IMPLEMENTASI APLIKASI ENKRIPSI DATA MENGGUNAKAN ALGORITMA AES 128 UNTUK MENINGKATKAN KEAMANAN INFORMASI BERBASIS WEBSITE DI SMK KUSUMA BANGSA

Tyas Tia Mutiara[1], Bambang Wisnu Widagdo[2]

[1]Program Studi Teknik Informatika, University Pamulang, JL Puspitek Tangerang Selatan, Indonesia, 15310
e-mail: [1] tyastiam@gmail.com

Abstract

The use of web-based systems in education is increasing, including at SMK Kusuma Bangsa. The school website is used to store and manage important data such as student information, academic grades, and lesson schedules. However, weaknesses in the security system make data vulnerable to cyber attacks such as data breach and SQL injection. This research aims to implement data encryption using the AES-128 algorithm to improve information security at SMK Kusuma Bangsa. The research methods used include observation, interviews, and literature studies. The developed system was tested using the Black Box Testing method to ensure the reliability and security of data encryption. The results showed that the implementation of AES-128 is able to protect data well, prevent unauthorized access, and increase user confidence in the system. With this encryption, the risk of information leakage can be minimized, so that school data security becomes more secure.
Keywords*: implementation, security, AES-128, encryption.*

Abstrak

Penggunaan sistem berbasis website dalam dunia pendidikan semakin meningkat, termasuk di SMK Kusuma Bangsa. Website sekolah digunakan untuk menyimpan dan mengelola data penting seperti informasi siswa, nilai akademik, dan jadwal pelajaran. Namun, kelemahan dalam sistem keamanan menyebabkan data rentan terhadap serangan siber seperti data breach dan SQL injection. Penelitian ini bertujuan untuk mengimplementasikan enkripsi data menggunakan algoritma AES-128 guna meningkatkan keamanan informasi di SMK Kusuma Bangsa. Metode penelitian yang digunakan meliputi observasi, wawancara, dan studi pustaka. Sistem yang dikembangkan diuji menggunakan metode Black Box Testing untuk memastikan keandalan dan keamanan enkripsi data. Hasil penelitian menunjukkan bahwa implementasi AES-128 mampu melindungi data dengan baik, mencegah akses tidak sah, dan meningkatkan kepercayaan pengguna terhadap sistem. Dengan adanya enkripsi ini, risiko kebocoran informasi dapat diminimalkan, sehingga keamanan data sekolah menjadi lebih terjamin.
Kata Kunci : implementasi, keamanan, AES-128, enkripsi.

1. PENDAHULUAN

Pada era digital ini, perubahan dalam teknologi informasi telah membawa dampak signifikan terhadap cara kita berinteraksi dan berkomunikasi. Salah satu dampak tersebut adalah kemampuan untuk meningkatkan partisipasi masyarakat dalam memberikan pengaduan terkait berbagai isu di lingkungan tempat tinggal mereka.

Namun, dengan meningkatnya penggunaan sistem berbasis website, ancaman keamanan siber juga semakin berkembang. Serangan seperti data breach, man-in-the-middle attack, dan SQL injection dapat mengakibatkan kebocoran data penting. Menurut data dari Badan Siber dan Sandi Negara (BSSN), insiden keamanan siber di Indonesia terus meningkat dari tahun ke tahun, dengan banyak kasus kebocoran data yang terjadi pada sektor pendidikan. Pada tahun 2023, BSSN mencatat lebih dari 300 juta serangan siber yang menargetkan berbagai sektor, termasuk sekitar

20% di antaranya terjadi di sektor pendidikan. Salah satu insiden terbesar terjadi pada sebuah platform pendidikan daring di Indonesia, di mana lebih dari 1,3 juta data pribadi siswa dan guru bocor, termasuk informasi sensitif seperti nama lengkap, alamat email, nomor telepon, dan data akademikDi era digital saat ini, teknologi informasi memainkan peran penting dalam berbagai sektor, termasuk dunia pendidikan. Sekolah-sekolah semakin mengandalkan sistem berbasis website untuk menyimpan dan mengelola data penting, seperti informasi pribadi siswa, nilai akademik, jadwal pelajaran, serta catatan kehadiran. Salah satu sekolah yang menggunakan sistem ini adalah SMK Kusuma Bangsa.

Salah satu metode yang efektif untuk meningkatkan keamanan data adalah dengan melakukan enkripsi. Enkripsi adalah proses pengubahan data menjadi format yang tidak bisa dibaca tanpa menggunakan kunci dekripsi yang sesuai. Algoritma enkripsi yang sering digunakan dalam dunia siber adalah Advanced Encryption Standard (AES). AES merupakan algoritma simetris yang dikenal kuat dan efisien, serta diakui sebagai standar enkripsi oleh pemerintah Amerika Serikat sejak tahun 2001. AES memiliki beberapa variasi panjang kunci, yaitu AES-128, AES-192, dan AES-256. AES-128 sering dipilih karena keseimbangan antara tingkat keamanan dan kinerja yang efisien. AES merupakan enkripsi yang memiliki kunci yang lebih besar dibanding DES yaitu 128 bit, 192 bit, atau 256 bit. Proses enkripsi AES dengan panjang kunci 128 bit terdiri dari 4 tahapan yaitu AddRoundKey, SubBytes, ShiftRows, dan MixColumns. Karena adanya beberapa tahapan dalam proses enkripsi maka diperlukan subkey-subkey yang akan dipakai pada tiap tahap. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan key schedule (Haris, 2023:78-79).

