Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 5 Iss. 1 January 2025, pp: 232-241
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Security of Bumijo Village Archives Using Advanced Encryption Standard (AES-128) Method Based on Web

Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES-128) Berbasis Web

Andrea Pirlo Indraka[1*], Moh. Ali Romli[2]

[1]Program Studi Informatika, Fakultas Sains dan Teknologi,
Universitas Teknologi Yogyakarta, Indonesia
[2]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Teknologi Yogyakarta, Indonesia

E-Mail: [1]andreapirloxmipa3@gmail.com, [2]ali.romli@uty.ac.id

Received Oct 18th 2024; Revised Nov 24th 2024; Accepted Dec 12th 2024; Available Online Dec 15th 2024
Corresponding Author: Andrea Pirlo Indraka

Abstract

The problem in the management of archive security in Bumijo Village is that there is no adequate security system to protect important archives and files, which can cause vulnerability to data leaks and theft. Therefore, this study aims to design and build a Web-based archive security application that implements data encryption using the Advanced Encryption Standard (AES) 128-bit algorithm. The research method used is the system development method with the stages of needs analysis, design, implementation, and testing. The result of this study is an archive security application that can perform the process of encryption and file description using the AES 128-bit algorithm, with the encrypted data stored in a MySQL database to facilitate access and management. The implementation of the AES 128-bit algorithm is expected to be able to improve the security of archive storage owned by Bumijo Village. The results of the User Acceptance Testing (UAT) test showed a user satisfaction level of 56.52%, which indicates that although the system was well received, there is still room for further improvement. Meanwhile, blackbox testing produced a success rate of 99%, which indicates that the system functions according to the expected specifications and can overcome the tested functionality scenarios.

Keyword: AES 128, Application, Archive Security, Description, Encryption,

Abstrak

Permasalahan yang ada pada pengelolaan keamanan arsip Kelurahan Bumijo saat ini adalah belum terdapat sistem keamanan yang memadai dalam menjaga arsip dan file penting, yang dapat menyebabkan rentannya terjadinya kebocoran dan pencurian data. Oleh karena itu, penelitian ini bertujuan untuk merancang dan membangun sebuah aplikasi keamanan arsip berbasis Web yang menerapkan enkripsi data menggunakan algoritma *Advanced Encryption Standard* (AES) 128 bit. Metode penelitian yang digunakan adalah metode pengembangan sistem dengan tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian. Hasil dari penelitian ini adalah sebuah aplikasi keamanan arsip yang dapat melakukan proses enkripsi dan deskripsi file menggunakan algoritma AES 128 bit, dengan data hasil enkripsi disimpan pada database MySQL untuk memudahkan akses dan pengelolaan. Implementasi algoritma AES 128 bit ini diharapkan mampu meningkatkan keamanan penyimpanan arsip milik Kelurahan Bumijo. Hasil pengujian *User Acceptance Testing* (UAT) menunjukkan tingkat kepuasan pengguna sebesar 56.52%, yang menunjukkan bahwa meskipun sistem diterima dengan baik, masih ada ruang untuk perbaikan lebih lanjut. Sementara itu, pengujian blackbox menghasilkan tingkat keberhasilan 99%, yang menandakan bahwa sistem berfungsi sesuai dengan spesifikasi yang diharapkan dan dapat mengatasi skenario fungsionalitas yang diuji.

Kata Kunci: AES 128, Aplikasi, Deskripsi, Enkripsi, Keamanan Arsip

1. PENDAHULUAN

Perkembangan teknologi dan informasi yang semakin pesat berdampak langsung pada meningkatnya kebutuhan manusia akan akses informasi. Informasi telah menjadi salah satu elemen penting dalam berbagai kegiatan manusia saat ini. Informasi menjadi dasar dalam pengambilan keputusan strategis, baik di sektor

publik maupun swasta. Seiring dengan itu, terciptalah berbagai macam file dan media yang memudahkan manusia dalam menyimpan, mencari, dan menyebarkan informasi [1]. File-file ini dikenal sebagai arsip, yang berarti rekaman dari suatu peristiwa yang telah terjadi. Arsip memiliki peranan yang sangat penting dalam mendukung kelancaran aktivitas di berbagai institusi. Arsip yang baik dapat meningkatkan efisiensi kerja dan memastikan kelangsungan kegiatan administrasi. Namun, dengan semakin berkembangnya penggunaan teknologi informasi, muncul pula tantangan baru terkait dengan keamanan data [2] Keamanan data atau informasi merupakan aspek penting bagi pengguna jaringan internet saat ini. Insiden penyadapan data dan informasi telah meningkat secara signifikan dalam lima tahun terakhir, menunjukkan perlunya upaya yang lebih serius dalam melindungi data digital. Salah satu ancaman yang sering terjadi adalah penyalahgunaan data atau informasi yang dapat merugikan pengguna. Oleh karena itu, diperlukan langkah-langkah konkret untuk meningkatkan aspek keamanan data dalam pengelolaan arsip digital [3]

Salah satu solusi untuk menjaga keamanan informasi adalah dengan menerapkan algoritma kriptografi. Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki tingkat keamanan yang tinggi dalam pertukaran informasi. AES-128, khususnya, sering digunakan untuk enkripsi dan dekripsi file dalam format PDF, DOC, dan TXT. Penelitian ini berfokus pada implementasi algoritma AES-128 untuk mengenkripsi dan mendekripsi file, serta mengukur kecepatan proses tersebut. Di Kelurahan Bumijo, pengelolaan arsip masih kurang efisien, terutama dalam hal keamanan penyimpanan file. Kondisi ini meningkatkan risiko pencurian atau penyalahgunaan data penting yang dapat berdampak pada kerahasiaan informasi. Berdasarkan observasi, terdapat beberapa kekhawatiran terkait potensi kebocoran data karena belum adanya sistem pengelolaan arsip yang terintegrasi dan aman. Misalnya, beberapa kali ditemukan dokumen penting yang hilang atau sulit diakses kembali karena sistem penyimpanan manual yang tidak terorganisasi dengan baik. Oleh karena itu, diperlukan sebuah sistem yang dapat meningkatkan efisiensi dan keamanan dalam pengelolaan arsip di Kelurahan Bumijo, sehingga potensi kebocoran data dapat diminimalkan.

