IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI

SKRIPSI

DISUSUN OLEH

HANUM SABILA
NPM.2209010176

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

HANUM SABILA

2209010176

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

2026

LEMBAR PENGESAHAN

Judul Skripsi	:	Implementasi Algoritma Kriptografi AES-128 Pada Sistem Pengamanan Arsip Dokumen Digital Di Perusahaan Kontruksi
Nama Mahasiswa	:	Hanum Sabila
NPM	:	2209010176
Program Studi	:	Sistem Informasi

Menyetujui

Komisi Pembimbing

(Assoc. Prof. Dr. Al-Khowarizmi, M.Kom.)

NIDN. 0127099201

Ketua Program Studi

(Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom.)

NIDN. 0117088902

Dekan

(Assoc. Prof. Dr. Al-Khowarizmi, M.Kom.)

NIDN. 0127099201

PERNYATAAN ORISINALITAS

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, April 2024

Yang membuat pernyataan

Hanum Sabila

NPM. 2209010176

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Hanum Sabila
NPM	: 2209010176
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, April 2026

Yang membuat pernyataan

Hanum Sabila

2209010176

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Hanum Sabila
Tempat dan Tanggal Lahir	: MANUNGGAL, 29 Juli 2004
Alamat Rumah	: Jalan Veteran Pasar 8 Helvetia
Telepon/Faks/HP	: 08992900295
E-mail	: hanumsabila07@gmail.com

DATA PENDIDIKAN

SD	: YAYASAN PENDIDIKAN PANGERAN ANTASARI	TAMAT: 2016
SMP	: YAYASAN PENDIDIKAN PANGERAN ANTASARI	TAMAT: 2019
SMA	: SMAS DHARMAWANGSA MEDAN	TAMAT: 2022

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh

Alhamdulillahirabbil'alamin. Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya, sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik dan tepat waktu. Shalawat serta salam semoga senantiasa tercurah kepada Nabi Muhammad SAW, beserta keluarga, sahabat, dan seluruh umatnya hingga akhir zaman.

Tugas akhir ini berjudul "IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI" yang disusun sebagai salah satu syarat untuk menyelesaikan pendidikan Strata Satu (S1) pada Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara. Dalam proses penyusunan skripsi ini, penulis telah berupaya semaksimal mungkin untuk menyajikan hasil yang terbaik sesuai dengan kemampuan dan pengetahuan yang dimiliki. Namun demikian, penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat berbagai keterbatasan dan kekurangan, baik dari segi isi maupun penyajian.

Dalam proses penyusunan skripsi ini, penulis juga menyadari bahwa banyak pihak yang telah memberikan bantuan, bimbingan, serta dukungan. Dengan segala kerendahan hari, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Akrim, M.Pd., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU).
2. Bapak Assoc. Prof. Dr. Al-Khowarizmi, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi.
3. Ibu Dr. Firahmi Rizky, M.Kom selaku Wakil Dekan I Fakultas Ilmu Komputer dan Teknologi Informasi.
4. Bapak Mhd. Basri, S.Si, M.Kom selaku Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi.
5. Bapak Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom selaku Ketua Program Studi Sistem Informasi.
6. Bapak Mulkan Azhari, S.kom., M.Kom selaku Sekretaris Program Studi Sistem Informasi.
7. Bapak Assoc. Prof. Dr. Al-Khowarizmi, S.Kom., M.Kom. selaku dosen pembimbing tugas akhir yang telah berkontribusi membantu penulis dalam menyelesaikan tugas akhir. Serta memberikan ide, saran, kritik dan bimbingan kepada penulis dalam menyelesaikan tugas Akhir.
8. Kepada seluruh staf dan dosen Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara yang telah banyak memberikan ilmu, wawasan, motivasi dan pembelajaran berharga dari awal sampai akhir perkuliahan.
9. Kepada Ayah dan Ibu tercinta, yang selalu menjadi tempat penulis kembali dalam setiap keadaan. Terima kasih atas doa yang tidak pernah putus, dukungan yang selalu menguatkan, dan perhatian kepada penulis dalam setiap proses yang dilalui. Terima kasih atas segala usaha dan pengorbanan

yang telah diberikan demi masa depan penulis, serta kesungguhan dalam memenuhi dan mengupayakan setiap kebutuhan penulis dengan sebaik mungkin. Setiap pencapaian yang diraih hingga saat ini tidak terlepas dari peran Ayah dan Ibu yang selalu percaya dan mendukung penulis. Segala bentuk perhatian, pengorbanan, dan kasih sayang yang diberikan menjadi kekuatan bagi penulis untuk terus berusaha menyelesaikan pendidikan ini dengan sebaik mungkin. Ucapan terima kasih ini penulis sampaikan sebagai bentuk rasa hormat yang tulus atas segala yang telah diberikan. Semoga pencapaian ini dapat menjadi kebanggaan bagi Ayah dan Ibu, karena telah berhasil mengantarkan putri satu-satunya meraih gelar sarjana sebagaimana yang diharapkan. Penulis juga senantiasa mendoakan agar Ayah dan Ibu selalu diberikan kesehatan, kebahagiaan, serta umur yang panjang, sehingga penulis masih memiliki kesempatan untuk membalas semua kebaikan dan melihat senyum bangga Ayah dan ibu di setiap langkah keberhasilan penulis di masa yang akan datang.

10. Kepada Seseorang yang tidak kalah penting kehadirannya, Nursaid Fatahillah, penulis mengucapkan banyak terima kasih karena telah menjadi bagian dalam proses perjalanan penulis dalam menyusun skripsi ini, serta terima kasih telah setia menemani penulis sejak awak masa perkuliahan hingga saat ini. Terima kasih atas kebersamaan, dukungan perhatian, dan kesabaran yeng telah diberikan selama ini. Terima kasih karena selalu ada untuk mendengarkan setiap keluh kesah, memberikan semangat di saat penulis merasa lelah, serta menjadi teman berjuang dalam menghadapi berbagai tantangan selama perkuliahan hingga saat ini.

11. Kepada teman-teman penulis sejak masa sekolah dasar hingga sekolah menengah atas yang telah memberikan kebersamaan, dukungan, serta pengalaman yang berharga dalam perjalanan penulis. Terima kasih atas setiap momen, canda, dan kebersamaan yang telah dilalui bersama, serta dukungan yang masih terjaga hingga saat ini, sehingga menjadi bagian dari perjalanan penulis hingga dapat menyelesaikan skripsi ini.
12. Kepada sahabat terdekat penulis di lingkungan perkuliahan, Syifa dan Desvita, yang telah bersama-sama melalui berbagai proses selama masa perkuliahan. Penulis mengucapkan terima kasih atas kebersamaan, dukungan, dan semangat yang selalu diberikan. Berbagai pengalaman, tantangan, serta kebersamaan yang telah dilalui menjadi bagian penting dalam perjalanan penulis hingga dapat menyelesaikan skripsi ini dengan baik.
13. Dan yang tidak kalah penting, penulis juga ingin menyampaikan rasa terima kasih kepada diri sendiri. Terima Kasih karena telah mampu berjuang sejauh ini, tetap bertahan di tengah berbagai tekanan, rasa lelah dan keraguan yang sempat muncul selama proses penyusunan skripsi ini. Terima kasih karena tidak memilih untuk menyerah, meskipun dalam kondisi yang tidak selalu mudah.

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI

ABSTRAK

Dokumen digital banyak digunakan dalam berbagai aktivitas dan umumnya mengandung informasi penting yang harus dijaga kerahasiaannya. Namun, dokumen digital juga rentan terhadap ancaman seperti pencurian data, peretasan, dan kebocoran informasi. Pada PT. Asa Cipta Sarana, pengelolaan arsip dokumen masih memerlukan sistem yang mampu memberikan perlindungan data secara optimal. Oleh karena itu, penelitian ini bertujuan untuk merancang dan membangun sistem pengamanan arsip dokumen digital dengan menerapkan algoritma kriptografi Advanced Encryption Standard (AES) dengan panjang kunci 128-bit (AES-128).Metode yang digunakan dalam penelitian ini meliputi tahap analisis kebutuhan, perancangan sistem, implementasi, serta pengujian sistem. Sistem yang dibangun dilengkapi dengan fitur pengelolaan pengguna, pengarsipan dokumen, serta pengajuan dan verifikasi anggaran. Proses pengamanan dokumen dilakukan melalui enkripsi dan dekripsi menggunakan algoritma AES-128 untuk menjaga kerahasiaan dan keutuhan data.Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu berjalan dengan baik sesuai dengan fungsinya. Proses enkripsi dan dekripsi berhasil dilakukan dengan baik, dimana dokumen yang telah dienkripsi tidak dapat dibaca tanpa proses dekripsi, serta dapat dikembalikan ke bentuk semula tanpa mengalami perubahan. Berdasarkan hasil pengujian sistem, seluruh fitur dapat berfungsi sesuai dengan yang diharapkan. Dengan demikian, sistem ini mampu memberikan perlindungan terhadap dokumen digital dari akses yang tidak sah serta mendukung pengelolaan arsip dokumen secara lebih aman, terstruktur, dan efektif.

Kata Kunci : Dokumen Digital, Arsip dokumen, AES-128, Enkripsi, Dekripsi

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY ALGORITHM IN DIGITAL DOCUMENT ARCHIVE SECURITY SYSTEM IN CONSTRUCTION COMPANIES

ABSTRACT

Digital documents are widely used in various activities and generally contain important information that must be kept confidential. However, digital documents are also vulnerable to threats such as data theft, hacking, and information leaks. At PT. Asa Cipta Sarana, document archive management still requires a system capable of providing optimal data protection. Therefore, this study aims to design and build a digital document archive security system by implementing the Advanced Encryption Standard (AES) cryptographic algorithm with a 128-bit key length (AES-128). The methods used in this study include the stages of requirements analysis, system design, implementation, and system testing. The developed system is equipped with features for user management, document archiving, as well as budget submission and verification. Document security is ensured through encryption and decryption using the AES-128 algorithm to maintain data confidentiality and integrity. The research results show that the developed system functions properly as intended. The encryption and decryption processes were successfully executed, such that encrypted documents cannot be read without decryption and can be restored to their original form without alteration. Based on the system testing results, all features function as expected. Thus, this system is capable of providing protection for documents in

Keywords: Digital Documents, Document Archives, AES-128, Encryption, Decryption

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perusahaan konstruksi menghasilkan berbagai dokumen proyek yang berkaitan dengan proses perencanaan, pelaksanaan, hingga administrasi pekerjaan. Meningkatnya volume dokumen seiring banyaknya proyek yang dikerjakan menuntut adanya sistem pengarsipan yang terstruktur agar dokumen dapat disimpan secara rapi, mudah ditemukan kembali, serta mendukung kelancaran administrasi dan pengambilan keputusan perusahaan. Penggunaan dokumen digital membantu proses penyimpanan, pencarian, serta distribusi informasi menjadi lebih efisien. Namun, dokumen internal perusahaan umumnya memuat informasi penting yang bersifat sensitif dan strategis sehingga memerlukan perlindungan yang memadai agar tidak disalahgunakan.

Dokumen digital tersebut mengandung informasi internal perusahaan yang tidak boleh diakses atau dimodifikasi oleh pihak yang tidak berwenang. Oleh karena itu, aspek keamanan dokumen menjadi kebutuhan yang sangat penting. (Putra Pratama & Haryono, 2020) menyatakan bahwa keamanan data diperlukan karena banyak data bersifat rahasia dan tidak boleh diubah oleh pihak yang tidak memiliki hak akses. Hal ini menunjukkan bahwa pengelolaan dokumen digital harus memperhatikan aspek perlindungan data secara menyeluruh.

Seiring dengan meningkatnya ketergantungan terhadap dokumen digital, risiko kebocoran data juga semakin besar. (Akbar Ridho & Moh. Ali Romli, 2024) menyatakan bahwa dokumen digital yang memuat informasi sensitif dan rahasia rentan terhadap peretasan, pencurian data, dan kebocoran informasi yang dapat

menimbulkan kerugian finansial, reputasi, dan operasional perusahaan. Kondisi ini menjadi tantangan nyata bagi perusahaan kontruksi dalam menjaga keamanan arsip dokumen internalnya.

Salah satu teknik pengamanan data yang umum digunakan adalah kriptografi. Kriptografi merupakan teknik pengamanan informasi dengan cara mengubah data asli menjadi bentuk yang tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang. Data yang telah dienkripsi hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci tertentu. Dengan demikian, meskipun dokumen digital berhasil diakses oleh pihak yang tidak berhak, isi informasi di dalamnya tetap terlindungi.

Pada praktiknya, pengelolaan arsip dokumen digital di perusahaan kontruksi masih menghadapi berbagai keterbatasan. Di PT. Asa Cipta Sarana, dokumen internal perusahaan telah disimpan dalam bentuk digital, namun belum didukung oleh sistem pengarsipan dan pengamanan yang memadai. Dokumen masih disimpan sebagai file digital tanpa mekanisme perlindungan khusus, sehingga berpotensi diakses, disalin, atau dimodifikasi oleh pihak yang tidak berwenang. Kondisi ini menunjukkan adanya kesenjangan antara kebutuhan akan keamanan dokumen digital dengan sistem pengelolaan arsip yang masih bersifat sederhana.

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan kriptografi mampu meningkatkan keamanan dokumen digital. (Malik & Saifudin, 2023) menyatakan bahwa penerapan kriptografi pada sistem keamanan file terbukti dapat menjaga kerahasiaan data agar tidak dapat dilihat maupun dibaca oleh pihak yang tidak berkepentingan. Selain itu, algoritma kriptografi Advanced

Encryption Standard (AES) dikenal sebagai algoritma yang memiliki tingkat keamanan tinggi dan efesiensi yang baik. (Manullang *et al*., 2023) menjelaskan bahwa algoritma AES memiliki tingkat keamanan tinggi berdasarkan variasi panjang kunci yang dimiliki serta kompleksitas waktu dan ruang yang baik, sehingga sesuai untuk pengamanan data digital.

Berdasarkan pemaparan tersebut, dibutuhkan sebuah sistem pengelolaan arsip dokumen digital yang tidak hanya berfungsi sebagai media penyimpanan dan pengelolaan dokumen proyek secara teratur, tetapi juga memiliki perlindungan keamanan melalui penerapan kriptografi. Dengan demikian, penelitian ini diarahkan pada implementasi algoritma kriptografi AES-128 dalam sistem pengamanan arsip dokumen digital di PT. Asa Cipta Sarana. Penerapan ini diharapkan mampu meningkatkan perlindungan terhadap dokumen internal perusahaan serta mendukung proses pengelolaan informasi yang lebih aman dan sistematis.

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini yaitu sebagai berikut:

1. Bagaimana merancang sistem pengamanan arsip dokumen digital di PT.Asa Cipta Sarana?
2. Bagaimana penerapan algoritma AES-128 dalam sistem pengamanan arsip dokumen digital di PT.Asa Cipta Sarana?
3. Bagaimana menguji sistem pengamanan dokumen untuk memastikan fungsi enkripsi dan dekripsi dan hak akses berjalan dengan baik?

1.3 Batasan Masalah

Agar penelitian lebih terfokus, maka batasan masalah dalam penelitian ini ialah sebagai berikut:

1. Implementasi dan pengujian dokumen digital dilakukan pada satu proyek sebagai representasi.
2. Pengamanan dokumen hanya menggunakan algoritma kriptografi AES-128.
3. Sistem hanya mendukung pengamanan dokumen dalam format PDF.
4. Sistem yang dibangun hanya untuk penggunaan internal perusahaan dan tidak bersifat publik.
5. Sistem hanya melibatkan admin, keuangan dan user dengan hak akses berbeda.

1.4 Tujuan Penelitian

Terdapat beberapa tujuan yang ingin dicapai dalam proses penelitian ini yaitu:

1. Merancang dan membangun sistem pengamanan arsip dokumen digital di lingkungan internal perusahaan PT.Asa Cipta Sarana.
2. Menerapkan algoritma AES-128 pada sistem pengamanan arsip dokumen digital untuk melindungi dokumen dari akses tidak sah di PT.Asa Cipta Sarana.
3. Melakukan pengujian sistem pengamanan arsip dokumen digital untuk memastikan proses enkripsi, dekripsi, dan hak akses pengguna berjalan dengan baik

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Bagi Instansi

   Penelitian ini diharapkan dapat membantu instansi dalam menyediakan sistem pengamanan arsip dokumen digital berbasis web melalui penerapan algoritma AES-128 untuk menjaga kerahasiaan dan keutuhan dokumen proyek.

2. Bagi Keilmuan

   Menambah referensi akademik dan bahan kajian bagi pengembangan ilmu pengetahuan di bidang ilmu komputer & teknologi informasi, khususnya terkait penerapan algoritma kriptografi dalam pengamanan arsip dokumen digital, serta dapat dijadikan dasar untuk penelitian selanjutnya.

3. Bagi Penulis

   Penelitian ini memberikan tambahan wawasan dan pengalaman bagi penulis dalam menerapkan konsep kriptografi pada sistem informasi, khususnya dalam pengamanan arsip dokumen digital, serta meningkatkan kemampuan analisis dan pemecahan masalah di bidang keamanan data.

4. Bagi Masyarakat

   Meningkatkan pemahaman kepada masyarakat mengenai pentingnya pengelolaan dan perlindungan dokumen proyek, terutama dokumen yang bersifat sensitif, agar terhindar dari penyalahgunaan informasi yang dapat merugikan berbagai pihak.

BAB II

LANDASAN TEORI

2.1 Dokumen Digital

2.1.1 Definisi Dokumen Digital

Dokumen digital adalah sebuah konsep pengumpulan, penyimpanan, dan pengelolaan informasi dalam bentuk cetakan atau gambar yang dapat dipakai sebagai bukti atau keterangan. (Kusuma Nugraha *et al*., 2023) Dokumen digital tidak sekedar menggantikan dokumen fisik dengan format elektronik, tetapi berperan sebagai bagian dari sistem informasi yang mempermudah proses penyimpanan, pengaturan, dan distriusi informasi secara lebih efektif. Dengan penggunaan dokumen digital, informasi dapat diakses secara fleksibel dari berbagai perangkat, sehingga mendukung aktivitas administratif, operasional, dan pengambilan keputusan di perusahaan.

Dokumen digital juga memungkinkan organisasi untuk menyusun dan menyimpan informasi secara sistematis, sehingga mempermudahkan pencarian dan pengarsipan dokumen penting, termasuk surat, laporan, proposal dan data proyek. keunggulan lainnya adalah pengurangan risiko kehilangan data, efisiensi penggunaan ruang penyimpanan, serta kemampuan integrasi dengan sistem pengelolaan dokumen elektronik atau arsip digital. Jadi, dokumen digital tidak hanya menjadi elemen penting dalam modernisasi administrasi dan pengelolaan informasi di perusahaan.

2.1.2 Jenis Dokumen Digital

Jenis dokumen digital merupakan bentuk file elektronik yang digunakan untuk menyimpan informasi secara terstuktur sesuai kebutuhan pengolahan data. Beberapa jenis yang umum digunakan di perusahaan antara lain sebagai berikut:

1. Portable Document Format (PDF)

PDF (Portable Document Format) merupakan ssalah satu format dokumen digital yang digunakan untuk menyimpan dan mendistribusikan dokumen dalam bentuk final. Format ini dicrancang agar tampilan tetap konsisten, baik dari segi teks, gambar, maupun tata letak, ketika dibuka pada perangkat dan sistem operasi yang berbeda. Krakteristik tersebut menjadikan PDF banyak digunakan untuk dokumen resmi di perusahaan seperti kontrak, laporan proyek, dan dokumen administrasi, karena mampu menjaga keutuhan stuktur dokumen sehingga tampil profesional dan terorganisasi dengan baik, serta meminimalkan risiko perubahan isi atau tampilan saat dokumen dibuka oleh penerima.