SMK Kusuma Bangsa perlu menerapkan implementasi enkripsi *AES-128* untuk memastikan data siswa dan sistem informasi sekolah terlindungi dari serangan siber. Dengan adanya enkripsi ini, data yang tersimpan dan dikirimkan melalui website akan lebih aman, sehingga dapat meningkatkan kepercayaan siswa, guru, dan orang tua terhadap sistem yang digunakan. Selain itu, implementasi keamanan yang lebih baik juga dapat mencegah dampak negatif dari kebocoran data, seperti penyalahgunaan informasi dan hilangnya reputasi sekolah.

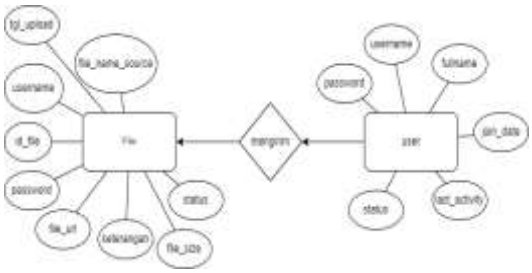
2. METODE

Penelitian ini menggunakan tiga metode yaitu Metode pengumpulan data terdiri dari observasi, wawancara, dan studi pustaka. Observasi digunakan untuk mengumpulkan data secara langsung dari sumbernya sebagai bahan informasi penelitian. Wawancara digunakan untuk memperoleh pemahaman tentang permasalahan kompleks yang dihadapi dan proses yang berjalan SMK Kusuma Bangsa. Studi pustaka dilakukan dengan mengumpulkan berbagai sumber referensi, seperti buku dan sumber lainnya, sebagai acuan dalam analisis sistem dan penyusunan laporan.

3. HASIL

3.1 *Entity Relationship Diagram (ERD)*

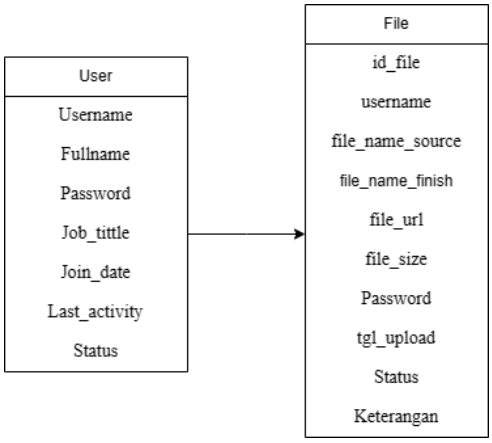
ERD (Entity-Relationship Diagram) adalah sebuah model visual yang digunakan untuk menggambarkan struktur data dalam sebuah sistem basis data. *ERD* secara grafis menggambarkan entitas (objek atau konsep) yang berperan dalam sistem, hubungan antara entitas-entitas tersebut, serta atribut-atribut yang terkait dengan entitas.



Gambar 1. *Entity-Relationship Diagram*

3.2 *LRS (Logical Record Structure)*

LRS (Logical Record Structure) adalah representasi dari struktur record-record pada tabel-tabel yang berbentuk dari hasil antar himpunan entitas. Rancangan LRS dapat dilihat dari gambar 2 berikut:



Gambar 2. *Logical Record Structure*

3.3 Spesifikasi Basis Data

a. Tabel Data User

Tabel I. User

No	Nama Field	Type	Length	Keterangan
1	Username	Varchar	15	Email Pengguna
2	Password	Varchar	100	*Password*
3	Fullname	Varchar	50	Nama Pengguna
4	Job_title	Varchar	50	Keterangan jabatan *user*
5	Join_Date	Timestamp	-	Keterangan kapan *user* terdaftar di aplikasi
6	Last_activity	Timestamp	-	Keterangan kapan *user* terakhir kali aktif di aplikasi
7	Status	Enum	-	Keterangan statur *user*

b. Tabel Data File

Tabel II. Data File

No	Nama Field	Type	Length	Keterangan
1	Id_file	Int	11	Berusi ID File
2	Username	Varchar	15	Berisi*Username* untuk *user*
3	File_name_source	Varchar	255	Berisi keterangan nama *file* sebelum dienkripsi

3.4 *Usecase Diagram*

Gambar 4. *Usecase Diagram*

Pada gambar 4 , Sistem enkripsi data di SMK Kusuma Bangsa dirancang untuk meningkatkan keamanan informasi berbasis website dengan melibatkan tiga aktor utama: Admin, Staff Sekolah, dan Kepala Sekolah. Setiap aktor memiliki peran dan tanggung jawab spesifik terkait pengelolaan data siswa dan keamanan informasi. Berikut adalah deskripsi masing-masing aktor beserta aktivitas yang terlibat:

a) Admin

Melakukan Enkripsi Data Siswa: Admin memiliki hak untuk mengenkripsi data siswa agar tidak dapat diakses tanpa izin. Proses ini memastikan data aman dari ancaman keamanan.

Melakukan Dekripsi Data Siswa: Admin bertugas mendekripsi data siswa jika diperlukan untuk keperluan tertentu, seperti audit atau permintaan data resmi.

b) Staff Sekolah

Mengelola File Data Informasi Siswa: Staff bertanggung jawab untuk mengatur, memperbarui, dan memelihara data informasi siswa sesuai kebutuhan operasional.