Penelitian ini bertujuan untuk merancang sebuah aplikasi keamanan berbasis algoritma AES-128 yang terintegrasi dengan MySQL, yang dapat mengenkripsi dan mendekripsi file secara aman. Aplikasi ini diharapkan dapat membantu kelurahan dalam menjaga kerahasiaan dan keamanan file penting, serta mencegah akses yang tidak sah. Dengan demikian, aplikasi ini menjadi solusi yang efektif dalam meningkatkan keamanan arsip di Kelurahan Bumijo.

2. PENELITIAN YANG TERKAIT

Berikut merupakan beberapa referensi penelitian yang telah dilakukan sebelumnya yang menjadi dasar dalam penelitian ini:

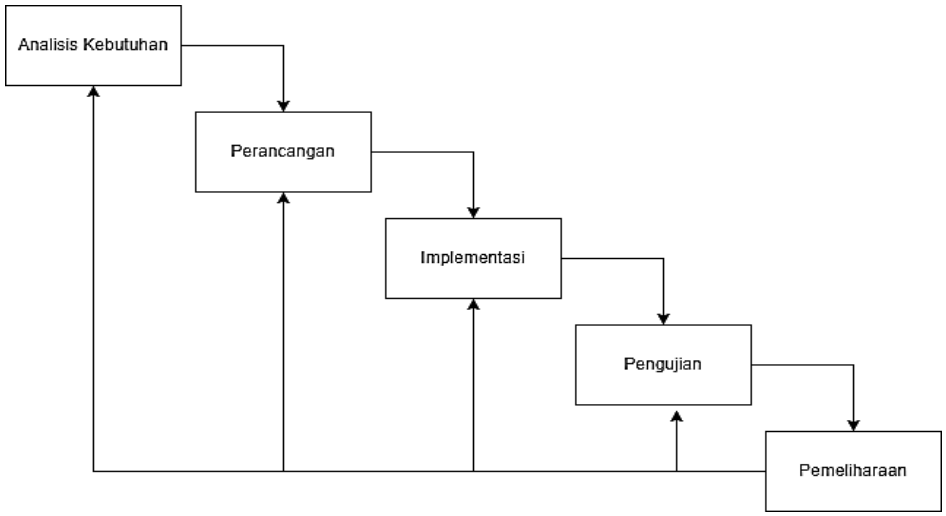
Penelitian pertama membahas mengamankan data keuangan siswa yang bersifat sensitif yaitu data uang Sumbangan Pembiayaan Pendidikan (SPP) di SMK Harapan Bangsa menggunakan metode *Advanced Encryption Standard* (AES) 128 bit. Metode AES digunakan karena mampu menyediakan tingkat keamanan yang tinggi berdasarkan kunci rahasia yang kompleks, sehingga dapat merahasiakan isi dari data uang SPP agar tidak dapat dibaca, dicuri, dimanipulasi, dan dibocorkan oleh pihak yang tidak bertanggung jawab [4]. Kemudian penelitian kedua membahas mengetahui konsep kriptografi untuk pengamanan data berbasis teks dengan menggunakan algoritma AES. Algoritma AES dipilih karena kemampuannya dalam mengenkripsi dan menDekripsikan data dengan panjang kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit dan perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES. Penelitian ini juga bertujuan untuk membuat aplikasi untuk mengenkripsi file dan pesan teks menggunakan algoritma Advanced Encryption Standard (AES). Implementasi algoritma AES juga dilakukan untuk mengenkripsi dan mendekripsi proses enkripsi email [5]. Lalu penelitian ketiga membahas penerapkan kriptografi Advanced Encryption Standard (AES) untuk keamanan data aplikasi pemesanan bibit ternak pada Balai Pengujian Standar Instrumen Unggas dan Aneka Ternak (BPSI UAT). Tujuan penelitian ini adalah untuk meningkatkan keamanan data pemesanan bibit ternak dengan melakukan enkripsi dan Dekripsi data menggunakan algoritma AES [6]. Kemudian penelitian keempat membahas menciptakan sebuah sistem e-marketplace untuk menangani proses transaksi jual beli bibit buah dan tanaman di Desa Sriwedari agar lebih efektif dan efisien. Sistem e-marketplace yang dibangun ini diharapkan mampu memperluas jangkauan pemasaran produk, memudahkan proses transaksi, serta mengamankan data transaksi pengguna dengan menerapkan algoritma kriptografi AES-256 untuk mengenkripsi data transaksi pembayaran. Dengan adanya sistem e-marketplace ini, diharapkan mampu meningkatkan pendapatan yang diperoleh oleh Toko Bibit Sriwedari serta memudahkan pelanggan dalam melakukan pemesanan dan pembayaran bibit secara online [7]. Terakhir penelitian kelima membahas menganalisis penerapan algoritma kriptografi *Advanced Encryption Standard* (AES) dalam mengamankan data karyawan PT. Telkom Indonesia Pematangsiantar. Algoritma AES merupakan salah satu metode keamanan data yang banyak digunakan karena mampu mengenkripsi file dengan berbagai ekstensi seperti word, excel, power point, PDF, serta gambar menjadi berkas yang tidak dapat dibaca oleh orang lain kecuali menggunakan kunci yang sama [8]

Dalam penelitian ini, terdapat sejumlah gap yang dapat diidentifikasi dari penelitian-penelitian sebelumnya yang menggunakan algoritma *Advanced Encryption Standard* (AES). Beberapa penelitian

menyoroti keamanan dengan penerapan AES 128 bit, namun kurang menekankan aspek penyimpanan data yang aman. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem yang tidak hanya mengenkripsi data tetapi juga menyediakan mekanisme penyimpanan yang aman untuk melindungi data tersebut dari akses yang tidak sah. Dengan demikian, penelitian ini tidak hanya mengimplementasikan AES 128 sebagai metode enkripsi, tetapi juga mengedepankan pentingnya pengamanan dan penyimpanan data dalam konteks perlindungan informasi yang lebih komprehensif.