2. Word Dokumen

Dokumen Word merupakan salah satu format digital yang digunakan dalam aplikasi pengolah kata Microsoft Word, yang merupakan bagian dari perangkat lunak Microsoft Office. Format ini berfungsi sebagai media utama dalam penyusunan dokumen berbasis teks dan mendukung berbagai fitur pengolahan dokumen, seperti pengaturan jenis dan ukuran huruf, warna teks, paragraf, serta tata letak halaman. Selain itu dokumen Word memungkinkan penyisipan elemen pendukung seperti tabel, gambar dan grafik, sehingga bersifat fleksibel dan mudah disesuaikan. Oleh karena itu, format Word banyak digunakan untuk pembuatan

laporan, surat resmi, makalah, dan dokumen administrasi yang masih memerlukan proses pengeditan dan revisi.

3. Microsoft Excel

Microsoft Excel merupakan salah satu format dokumen digital yang digunakan melalui aplikasi pengolah data berbasis angka dalam paket perangkat lunak Microsoft Office. Format ini dimanfaatkan untuk mengatur dan mengolah data numerik secara sistematis dalam bentuk tabel. Excel menyediakan berbagai fasilitas pengolahan data, seperti perhitungan otomatis dengan rumus dan fungsi tertentu serta penyajian data dalam bentuk grafik. Dengan kemampuan tersebut, dokumen Excel sering digunakan untuk mengelola data keuangan, menyusun anggaran, membuat laporan statistik, dan melakukan rekapitulasi data yang menuntut tingkat ketelitian dan ketepatan yang tinggi.

2.2 Arsip

Arsip merupakan informasi yang terekam dalam berbagai bentuk media, baik fisik maupun digital, yang dibuat atau diterima serta dikelola oleh individu maupun organisasi untuk mendukung aktivitas operasional. Arsip berfungsi sebagai sumber informasi, bukti kegiatan, serta sarana pengelolaan data yang dapat digunakan kembali ketika diperlukan. (Ardiyansa *et al*., 2025) arsip merupakan dokumen yang berisi informasi, seperti surat atau proposal, yang berperan dalam mendukung berbagai aktivitas dalam suatu instansi. Pengelolaan arsip bertujuan untuk mempermudah administrasi, menjaga keaslian dan ketersediaan informasi, serta membantu proses pengambilan keputusan. Sesuai Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan, arsip merupakan rekaman kegiatan atau peristiwa dalam berbagai bentuk dan

media yang dihasilkan oleh lembaga, organisasi, maupun perorangan dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Dengan demikian, arsip tidak hanya berbentuk dokumen tertulis, tetapi juga mencakup data elektronik dan file digital yang menjadi bukti autentik aktivitas serta sarana pengelolaan informasi.

Seiring perkembangan teknologi, pengelolaan arsip mengalami perubahan menuju bentuk digital yang memungkinkan proses penyimpanan dan temu kembali informasi dilakukan secara lebih cepat dan efisien. Hal ini didukung oleh pendapat (Sahal & Winardi, 2021) bahwa arsip digital ini berfungsi sebagai media penyimpanan dan dapat ditampilkan kembali bila sewaktu-waktu diperlukan, sehingga memudahkan pengambilan keputusan manajemen, menunjang efisiensi penggunaan sumber daya, serta menjadi rujukan historis kinerja organisasi. Oleh karena itu, khususnya pada perusahaan kontraktor yang menghasilkan banyak dokumen kegiatan, arsip menjadi catatan strategis yang perlu dikelola secara sistematis dan terstruktur guna menjaga integritas informasi serta mendukung keberlanjutan operasional dan pengambilan keputusan.

2.3 Keamanan Informasi

Keamanan informasi adalah upaya untuk melindungi semua jenis sumber daya informasi dari ancaman atau penyalahgunaan pihak yang tidak berwenang (Maulida *et al*., 2023). Informasi merupakan aset penting bagi organisasi karena berisi data yang sensitif dan bernilai, sehingga perlu dijaga agar operasional berjalan lancar, risiko kerugian dapat diminimalkan, dan penyalahgunnaan data dapat dicegah, Menurut (Al-Khowarizmi, 2021) keamanan informasi merupakan

subsistem dalam organisasi yang bertanggung jawab untuk mengendalikan risiko yang terkait dengan sistem informasi berbasis komputer.

Aspek dasar dalam keamanan informasi terdapat 3 aspek yaitu : (Al-Khowarizmi, 2021)

1. *Confidentiality*

   Keamanan informasi menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu. *Confidentiality* merupakan tindakan pencegahan dari orang atau pihak yang tidak berhak mengakses informasi.

2. *Integrity*

   Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari *Integrity* adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak

3. *Availability*

   Keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses informasi. *Availability* meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi

2.4 Sistem Pengamanan Dokumen

Pengamanan dokumen merupakan kebutuhan penting bagi berbagai instansi untuk menjamin proses penyimpanan yang kredibel sehingga dokumen dapat digunakan kembali ketika diperlukan (Qadriah *et al*., 2023). Dokumen yang dikelola dalam pelaksanaan proyek umumnya memuat informasi sensitif yang hanya boleh diakses oleh pihak yang berwenang. Tanpa dukungan sistem pengamanan yang memadai, dokumen berisiko mengalami akses ilegal, penggandaan tanpa izin, memanipulasi data, serta penyebaran informasi yang tidak terkontrol, yang pada akhirnya dapat menimbulkan kerugian bagi instansi terkait. Kondisi ini menunjukkan bahwa pengelolaan dokumen proyek memerlukan sistem pengamanan yang terstuktur dan tidak hanya bergantung dengan prosedur manual saja.

Pernyataan ini diperkuat oleh (Nisfu Melati Sukma *et al*., 2023) yang menyatakan bahwa keamanan sistem informasi menjadi sangat penting karena dalam era digital saat ini, manusia semakin mengandalkan teknologi innformasi dan menyimpan data sensitif secara digital. Oleh karena itu, diperlukan sistem pengamanan dokumen yang mampu melindung isi dokumen secara menyeluruh, salah satunya melalui penerapan teknik kriptografi untuk menjaga kerahasiaan informasi agar hanya dapat diakses oleh pihak yang memiliki kewenangan.

2.5 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu ”*cryptos*” yang berarti rahasia dan ”*graphein*” yang berarti tulisan. Berdasarkan makna tersebut, kriptografi dapat dipahami sebagai bidang ilmu yang membahas cara melindungi informasi agar tidak dapat diketahui oleh pihak yang tidak berhak. Perlindungan

ini dilakukan dengan mengubah data dari bentuk yang masih dapat dibaca menjadi bentuk lain yang sulit atau tidak dapat dipahami. Seiring berkembangnya teknologi informasi, kriptografi tidak lagi hanya digunakan untuk menyembunyikan pesan, tetapi juga berperan dalam menjaga keutuhan data, memastikan keaslian identitas pengirim, serta memberikan jaminan agar informasi yang dikirim tidak dapat disangkal dalam komunikasi digital.

Kriptografi digunakan untuk melindungi informasi agar data tidak dapat diakses oleh pihak yang tidak sah. Dalam penerapannya, kriptografi memiliki beberapa tujuan utama dalam menjaga keamanan informasi, yang dijelaskan sebagai berikut:

1. Kerahasiaan (*Confidentialy*) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan. Dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi pesan yang tidak terbaca oleh pihak yang berhak.
2. Integritas data (*Data Integrity*) adalah layanan yang menjamin bahwa pesan masih asli atau belum dimanipulasi selama dalam penyimpanan dan pengiriman.
3. Autentikasi (*Authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasikan kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi dari sumber pesan.
4. Nirpenyangkalan (*Non-repudiation*) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman dan penerima pesan menyangkal telah menerima pesan.

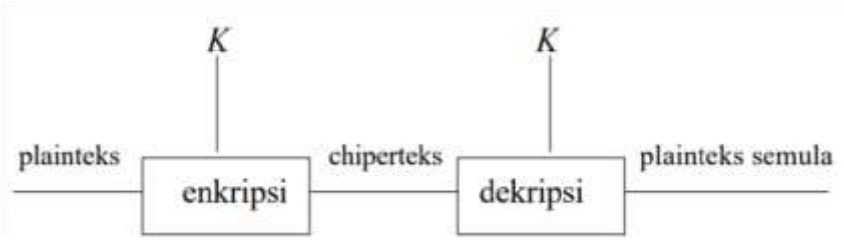
2.5.1 Jenis Kriptografi

Secara umum, terdapat dua jenis teknik kriptografi yang ada, yaitu:

1. Kriptografi Simetris

Kriptografi simetris atau disebut juga dengan algoritma konvensional adalah algoritma yang menggunakan satu kunci yang sama pada proses enkripsi dan dekripsi. Dengan kata lain, kunci yang dipakai untuk mengubah data asli (*plaintext*) menjadi data terenkripsi (*chipertext*) juga digunakan untuk mengembalikan data tersebut kebentuk semula. Karena hanya menggunakan satu kunci, tingkat keamanannya sangat bergantung pada kerahasiaan kunci agar data hanya diakses oleh pihak yang berwenang.

Beberapa algoritma kriptografi simetris yang umum digunakan antara lain Data Encyption Standard (DES), Advanced Encryption Standard (AES), Triple DES (3DES), International Data Encryption Algoritma (IDEA), dan Blowfish. Algoritma ini bekerja dengan cara mengolah data menggunakan satu kunci tertentu, sehingga hanya pihak yang memiliki kunci tersebut yang dapat membuka kembali informasi yang sudah dienkripsi. Kecepatan menjadi salah satu keunggulan utama kriptografi simetris karena proses enkripsi dan dekripsi dilakukan dengan kunci yang sama, sehingga lebih efesien dibandingkan asimetris. Namun, penggunaan satu kunci juga menimbulkan masalah keamanan terutama saat kunci harus dibagikan. Jika kunci jatuh ketahan pihak yang tidak berwenang, pesan dapat dengan mudah diakses.

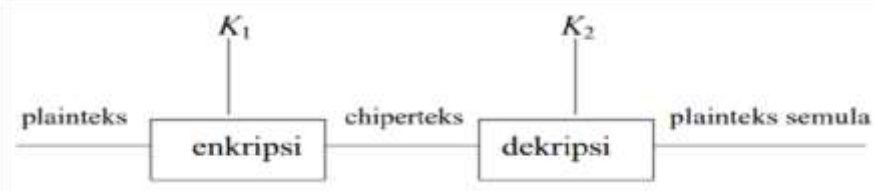


Gambar 2. 1 Enkripsi dan Dekripsi Simetris

2. Kriptografi Asimetris

Kriptografi asimetris merupakan algoritma yang menggunakan dua kunci berbeda, yaitu kunci enkripsi dan kunci dekripsi. Pada metode ini kunci yang digunakan untuk mengunci pesan tidak dapat dipakai untuk membukanya kembali, sehingga proses pembacaan hanya dapat dilakukan dengan kunci dekripsi yang sesuai. Kunci enkripsi dapat dibagikan secara terbuka, sedangkan kunci dekripsi harus dijaga kerahasiaannya oleh pemiliknya, sehingga sistem ini dikenal sebagai kriptografi kunci publik dan memungkinkan komunikasi yang aman tanpa perlu pertukaran kunci rahasia secara langsung.

Algoritma yang menerapkan prinsip kriptografi asimetris antara lain RSA, Diffie-Hellman, Elliptic Curve Cryptography (ECC), dan Digital Signature Algorithm (DSA). Keunggulan utama metode ini terletak pada distribusi kunci, keamanan algoritma asimetris lebih terjamin karena proses enkripsi dan dekripsi tidak menggunakan kunci yang sama. Namun, estimasi waktu algoritma asimetris jauh lebih lama dibandingkan algoritma simetris. Metode ini mempermudah pertukaran informasi pengiriman data atau dokumen rahasia melalui internet, serta proses autentikasi digital seperti tanda tangan elektronik yang memerlukan tingkat keamanan dan kepercayaan yang tinggi.



Gambar 2. 2 Enkripsi dan Dekripsi Asimetris

2.5.2 Algoritma Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah kriptografi modern dengan algoritma kriptografi simetris pengganti Data Encryption Standard (DES) yang dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001. DES dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan dalam beberapa hari (Ferdi Riza *et al*., 2025). Algoritma ini dikembangkan oleh Joan Daeman dan Vincent Rijment yang memenangkan sayembara pengganti algoritma DES. Algoritma ini terpiilih karena mampu bertahan terhadap serangan analisis dan serangan brute force, memiliki biaya komputasi dan memori yang efesien, serta menawarkan stuktur yang terbuka, fleksibel, dan sederhana sehingga mudah diimplementasikan pada berbagai platform dan kebutuhan keamanan data modern.

NIST menetapkan sejumlah persyaratan untuk calon algoritma pengganti DES, yaitu harus termasuk kategori simetris yang berorientasi pada sandi blok, memiliki desain terbuka, memiliki panjang kunci fleksibel 128, 192, dan 256, ukuran blok yang dienkripsi 128 bit, serta dapat diimplementasikan dalam perangkat lunak dan perangkat keras. Dari 15 proposal yang diajukan, NIST kemudian mengevaluasi memalui konferensi terbuka dan memilih lima algoritma yang dinilai paling kuat dan efesien yaitu *Rijndael* (Vincent Rijmen dan Joan daemen), *Serpent* (Ross Anderson, Eli Biham, dan Lars Knudsen), Twofish (Bruce

Schneier), MARS (IBM) dan RC6. Setelah melalui proses penilaian lanjutan, pada Oktober 2000 Rijndael ditetapkan sebagai kandidat utama dan disahkan sebagai Advanced Encryption Standard (AES) pada November 2001.

Algoritma kriptografi Advanced Encryption Standard (AES) bekerja dengan blok berukuran 128 bit dengan menggunakan kunci yang berbeda beda, yaitu 128 bit, 192 bit, dan 256 bit. Proses enkripsi dilakukan secara berulang dalam tiap putaran, yang dikenal sebagai ronde. Jumlah ronde yang dijalankan tergantung pada panjang kunci yang digunakan. Berikut ini dijelaskan hubbungan antara panjang kunci dan jumlah ronde.

Tabel 2. 1 Panjang Kunci dan Jumlah Ronde

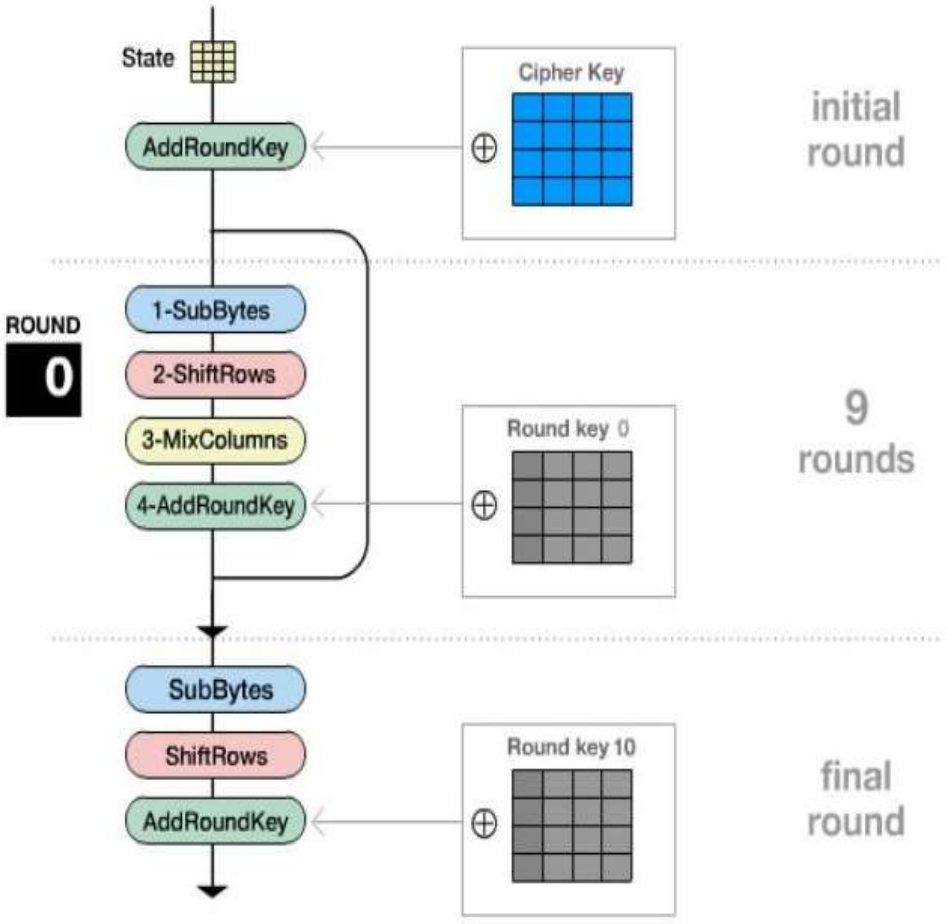
	Panjang Kunci (Nk words)	Ukuran Blok (Nb words)	Jumlah Putaran (Nr)
AES- 128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Algoritma AES mempunyai 3 parameter utama: (Ferdi Riza *et al*., 2025)

1. *Plaintext* : array yang berukuran 16-*byte*, yang berisi data masukan
2. *Ciphertext* : array yang berukuran 16-*byte*, yang berisi hasil enkripsi
3. Key: array yang berukuran 16-*byte*, yang berisi kunci *ciphering* (*cipherkey*).