Melakukan Enkripsi Data Siswa: Staff dapat mengenkripsi data siswa untuk melindungi informasi sensitif sebelum penyimpanan atau pengiriman.

Melakukan Dekripsi Data Siswa: Staff juga memiliki akses untuk mendekripsi data siswa yang mereka kelola saat diperlukan untuk aktivitas administratif.

c) Kepala Sekolah

Mengelola Pengguna: Kepala sekolah bertanggung jawab atas pengaturan akun

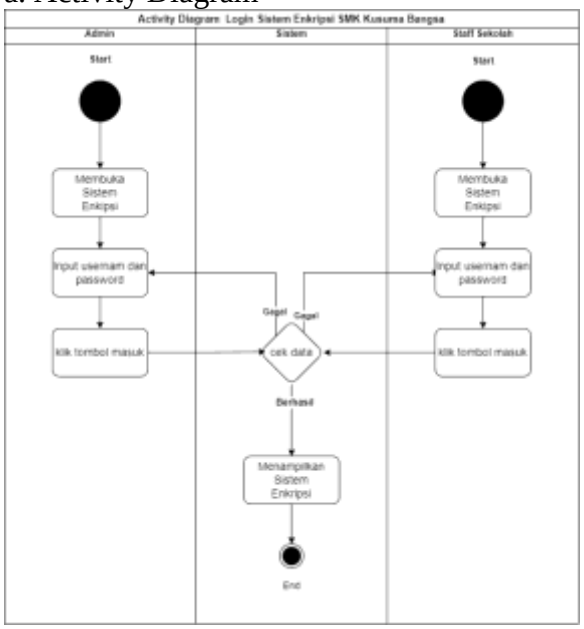
pengguna, termasuk memberikan hak akses kepada admin dan staff sesuai peran mereka.

Mengelola File Informasi Siswa: Kepala sekolah dapat meninjau, memperbarui, atau menghapus data informasi siswa untuk memastikan konsistensi dan akurasi.

Mengelola File Data Siswa: Kepala sekolah bertugas memantau dan mengelola data siswa secara keseluruhan untuk memastikan keamanan dan kepatuhan terhadap kebijakan sekolah.).

3.5 *Activity Diagram*

a. Activity Diagram



Gambar 5 *Activity Diagram Login*

Gambar 5 Diagram Aktivitas ini menggambarkan langkah-langkah yang terjadi selama proses login dalam Sistem Enkripsi Smk Kusuma Bangsa melibatkan Administrator dan staff sekolah, serta bagaimana Sistem melakukan validasi terhadap data login yang dimasukkan.

a). admin:

1. admin memulai proses login dengan membuka tampilan menu login.
2. admin kemudian memasukkan username dan kata sandi yang sudah terdaftar dalam sistem.
3. Setelah data login dimasukkan, sistem melakukan validasi terhadap data tersebut.
4. Jika validasi berhasil, admin akan diarahkan ke beranda sistem enkripsi.

b). Sistem:

1. Sistem mendeteksi permintaan login dari admin dan staff sekolah.
2. Sistem melakukan validasi terhadap data login yang dimasukkan oleh admin dan staff sekolah untuk memeriksa kecocokan dengan data yang tersimpan dalam sistem.
3. Jika data yang dimasukkan sesuai dengan data yang ada dalam sistem, sistem memberikan akses ke beranda system ensripsi. Jika tidak, sistem memberikan pesan kesalahan dan meminta admin dan staff sekolah untuk mencoba lagi.

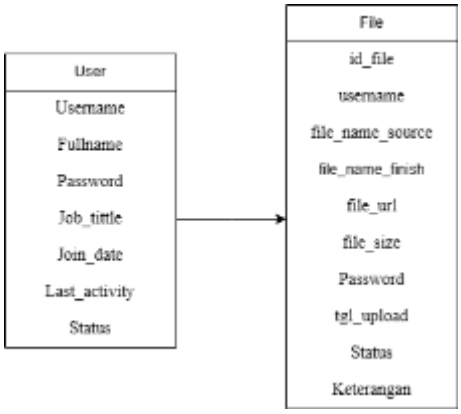
c). Staff Sekolah:

1. Staff Sekolah memulai proses login dengan membuka tampilan menu login.
2. Staff Sekolah memasukkan username dan kata sandi yang sudah terdaftar dalam sistem.
3. Sistem melakukan validasi terhadap data login yang dimasukkan oleh staff sekolah.
4. Jika validasi berhasil, Staff sekolah akan diarahkan ke beranda sistem Enkripsi.

Dalam diagram aktivitas ini, setiap langkah dalam proses login telah dijelaskan, termasuk tindakan yang dilakukan oleh Staff Sekolah dan Admin. Diagram ini memberikan gambaran visual tentang bagaimana interaksi antara pengguna (Staff sekolah dan Admin) dengan sistem berlangsung selama proses login..

3.6 Class Diagram

Class Diagram merupakan sebuah class yang menggambarkan struktur dan penjelasan class, paket, dan objek serta hubungan satu sama lain seperti containmnet, pewarisan, asosiasi dan lain-lain. Class diagram juga menjelaskan gubungan antar class dalam sebua sistem yang sedang dibuat dan bagaimana caranya agar saling berhubungan untuk mencapai suatu tujuan.