3. METODE PENELITIAN

Dalam pengembangan sistem ini akan diterapkan metode *Software Development Life Cycle* (SDLC) SDLC Waterfall. Metode SDLC ini cocok digunakan untuk pengembangan sistem jangka pendek yang memerlukan penyesuaian cepat terhadap perubahan [9]. Tahapan-tahapan dari SDLC Waterfall dapat dilihat pada Gambar 1.



Gambar 1. Metode Penelitian

Pengembangan sistem ini diawali dengan memahami kebutuhan dan tujuan perangkat lunak yang akan dibuat. Tim pengembang terlebih dahulu mempelajari kebutuhan pengguna dan menentukan fitur serta fungsi yang dibutuhkan. Setelah itu, mereka merancang arsitektur, desain, dan spesifikasi teknis perangkat lunak. Proses perancangan ini juga melibatkan pembuatan diagram alir serta desain antarmuka pengguna. Tahap selanjutnya adalah implementasi, yaitu penulisan kode program yang kemudian diikuti dengan pengujian untuk memastikan kualitas perangkat lunak. Setelah semua kode selesai dibuat, pengujian dilakukan untuk memastikan perangkat lunak bekerja sesuai dengan persyaratan yang ditentukan. Apabila semua sudah berfungsi dengan baik, perangkat lunak siap dirilis kepada pengguna. Pemeliharaan dilakukan setelah perangkat lunak dirilis, dengan tujuan memperbaiki, memperbarui, dan menambah fitur sesuai kebutuhan pengguna. Tahap ini juga memastikan perangkat lunak tetap berjalan dengan optimal dan dilakukan pembaruan secara berkala untuk meningkatkan kepuasan pengguna.

Metode Waterfall ini mengharuskan setiap tahap diselesaikan secara berurutan sebelum melanjutkan ke tahap berikutnya. Meskipun metode ini mudah dipahami dan diterapkan, kekurangannya terletak pada fleksibilitas yang rendah, sehingga lebih cocok digunakan untuk proyek-proyek dengan persyaratan yang sudah jelas dari awal.

3.1 Pengumpulan Data

Pada penelitian ini, data yang digunakan meliputi data sekunder yang diperoleh dari Data Krematorium Yogyakarta, berupa informasi nama data dan tanggal, yang ditampilkan dalam Tabel 1.

Tabel 1. Data Krematorium Yogyakarta

No	Data	Tanggal
1	Data Krematorium Yogyakarta	Tanggal 03 April 2024
2	Data Krematorium Yogyakarta	Tanggal 17 April 2023
3	Data Krematorium Yogyakarta	Tanggal 26 Maret 2024
4	Data Krematorium Yogyakarta	Tanggal 30 Maret 2024
5	Data Krematorium Yogyakarta	Tanggal 30 Maret 2024
6	Data Krematorium Yogyakarta	Tanggal 30 Maret 2024
7	Data Krematorium Yogyakarta	Tanggal 28 Maret 2024
8	Data Krematorium Yogyakarta	Tanggal 15 Maret 2024

Data dalam penelitian ini diperoleh melalui observasi, studi literatur, pencarian internet, dan pengambilan data langsung dari Kelurahan Bumijo. Observasi dilakukan untuk memahami kondisi di lapangan, mengidentifikasi masalah yang dihadapi pelanggan serta pihak bengkel. Studi literatur digunakan untuk memperoleh dasar teori yang relevan, khususnya terkait dengan konsep implementasi algoritma Haversine. Selain itu, pencarian internet dilakukan untuk mencari data tambahan yang mendukung penelitian.

Selain metode tersebut, data juga didapatkan langsung dari Kelurahan Bumijo, di mana data diperoleh dengan cara memfoto dokumen satu per satu yang diberikan langsung oleh pihak kelurahan. Pengumpulan data ini berlangsung selama satu hari, pada 22 Mei 2024 untuk mendapatkan data Kelurahan pada tahun 2024.

3.2 Landasan Teori

3.2.1 Kriptofrafi

Kriptografi adalah teknik penting yang digunakan untuk mengamankan informasi melalui proses enkripsi data, terutama dalam melindungi arsip digital yang sensitif. Salah satu algoritma kriptografi yang banyak digunakan adalah *Advanced Encryption Standard* (AES), khususnya dengan panjang kunci 128-bit (AES-128), yang menawarkan tingkat keamanan tinggi dengan efisiensi yang baik. AES-128 dirancang untuk memastikan data tetap rahasia dan terlindungi dari akses yang tidak sah, sehingga sangat cocok untuk menjaga keamanan arsip dalam berbagai aplikasi [10].

Proses kriptografi dengan AES-128 melibatkan pengubahan data sederhana (plaintext) menjadi data terenkripsi (ciphertext) yang hanya dapat diakses dengan kunci tertentu. Dengan keunggulan seperti kecepatan enkripsi, tingkat keamanan yang kuat, dan kompatibilitas dengan berbagai platform, AES-128 menjadi pilihan utama dalam pengamanan data. Oleh karena itu, penerapan algoritma AES-128 sangat direkomendasikan untuk memastikan kerahasiaan, integritas, dan keamanan arsip dalam sistem yang dirancang [11].

3.2.2 Advanced Encryption Standart (AES 128)

Andvanced Encryption Standart (AES 128) merupakan algoritma kriptografi yang dirancang untuk mengamankan data dengan tingkat keamanan yang tinggi. Algoritma ini berfungsi sebagai teknik penyembunyian data rahasia dalam suatu wadah (media) sehingga informasi yang disembunyikan menjadi sulit untuk dikenali oleh indera manusia. Kelebihan dari algoritma AES meliputi kecepatan dalam proses enkripsi dan dekripsi, serta kemampuan untuk memproses data dalam blok 128 bit. Selain itu, AES juga menawarkan ketahanan terhadap serangan kriptanalisis, menjadikannya pilihan yang ideal untuk melindungi data sensitif dari akses yang tidak sah. Implementasi AES dapat ditemukan dalam berbagai aplikasi, mulai dari pengamanan data di server hingga perlindungan informasi dalam komunikasi internet. Dengan demikian, AES merupakan salah satu pilar penting dalam menjaga keamanan informasi di era digital ini [12].