Berdasarkan tiga parameter utama tersebut, proses enkripsi dilakukan melalui serangkaian langkah sistematis yang menstransformasi data masukan menjadi *chipertext*. Proses ini melibatkan beberapa tahapan yang dirancang untuk memastikan keamanan data secara maksimal

1. *AddRoundKey* merupakan langkah pembuka yang menggabungkan keadaan awal data (*plaintext*) dengan kunci chiper melalui operasi XOR. Tahap ini disebut juga sebagai initial round.
2. Ronde utama (putaran 1-9) proses yang dilakukan pada setiap putaran adalah:
    a. *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (S-Box).
    b. *ShiftRows*: proses pergeseran baris-baris state array secara melingkar (wrapping).
    c. *Mixcolumns*: mengacak data dengan melakukan pengalian dari hasil *ShiftRows* dengan bilangan polinomial yang sudah ditetapkan.
    d. *AddRoundKey*: melakukan XOR antara hasil *MixColumns* dengan round key.
3. Final round: proses pada putaran terakhir
    a. SubBytes
    b. ShiftRows
    c. AddRoundKey



Gambar 2. 3 Proses Enkripsi AES

2.5.3 Transformasi-transformasi AES

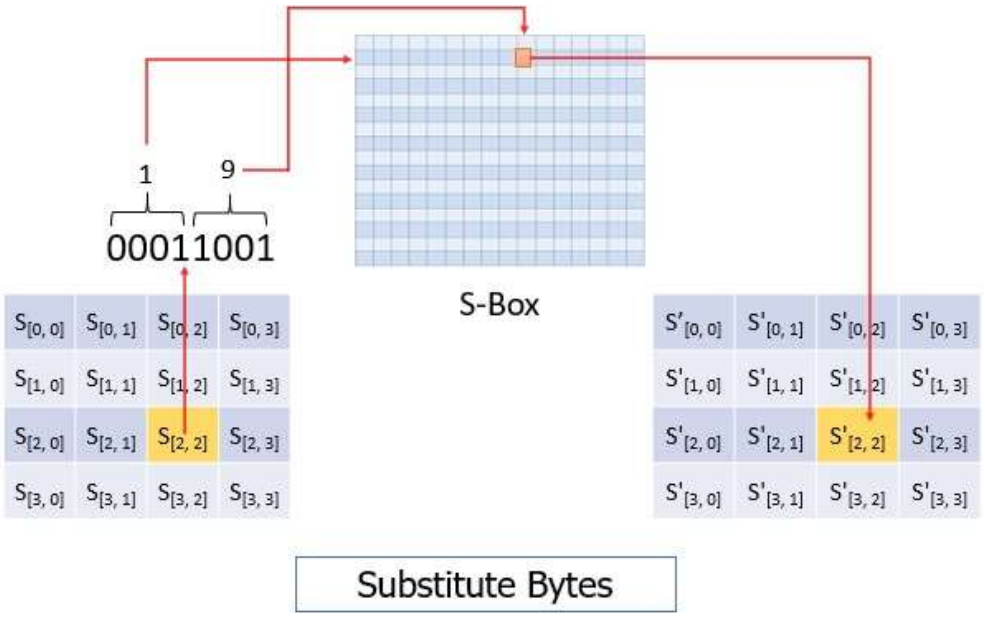
a. *Subbytes*

Subbytes adalah proses menggantikan setiap *byte* dalam state dengan *byte* baru menggunakan tabel substitusi yang disebut S-Box. Setiap *byte* dicocokkan dengan posisi tertentu di dalam S-Box, lalu diganti sesuai nilai yang terdapat pada tabel tersebut untuk menghasilkan perubahan yang lebih acak.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Gambar 2. 4 Tabel S-Box

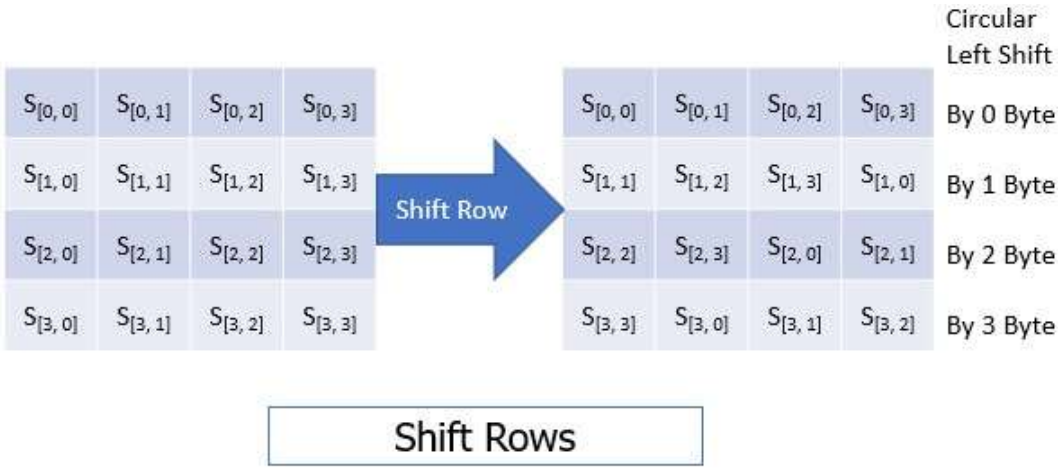
Untuk setiap *byte* dalam rangkaian keadaan (*state*), misalnya S[r, c] = xy, yang dalam hal ini merupakan representasi heksadesimal dari nilai S[r, c], nilai baru tersebut, yaitu S'[r, c], ditentukan dari S-Box yang merupakan titik perpotongan baris x dengan kolom y.



Gambar 2. 5 Proses Sub*Byte*s

b. *ShiftRows*

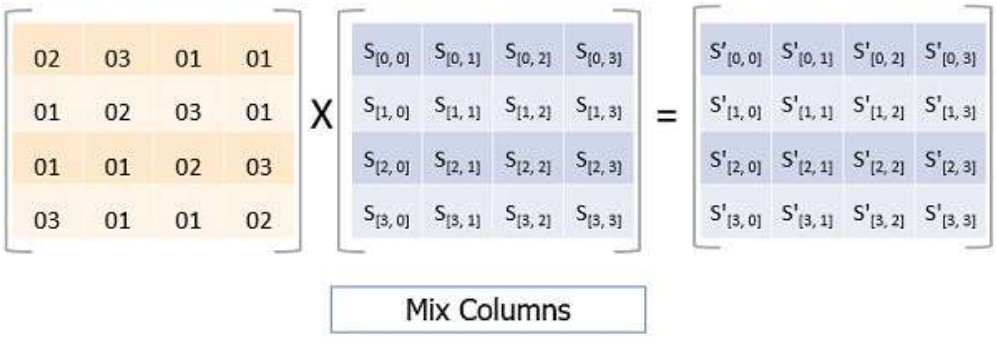
ShiftRows adalah transformasi yang mengubah posisi *byte* tanpa mengganti nilainya. Jumlah pergeserannya diatur berdasarkan indeks baris (r), dimana baris r = 0 tidak mengalami pergeseran, baris r = 1 digeser ke kiri sebanyak 1 *byte*, baris r = 2 digeser ke kiri sebanyak 2 *byte*, baris r = 3 digeser kekiri sebanyak 3 *byte*.



Gambar 2. 6 Proses ShiftRows

c. *MixColumns*

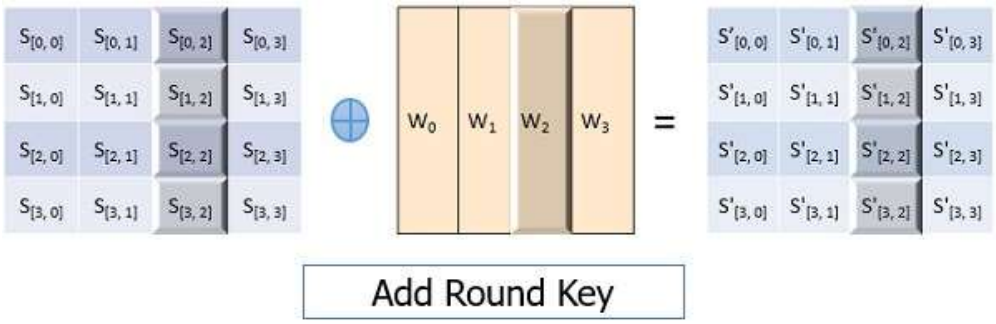
MixColumns adalah proses pencampuran nilai pada setiap kolom dalam state dengan cara mengkalikan kolom tersebut menggunakan matriks khusus yang sudah ditetapkan. Transformasi *MixColumns* bertujuan untuk mengubah dan menyebarkan data pada tiap kolom dalam state, sehingga susunannya menjadi lebih acak dan sulit ditebak. Dalam proses ini, satu baris pada matriks konstan akan dikalikan dengan satu kolom dari matriks state, lalu hasil perkalian tersebut dijumlahkan untuk membentuk nilai baru pada kolom tersebut.



Gambar 2. 7 Proses MixColumns

d. Add Round Key

AddRoundKey adalah transformasi yang menggabungkan setiap *byte* pada matriks state dengan *byte* kunci putaran (*round key*) menggunakan operasi XOR. Pada proses ini, matriks kunci disejajarkan dengan matriks state pada sehingga setiap elemen memiliki pasangan pada posisi yang sama, lalu diproses XOR untuk menghasilkan nilai baru.



Gambar 2. 8 Proses AddRoundKey

2.6 Tools Pengembangan Sistem

Perangkat lunak dan alat yang digunakan untuk merancang, membangun, serta menguji sistem pengamanan arsip dokumen digital dipilih berdasarkan kemampuan untuk mendukung penyimpanan, pengelolaan, dan pengamanan dokumen secara terstruktur. Tools pengembangan sistem mencakup bahasa markup dan pemrograman untuk membangun antarmuka pengguna dan

interaktivitas sistem, server lokal dan basis data untuk menyimpan serta mengelola dokumen, serta editor kode untuk menulis dan mengelola program. Penggunaan tools yang tepat memungkinkan pengembang membangun sistem yang tidak hanya menampilkan dan mengelola arsip dokumen digital, tetapi juga menjamin keamanan data melalui integrasi dengan mekanisme enkripsi dan kontrol akses, sehingga proses pengujian, debugging, dan implementasi dapat dilakukan secara efektif dan aman.

2.6.1 PHP

Php merupakan bahasa pemogramann yang banyak dipakai dalam pembuatan aplikasi web karena mampu mengolah permintaan pengguna dan menghasilkan tampilan yang dinamis. (Dr. Budi Raharjo, 2025) menyatakan bahwa php adalah salah satu bahasa pemograman sever-side yang sangat populer dan banyak digunakan dalam dunia pengembangan web karena kemudahan, fleksibilitas, serta kemampuannya untuk membuat konten web dinamis dan interafktf. Maksud dari *sever-side* ini proses logika program dijalankan di sisi server. PHP akan memproses permintaan, mengakses database jika diperlukan, lalu menghasilkan keluaran dalam bentuk HTML sehingga informasi pada halaman dapaat berubah tanpa mengubah struktur tampilan.

Keunggulan PHP tidak hanya terletak pada proses kerjanya, tetapi juga pada sifatnya yang terbuka dan dapat dikembangkan sesuai kebutuhan. (Santoso *et al*., 2022) menyatakan bahwa PHP adalah bahasa pemograman yang bersifat open source, artinya pengguna diberikan kebebasan untuk mengembangkan dan memodifikasi sesuai dengan keinginanya. Dalam penerapannya, HTML berperan sebagai kerangka dasar tampilan, sedangkan PHP mengolah data di server dan

mengirimkan hasilnya untuk mengisi atau memperbaharui bagian tertentu pada halaman. Integrasi antara HTML dan PHP ini menghasilkan struktur aplikasi web yang fleksibel, mudah dikembangkan dan responsif terhadap kebutuhan pengguna. Dalam konteks pengembangan sistem pengamanan dokumen, PHP efektif digunakan untuk menngelola enkripsi, dekripsi dan kontrol akses data secara aman.

2.6.2 MySQL

MySQL adalah sebuah sistem manajemen basis data relasional (RDBMS) yang memanfaatkan SQL (*Structured Query Language*) sebagai bahasa utama untuk mengatur dan mengelola data. Database ini sering dipadukan dengan PHP dalam pembuatan aplikasi web dinamis karena kemampuannya dalam menyimpan, mengorganisir, serta mengakses data secara cepat dan efisien. Sebagai salah satu RDBMS yang populer, MySQL digunakan oleh banyak aplikasi web sebagai solusi penyimpanan data berskala besar dengan akses yang responsif. MySQL merupakan database yang sering digunakan oleh para Programmer Web karena database ini dinilai lebih stabil dan sangat kuat untuk media penyimpanan data dibandingkan database lainnya (Penulis *et al*., 2023). Dalam sistem pengamanan dokumen, MySQL digunakan untuk menyimpan data dokumen yang sudah terenkripsi, data pengguna, catatan aktivitas, sehingga semua informasi dapat dikelola secara aman, terstruktur, dan terintegrasi.

2.6.3 Visual Studio Code

Visual Studio Code (VS Code) adalah editor kode ringan yang digunakan untuk menulis dan mengelola program dalam pengembangan sistem. Aplikasi ini dikembangkan oleh Microsoft dan dapat dijalankan pada berbagai sistem operasi

seperti Windows, Linux, dan MacOS. Visual studio code mendukung berbagai bahasa markup dan pemrograman, seperti HTML, CSS, JavaScript, dan PHP, serta dilengkapi fitur seperti penulisan kode rapi, saran otomatis, dan pengecekan kesalahan, sehingga memudahkan pengembang dalam membuat aplikasi berbasis web maupun sistem lainnya.

2.6.4 HTML

HTML (*HyperText Markup Language*) merupakan bahasa markup yang digunakan untuk membangun struktur halaman web dalam pengembangan sistem ini. HTML berfungsi sebagai kerangka dasar untuk menampilkan konten seperti teks, gambar, tautan, tabel, dan elemen interaktif lainnya di antarmuka pengguna. Dalam sistem ini, HTML digunakan untuk menyusun tampilan dashboard, halaman pengelolaan dokumen, dan formulir input data, sehingga informasi dapat ditampilkan secara terstruktur dan mudah diakses oleh pengguna. Elemen-elemen HTML dilengkapi dengan atribut yang mendukung fungsionalitas tambahan, seperti penunjuk sumber gambar atau identifikasi form, yang mempermudah integrasi dengan CSS untuk tampilan dan JavaScript untuk interaktivitas. Dengan demikian, HTML menjadi komponen utama dalam memastikan sistem dapat menampilkan data secara jelas dan terorganisir sesuai kebutuhan pengguna.

2.6.5 Xampp

XAMPP adalah perangkat lunak bebas yang mendukung berbagai sistem operasi dan merupakan paket yang menggabungkan beberapa program penting untuk membangun server lokal (localhost). XAMPP terdiri dari Apache sebagai web server, MySQL/MariaDB sebagai basis data, serta PHP dan Perl sebagai

bahasa pemrograman sisi server. Fungsinya adalah memungkinkan pengembangan dan pengujian aplikasi berbasis web secara offline. Dalam pengembangan sistem ini, XAMPP digunakan untuk menjalankan aplikasi secara lokal, sehingga pengembang dapat menguji fungsionalitas sistem, termasuk pengelolaan data, dashboard, dan interaksi dengan basis data, sebelum diterapkan pada server online. Dengan seluruh komponen yang terintegrasi, XAMPP mempermudah instalasi, konfigurasi, dan proses debugging sistem

2.7 UML

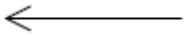
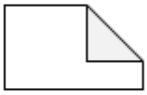
UML (*Unified Modeling Language*) adalah sebuah Bahasa yang berdasarkan grafik/gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian dari sebuah sistem pengembangan software berbasis OO (*Object Oriented*).(Dedi Saputra *et al*., 2023) Melalui beragam diagram yang disusun secara terpadu, UML memberikan kerangka yang jelas untuk menggambarkan struktur sistem, perilaku komponen, alur kegiatan, serta pola interaksi antarelemen yang terlibat. Pemodelan ini berperan sebagai rancangan awal atau blueprint yang membantu pengembang, analis sistem, maupun pihak berkepentingan lainnya memahami keterkaitan bagian-bagian sistem dan cara kerjanya secara menyeluruh. Di samping memfasilitasi visualisasi proses bisnis, UML juga dimanfaatkan untuk menyusun rancangan kelas, struktur basis data, komponen perangkat lunak, dan urutan aktivitas yang terjadi dalam sistem. Dengan cakupan tersebut, UML menjadi sarana penting dalam kegiatan analisis dan perancangan karena mampu menghadirkan model yang terstandar, terstruktur, serta mudah ditinjau kembali sepanjang siklus pengembangan

perangkat lunak. Diagram dasar dalam *Unified Modelling Language* (UML) antara lain:

1. Use case Diagram

   Use case digunakan untuk menggambarkan hubungan antara sistem dengan pihak eksternal maupun pengguna, melalui skenario yang disusun sesuai langkah-langkah operasional yang telah ditetapkan. Use case diagram menjadi metode yang tepat untuk menampilkan pola interaksi tersebut karena mampu memperlihatkan secara jelas aktor yang terlibat, fungsi yang tersedia, serta keterkaitan di antara keduanya. Diagram ini menyajikan kumpulan use case beserta aktor yang berinteraksi dengannya, sehingga kebutuhan atau requirements yang diharapkan oleh pengguna dapat dijelaskan secara lebih terstruktur. Selain memperjelas apa saja layanan yang harus disediakan oleh sistem, visualisasi ini juga membantu dalam memahami ruang lingkup sistem secara keseluruhan serta mendukung penentuan organisasi dan model rancangan yang sesuai dalam proses pengembangan perangkat lunak.

Tabel 2. 2 Simbol Use Case Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Actor	Mengspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi ddengan use case.
2		Dependency	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri(indenpendent) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (indenpendent).
3		Generalization	Hubungan dimana objek anak (descendent) berbagai perilaku dan struktur data dari objek yang ada di atasnya objek induk (ancestor).
4		Include	Mengspesifikasikan bahwa use case sumber secara eksplisit.
5		Extend	Mengspesifikasikan bahwa use case target memperluas perilaku dari use case sumber pada suatu titik yang diberikan.
6		Association	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		System	Mengspesifikasikan paket yang menampilkan sistem secara terbatas.
8		Use Case	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor.
9		Collaboration	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemennya (sinergi).
10		Note	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi.

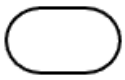
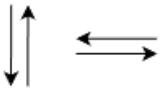
2. Activity diagram

Activity diagram adalah diagram dalam UML yang menggambarkan alur aktivitas atau proses kerja dalam suatu sistem, mulai dari langkah awal hingga akhir. Diagram ini menunjukkan urutan tindakan, keputusan, percabangan, serta aktivitas yang dapat berlangsung secara paralel. Melalui activity diagram, alur proses dapat dipahami dengan jelas sehingga membantu pengembang dan analis dalam memetakan proses

bisnis dan memastikan setiap tahapan operasional telah terdefinisi sebelum sistem dirancang atau diimplementasikan.

Tabel simbol activity diagram

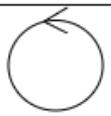
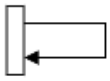
Tabel 2. 3 Simbol Activity Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Activity	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain.
2		Action	State dari sistem yang mencerminkan eksekusi dari suati aksi.
3		Initial Node	Bagaimana objek dibentuk atau diawali.
4		Activity Final Node	Bagaimana objek dibentuk atau diakhiri.
5		Decision	Digunakan untuk menggambarkan suatu keputusan / tindakan yang harus diambil pada kondisi tertentu.
6		Line Connector	Digunakan untuk menghubungkan satu simbol dengan simbol lainnya.

3. Sequence Diagram

Sequence diagram merupakan salah satu diagram dalam UML yang digunakan untuk menganalisis dan merancang alur logika dalam pengembangan perangkat lunak. Diagram ini menampilkan interaksi antar objek secara kronologis, sehingga terlihat urutan pesan dan komunikasi yang terjadi selama suatu skenario atau proses berlangsung. Melalui sequence diagram, hubungan dan pertukaran informasi antar objek dapat dipahami dengan lebih jelas, termasuk kapan suatu pesan dikirim, diterima, dan bagaimana setiap objek meresponsnya dalam rangkaian eksekusi sistem.

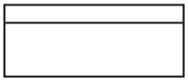
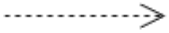
Tabel 2. 4 Simbol Sequence Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Entity Class	Gambaran sistem sebagai landasan dalam menyusun basis data.
2		Boundary Class	Menangani komunikasi antar lingkungan sistem.
3		Control Class	Bertanggung jawab terhadapa kelas-kelas terhadap objek yang berisi logika.
4		Recursive	Pesan untuk dirinya.
5		Activation	Mewakili proses durasi aktivitasi sebuah operasi.
6		Life Line	Komponen yang digambarkan garis putus terhubung dengan objek.