Gambar 6 Class Diagram

3.7 Flowchart

Flowchart atau bagan alur adalah diagram yang menampilkan langkah-langkah dan keputusan untuk melakukan sebuah proses dari suatu program. Setiap langkah digambarkan dalam bentuk diagram dan dihubungkan dengan garis atau arah panah. Flowchart membantu dalam memahami, mendokumentasikan, dan menganalisis alur kerja atau proses. Berikut ada beberapa Flowchart dibawah ini:

Gambar 7 Flowchart

Flowchart ini menggambarkan alur kerja sistem enkripsi yang digunakan oleh admin dalam mengelola file di sistem enkripsi SMK Kusuma Bangsa. Proses dimulai ketika admin melakukan login dengan memasukkan username dan password. Jika validasi login berhasil, sistem akan menampilkan menu utama dan membawa admin ke dashboard utama.

Di dalam dashboard, admin memiliki beberapa opsi, yaitu enkripsi file, dekripsi file, manajemen file, dan melihat informasi sistem. Jika admin memilih enkripsi, maka sistem meminta admin untuk menginput file dan memberikan kunci enkripsi. Setelah proses enkripsi selesai, sistem akan memeriksa apakah file berhasil terenkripsi. Jika berhasil, file akan tersimpan di dalam sistem, tetapi jika gagal, admin harus mengulangi proses atau mereset input. Untuk dekripsi, admin harus memasukkan kunci dekripsi yang sesuai, kemudian sistem akan memproses file. Jika berhasil, file akan tersimpan dalam bentuk terdekripsi, sedangkan jika gagal, admin dapat membatalkan atau menghapus file.

Selain itu, admin juga dapat mengelola file yang telah terenkripsi dengan memeriksa statusnya dan mengunduh file yang telah berhasil didekripsi. Admin juga dapat mengakses menu informasi terkait aplikasi enkripsi. Setelah semua proses selesai, admin dapat memilih untuk logout dan sistem akan mengakhiri sesi pengguna. Flowchart ini memberikan gambaran jelas mengenai bagaimana admin dapat mengelola file dengan aman menggunakan sistem enkripsi.

3.8 Implementasi Antarmuka *(Interface)*

Implementasi antarmuka (Interface) dari suatu perangkat lunak dilakukan berdasarkan perancangan yang telah dilakukan. Implementasi ditampilkan dari screenshoot dari halaman website yang digunakan sebagai alat dan bahan penelitian yang telah dirincikan sebelumnya.

A. Antar Muka Login

Gambar 8 Antarmuka Login

Antarmuka login merupakan bagian awal yang menjadi gerbang akses ke dalam sistem enkripsi data. Halaman ini dirancang dengan sederhana namun tetap memperhatikan aspek estetika dan fungsionalitas. Pada bagian kanan atas halaman login, terdapat logo SMK Kusuma Bangsa

yang menjadi identitas visual sistem. Logo ini memberikan kesan profesional sekaligus mempertegas branding institusi. Penempatan logo pada pojok kanan atas dirancang untuk tidak mengganggu fokus pengguna terhadap elemen-elemen utama pada antarmuka.

Di kanan halaman, terdapat formulir login yang terdiri dari dua kolom input: Username dan Password. Kolom ini dilengkapi dengan label yang jelas serta placeholder untuk membantu pengguna mengisi data dengan benar. Formulir ini juga memiliki validasi untuk memastikan input sesuai dengan format yang dibutuhkan. Tepat di bawah kolom input, terdapat tombol Login yang berfungsi untuk mengirimkan data ke sistem untuk diproses. Tombol ini dirancang dengan warna yang kontras untuk memberikan perhatian utama, serta dilengkapi dengan efek interaktif, seperti perubahan warna atau bayangan saat tombol ditekan, guna memberikan umpan balik visual kepada pengguna.

Antarmuka login juga telah dirancang responsif agar dapat diakses dengan baik pada berbagai perangkat, mulai dari desktop hingga ponsel pintar. Dengan desain yang intuitif, pengguna, baik admin maupun staff sekolah, dapat dengan mudah mengakses sistem tanpa kebingungan. Hal ini memastikan pengalaman pengguna yang optimal serta mendukung efisiensi dalam proses kerja.

B. Antarmuka Dashboard system enkripsi

Gambar 9 Antarmuka Dashboard

Antarmuka dashboard sistem enkripsi dirancang untuk memberikan navigasi yang mudah dan intuitif bagi pengguna. Pada bagian atas dashboard, terdapat header yang mencantumkan nama sistem serta logo SMK Kusuma Bangsa, memberikan identitas visual yang konsisten. Di bawah header, pengguna akan menemukan menu navigasi utama yang mencakup lima opsi utama: *Enkripsi*, *Dekripsi*, *File*, *Tentang Aplikasi*, dan *Panduan Aplikasi*. Setiap menu dirancang dengan ikon dan teks pendamping untuk memudahkan identifikasi fungsi masing-masing menu.

a) Menu Enkripsi:
Menu ini memungkinkan pengguna untuk mengunggah file yang akan dienkripsi. Setelah file diunggah, pengguna dapat memberikan *key* untuk proses enkripsi. Halaman ini juga menampilkan riwayat file yang telah dienkripsi, memudahkan pengguna untuk melacak aktivitas mereka.