3.2.3 *Entity Relationship Diagram* (ERD)

Entity Relationship Diagram (ERD) adalah model konseptual yang menggambarkan hubungan antar data dalam sistem basis data, membantu pengembang merancang struktur yang efisien dan konsisten [13]. *Entity Relationship Diagram* (ERD) juga berfungsi sebagai dokumentasi untuk memperjelas spesifikasi sistem dan memfasilitasi komunikasi antar tim [14]. Selain itu, ERD mendukung perencanaan dan pengembangan sistem di masa depan dengan memberikan gambaran menyeluruh tentang hubungan data [15].

3.2.4 Database

Database adalah kumpulan data yang terorganisir dan terstruktur dalam sistem komputer, terdiri dari beberapa tabel yang saling terhubung melalui relasi tertentu [16]. Dalam penelitian ini, database yang digunakan adalah MySQL, karena MySQL memiliki keunggulan dalam efisiensi akses data, kemudahan integrasi dengan metode enkripsi seperti AES (Advanced Encryption Standard), serta kemampuan untuk memastikan keamanan data. MySQL menyediakan fitur bawaan yang mendukung pengelolaan data terenkripsi, sehingga sangat sesuai untuk aplikasi yang memerlukan perlindungan data sensitif.

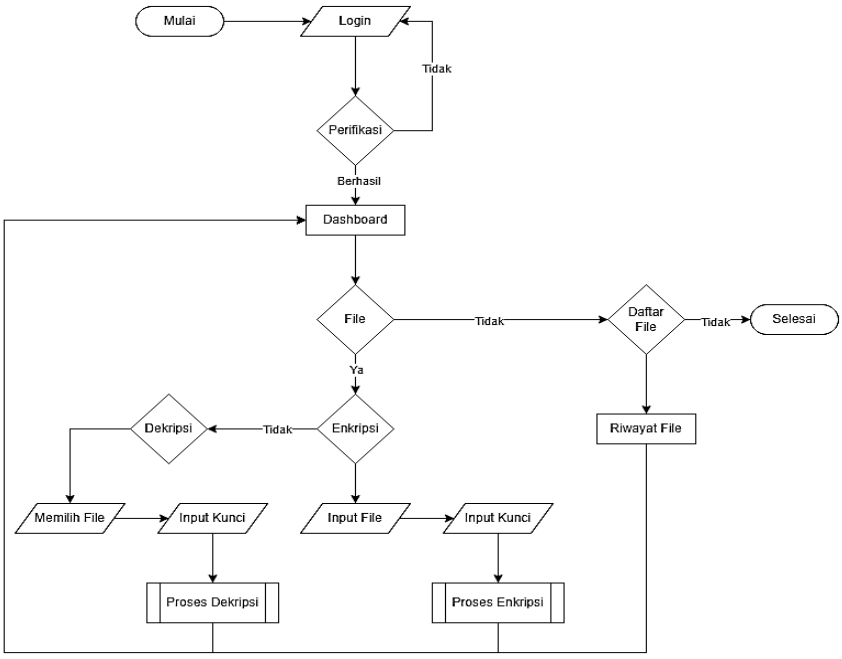
Tahapan penelitian dimulai dengan perancangan database, di mana tabel-tabel dirancang untuk mendukung struktur aplikasi secara optimal, termasuk penyimpanan data hasil enkripsi. Setelah itu, data diolah menggunakan DBMS MySQL yang memungkinkan proses penyimpanan, pencarian, pembaruan, dan penghapusan data berjalan efisien. Selain itu, MySQL mempermudah integrasi dengan sistem aplikasi melalui berbagai pustaka atau API yang mendukung implementasi metode enkripsi, sehingga data tetap aman dan mudah diakses [17]. Dengan menggunakan MySQL, penelitian ini memastikan data dapat dikelola secara efektif, mengurangi redundansi, meningkatkan integritas, dan mempermudah pengambilan keputusan berdasarkan data yang telah diolah [18]. Hal ini membuktikan bahwa MySQL tidak hanya unggul dalam performa tetapi juga mendukung pengelolaan data dengan tingkat keamanan yang tinggi, khususnya dalam konteks aplikasi berbasis enkripsi data.

4. HASIL DAN PEMBAHASAN

4.1 Analisa dan Perancangan Sistem

Sistem yang dikembangkan dalam bentuk Aplikasi Arsip Elektronik Kelurahan Bumijo berbasis web dirancang untuk meningkatkan efisiensi serta keamanan dalam pengelolaan arsip internal secara digital. Aplikasi ini bertujuan untuk memfasilitasi staf kelurahan dalam proses unggah, penyimpanan, manajemen, dan pencarian arsip dengan lebih mudah. Dengan demikian, ketergantungan terhadap arsip fisik dapat diminimalisir, yang pada gilirannya akan meningkatkan keandalan, integritas, serta keamanan data.

Selain itu, sistem ini diharapkan mampu mempercepat dan mengorganisir proses pencarian dan pengelolaan arsip, sehingga produktivitas staf dalam mengakses dan memanfaatkan informasi meningkat secara signifikan. Dengan adanya pengelolaan berbasis digital, potensi risiko kehilangan atau kerusakan file fisik juga dapat ditekan, sekaligus memungkinkan pengelolaan arsip yang lebih transparan dan terdokumentasi dengan baik. Inovasi ini tidak hanya mendukung efektivitas kerja di tingkat kelurahan, tetapi juga memastikan bahwa arsip-arsip penting terlindungi dari akses yang tidak sah, sehingga menjaga kerahasiaan data dan informasi penting yang tersimpan.