4. Class Diagram

Diagram kelas (class diagram) adalah diagram UML yang digunakan untuk menggambarkan struktur statis suatu sistem berorientasi objek, meliputi kelas-kelas yang menyusun sistem beserta atribut, operasi, dan hubungan antarkelas. Diagram ini membantu menunjukkan bagaimana data dan fungsi saling terhubung sehingga pengembang dapat memahami dan merancang arsitektur sistem secara lebih terstruktur sebelum diimplementasikan.

Tabel 2. 5 Simbol Class Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Generalization	Hubungan dimana objek anak (descendant) berbagi prilaku dan struktur data dari objek yang ada di atasnya objek induk(ancestor).
2		Nary Association	Upaya untuk menghindari asosiasi dengan lebih dari 2 objek.
3		Collaboration	Deskripsi dari urutan aksi-aksi yang menghasilkan suatu hasil yang terukur bagi suatu aktor
4		Class	Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama.
5		Realization	Operasi yang benar-benar dilakukan oleh usatu objek.
6		Dependency	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri.
7		Association	Apa yang menghubungkan antara objek satu dengan objek lainnya.

2.8 Flowchart

Flowchart atau diagram alir merupakan representasi grafis yang digunakan untuk menggambarkan alur proses suatu sistem secara sistematis dengan menggunakan simbol-simbol tertentu. Flowchart berfungi untuk mempermudah pahaman terhadap urutan proses, hubungan antar proses, serta mekanisme kerja sistem secara terstuktur. Dalam pengembangan sistem informasi, flowchart digunakan sebagai alat bantu analisis dan perancangan sistem agar proses pengolahan data dan alur kerja sistem dapat divisualisasikan dengan jelas sehingga memudahkan proses implementasi dan meminimalkan kesalahan sistem.

Tabel 2.6 Simbol Flowchart

SIMBOL	NAMA	FUNGSI
	Terminator	Permulaan atau akhiran program
	Input / Output data	Proses input / output data, parameter, dan informasi
	Decision	Pemilihan proses berdasarkan kondisi yang ada
	Process	Pengolahan data yang dilakukan oleh komputer
	On Page Connector	Simbol keluar masuk atau penyambungan proses pada lembar / halaman yang sama
	Off Page Connector	Simbol keluar masuk atau penyambungan proses pada lembar / halaman yang berbeda
	Predefined Process	Permulaan sub program atau proses menjalankan sub program
	Manual Operation	Pengolahan data yang tidak dilakukan oleh komputer
	Dokumen	Menyatakan input yang berasal dari dokumen dalam bentuk kertas atau output dicetak ke kertas

2.9 Penelitian Terdahulu

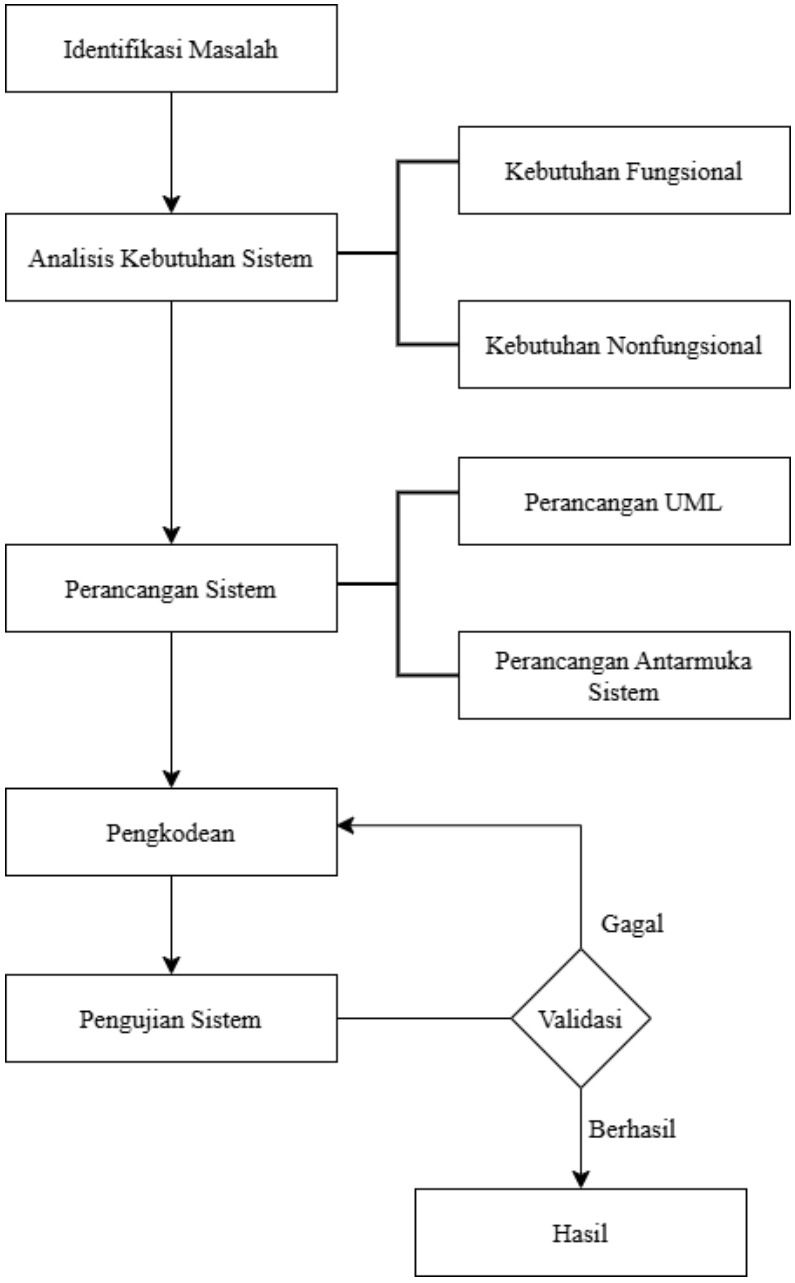
Tabel 2. 7 Penelitian Terdahulu

NO	Judul Penelitian	Penulis & Tahun	Metodologi/ algotitma	Temuan Utama	Relevansi dengan Penelitian
1	Implementasi Algoritma AES-128 untuk Pengamanan Data Berbasis Web	Arif alvian dkk., 2024	AES-128	Sistem berhasil melindungi dokumen digital melalui AES	Menjadi landasan dalam penerapan algoritma AES-128 pada sistem pengamanan dokumen digital
2	Analisa Metode Kriptoografi Advanced	Sekar Putri	AES- 128	AES-128 terbukti efektif dalam	Menjadi penguat teoritis terkait efektivitas

	Encryption Standard (AES) 128 bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital	Ananda dkk., 2022		menjaga kerahasiaan dokumen digital	algoritma AES-128 dalam pengamanan dokumen digital.
3	Implementasi pengarsipan Elektronik Menggunakan Enkripsi dan Dekripsi Metode AES di UNISKA	Bagus Arianto dkk., 2023	AES-128	Sistem arsip elektronik dengan enkripsi mampu menjaga keamanan data	Landasan untuk membangun sistem arsip pada perusahaan kontruksi
4	Perancangan Sistem Informassi Pengarsipan Data Internal Berbasis Web dengan Fitur Keamanan Enkripsi di BPSIP Jambil	Melky Ardiyansa dkk., 2023	AES 128	Sistem pengarsipan dengan enkripsi AES sangat layak dan mampu menjaga keamanan dokumen internal	Menjadi acuan dalam merancang dan mendesain sistem pengamanan arsip dokumen digital berbasis web
5	Rancang Bangun Sistem Informasi Arsip Online Berbasis Website pada Perusahaan Kontruksi	Ahmad safrizal dkk., 2023	Waterfall	Sistem arsip online mempermudah penyimpanan dan pencarian dokumen	Menjadi dasar bahwa digitalisasi arsip sangat dibutuhkan pada lingkungan kontruksi.

2.10 Kerangka Berpikir

Kerangka berpikir menjelaskan alur logis untuk melihat hubungan antara masalah dan solusi. Hal ini membantu menyusun langkah-langkah penelitian atau pengembangan sistem secara teratur agar tujuan dapat tercapai dengan jelas.



Gambar 2. 9 Kerangka Berpikir

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisis Permasalahan

Pengelolaan arsip dokumen digital merupakan aspek penting dalam operasional perusahaan kontraktor, karena dokumen seperti kontrak proyek, laporan harian, proposal, dan file anggaran memuat informasi strategis dan sensitif yang harus dijaga kerahasiaannya. Arsip tersebut berfungsi sebagai bukti kegiatan peusahaan sekaligus dasar pengambilan keputusan dalam setiap proyek, sehingga pengelolaan yang tepat sangat dibutuhkan.

Namun, saat ini pengelolaan arsip di perusahaan masih terbatas. Dokumen hanya disimpan dilaptop tanpa adanya sistem penyimpanan yang terstruktur maupun mekanisme pengamanan yang memadai. Kondisi ini membuat dokumen sulit dicari, rawan hilang dan berpotensi diakses atau disalahgunakan oleh pihak yang tidak berwenang. Selain itu, prosedur manual yang digunakan untuk pengelolaan arsip menyebabkan kontrol terhadap akses dan pemeliharaan dokumen menjadi lemah, sehingga risiko kebocoran atau kerusakan data semakin tinggi.

Kondisi tersebut menunjukkan bahwa sistem pengelolaan arsip saat ini belum mampu memenuhi kebutuhan perusahaan dalam menjaga kerahasiaan, integritas, dan ketersediaan dokumen digital. Untuk itu, diperlukan penerapan sistem pengamanan arsip dokumen digital yang dapat menyimpan dokumen secara terstuktur, mengatur hak akses pengguna, dan memastikan keamanan dokumen melalui enkripsi. Dalam hal ini, algoritma AES 128 dipilih sebagai dasar perancangan sistem karena kemampuannya dalam mengenkripsi dokumen secara

aman dan efesien. Dengan penerapan algoritma ini, arsip digital perusahaan kontraktor diharapkan dapat tersimpan dengan rapi, terlindungi dari akses yang tidak sah, serta dapat digunakan sebagai bukti resmi sesuai prinsip pengarsipan modern.

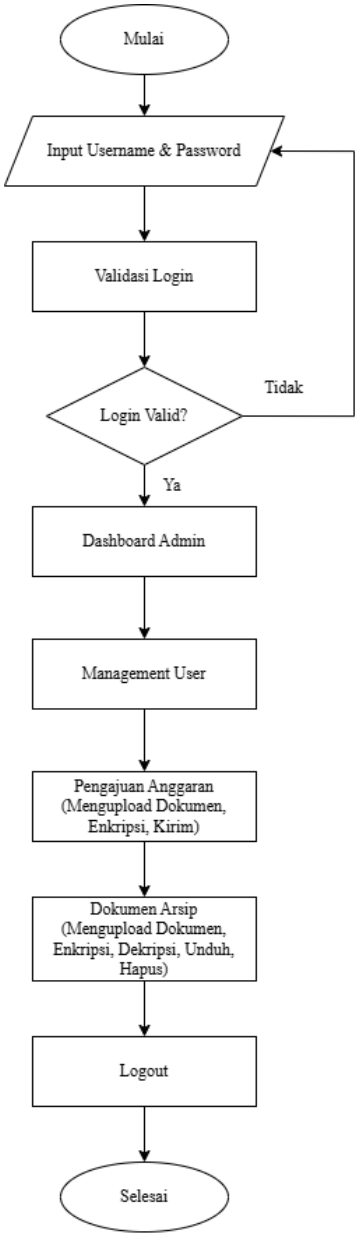
3.2 Alur Kerja Sistem

Sistem yang dikembangkan dalam penelitian ini merupakan sistem pengelolaan dan pengamanan dokumen digital yang bertujuan untuk menjaga kerahasiaan, keamanan, dan keteraturan dokumen yang disimpan di dalam sistem. Sistem ini dirancang agar hanya pengguna yang memiliki hak akses yang sah yang dapat mengakses dan memanfaatkan dokumen sesuai dengan perannya. Alur sistem dimulai dari proses login pengguna dengan memasukkan username dan password. Sistem kemudian melakukan validasi login untuk memastikan bahwa data yang dimasukkan sesuai dengan data pengguna yang terdaftar. Setelah login berhasil, sistem akan menentukan hak akses pengguna, sehingga fitur yang ditampilkan akan disesuaikan dengan peran pengguna tersebut.

Pengguna dengan hak akses tertentu dapat melakukan aktivitas sesuai kewenangannya, seperti mengelola dokumen, mengunggah, mencari, atau mengakses dokumen yang tersedia. Dalam sistem ini, dokumen yang dikelola dilengkapi dengan mekanisme pengamanan sehingga isi dokumen tidak dapat diakses oleh pihak yang tidak berwenang. Setelah seluruh proses penggunaan sistem selesai, pengguna dapat melakukan log out untuk mengakhiri sesi penggunaan. Dengan alur sistem tersebut, pengelolaan dan pengamanan dokumendigital dapat dilakukan secara terstruktur, aman, dan terkontrol.

3.2.1 Alur Kerja Sistem Admin

Admin merupakan staf administrasi kantor atau staf IT pada perusahaan kontruksi yang ditunjuk sebagai pengelola sistem. Admin bertanggung jawab dalam mengatur data pengguna, mengelola dokumen, serta mengawasi jalannya sistem secara keseluruhan. Dengan hak akses penuh yang dimiliki, admin dapat mengontrol seluruh fitur dalam sistem.



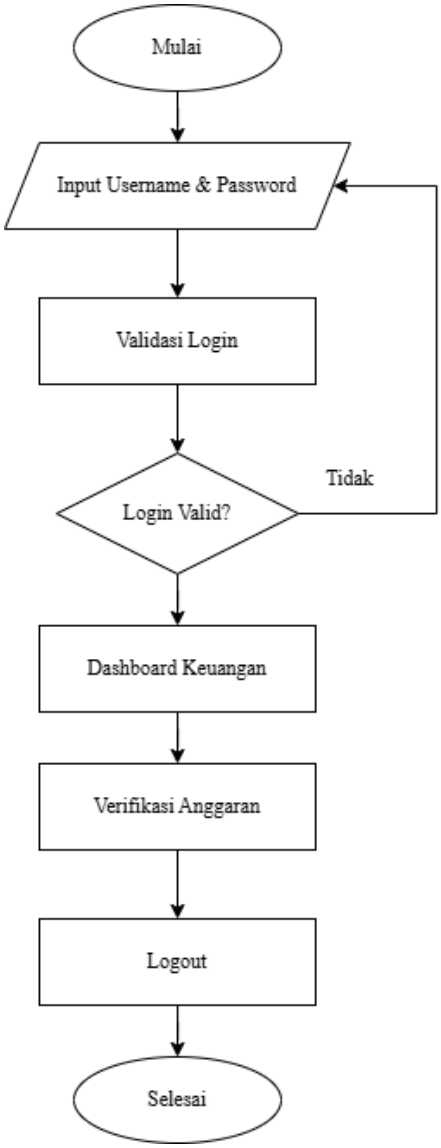
Gambar 3. 1 Alur Kerja Sistem Admin

Berdasarkan gambar alur kerja sistem pada admin, berikut penjelasannya:

1. Proses dimulai ketika admin membuka sistem
2. Admin memasukkan username dan password sebagai data autentikasi untuk dapat mengakses sistem.
3. Sistem melakukan validasi data login dengan mencocokkan username dan password yang dimasukkan dengan data yang tersimpan di basis data.
4. Jika login tidak valid (username atau password salah), maka admin tidak dapat melanjutkan proses dan harus mengulangi login. Jika login valid, admin berhasil masuk ke halaman dashboard.
5. Admin dapat menambah, mengubah, atau menghapus data pengguna pada menu managemen user.
6. Admin dapat mengajukan anggaran dan mengirimkan ke bagian keuangan pada menu pengajuan anggaran.
7. Admin dapat membuat folder dan menambah dokumen kedalam folder, mengenkripsi dan mendekripsi dokumen, mengunduh dokumen, menghapus dokumen pada menu dokumen arsip.
8. Setelah selesai menggunakan sistem dapat melakukan logout untuk mengakhiri sesi penggunaan.
9. Proses sistem berakhir setelah admin keluar dari sistem.

3.2.2 Alur Kerja Sistem Keuangan

Keuangan merupakan staf bagian keuangan/akuntan di perusahaan kontruksi yang bertugas menangani administrasi keuangan, termasuk pengelolaan dokumen pengajuan anggaran dan verifikasi anggaran.



Gambar 3. 2 Alur Kerja Sistem Keuangan

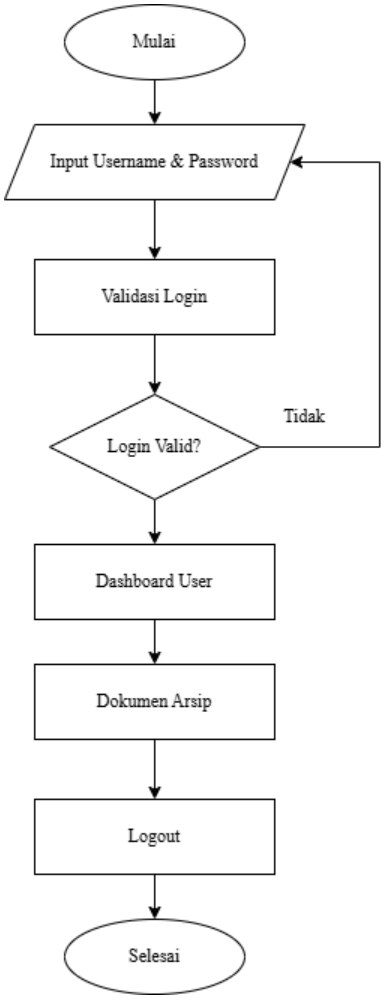
Berdasarkan gambar alur kerja sistem pada keuangan, berikut penjelasannya:

1. Proses dimulai ketika keuangan membuka sistem
2. keuangan memasukkan username dan password sebagai data autentikasi untuk dapat mengakses sistem.
3. Sistem melakukan validasi data login dengan mencocokkan username dan password yang dimasukkan dengan data yang tersimpan di basis data.

4. Jika login tidak valid (username atau password salah), maka keuangan tidak dapat melanjutkan proses dan harus mengulangi login. Jika login valid, keuangan berhasil masuk ke halaman dashboard.
5. Keuangan dapat melihat dokumen-dokumen pengajuan anggaran yang telah dikirim oleh admin.
6. Keuangan dapat melihat dokumen dan melakukan pengecekan kemudian memverifikasi dokumen jika sudah sesuai, dan jika belum sesuai maka keuangan akan merevisi dokumen pengajuan.
7. Setelah selesai menggunakan sistem dapat melakukan logout untuk mengakhiri sesi penggunaan.
8. Proses sistem berakhir setelah keuangan keluar dari sistem.

3.2.3 Alur Kerja Sistem User

User merupakan staf administrasi proyek yang memanfaatkan dokumen arsip sebagai bahan dalam penyusunan laporan, verifikasi, dan audit. Oleh karena itu, user hanya diberikan hak akses untuk melihat dokumen tanpa memiliki kewenangan untuk menambah, mengubah, maupun menghapus data.



Gambar 3. 3 Alur Kerja Sistem User

Berdasarkan gambar alur kerja sistem pada user, berikut penjelasannya:

1. Proses dimulai ketika user membuka sistem
2. User memasukkan username dan password sebagai data autentikasi untuk dapat mengakses sistem.
3. Sistem melakukan validasi data login dengan mencocokkan username dan password yang dimasukkan dengan data yang tersimpan di basis data.
4. Jika login tidak valid (username atau password salah), maka user tidak dapat melanjutkan proses dan harus mengulangi login. Jika login valid, user berhasil masuk ke halaman dashboard.
5. User dapat melihat folder-folder arsip dokumen.