b) Menu Dekripsi:
Menu dekripsi menyediakan fitur untuk mengunggah file yang sebelumnya telah terenkripsi. Pengguna harus memasukkan *key* yang sesuai untuk membuka file. Jika validasi berhasil, file akan tersedia untuk diunduh dalam format asli.

c) Menu File:
Pada menu ini, pengguna dapat melihat daftar file yang telah mereka unggah dan olah. Sistem menyediakan fungsi pencarian dan filter untuk membantu pengguna menemukan file tertentu dengan cepat.

d) Tentang Aplikasi:
Menu ini berisi deskripsi singkat tentang sistem enkripsi, tujuan pengembangannya, dan teknologi yang digunakan. Informasi ini dirancang untuk memberikan pemahaman kepada pengguna tentang manfaat sistem.

e) Panduan Aplikasi:
Panduan aplikasi menyediakan langkah-langkah penggunaan sistem secara detail, mulai dari proses enkripsi hingga dekripsi. Teks dan ilustrasi panduan dibuat sederhana agar dapat dipahami oleh semua kalangan pengguna.

Dengan antarmuka dashboard yang terstruktur dan mudah digunakan ini, pengguna dapat dengan efisien mengakses dan memanfaatkan fitur-fitur yang tersedia untuk meningkatkan keamanan informasi. Desain responsif juga memastikan dashboard dapat diakses dengan nyaman di berbagai perangkat.

C. Antarmuka Menu Enkripsi

Gambar 10Antarmuka Menu Enkripsi

Antarmuka menu enkripsi dirancang untuk memberikan kemudahan dan efisiensi dalam proses pengamanan data menggunakan algoritma AES 128. Pada halaman ini, pengguna dihadapkan dengan sebuah *form* enkripsi yang memiliki elemen-elemen utama untuk memastikan data terenkripsi dengan aman dan terstruktur. Desainnya minimalis namun tetap informatif, sehingga pengguna dapat langsung memahami langkah-langkah yang perlu dilakukan.

Form enkripsi terdiri dari beberapa kolom input:

a) Tanggal: Kolom ini secara otomatis menampilkan tanggal sistem saat pengguna membuka menu enkripsi, memastikan setiap proses dicatat berdasarkan waktu.

b) File: Kolom ini memungkinkan pengguna untuk memilih file yang akan dienkripsi melalui tombol *Browse*. Setelah file dipilih, nama file akan muncul di kolom untuk memastikan file yang benar telah dipilih.

c) Kunci Enkripsi: Pengguna diharuskan mengisi kunci enkripsi secara manual. Kolom ini memberikan panduan agar kunci bersifat kompleks dan aman, seperti kombinasi huruf, angka, dan simbol.

d) Keterangan: Kolom opsional ini memungkinkan pengguna menambahkan catatan atau deskripsi terkait file yang akan dienkripsi, memudahkan identifikasi file di kemudian hari.

Enkripsi File Tombol ini berfungsi untuk memulai proses enkripsi setelah semua data yang diperlukan telah diisi. Saat tombol ditekan, sistem akan menjalankan algoritma AES 128 untuk mengamankan file. Reset Tombol ini memungkinkan pengguna untuk menghapus semua input yang telah dimasukkan pada *form*, sehingga dapat memulai kembali dengan data yang baru.

Antarmuka ini dirancang responsif untuk mendukung berbagai perangkat. Dengan tata letak yang jelas dan fungsi yang mudah dipahami, menu enkripsi ini membantu pengguna memastikan data sensitif dapat terenkripsi dengan cepat dan aman.

D. Antarmuka menu dekripsi

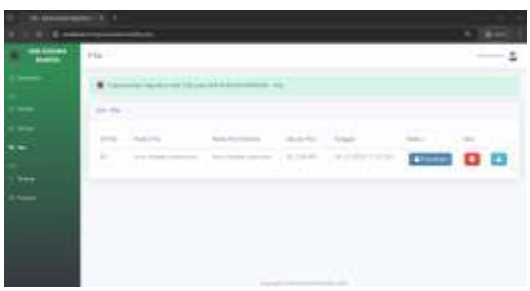
Gambar 11 Antarmuka Deksripsi

Antarmuka menu dekripsi pada sistem enkripsi SMK Kusuma Bangsa dirancang untuk mempermudah pengguna dalam mengelola file yang memerlukan proses dekripsi. Pada antarmuka ini, terdapat **form dekripsi** di bagian atas yang menjadi pusat aktivitas pengguna. Form ini memungkinkan pengguna untuk memilih file yang akan didekripsi dengan mengisi informasi terkait seperti nama file dan kunci dekripsi. Selain itu, form ini juga menyediakan tombol aksi yang dirancang untuk memulai proses dekripsi file secara cepat dan efisien.

Di bawah form dekripsi, terdapat tabel informasi file yang berisi data detail tentang file yang telah diunggah atau diproses. Tabel ini memiliki beberapa kolom, yaitu **Nomor Urut** untuk mempermudah identifikasi file, **Nama File** untuk menunjukkan nama file yang diproses, **File Enkripsi** untuk menampilkan file asli yang telah terenkripsi, **Tanggal** untuk memberikan informasi kapan proses enkripsi dilakukan, dan **Status File** yang menunjukkan kondisi file, apakah "Terenkripsi" atau "Tidak Terenkripsi." Pada kolom terakhir, yaitu **Aksi**, terdapat tombol yang memungkinkan pengguna untuk memulai dekripsi, mengunduh file hasil dekripsi, atau menghapus file dari daftar.