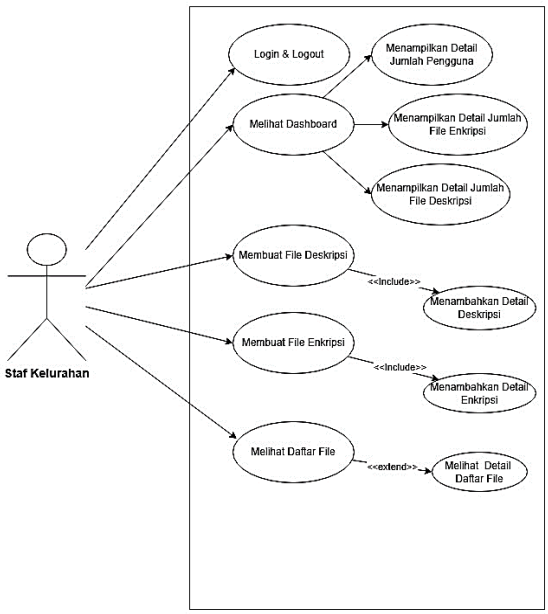


Gambar 2. *Flowchart Diagram* Sistem

Flowchart yang ditampilkan pada Gambar 2 menggambarkan secara rinci alur kerja sistem pengelolaan arsip elektronik yang dirancang. Proses dimulai dengan langkah autentikasi, di mana pengguna diwajibkan untuk melakukan login menggunakan username dan password. Proses ini bertujuan untuk memastikan bahwa hanya pengguna yang memiliki izin atau hak akses yang dapat masuk ke dalam sistem. Setelah login berhasil, pengguna akan diarahkan ke dashboard utama, yang menyajikan informasi penting seperti status arsip terkini, statistik penggunaan sistem, dan notifikasi terkait aktivitas pengelolaan arsip. Dashboard juga menyediakan akses cepat ke berbagai fitur, seperti pencarian arsip, pengunggahan arsip baru, manajemen pengguna, dan pengaturan sistem.

Jika login gagal, *flowchart* menunjukkan mekanisme penanganan kesalahan yang akan memberi notifikasi kepada pengguna dan mengarahkan mereka untuk mencoba kembali atau menggunakan fitur pemulihan akun. Selain itu, *flowchart* juga mencakup alur kerja lanjutan, seperti pencarian arsip, pengeditan data arsip, dan penghapusan arsip yang tidak relevan. Setiap tindakan yang dilakukan pengguna tercatat dalam log aktivitas untuk keperluan audit dan pemantauan, menjamin transparansi dan keamanan. Dengan demikian, flowchart ini tidak hanya menggambarkan langkah-langkah operasional, tetapi juga mengutamakan efisiensi dan keamanan dalam pengelolaan arsip elektronik secara keseluruhan.

Diagram *use case* pada gambar 3 menggambarkan fitur utama sistem keamanan arsip yang dapat diakses oleh staf kelurahan. Fitur tersebut meliputi login/ logout, melihat *dashboard*, membuat file enkripsi dan deskripsi, serta mengelola daftar file. Pada *dashboard*, staf dapat melihat statistik, seperti jumlah file terenkripsi dan terdeskripsi. Selain itu, proses pembuatan file enkripsi dan deskripsi mencakup penambahan detail terkait, untuk memastikan pengelolaan arsip dilakukan secara sistematis.

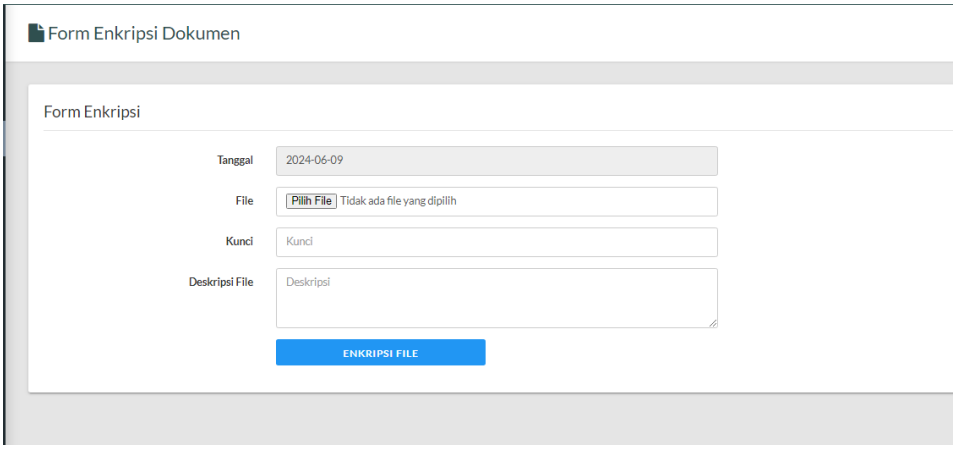


Gambar 3. *Use Case* Sistem

Sistem ini juga menyediakan opsi bagi staf untuk melihat detail file yang telah diolah. Semua fitur dirancang untuk mendukung keamanan arsip menggunakan algoritma AES-128, yang memastikan perlindungan data penting kelurahan dari akses yang tidak sah. Dengan fitur-fitur ini, sistem diharapkan mampu meningkatkan efisiensi dan keamanan dalam pengelolaan arsip digital.

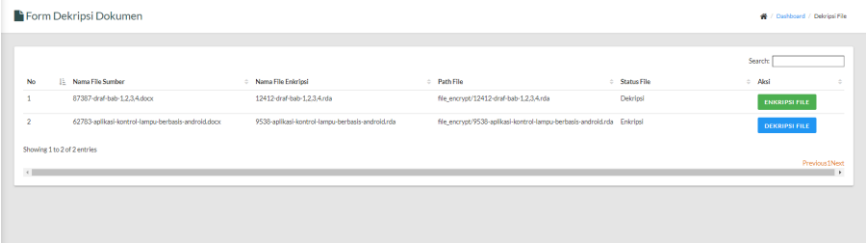
4.2. Website untuk Admin

Pada Gambar 3 menampilkan tampilan halaman enkripsi. Di halaman ini, terdapat beberapa komponen penting, yaitu tanggal, file, kunci, dan deskripsi file. Pada bagian tanggal, pengguna dapat memasukkan tanggal ketika proses enkripsi dilakukan. Di bagian file, pengguna memiliki opsi untuk memilih file mana yang akan dienkripsi. Pada bagian kunci, pengguna harus memasukkan kunci yang akan digunakan saat melakukan proses deskripsi di kemudian hari. Selain itu, pada bagian deskripsi file, pengguna dapat menambahkan informasi tambahan yang relevan.