6. User dapat melihat isi dokumen jika status dokumen tidak terkunci.
7. Setelah selesai menggunakan sistem dapat melakukan logout untuk mengakhiri sesi penggunaan.
8. Proses sistem berakhir setelah user keluar dari sistem..

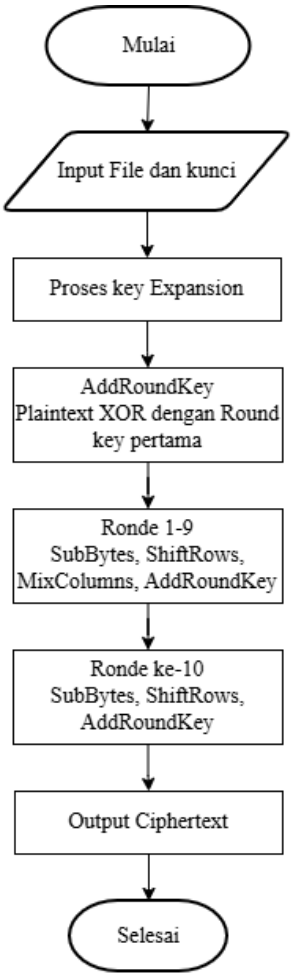
3.3 Tahapan Algoritma AES

Algoritma AES 128 digunakan dalam sistem untuk mengamanan dokumen digital perusahaan dengan cara mengubah data asli (*plaintext*) menjadi data terenkripsi (*ciphertext*) menggunakan kunci rahasia, sehingga informasi tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang. Penerapan algoritma ini bertujuan menjaga kerahasiaan serta keamanan dokumen yang tersimpan di dalam sistem arsip digital. Tahapan kerja AES-128 pada sistem terdiri dari dua proses utama, yaitu proses enkripsi untuk melindungi data sebelum disimpan ke dalam sistem, serta proses dekripsi untuk mengembalikan data terenkripsi ke bentuk aslinya agar dapat diakses kembali oleh pengguna yang memiliki hak akses.

3.3.1 Tahapan Enkripsi AES-128

Proses enkripsi bertujuan untuk mengamankan dokumen digital agar tidak dapat dibaca oleh pihak yang tidak berwenang. Tahapan enkripsi dilakukan dengan cara yaitu, *AddRoundKey* untuk menggabungkan data asli dengan kunci rahasia sebagai langkah awal pengamanan. Selanjutnya data diproses melalui transsformasi yang berurutan, meliputi *SubBytes* untuk menghilangkan pola data dengan mensubstitusi nilai *byte* dengan tabel S-Box, *ShiftRows* untuk pergeseran susunan baris agar lebih sulit dikenali,

MixColumns untuk mencampur data pada setiap kolom sehingga meningkatkan tingkat keacakan. Pada tahap akhir, sistem kembali melakukan *AddRoundKey* untuk menghasilkan *Ciphertext*.



Gambar 3. 4 Tahapan Enkripsi AES

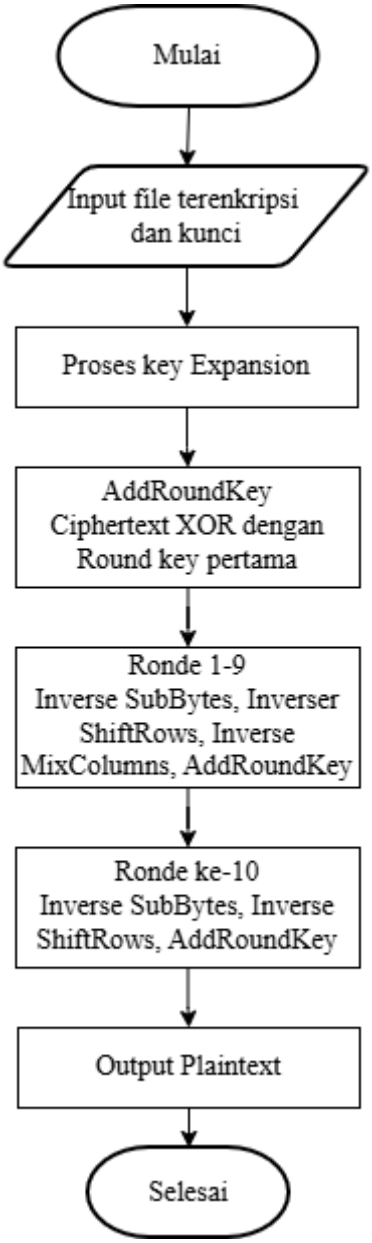
Berdasarkan gambar tahapan enkripsi berikut penjelasannya:

1. Admin membuka sistem pengamanan arsip dokumen.
2. Admin memilih file dokumen yang akan diamankan.
3. Admin memasukkan kunci password sebagai dasar pembentukan kunci AES-128
4. Validasi kunci Rahasia, jika tidak valid admin diminta memasukkan ulang password dan jika valid sistem akan melanjutkan proses enkripsi

5. Proses enkripsi AES, sistem mengubah file *plaintext* menjadi *ciphertext* menggunakan algoritma AES.
6. Output Chiptertext, file yang dihasilkan sudah dalam bentuk terenkripsi dan tidak dapat dibaca secara langsung.
7. File *ciphertext* disimpan ke database.
8. Proses enkripsi dinyatakan selesai.

3.3.2 Tahapan Dekripsi AES

Proses dekripsi berfungsi untuk mengembalikan file yang telah terenkripsi ke bentuk aslinya, sehingga akses terhadap dokumen digital hanya dapat dilakukan oleh pengguna yang memiliki kunci yang valid. Tahapan dekripsi dilakukan dengan menjalankan proses yang berlawanan atau kebalikan dari tahapan enkripsi, yaitu *Inserve ShiftRows* untuk mengembalikan susunan data seperti semula, *Inverse SubBytes* untuk memulihkan nilai setiap *byte*, *AddRoundKey* untuk menggabungkan data dengan kunci rahasia, dan *Inverse MixColumns* untuk mengembalikan struktur kolom data. Setelah seluruh tahapan tersebut diselesaikan, file dapat dipulihkan ke kondisi awal.



Gambar 3. 5 Tahapan Dekripsi AES

Berdasarkan gambar tahapan dekripsi berikut penjelasannya:

1. Proses dekripsi diawali dengan admin membuka sistem pengamanan arsip dokumen digital.
2. Admin memilih file yang telah terenkripsi dan tersimpan dalam sistem.
3. Admin memasukkan kunci rahasia yang digunakan saat proses enkripsi.

4. Validasi kunci rahasia, sistem memverifikasi apakah password yang dimasukkan sesuai dengan kunci enkripsi. Jika tidak valid sistem meminta pengguna untuk memasukkan ulang password dan jika valid sistem melanjutkan ke proses dekripsi.
5. Sistem menjalankan algoritma AES 128 dengan menggunakan kunci rahasia untuk mengubah *ciphertext* kembali menjadi *plaintext*.
6. Hasil proses dekripsi berupa file dalam bentuk aslinya, sehingga dapat dibaca kembali.
7. File hasil dekripsi dapat ditampilkan kepada pengguna atau disimpan kembali sesuai kebutuhan.
8. Proses dekripsi dinyatakan selesai setelah file berhasil dipulihkan.

3.4 Pemodelan Sistem

Pemodelan sistem dilakukan sebagai tahap lanjutan setelah analisis kebutuhan sistem selesai dilaksanakan. Tahap ini bertujuan untuk menyusun rancangan sistem secara lebih detail sehingga alur kerja, stuktur sistem, serta keterkaitan antar komponen dalam proses pengamanan arsip dokumen digital dapat dipahami dengan jelas sebelum sistem dikembangkan dan diimplementasikan. Melalui pemodelan sistem, rancangan yang dibuat dapat menggambarkan bagaimana proses enkripsi dan dekripsi dokumen menggunakan algoritma AES diterapkan, serta bagaimana pengguna berinteraksi dengan fitur-fitur yang tersedia dalam sistem pengamanan arsip dokumen digital, sehingga proses pengembangan dapat berjalan lebih terarah dan sesuai dengan kebutuhan keamanan data serta pengelolaan dokumen yang telah dianalisis sebelumnya.

Dalam penelitian ini, pendekatan Unified Modeling Language (UML) digunakan sebagai alat bantu untuk memvisualisasikan rancangan sistem secara terstuktur. UML dipilih karena mampu merepresentasikan fungsi sistem, alur aktivitas pengelolaan dan pengamanan arsip dokumen, serta stuktur data yang terlibat secara sistematis dan mudah dipahami. Pemodelan sistem mencakup beberapa diagram yaitu, Use Case Diagram, Activity Diagram, Sequence Diagram, dan Class Diagram yang masing-masing berperan dalam menjelaskan interaksi antara pengguna dan sistem, alur aktivitas pengelolaan dokumen serta proses enkripsi dan dekripsi, urutan pemrosesan data, serta stuktur kelas dan hubungan antar data, sehingga rancangan sistem dapat menjadi acuan yang jelas dalam tahap pengembangan dan implementasi sistem pengamanan arsip dokumen digital di perusahaan kontraktor.

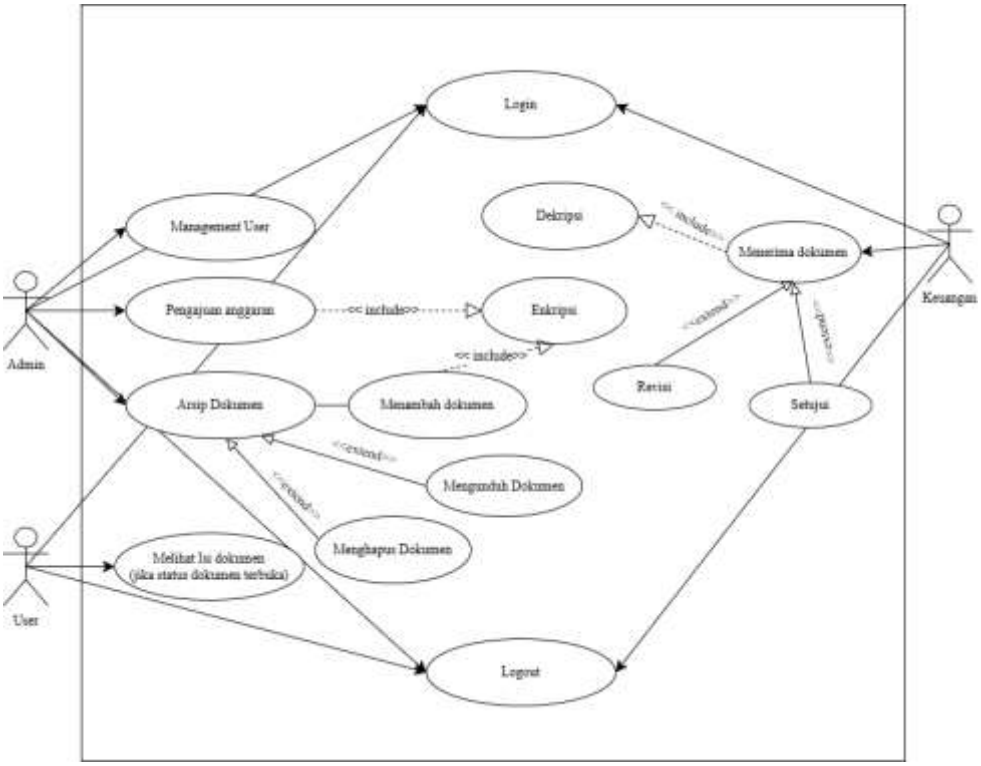
3.4.1 Use Case Diagram

Use Case diagram digunakan untuk menggambarkan hubungan antara pengguna dan sistem pengamanan arsip dokumen digital, serta menunjukkan fungsi utama yang disediakan dalam proses pengelolaan dan perlindungan dokumen proyek di perusahaan kontruksi. Diagram ini memberikan gambaran umum mengenai layanan apa saja yang dapat diakses pengguna, serta bagaimana sistem mendukung proses pengamanan data menggunakan algoritma AES-128.

Aktor dalam sistem terdiri dari Admin, User dan Keuangan yang memiliki peran hak akses berbeda sesuai kebutuhan operasional. User dapat melakukan aktivitas seperti login ke sistem, melihat daftar arsip dokumen digital dan melihat dokumen. Sementara itu, Admin memiliki kewenangan

penuh dalam pengelolaan sistem, seperti menggunggah dokumen proyek, mengelola data user, melakukan enkripsi dan dekripsi dokumen menggunakan algoritma AES-128, serta mengatur dan memelihara arsip digital yang tersimpan dalam sistem. Pembagian hak akses ini bertujuan menjaga dokumen dan memastikan setiap proses pengelolaan dilakukan oleh pihak yang berwenang.

Selain itu, Use Case Diagram berperan dalam menggambarkan interaksi pengguna dengan sistem serta memperjelas ruang lingkup layanan yang tersedia. Digram ini juga menjadi dasar dalam perancanngan alur proses dan antarmuka pengguna, sehingga pengembangan sistem pengamanan arsip dokumen digital dapat dilakukan secara lebih terstuktur, efisien, dan sesuai dengan kebutuhan pengelolaan serta perlindungan informasi proyek di lingkungan perusahaan kontruksi.



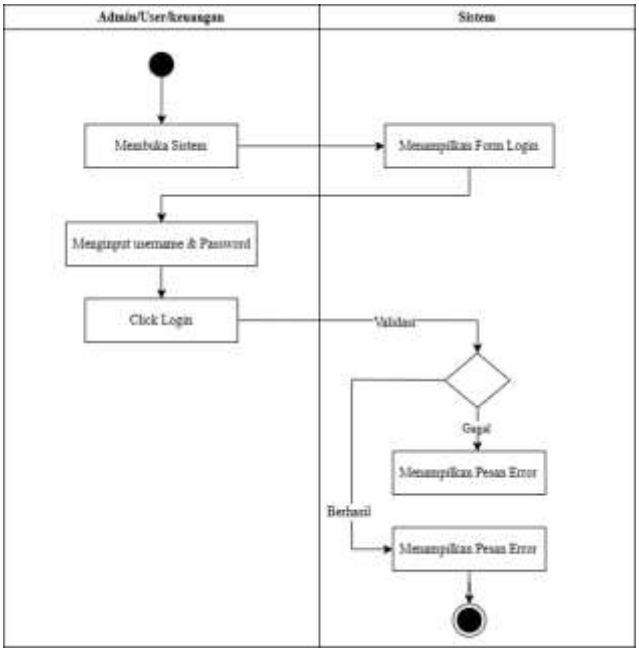
Gambar 3. 6 Use Case Diagram Sistem

3.4.2 Activity Diagram

Activity Diagram digunakan untuk menggambarkan alur aktivitas dan tahapan proses yang berbeda-beda dalam sistem. Diagram ini menunjukkan bagaimana setiap alur dimulai, keputusan-keputusan yang dapat diambil selama proses berlangsung, serta bagaimana sistem tersebut berakhir. Adapun beberapa rangkaian Activity Diagram adalah sebagai berikut:

1. Activity Diagram Login

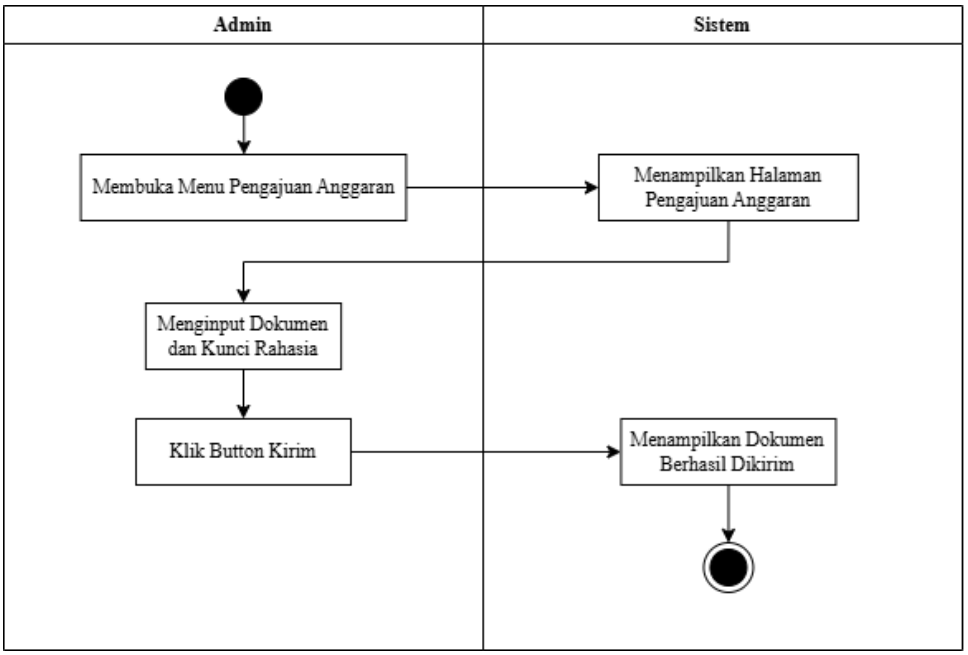
   Menjelaskan proses ketika pengguna masuk ke dalam sistem menggunakan akun yang telah terdaftar. Proses dimulai dari pengguna membuka halaman login dan memasukkan data yang dimasukkan. Jika informasi benar, pengguna akan diarahkan ke halaman utama sistem, sedangkan jika tidak sesuai maka sistem akan menampilkan pemberitahuan kesalahan dan meminta pengguna mengisi ulang data login. Tampilan activity diagram untuk login adalah sebagai berikut:



Gambar 3. 7 Activity Diagram Login pada Admin, User dan Keuangan

2. Actuvity Diagram Pengajuan Anggaran

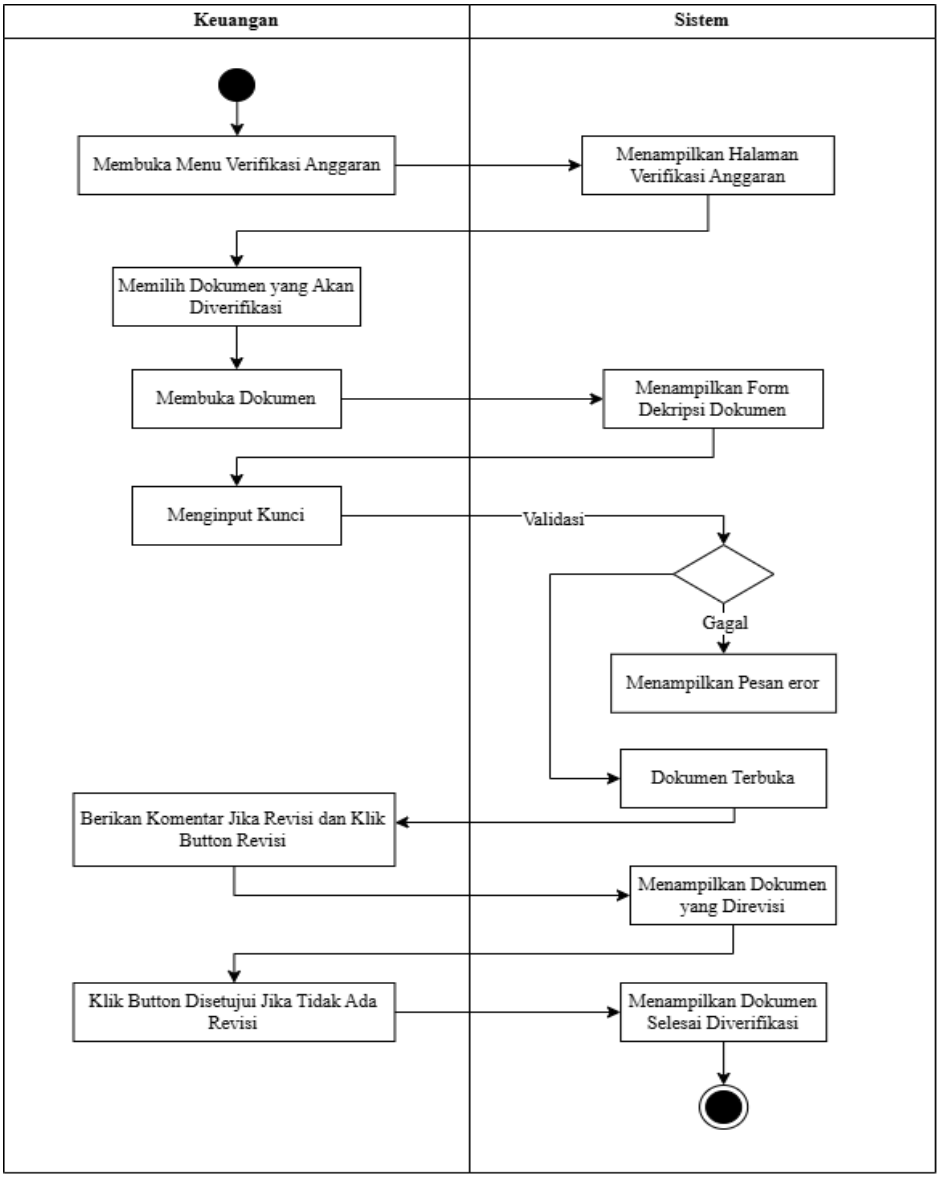
Menjelaskan langkah langkah yang dilakukan admin saat melakukan pengajuan anggaran dalam sistem. Proses dimulai dari admin mengunggah dokumen yang akan diajukan dan mengenkripsi dokumen kemudian kirim ke bagian keuangan dan menunggu keuangan memverifikasi.