Desain antarmuka ini dibuat sederhana namun informatif sehingga pengguna, baik admin maupun staf sekolah, dapat dengan mudah memahami status file dan mengambil tindakan yang diperlukan. Dengan alur yang jelas dan navigasi yang intuitif, menu dekripsi ini mendukung proses pengelolaan data secara lebih aman, cepat, dan efektif.

E. Antarmuka Menu File



Gambar 12 Antarmuka Menu File

Antarmuka menu file pada sistem enkripsi SMK Kusuma Bangsa dirancang untuk memberikan gambaran lengkap tentang file-file yang telah dikelola dalam sistem. Menu ini menyajikan list file yang berisi data-data penting dari setiap file yang diunggah atau diproses. List file ditampilkan dalam bentuk tabel yang terstruktur dengan kolom-kolom informatif, sehingga memudahkan pengguna untuk melakukan pencarian, pengelolaan, dan pemantauan status file.

Kolom pertama pada tabel adalah ID File, yang berfungsi sebagai identitas unik untuk setiap file. Selanjutnya, terdapat kolom Nama File dan Nama File Enkripsi, yang masing-masing menunjukkan nama asli file serta nama file setelah proses enkripsi dilakukan. Informasi terkait ukuran file juga ditampilkan pada kolom Ukuran File, yang membantu pengguna memahami besar file yang sedang dikelola. Selain itu, terdapat kolom Tanggal, yang mencatat waktu kapan file tersebut diunggah atau diproses, serta kolom Status, yang menunjukkan apakah file saat ini "Terenkripsi" atau "Tidak Terenkripsi."

Pada kolom terakhir, yaitu Aksi, tersedia beberapa tombol tindakan yang memungkinkan pengguna untuk melakukan berbagai operasi seperti mengunduh file, menghapus file, atau mengakses file lebih lanjut. Antarmuka menu file ini dirancang untuk memberikan pengalaman pengguna yang sederhana dan intuitif, sehingga proses pengelolaan file dapat dilakukan dengan lebih efisien dan terorganisir.

F. Antarmuka Menu Tentang

Gambar 13 Antarmuka Menu Tentang

Antarmuka menu Tentang pada sistem enkripsi SMK Kusuma Bangsa dirancang untuk memberikan informasi lengkap mengenai aplikasi enkripsi yang digunakan. Menu ini berfungsi sebagai panduan bagi pengguna untuk memahami tujuan, fitur, dan manfaat dari aplikasi enkripsi, serta bagaimana aplikasi ini diimplementasikan di SMK Kusuma Bangsa.

Pada halaman ini, pengguna dapat menemukan penjelasan singkat mengenai latar belakang pengembangan aplikasi, termasuk kebutuhan untuk meningkatkan keamanan data siswa dan dokumen sekolah melalui teknologi enkripsi. Dijelaskan pula bahwa aplikasi ini menggunakan algoritma Advanced Encryption Standard (AES) 128-bit, yang diakui sebagai salah satu metode enkripsi paling aman dan efisien.

Selain itu, antarmuka menu Tentang juga menyajikan informasi tentang pengembang aplikasi, tujuan utama implementasi, dan cara aplikasi ini membantu mengamankan informasi sensitif dalam lingkungan sekolah. Desain halaman ini dibuat sederhana, dengan tata letak yang rapi dan mudah dibaca, sehingga pengguna dapat dengan cepat memahami peran penting aplikasi dalam mendukung sistem informasi di SMK Kusuma Bangsa.

G. Antarmuka Menu Panduan

Gambar 14 Antarmuka Menu Panduan

Antarmuka menu Panduan pada aplikasi enkripsi SMK Kusuma Bangsa dirancang untuk memberikan petunjuk lengkap mengenai cara penggunaan sistem enkripsi. Menu ini bertujuan untuk memastikan bahwa setiap pengguna, baik admin, staf sekolah, maupun kepala sekolah, dapat dengan mudah memahami langkah-langkah yang diperlukan untuk menjalankan fungsi-fungsi utama aplikasi.

Halaman panduan ini disusun dalam format yang terstruktur dan mudah diikuti, dimulai dengan pengenalan dasar antarmuka aplikasi. Panduan mencakup langkah-langkah untuk melakukan enkripsi file, seperti mengunggah file, memberikan kunci enkripsi, dan memulai proses enkripsi. Selain itu, dijelaskan pula cara menggunakan fitur dekripsi, termasuk memasukkan kunci file terenkripsi dan mengunduh hasil file dekripsi. Setiap langkah dilengkapi dengan penjelasan singkat serta ilustrasi atau tangkapan layar untuk mempermudah pemahaman pengguna.

Antarmuka menu Panduan juga mencakup informasi tambahan tentang pengelolaan file, seperti cara melihat status file, menghapus file yang tidak diperlukan, serta menjaga kerahasiaan kunci enkripsi. Dengan tampilan yang user-friendly, halaman panduan ini membantu memastikan bahwa pengguna dapat memaksimalkan manfaat

aplikasi enkripsi untuk meningkatkan keamanan data di lingkungan SMK Kusuma Bangsa.