Gambar 3. Form Enkripsi Dokumen

Gambar 4 menampilkan tampilan halaman deskripsi dalam aplikasi. Di halaman ini, pengguna dapat memilih file yang telah tersimpan sebelumnya untuk didekripsi. Setelah memilih file, pengguna cukup memasukkan kunci yang digunakan saat enkripsi untuk melanjutkan proses dekripsi. Halaman ini dirancang dengan antarmuka yang intuitif, memudahkan navigasi dan akses ke file, serta memberikan petunjuk yang jelas tentang langkah-langkah yang harus diikuti. Fitur ini memungkinkan pengguna mengakses informasi yang telah terenkripsi dengan aman, sambil menjaga kontrol penuh atas data mereka.



Gambar 4. Form Deskripsi Dokumen

4.3. Pengujian

Selanjutnya untuk mengevaluasi kinerja dan kualitas sistem yang dikembangkan, dua jenis pengujian dilakukan, yaitu pengujian *black box* dan *user acceptance testing* (UAT). Pengujian *black box* bertujuan untuk mengidentifikasi kesalahan pada antarmuka pengguna, interaksi, dan integrasi sistem tanpa memperhatikan detail internal sistem [19]. Sementara itu, pengujian UAT difokuskan pada memastikan bahwa sistem memenuhi harapan pengguna dan sesuai dengan kebutuhan fungsional yang telah ditetapkan. Kedua pengujian ini dilakukan secara menyeluruh untuk menilai efektivitas sistem dan memberikan masukan untuk perbaikan lebih lanjut [20].

Pada bagian pengujian, dilakukan pengujian black box untuk mengevaluasi kinerja sistem yang dikembangkan, memastikan bahwa situs berfungsi sesuai dengan harapan pengguna dan spesifikasi yang ditetapkan. Metode ini efektif dalam mengidentifikasi kesalahan dalam antarmuka pengguna, interaksi, dan integrasi sistem, tanpa memerlukan pemahaman tentang detail internal sistem. Pengujian dilakukan melalui berbagai skenario, seperti pengisian formulir, pengunggahan file, dan proses login, untuk menilai respons sistem terhadap kondisi penggunaan yang berbeda. Hasil pengujian ini disajikan dalam Tabel 4.1, yang mencakup skenario pengujian, langkah-langkah yang dilakukan, dan hasil yang diperoleh. Tabel ini memberikan gambaran mengenai kinerja sistem dan area yang perlu diperbaiki untuk meningkatkan kualitas dan keandalan sistem secara keseluruhan.

Tabel 2. Pengujian Black Box

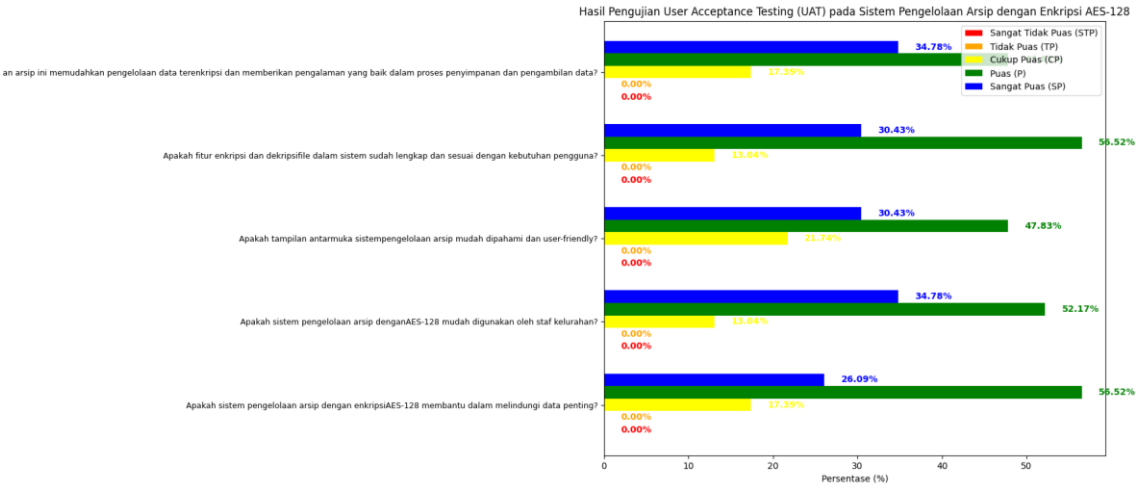
No	Skenario Pengujian	Hasil	Kesimpulan
1	Melakukan login	Dapat masuk menggunakan username dan password	Berhasil
2	Masuk kehalaman dashboard	Menampilkan halaman dashboard	Berhasil
3	Masuk kehalaman *enkripsi*	Menampilkan halaman *enkripsi*	Berhasil
4	Melakukan *enkripsi*	*File* berhasil ter*enkripsi*	Berhasil
5	Masuk kehalaman *deskripsi*	Menampilkan halaman *deskripsi*	Berhasil
6	Melakukan *deskripsi*	*File enkripsi* berhasil ter*deskripsi*	Berhasil
7	Masuk kehalaman daftar *file*	Menampilakan halaman daftar *file*	Berhasil

Pengujian terhadap sistem website yang mengimplementasikan enkripsi data menggunakan algoritma AES-128 menunjukkan hasil yang sangat memuaskan, dengan 7 skenario pengujian berjalan tanpa kegagalan. Seluruh tahapan, mulai dari login, navigasi ke halaman dashboard, hingga proses enkripsi dan deskripsi file, berfungsi dengan lancar. Halaman yang diuji, seperti halaman enkripsi, deskripsi, dan daftar file, semuanya berhasil menampilkan informasi dengan tepat, serta memastikan bahwa file dapat dienkripsi dan didekripsi dengan efisien. Dengan tingkat keberhasilan 99%, hasil ini menunjukkan bahwa sistem mampu mengelola dan melindungi data dengan aman, serta memberikan pengalaman pengguna yang optimal, siap digunakan untuk meningkatkan keamanan data di Kelurahan Bumijo.