Gambar 3. 8 Activity Diagram Pengajuan Anggaran

3. Activity Diagram Memverifikasi Anggaran

Menjelaskan langkah langkah yang dilakukan keuangan saat memverifikasi anggaran. Proses dimulai dari keuangan membuka dan memeriksa data serta pengajuan yang telah dikirim. Selanjutnya dilakukan proses verifikasi untuk memastikan kesesuaian isi dokumen pengajuan. Apabila ditemukan ketidaksesuaian, maka pengajuan akan direvisi atau ditolak. Namun jika dokumen telah sesuai, maka pengajuan disetujui dan proses dinyatakan selesai. Tampilan Activity Diagram Memverifikasi Anggaran sebagai berikut :

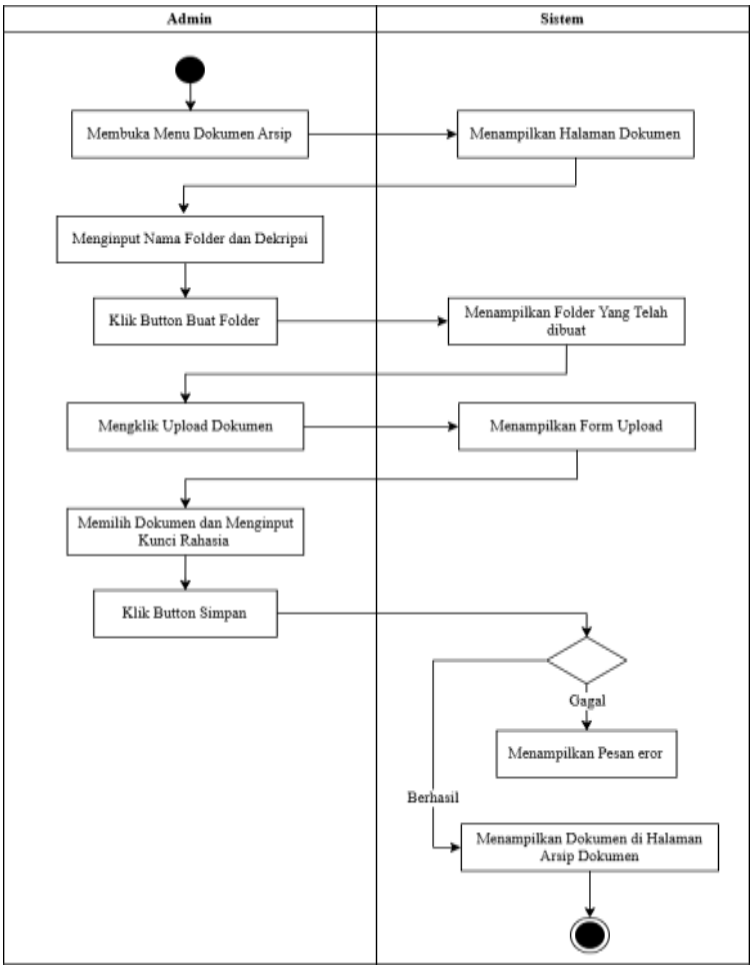


Gambar 3. 9 Activity Diagram Verifikasi Anggaran

4. Diagram Membuat Folder, Menambah Dokumen dan Enkripsi

   Menjelaskan langkah-langkah yang dilakukan admin saat membuat folder dan mengunggah dokumen ke dalam sistem. Proses diawali dengan membuat folder dan memilih file yang akan diunggah, kemudian mengisi data atau informasi dokumen, serta memasukkan kunci enkripsi sebagai pengamanan. Setelah semua data dilengkapi, sistem secara otomatis mengenkripsi dokumen menggunakan kunci tersebut sebelum

menyimpannya kedalam database. Tampilan activity diagram untuk melakukan upload dokumen dan mengenkripsi dokumen adalah sebagai berikut:

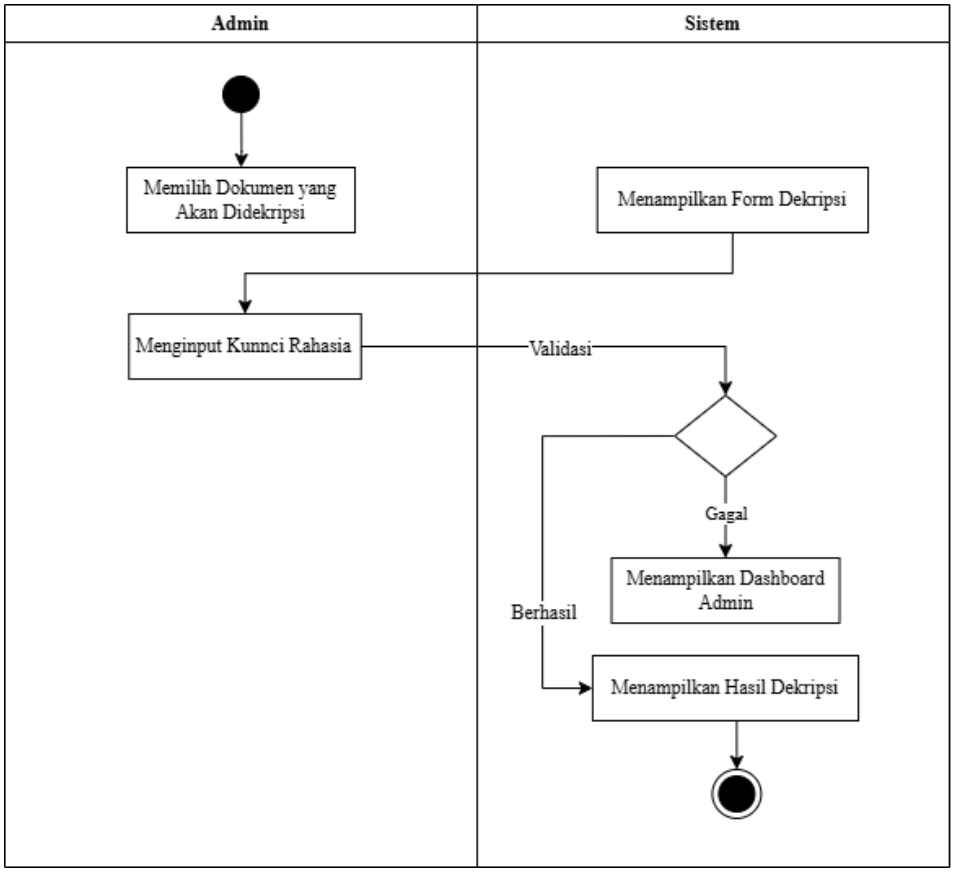


Gambar 3. 10 Activity Diagram Arsip Dokumen

5. Activity Diagram Dekripsi

Menjelaskan alur proses ketika admin ingin membuka kembali dokumen yang sebelumnya telah diamankan dengan enkripsi. Proses dimulai dari pemilihan dokumen yang akan diakses, kemudian admin memasukkan kunci dekripsi yang sesuai. Setelah kunci verifikasi , sistem melakukan proses dekripsi untuk mengembalikan dokumen ke bentuk aslinya sehingga isi dokumen dapat dilihat atau digunakan kembali sesuai

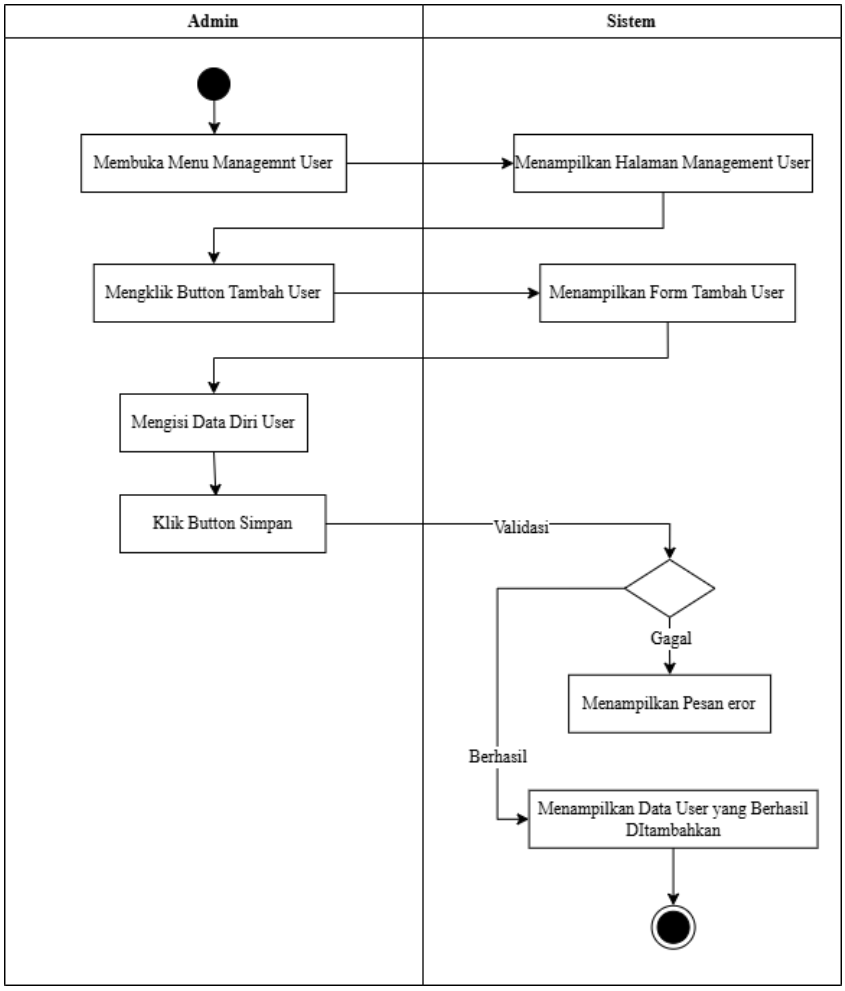
kebutuhan. Tampilan activity diagram untuk melakukan dekripsi dokumen adalah sebagai berikut:



Gambar 3. 11 Activity Diagram Dekripsi

6. Activity Diagram Menambah User

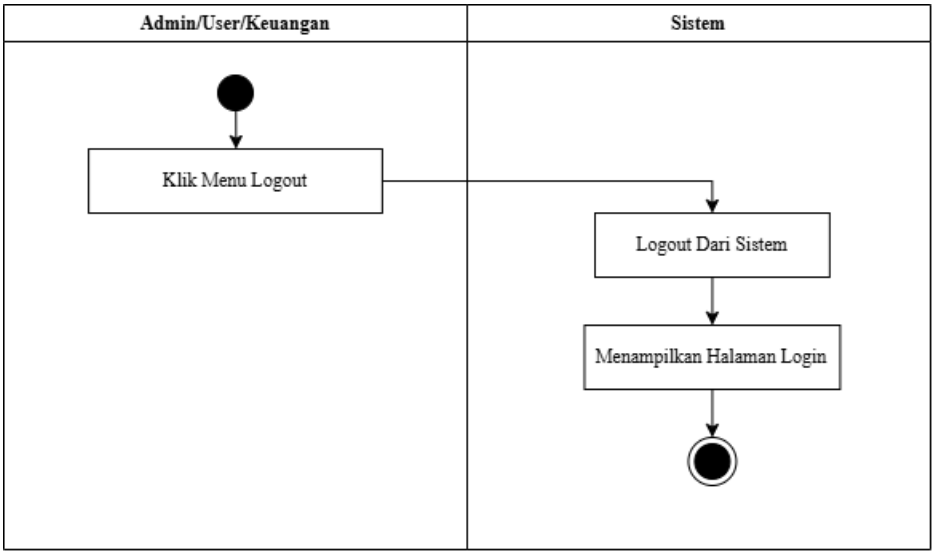
Menjelaskan alur proses ketika admin menambahkan data pengguna baru kedalam sistem. Proses dimulai dari admin membuka menu management user, kemudian mengisi informasi pengguna seperti nama, username, password, dan jenis pengguna. Setelah data dimasukkan, sistem melakukan pemeriksaan untuk memastikan data sudah lengkap dan tidak terjadi duplikasi. Jika seluruh data valid, sistem akan menyimpan informasi pengguna ke dalam basis data sehingga akun dapat digunakan untuk masuk ke dalam sistem. Tampilan activity diagram untuk menambah user adalah sebagai berikut:



Gambar 3. 12 Activity Diagram Management User

7. Activity Diagram Logout

Menjelaskan proses ketika pengguna keluar dari sistem setelah selesai menggunakan sistem. Proses dimulai saat pengguna memilih menu logout, kemudian sistem menerima perintah tersebut dan mengakhiri sesi yang sedang aktif. Setelah itu, pengguna akan dialihkan kembali ke halaman login yang menandakan bahwa proses keluar dari sistem telah selesai. Tampilan activity diagram untuk logout adalah sebagai berikut:



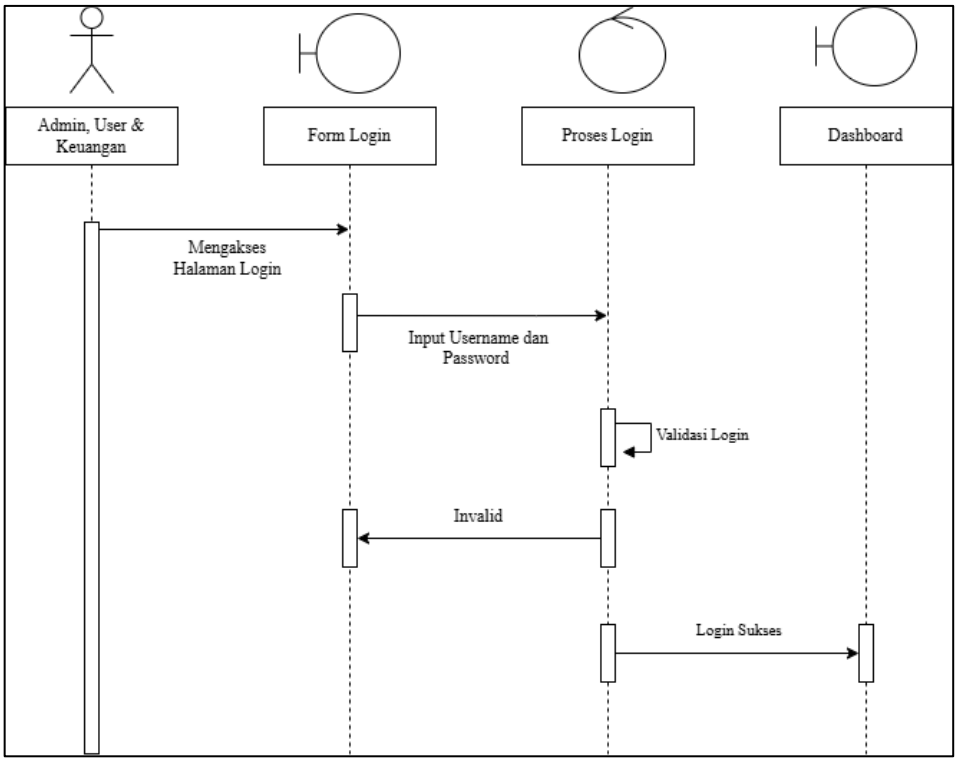
Gambar 3. 13 Activity Diagram Logout

3.4.3 Sequence Diagram

Sequence Diagram digunakan untuk menggambarkan urutan interaksi antara pengguna dan sistem berdasarkan alur waktu dalam menjalankan suatu proses. Diagram ini menunjukkan tahapan komunikasi secara berurutan, mulai dari pengguna mengirim permintaan, sistem memproses permintaan tersebut, hingga sistem memberikan respons.