3.9 Pengujian Sistem

Pengujian sistem merupakan tahap penting dalam pengembangan perangkat lunak untuk memastikan bahwa aplikasi atau sistem berjalan sesuai dengan fungsionalitas yang diharapkan. Dalam konteks ini, terdapat dua jenis metode pengujian utama yang sering digunakan, yaitu pengujian White Box dan Black Box.

White Box Testing atau pengujian kotak putih, adalah metode pengujian yang berfokus pada struktur internal atau logika kode dari sebuah aplikasi. Dalam pengujian ini, penguji memiliki akses penuh ke kode sumber dan memahami bagaimana aplikasi bekerja secara teknis. Tujuan utamanya adalah untuk mengidentifikasi kesalahan logika, memastikan semua jalur kode dieksekusi, dan memverifikasi algoritma yang digunakan. White Box Testing sering mencakup pengujian seperti unit testing, pengujian jalur logika, dan pengujian kontrol aliran data.

Sementara itu, Black Box Testing atau pengujian kotak hitam, lebih berfokus pada pengujian fungsionalitas sistem dari sudut pandang pengguna tanpa mengetahui bagaimana kode di balik aplikasi bekerja. Penguji hanya mengamati input yang diberikan dan output yang dihasilkan, serta membandingkannya dengan spesifikasi atau kebutuhan yang diharapkan. Black Box Testing bertujuan untuk memastikan bahwa fitur aplikasi berjalan sesuai desain, tanpa perlu memeriksa struktur internalnya. Contoh pengujian ini meliputi pengujian validasi input, pengujian antarmuka pengguna, dan pengujian integrasi sistem.

Pengujian White Box sangat efektif untuk menemukan kesalahan logika yang mungkin tidak terlihat dari pengujian berbasis fungsional. Metode ini juga membantu dalam mengoptimalkan kode, seperti mendeteksi loop yang tidak efisien atau kondisi yang tidak diperlukan. Namun, metode ini memerlukan pemahaman teknis mendalam terhadap aplikasi dan cenderung lebih memakan waktu karena kompleksitas analisis kode.

Di sisi lain, Black Box Testing memberikan manfaat dalam mengidentifikasi kesalahan dari perspektif pengguna. Metode ini memastikan bahwa aplikasi memberikan hasil sesuai harapan tanpa harus memahami implementasi teknisnya. Pengujian ini cocok digunakan untuk memeriksa kebutuhan pengguna akhir, seperti validasi form, respons sistem terhadap input yang salah, dan kelengkapan fungsionalitas.

Pengujian fungsi-fungsi yang terdapat pada aplikasi yang dibuat, berikut tabel rancangan pengujian.

Tabel III Pengujian Sistem Black Box

Pengujian Ke -	Test Case	Hasil Yang diharapkan	Hasil Pengujian
1	Login dengan username dan password valid	Pengguna berhasil masuk ke sistem	Berhasil
2	Login dengan username atau password salah	Sistem menampilkan pesan error “Username atau Password salah”	Berhasil
3	Input data file di menu enkripsi	File berhasil ditambahkan ke daftar file yang akan dienkripsi	Berhasil
4	Proses enkripsi file dengan kunci enkripsi valid	File berhasil terenkripsi, status file berubah menjadi “Terenkripsi”	Berhasil
5	Proses enkripsi file dengan kunci enkripsi kosong	Sistem menampilkan pesan error “Kunci enkripsi tidak boleh kosong”	Berhasil
6	Proses dekripsi file dengan kunci enkripsi valid	File berhasil didekripsi, status file berubah menjadi “Tidak Terenkripsi”	Berhasil
7	Proses dekripsi file dengan kunci enkripsi salah	Sistem menampilkan pesan error “Kunci enkripsi salah”	Berhasil
8	Akses menu “Panduan Aplikasi”	Sistem menampilkan informasi panduan penggunaan aplikasi	Berhasil
9	Hapus file dari daftar file yang terenkripsi	File berhasil dihapus dari sistem	Berhasil
10	Tambah pengguna baru oleh admin	Pengguna baru berhasil ditambahkan ke sistem	Berhasil
11	Simpan perubahan data file di menu file management	Sistem berhasil menyimpan perubahan data file	Berhasil

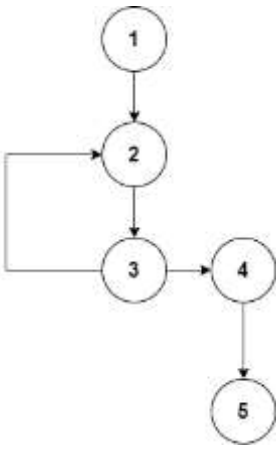
Pada Pengujian white box ini merupakan pengujuan yang dilakukan untuk menguji dan menganalisis kode program bilamana terjadi kesalahan pada proses nya program, Berikut saya lampirkan hasil pengujuan white box :

a). Pengujian Login

Berikut source code pada file Login.php yang akan di uji

Gambar 15 souce code login

Berikut hasil Flowgraph pada souce code tersebut



Gambar 16Flowgraph souce code login

Pada Gambar diatas terdapat 1 verifikasi pada nomer 3, dan pada nomer 4 yang artinya berhasil Login dan Berlanjut ke Menu Home Dashboard. Dan jika gagal Login akan kembeli ke nomer 2 yaitu from verifikasi username dan password.