Sebelum menerapkan aplikasi pengelolaan arsip dengan enkripsi data menggunakan AES-128 di Kelurahan Bumijo, dilakukan pengujian UAT untuk menilai tingkat kepuasan dan penerimaan pengguna terhadap sistem. Pengujian ini melibatkan 23 responden yang merupakan staf kelurahan yang menggunakan sistem secara langsung. Responden diminta untuk menilai berbagai aspek aplikasi, seperti kemudahan penggunaan, antarmuka yang ditampilkan, kelengkapan fitur enkripsi dan dekripsi file, serta kemudahan dalam mengelola data yang telah terenkripsi. Hasil dari penilaian ini kemudian dianalisis dengan menggunakan skala Likert untuk mengetahui sejauh mana aplikasi ini memenuhi harapan dan kebutuhan pengguna dalam memastikan keamanan data. Hasil pengujian dari para responden dapat dilihat pada Tabel 3.

Berdasarkan hasil *User Acceptance Testing* (UAT**)** yang dilakukan terhadap sistem pengelolaan arsip dengan menggunakan enkripsi AES-128 di Kelurahan Bumirjo, data penilaian telah dikumpulkan dari 23 responden untuk mengukur tingkat kepuasan pengguna. Pengujian ini melibatkan lima aspek utama, yaitu efektivitas enkripsi AES-128 dalam melindungi data penting, kemudahan penggunaan sistem oleh staf kelurahan, daya tarik antarmuka pengguna, kelengkapan fitur enkripsi dan dekripsi file, serta kemudahan dalam mengelola arsip terenkripsi. Penilaian dilakukan menggunakan skala mulai dari "Sangat Tidak Puas (STP)"

hingga "Sangat Puas (SP)", dengan hasil yang menunjukkan tingkat kepuasan yang bervariasi. Data hasil pengujian ini memberikan gambaran mengenai pengalaman pengguna dalam mengoperasikan sistem pengelolaan arsip dengan enkripsi AES-128, serta menunjukkan area yang perlu diperbaiki untuk meningkatkan efektivitas dan kepuasan pengguna. Selanjutnya adalah visualisasi hasil penilaian yang menggambarkan distribusi persentase jawaban dari para responden terhadap setiap pertanyaan yang diajukan.



Gambar 5. Visualisasi *User Acceptance Testing* (UAT)

Berdasarkan hasil UAT yang melibatkan 23 responden, dapat disimpulkan bahwa sistem pengelolaan arsip dengan enkripsi AES-128 di Bumirjo diterima dengan baik oleh pengguna. Mayoritas responden memberikan penilaian positif terkait kemudahan penggunaan dan kelengkapan fitur, dengan persentase Sangat Tidak Kepuasan (STP) dan Sangat Puas (SP) mencapai 56.52% dengan persentase tertinggi yaitu Puas (Puas). Meskipun demikian, terdapat beberapa aspek yang perlu diperbaiki, terutama pada tampilan antarmuka sistem yang masih mendapatkan penilaian cukup dari beberapa responden. Hal ini menunjukkan bahwa meskipun sistem dapat memenuhi sebagian besar kebutuhan pengguna, perbaikan lebih lanjut tetap diperlukan untuk meningkatkan pengalaman pengguna secara keseluruhan.

4.4. Pembahasan

Berdasarkan analisis dan pengujian yang telah dilakukan, dapat disimpulkan bahwa sistem ini berhasil mencapai tujuan utamanya, yaitu meningkatkan keamanan file di Kelurahan Bumijo. Dengan implementasi sistem ini, kelurahan dapat menjaga keamanan file-file yang rentan terhadap pencurian. Berikut adalah pencapaian signifikan dari penelitian ini:

1. Kemampuan Enkripsi dan Deskripsi: Sistem ini telah berhasil mengenkripsi dan mendeskripsi file dengan efektif. Proses enkripsi yang dilakukan tidak hanya menghasilkan file yang aman, tetapi juga memastikan bahwa hasil enkripsi dan deskripsi dapat disimpan dengan akurat dalam database. Ini memenuhi kebutuhan pengguna yang mengharapkan akses yang cepat dan aman terhadap data sensitif mereka.
2. Desain Antarmuka Pengguna yang Responsif: Desain antarmuka pengguna (UI/UX) yang responsif dan intuitif memastikan pengalaman pengguna yang positif. Pengguna dapat dengan mudah memahami dan menggunakan sistem untuk melakukan proses keamanan file, tanpa mengalami kebingungan. Dengan demikian, sistem ini tidak hanya aman, tetapi juga ramah pengguna, yang penting untuk meningkatkan adopsi teknologi di lingkungan pemerintahan.
3. Peningkatan Keamanan File: Dengan implementasi sistem ini, diharapkan keamanan file penting milik Kelurahan Bumijo dapat ditingkatkan secara signifikan. Sistem ini tidak hanya memberikan solusi jangka pendek untuk masalah keamanan, tetapi juga dapat berfungsi sebagai landasan bagi peningkatan keamanan data di masa depan. Dengan menggunakan algoritma AES-128, sistem ini menawarkan perlindungan yang kuat terhadap data sensitif, sehingga mengurangi risiko kebocoran informasi.

Secara keseluruhan, sistem ini diharapkan tidak hanya memenuhi kebutuhan keamanan saat ini, tetapi juga dapat beradaptasi dengan perkembangan teknologi di masa depan, memberikan Kelurahan Bumijo kepercayaan dalam pengelolaan data mereka.

5. KESIMPULAN

Sistem implementasi algoritma AES-128 untuk pengamanan file di Kelurahan Bumirjo telah berhasil mencapai tujuan utama dalam meningkatkan keamanan data. Dengan kemampuan enkripsi dan deskripsi yang efisien, sistem ini berhasil melindungi file-file penting yang dikelola oleh kelurahan dari potensi pencurian dan akses yang tidak sah. Hasil pengujian menunjukkan bahwa sistem ini mampu mengenkripsi dan mendeskripsi file dengan akurat serta menyimpan hasilnya dalam database dengan efektif, sesuai dengan kebutuhan pengguna. Selain itu, desain antarmuka pengguna yang responsif dan intuitif memberikan pengalaman pengguna yang positif, memudahkan staf kelurahan dalam mengoperasikan sistem tanpa kesulitan.

Dalam pengujian User Acceptance Testing (UAT), sistem ini memperoleh hasil sebesar 56.52%, yang menunjukkan bahwa sebagian besar pengguna merasa puas dengan kinerja sistem. Di sisi lain, pengujian blackbox menunjukkan hasil yang sangat baik, yakni 99%, yang menandakan bahwa sistem berjalan sesuai dengan spesifikasi yang diharapkan dan tidak mengalami masalah signifikan saat diuji di tingkat fungsionalitas.