1. Sequence Diagram Login

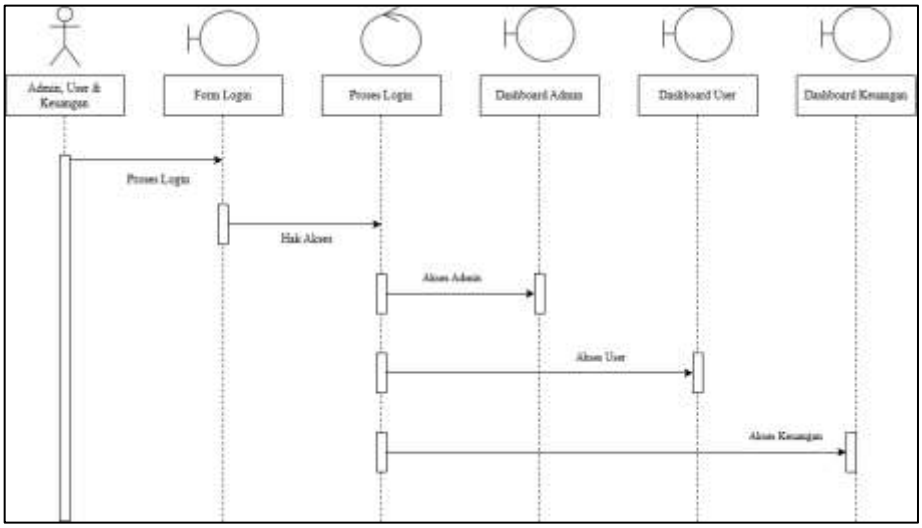
   Menggambarkan urutan proses ketika pengguna masuk ke dalam sistem melalui halaman login. Proses dimulai dari pengguna memasukkan username dan password, kemudian sistem melakukan validasi terhadap data yang dimasukkan. Jika data sesuai, sistem akan menampilkan halaman dashboard sebagai tampilan utama. Namun jika tidak sesuai, sistem akan meminta pengguna untuk mengisi kembali data login. Tampilan sequence diagram untuk melakukan login adalah sebagai berikut:



Gambar 3. 14 Sequence Diagram Login

2. Sequence Diagram Menu Dashboard Sistem

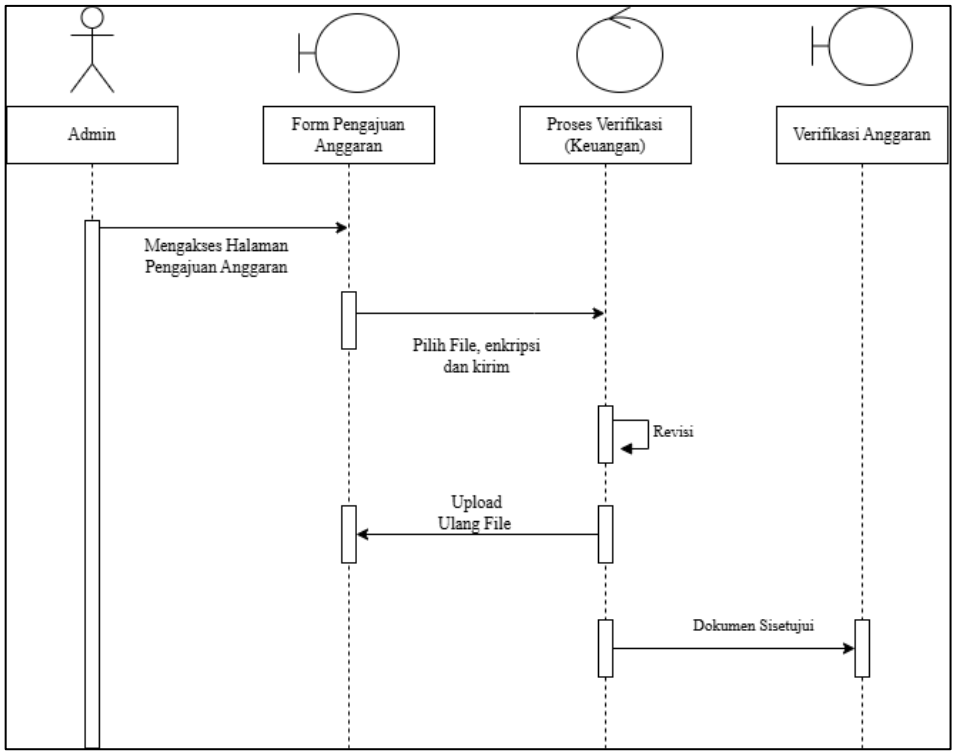
Menjelaskan urutan proses saat pengguna berhasil login dan sistem akan menampilkan halaman dashboard. Setelah login, sistem memproses data pengguna dan menyesuaikan tampilan dashboard sesuai hak akses. Tampilan sequence diagram untuk menu dashboard adalah sebagai berikut:



Gambar 3. 15 Sequence Diagram Dashboard

3. Sequence Diagram Pengajuan Anggaran

Menjelaskan urutan proses ketika admin mengunggah dokumen penawaran, kemudian mengkunnci dokumen lalu mengirimkan pengajuan kebagian keuangan. Selanjutnya, admin menunggu hasil verifikasi. Jika penngajuan direvisi, admin akan mengunggah ulang dokumen yang telah diperbaiki dan mengirimkannya kembali. Namun jika pengajuan disetujui, maka proses pengajuan selesai. Tampilan Sequence Diagram pengajuan anggaran sebagai berikut:

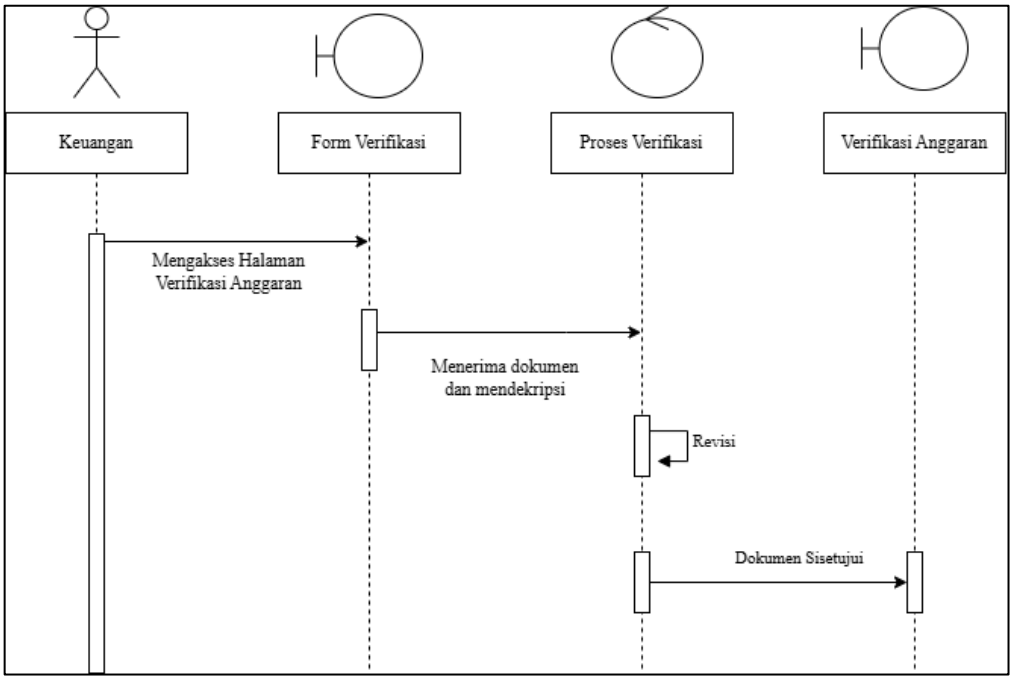


Gambar 3. 16 Sequence Diagram Pengajuan Anggaran

4. Sequence Diagram Verifikasi Anggaran

Menjelaskan urutan proses Ketika bagian keuangan melakukan verifikasi anggaran. Proses dimulai dengan mengakses halaman verifikasi, kemudian menerima dan membuka dokumen penawaran. Selanjutnya dilakukan

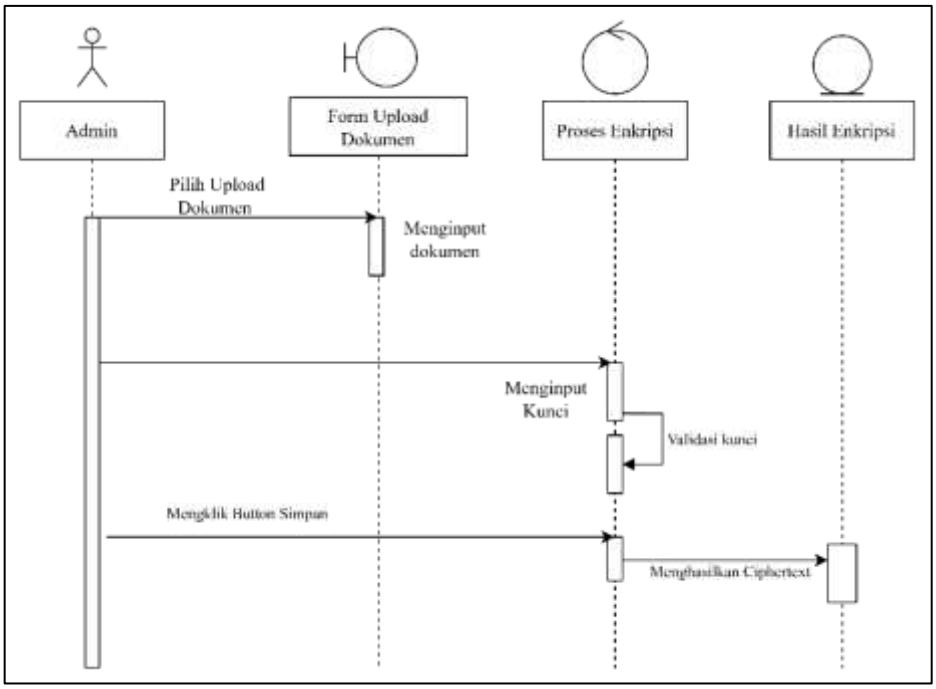
pengecekan isi dokumen, lalu memberikan keputusan berupa persetujuan atau revisi. Jika revisi maka akan dikembalikan keadmin, jika disetujui proses pengajuan selesai. Tampilan Sequence Diagram verifikasi anggaran sebagai berikut:



Gambar 3. 17 Sequence Diagram Verifikasi Anggaran

5. Sequence Diagram Menambah Dokumen dan Mengenkripsi

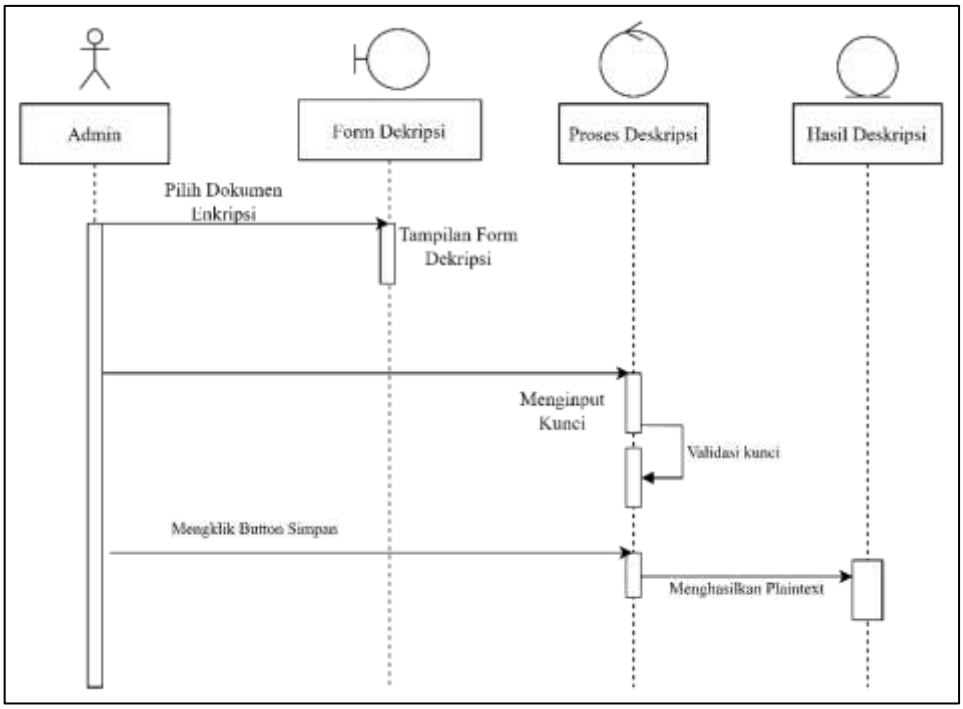
Menjelaskan urutan proses ketika admin menambahkan dokumen baru kesistem. Admin memilih file, mengisi informasi dokumen, dan memasukkan kunci enkripsi. Setelah itu, sistem memproses data, mengenkripsi dokumen, dan menyimpannya. Tampilan sequence diagram untuk menambah dokumen dan mengenkripsi adalah sebagai berikut:



Gambar 3. 18 Sequence Diagram Menambah dan Enkripsi

6. Sequence Diagram Dekripsi

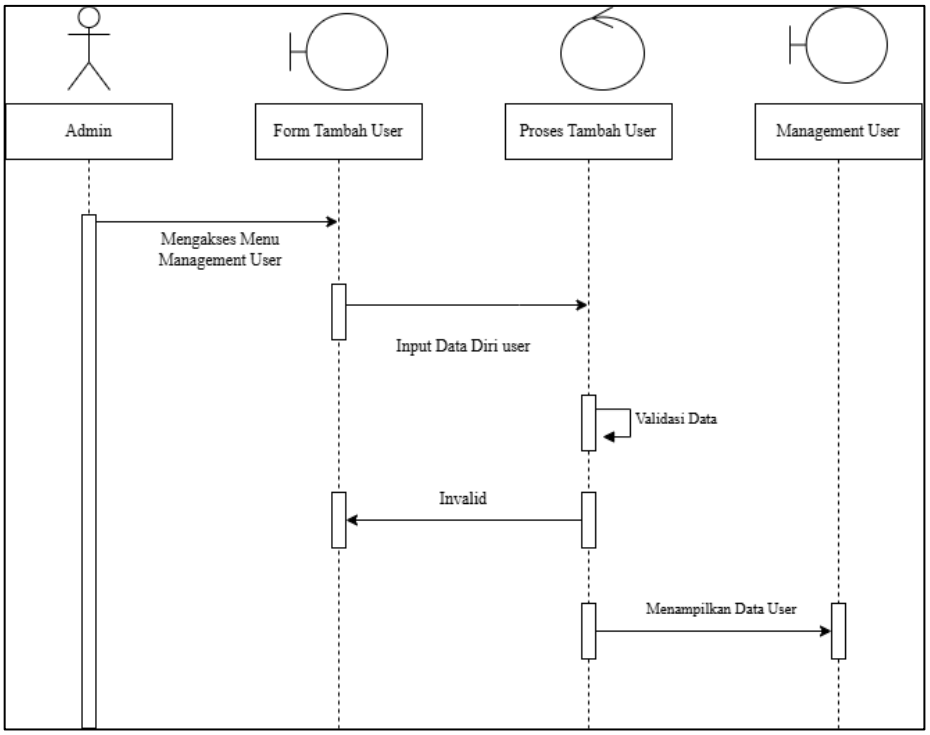
Menjelaskan urutan proses ketika admin membuka kembali dokumen yang sebelumnya telah dienkripsi. Proses dimulai dari admin memilih dokumen dan memasukkan kunci dekripsi, kemudian sistem memproses kunci tersebut dan melakukan dekripsi. Setelah proses selesai, dokumen kembali kebentuk aslinya sehingga dapat dilihat atau digunakan. Tampilan sequence diagram untuk mendekripsi dokumen adalah sebagai berikut:



Gambar 3. 19 Sequence Diagram Dekripsi

7. Sequence Diagram Menambahkan User

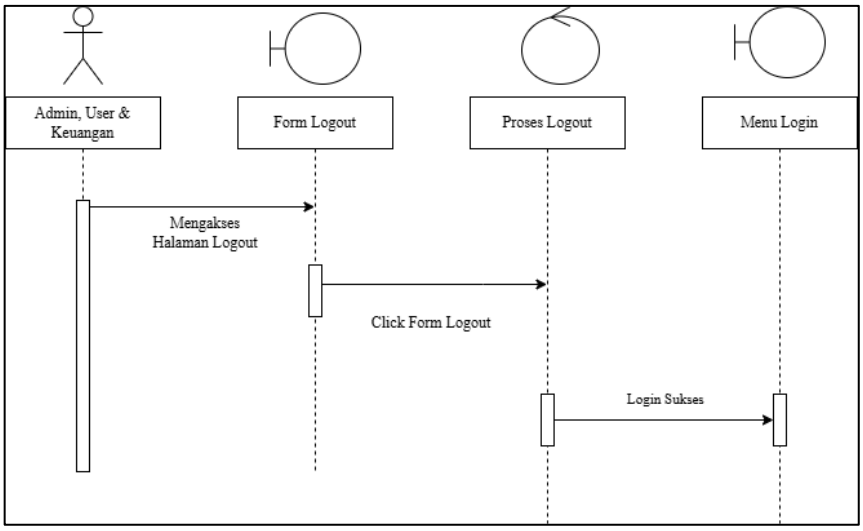
Menjelaskan urutan proses ketika admin menambahkan pengguna baru kedalam sistem. Proses dimulai ketika saat admin membuka menu tambah user dan mengisi data seperti nama, username, serta password. Setelah data dikirim, sistem melakukan pemeriksaan kelengkapan data. Jika sesuai, sistem menyimpan informasi pengguna dan akun baru berhasil ditambahkan. Tampilan sequence diagram untuk menambah user adalah sebagai berikut:



Gambar 3. 20 Sequence Diagram Menambahkan User

8. Sequence Diagram Logout

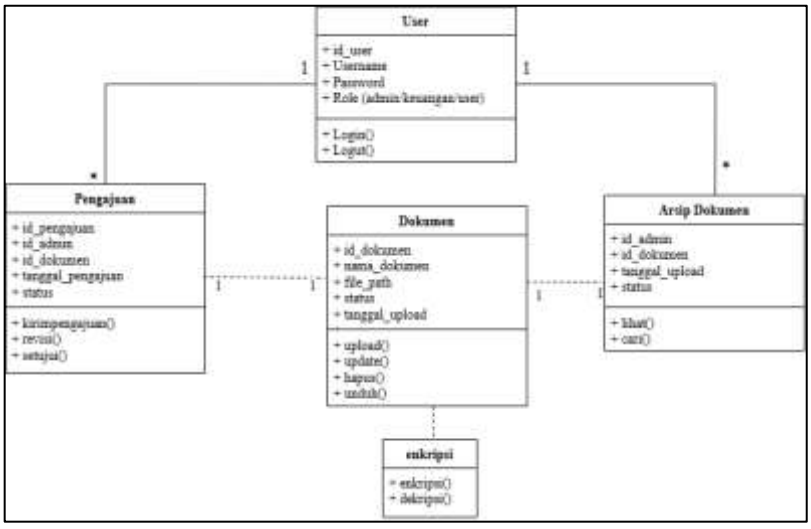
Menjelaskan proses ketika pengguna keluar dari sistem. Proses dimulai saat pengguna memilih menu logout, kemudian sistem menerima permintaaf tersebut dan mengakhiri sesi yang sedang aktif. Setelah proses selesai, sistem mengarahkan pengguna kembali ke halaman login. Tampilan sequence diagram untuk logout adalah sebagai berikut:



Gambar 3. 21 Sequence Diagram logout

3.4.4 Class diagram

Class Diagram digunakan untuk menggambarkan stuktur statis sistem pengamanan dokumen digital dengan menunjukkan hubungan antar kelas, atribut, dan metode yang mendukung pengelolaan pengguna dan dokumen. Diagram ini memberikan gambaran mengenai komponen utama sistem serta interaksi antar kelas yang terlibat dalam proses pengelolaan dan pengamanan dokumen. Adapun rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat sebagai berikut:



Gambar 3. 22 Class Diagram

3.5 Desain Antarmuka Sistem

Desain antarmuka sistem bertujuan untuk menampilkan tampilan sistem yang mudah digunakan dan nyaman bagi pengguna. Tampilan dirancang agar setiap fitur mudah dipahami dan diakses, sehingga pengguna dapat menjalankan proses penggunaan sistem dengan lancar, mulai dari login hingga pengelolaan dokumen. Dalam perancangannya, antarmuka memperhatikan susunan menu, kejelasan informasi yang ditampilkan, serta kemudahan berpindah antar halaman. Dengan tampilan yang sederhana dan tertata rapi, pengguna diharapkan dapat menggunakan sistem dengan lebih mudah, efisien, dan tanpa mengalami kesulitan.