Cyclomatic complexity adalah software yang menyediakan acuan kuantitatif kompleksitas suatu logika dalam program. Pada gambar diatas terdapat beberapa nodes, edges, dan predicated nodes untuk menghitung Cyclomatic Complexity berikut:

V(G) = E – N + 2

Keterangan :

E = jumlah edges pada flowgraph **N** = jumlah nodes pada flowgraph

P = jumlah predicates nodes pada flowgraph **V(G) = 5 – 5 + 2 = 2**

Independent Path:

Dari hasil penghitungan Cyclomatic Complexity terpadat 2 path berikut:

Path 1: 1 – 2 – 3 – 4 – 5

Path 2: 1 – 2 – 3 – 4 – 5

4. KESIMPULAN

Tingkat kerentanan data terhadap serangan siber di SMK Kusuma Bangsa cukup tinggi akibat kurangnya penerapan sistem keamanan yang memadai. Risiko kebocoran informasi, seperti data pribadi siswa, nilai akademik, dan catatan kehadiran, semakin meningkat tanpa adanya mekanisme perlindungan yang efektif. Salah satu faktor yang memperburuk kondisi ini adalah kurangnya enkripsi data dalam sistem berbasis website, yang berkontribusi terhadap tingginya risiko serangan siber, seperti data breach dan man-in-the-middle attack. Akibatnya, kepercayaan pengguna, termasuk siswa, guru, dan orang tua, dapat menurun serta berpotensi merusak reputasi sekolah. Untuk mengatasi masalah ini, implementasi algoritma enkripsi AES-128 dalam sistem informasi sekolah terbukti dapat meningkatkan keamanan data dengan memastikan bahwa informasi yang tersimpan dan dikirimkan melalui website tetap terlindungi. Enkripsi ini membuat data sulit diakses oleh pihak yang tidak berwenang, sehingga dapat mengurangi risiko kebocoran dan penyalahgunaan informasi. Dengan diterapkannya sistem enkripsi AES-128, SMK Kusuma Bangsa diharapkan dapat meningkatkan kepercayaan pengguna terhadap keamanan sistem informasi yang digunakan. Selain itu, penerapan enkripsi juga menjadi langkah penting dalam menjaga integritas data serta mencegah dampak buruk dari insiden keamanan siber.

5. UCAPAN TERIMAKASIH

Proses penyelesaian skripsi ini tidak lepas dari berbagai bantuan, dukungan, saran, dan kritik yang telah penulis dapatkan, oleh karena itu dalam kesempatan ini peneliti ingin mengucapkan terima kasih kepada para pihak yang terlibat dalam pembuatan jurnal.

6. DAFTAR PUSTAKA

[1] A.S, R., & Shalahuddin, M. (2018). Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. Bandung : Informatika. In Pilar Nusa Mandiri (p. 28).

[2] Arther Ignasius Suranta, Dolly Virgian Shaka Yudha Sakti. (2022). *Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi*. SKANIKA: Sistem Komputer dan

Teknik Informatika Volume 5, Nomor 1, Januari 2022, Halaman 1-10, E-ISSN: 2721-4788.

[3] Firman, F., Fauziyah, F., & Komalasari, R. T. (2021). *Aplikasi Pengingat Dan Pendataan Kenaikan Golongan Gaji Berbasis Web Menggunakan Metode White Box Testing Dan Black Box Testing*. Jurnal Teknologi Informasi, *7*(1), 50–57.Https://Doi.Org/10.52643/Jti.V7i1.1387.

[4] Hendri, H., Hasiholan Manurung, J. W., Ferian, R. A., Hanaatmoko, W. F., & Yulianti, Y. (2020). *Pengujian Black Box Pada Aplikasi Sistem Informasi Pengelolaan Masjid Menggunakan Teknik Equivalence Partitions*. Jurnal Teknologi Sistem Informasi Dan Aplikasi, *3*(2), 107.

[5] Isra Priambudi, Mufti. (2023). *Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa*. SKANIKA: Sistem Komputer dan Teknik Informatika Volume 6, Nomor 1, Januari 2023, Halaman 22-31, E-ISSN: 2721-4788.

[6] Jaya, T. S. (2018). *Pengujian Aplikasi Dengan Metode Blackbox Testing Boundary Value Analysis*. Jurnal Informatika, 4.

[7] Rahmawati, M., & Annisa, M. (2019). *Analisa Perancangan Sistem Informasi Akuntansi Event Organizer Dengan Aplikasi Accurate Versi 5 (Studi Kasus: PT. Inti Nuansa Ciptavisi)*. Informatika Bandung., *6*.

[8] Tachiyya Nailal Khusna, Bambang Sugiantoro. (2023). *Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2*. JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika). Vol. 8, No. 3, September 2023, Pp. 847-856. ISSN: 2540-8984.

[9] Uci, P., Khana, W., & Fajriyah. (2021). *Penerapan Metode Prototype Pada Perancangan Sistem Administrasi Pembayaran Karate Berbasis Website: Studi Kasus Lemkari Prabumulih.* Jurnal Pengembangan Sistem Informasi danInformatika.Vol2,No3,157-173.

[10] Yusmaifany, Tommy , Rosyidah Siregar. (2024). *Aplikasi Enkripsi Data Video Menggunakan Metode Rsa Dan Blowfish Berbasis Web*. Jurnal Komputer Teknologi Informasi Sistem Komputer. e-ISSN : 2963-7104 (Online), p-ISSN : 2962-3022 (Print), Volume 2 No 3 Februari 2024 - Page: 535-544.