Namun, meskipun sistem ini berhasil dalam banyak aspek, terdapat beberapa kelemahan yang perlu diperhatikan. Salah satunya adalah kinerja sistem yang dapat terpengaruh oleh ukuran file yang sangat besar, yang mempengaruhi waktu enkripsi dan dekripsi. Selain itu, mekanisme pemulihan data masih perlu diperbaiki apabila terjadi kesalahan atau kerusakan pada file yang telah dienkripsi. Sebagai saran untuk penelitian ke depan, disarankan untuk mengoptimalkan algoritma enkripsi agar dapat menangani file yang lebih besar dengan lebih efisien, serta meningkatkan aspek pemulihan data dan pengelolaan kunci enkripsi. Dengan adanya perbaikan tersebut, sistem ini diharapkan dapat lebih optimal dan siap diimplementasikan pada skala yang lebih luas, serta menjadi model bagi kelurahan lain dalam mengadopsi teknologi untuk meningkatkan efisiensi dan keamanan pengelolaan informasi.

REFERENSI

[1] Aldina Esti Purwanti & Feri Lupiana. (2023). Peran Sistem Informasi Pemasaran dalam Mengelola Proses PemasaranMelalui Digital Marketing. Jurnal Ilmiah Manajemen, Ekonomi dan Bisnis 2(1), 99-102.

[2] Alvina Tri Amalia & Lifa Farida Panduwinata. (2022). Sistem Informasi Manajemen Arsip Elektronik (E-Arsip) Berbasis Microsoft Access Terhadap Efektivitas Penemuan Kembali Arsip Pada SMKN 4 Surabaya. Jurnal Pendidikan Administrasi Perkantoran (JPAP). 10(3) 195-210.

[3] Dyah Ayu Suci Ilhami. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi. 2(1) 51-60

[4] Cristy, N., & Riandari, F. (2021). Niolinda Cristy 1 , Fristi Riandari 2 [Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. 4(2), 75.

[5] Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada File Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(1), 2809–476. https://doi.org/10.47709/jpsk.v2i1.1390

[6] Nanda Rahmat Herlambang, D., & Pravitasari, N. (2024). (2024). Penerapan Kriptografi AES untuk Keamanan Data. Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer, 8(1). https://doi.org/10.33395/remik.v8i1.13157

[7] Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. Journal of Computer System and Informatics (JoSYC), 4(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

[8] Fahri, M., Damanik, H., Gunawan, I., Nasution, Z. M., Sumarno, S., & Kirana, I. O. (2022a). Pemanfaatan algoritma aes untuk keamanann data karyawan pt. Telkom indonesia pematangsiantar. 1(1), 32–37. Https://doi.org/10.55123

[9] Kirman & Erdi Epta Saputra. (2022). Metode SDLC Waterfall Pada Rancang BangunSistem Informasi Sekolah SMP Negeri 10 Kaur. JUSIBI (Jurnal Sistem Informasi Dan E-Bisnis) 4(2) 112-118.

[10] Nanda Amalya, Santa Maria Sopiana Silalahi, Della Fatricia Nasution, Melia Sari, Indra Gunawaa (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. JURNAL MEDIA INFORMATIKA [JUMIN].

[11] Dwi Nurcahya, S. (2022). Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java. Jurnal Nasional Komputasi Dan Teknologi Informasi, 5(4).

[12] Fahri, M., Damanik, H., Gunawan, I., Nasution, Z. M., Sumarno, S., & Kirana, I. O. (2022b). Pemanfaatan algoritma aes untuk keamanann data karyawan pt. Telkom indonesia pematangsiantar. 1(1), 32–37. Https://doi.org/10.55123

[13] Togatorop, P., Simanjuntak, R. P., Manurung, S. B., & Silalahi, M. C. (2021). Pembangkit entity relationship diagram dari spesifikasi kebutuhan menggunakan natural language processing untuk bahasa indonesia. Icon, 196-206.

[14] Mukhlis, I. R., Hermansyah, D., & Lantang, V. M. (2023). Rancangan Basis Data Transaksi Pada PT.Bank Perkreditan Rakyat ABC Menggunakan mysql Dengan Model Entity relationshipdiagram (ERD) dan Physical Data Model (PDM). JAIIT (Journal of Advances in Information and Industrial Technology), 1-10

[15] Choi, M., & Kim, J. (2022). A Study on the Potential Integration of AR-based Games in Learning Information System Documentation. Journal of Digital Art Engineering and Multimedia, 9(1), 13–23. https://doi.org/10.29056/jdaem.2022.03.02
[16] Santoso, J. M., & Iskandar, A. R. (2020). Rancang Bangun Aplikasi Jurnal Dan Absensi Pada Study Center Di Wilayah Cengkareng Barat Berbasis Android. Ejurnal "Mahasiswa" Informatika dan Telekomunikasi.
[17] Wahyuddin, & Wafiah, A. (2022). Aplikasi pemesanan menu pada warkop shearlock . Jurnal sintaks logika, 11-16.
[18] Gede, W., Bratha, E., Program, M., Manajemen, M., Bhayangkara, U., Raya, J., & Penulis, K. (2022). Literature Review Komponen Sistem Informasi Manajemen: Software, Database Dan Brainware. 3(3). https://doi.org/10.31933/jemsi.v3i3
[19] Febiharsa, D., Sudana, I. M., & Hudallah, N. (2019). Uji Fungsionalitas (Blackbox Testing) Sistem Informasi Lembaga Sertifikasi Profesi (SILSP) Batik Dengan Appperfect Web Test dan Uji Pengguna. Joined Journal Jurnal Of Information Edukation, 1(2), 117-126. https://doi.org/https://doi.org/10.31331/joined.v1i2.752
[20] Wulandari, Nofiyani & Humisar Hasugian. (2023). User Acceptance Testing (Uat) Pada Electronic Data Preprocessing Guna Mengetahui Kualitas Sistem. JMIK (Jurnal Mahasiswa Ilmu Komputer). 4(1) 20-27