 1, pp. 74–104, 2024.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

All author: Asep Sapaatullah, Mochammad Darip

[15] M. Darip and S. Auliana, "Optimalisasi Penjualan dengan Aplikasi Web Berbasis Codeigniter pada Toko Kelontong," *JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK)*, vol. 15, no. 2, pp. 232–244, Sep. 2024, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JTIKP

[16] B. R. S. Permana, M. Darip, and A. A. Sayyidah, "Perancangan Aplikasi Pengajuan Cuti Berbasis Android di Rumah Sakit Umum Ibunda Serang," *INNOVATIVE: Journal Of Social Science Research*, no. 1, pp. 5265–5280, 2024.

[17] M. L. Simanjuntak and F. Masya, "Perancangan dan Implementasi Sistem Informasi Inventory Berbasis Website Menggunakan Iterative Waterfall," *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 6, no. 2, pp. 83–91, Jul. 2021, doi: 10.36341/rabit.v6i2.1687.

[18] S. Auliana, G. Untirtha Pratama, B. Rakhim Setya Permana, and O. Firmansyah, "Design of a Mobile Phone Sales System Website at Vivo Store," *ARRUS Journal of Engineering and Technology*, vol. 4, no. 1, pp. 126–140, 2024, doi: 10.35877/jetech2710.

[19] F. Purwani, M. Ridho Karunia, R. E. Saputra, and M. A. Salam, "Implementasi Metode Design Thingking Dalam Perancangan UI/UX Pada Website SIKATAMA Universitas Islam Negeri (UIN) Raden Fatah Palembang," *JURNAL RISET TEKNIK KOMPUTER*, vol. 1, no. 4, pp. 16–22, 2024, doi: 10.69714/4qn55j80.

[20] R. G. Putra, H. P. Herlyansyah, P. Windriyani, and Q. RS, "Implementasi Website K-Etik untuk Digitalisasi Manajemen Etik Penelitian di Universitas YARSI," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 10, no. 1, pp. 50–61, Jan. 2025, doi: 10.30591/jpit.v10i1.8055.

Received: 21-04-2025 | Accepted: 25-04-2025 | Published Online: 30-04-2025

All author: Asep Sapaatullah, Mochammad Darip