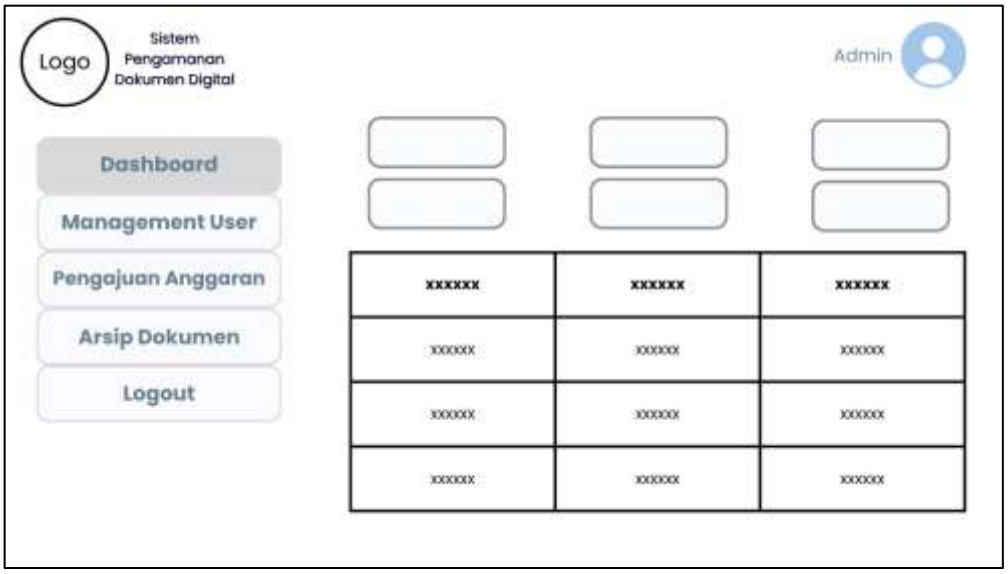
3.5.1 Desain Antarmuka Login

Menampilkan halaman awal yang digunakan pengguna untuk masuk ke dalam sistem. Pada halaman ini terdapat input username dan password sebagai proses autentikasi pengguna sebelum mengakses fitur sistem pengamanan arsip dokumen digital. Seperti yang ditunjukkan pada gambar berikut

Gambar 3. 23 Desain Halaman Login

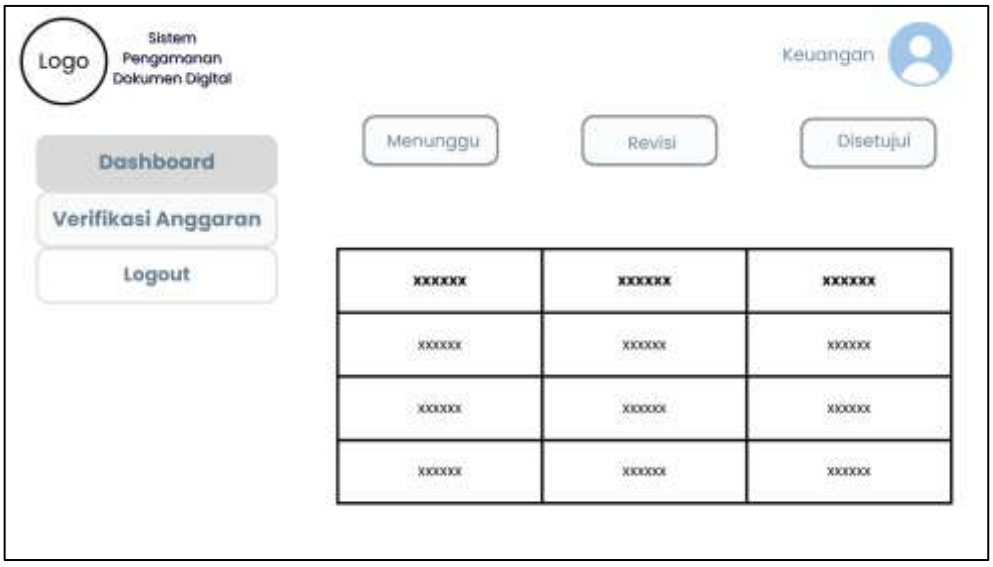
3.5.2 Desain Halaman Dashboard Admin, User dan Keuangan

Menampilkan halaman utama setelah admin masuk ke sistem yang berisi ringkasan informasi serta akses menuju menu pengelolaan data, seperti dokumen arsip dan kelola user dan profil. Seperti yang ditunjukkan pada gambar berikut:



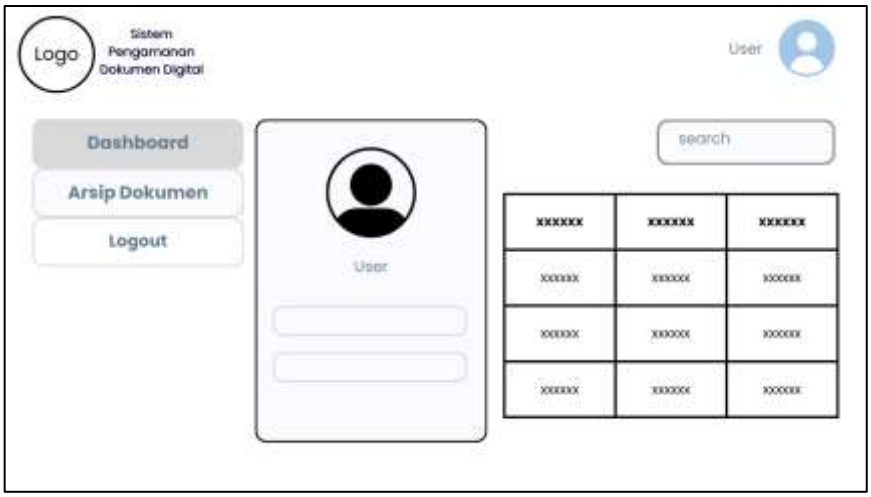
Gambar 3. 24 Desain Halaman Dashboard pada Admin

Menampilkan halaman utama setelah user masuk berhasil login yang menampilkan informasi serta akses ke menu yang dapat digunakan sesuai kebutuhan. Seperti yang ditunjukkan pada gambar berikut:



Gambar 3. 25 Desain Halaman Dashboard pada Keuangan

Menampilkan halaman utama setelah user masuk berhasil login yang menampilkan informasi serta akses ke menu yang dapat digunakan sesuai kebutuhan. Seperti yang ditunjukkan pada gambar berikut:

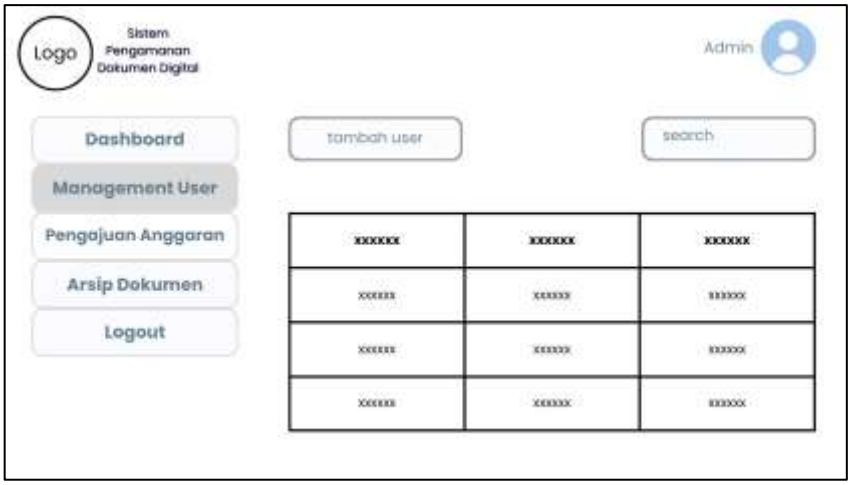


Gambar 3. 26 Desain Halaman Dashboard pada User

3.5.3 Desain Halaman Management User

Halaman management user merupakan tampilan yang digunakan admin untuk mengatur data pengguna di dalam sistem. Pada bagian ini admin dapat melihat daftar pengguna yang terdaftar, menambah data baru, serta memperbarui

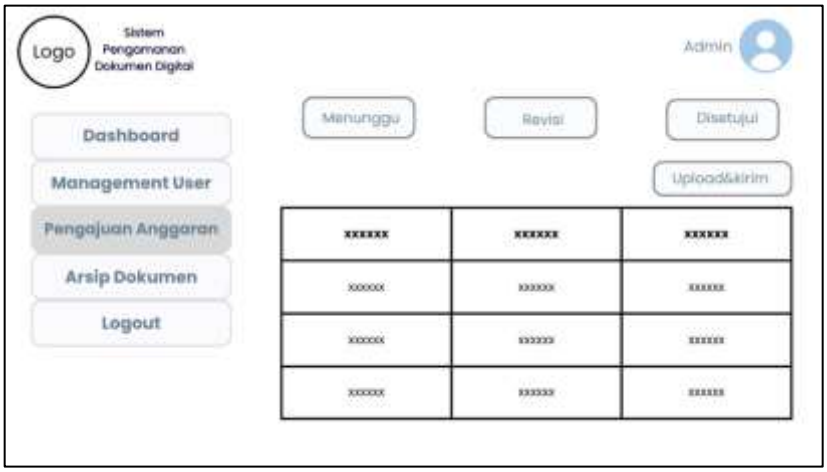
atau menghapus informasi pengguna sesuai kebutuhan. Seperti yang ditunjukkan pada gambar berikut:



Gambar 3. 27 Desain Halaman Management User pada Admin

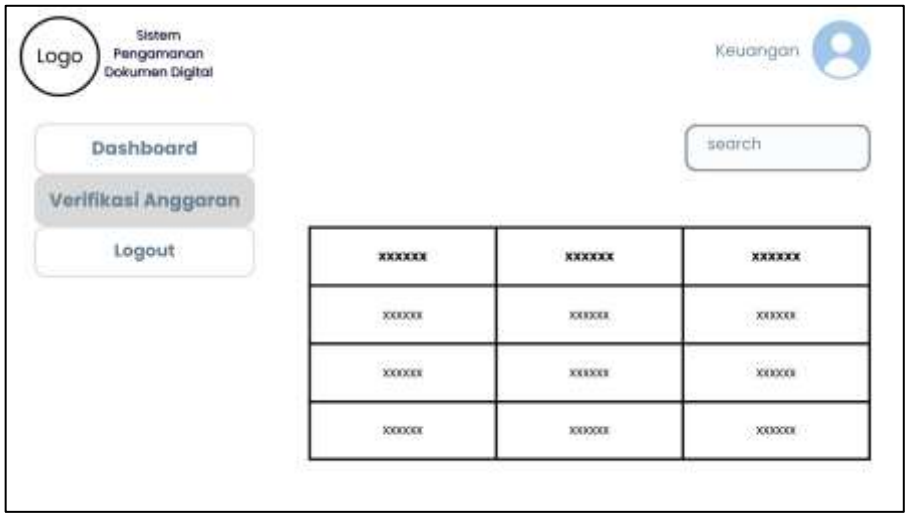
3.5.4 Desain Halaman Pengajuan & Verifikasi Anggaran

Halaman Pengajuan Anggaran merupakan tampilan yang digunakan admin untuk melakukan pengajuan anggaran. Pada bagian ini, admin dapat melihat daftar dokumen pengajuan, mengunggah dokumen penawaran, mengunci file, serta mengirimkan pengajuan ke bagian keuangan untuk diproses lebih lanjut. Seperti yang ditunjukkan pada gambar berikut :



Gambar 3. 28 Desain Halaman Pengajuan Anggaran pada Admin

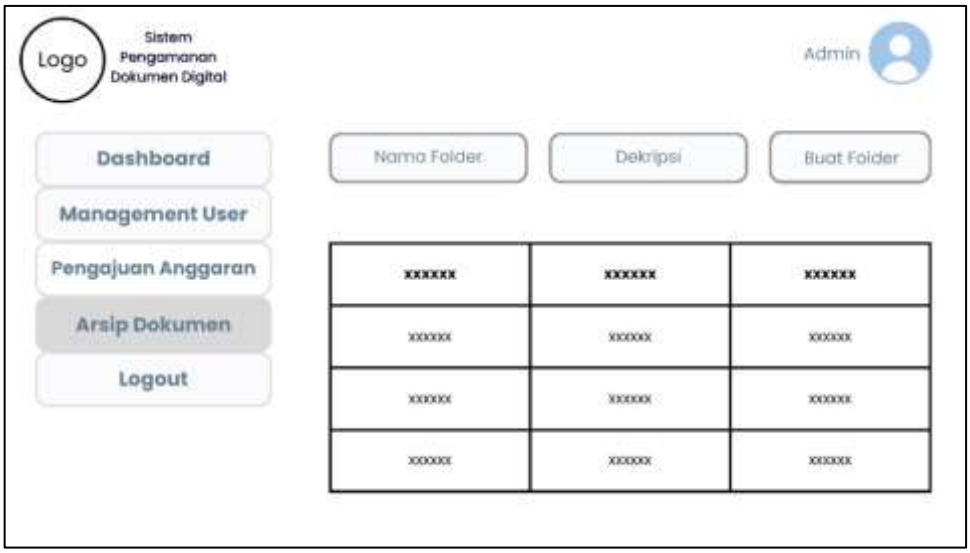
Halaman Verifikasi anggaran merupakan tampilan yang digunakan oleh bagian keuangan untuk memeriksa pengajuan anggaran yang telah dikirim oleh admin. Pada halaman ini, bagian keuangan dapat melihat daftar pengajuaan, membuka dokumen penawaran, serta melakukan pengecekan isi dokumen sebelum memberikan keputusan berupa persetujuan atau revisi. Seperti yang ditunjukkan pada gambar berikut :



Gambar 3. 29 Desain Halaman Verifikasi Anggaran pada Keuangan

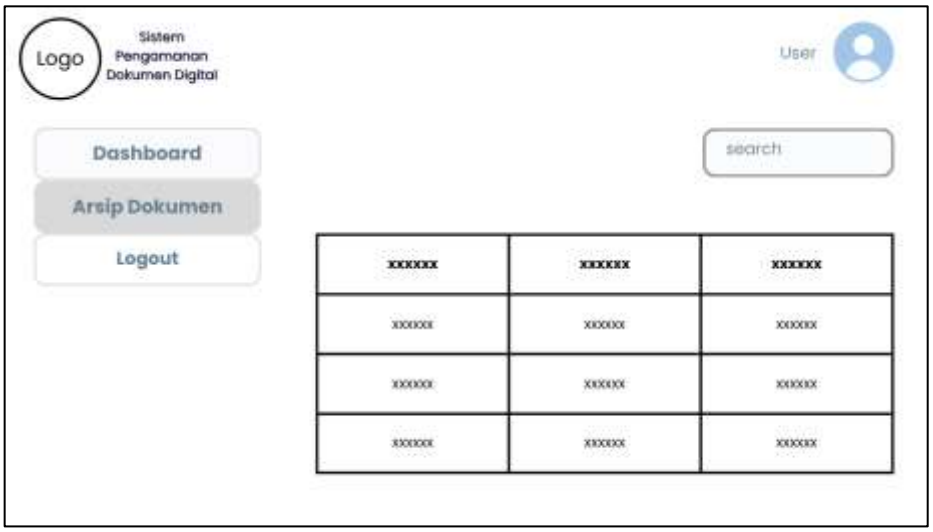
3.5.5 Desain Halaman Arsip Dokumen

Halaman arsip dokumen pada admin menampilkan daftar berkas yang dapat dilihat oleh admin setelah masuk ke sistem. Pada tampilan ini, admin dapat membuat folder, mengunggah dokumen, mengunci dokumen, melihat daftar dokumen, mengunduh, menghapus dokumen dan melakukan pencarian file sesuai kebutuhan. Seperti yang ditunjukkan pada gambar berikut.



Gambar 3. 30 Desain Halaman Arsip Dokumen pada Admin

Halaman arsip dokumen pada user menampilkan daftar berkas yang dapat dilihat oleh user setelah masuk ke sistem. Pada tampilan ini, user dapat melihat isi dokumen sesuai hak akses user. Seperti yang ditunjukkan pada gambar berikut :



Gambar 3. 31 Desain Halaman Arsip Dokumen User

3.6 Perhitungan Manual AES 128

AES merupakan algoritma block cipher yang memproses data dalam blok 128 bit berbentuk matriks 4x4 *byte*. Proses enkripsi dilakukan melalui tahapan *AddRoundkey*, *SubBytes*, *ShiftRows*, dan *MixColumns* yang diulang dalam

beberapa ronde, dengan ronde terakhhir tanpa *MixColumns*. Pada tahap ini dilakukan simulasi perhitungan manual prosses enkripsi AES menggunakan contoh plaintext dan kunci.

Plaintext: UMSUUNGGULCERDAS

Chiperkey: AKUSEMANGATLULUS

Langkah pertama yang dilakukan adalah mengubah *plaintext* dan kunci ke dalam bentuk blok 4x4 dan mengubah ke dalam bentuk heksadesimal.

Plaintext =

U	U	U	R
M	N	L	D
S	G	C	A
U	G	E	S

=

55	55	55	52
4D	4E	4C	44
53	47	43	41
55	47	45	53

Chiperkey =

A	E	G	U
K	M	A	L
U	A	T	U
S	N	L	S

=

41	45	47	55
4B	4D	41	4C
55	41	54	55
53	4E	4C	53

3.6.1 Penjadwalan Kunci

Langkah kedua adalah menghitung key schedule, yang hasilnya digunakan sebagai dasar pada tahap enkripsi berikutnya.

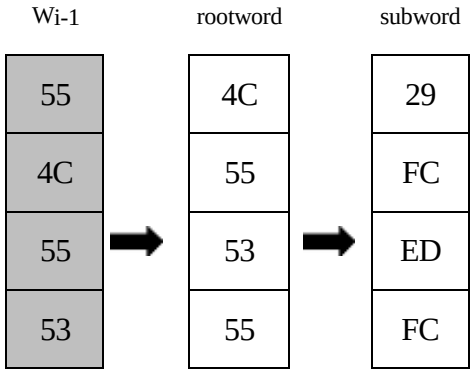
Tabel 3. 1 S-box

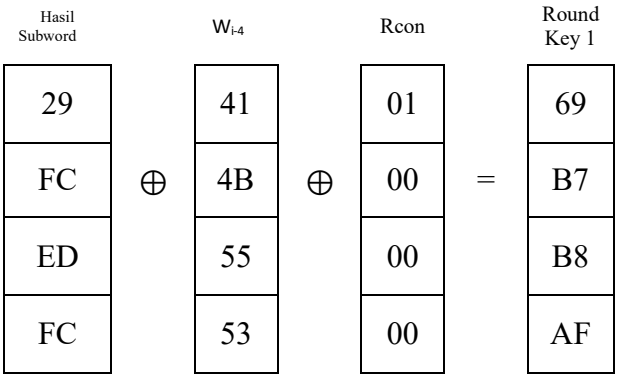
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tabel 3. 2 Rcon

THE CONTENT OF THE RCON[ROUND]

Round	1	2	3	4	5	6	7	8	9	10
Rcon[]	01	02	04	08	10	20	40	80	1b	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00





Proses pencarian nilai sebagai berikut dan lakukan pada setiap baris

29 = 0 0 1 0 1 0 0 1

41 = 0 1 0 0 0 0 0 1

01 = 0 0 0 0 0 0 0 1 ⊕

---

69 = 0 1 1 0 1 0 0 1

W_{i-1}		W_{i-4}		W_i
69		45		2C
B7		4D		FA
B8	⊕	41	=	F9
AF		4E		E1

69 = 0 1 1 0 1 0 0 1

45 = 0 1 0 0 0 1 0 1 ⊕

2C= 0 0 1 0 1 1 0 0

W_{i-1}		W_{i-4}		W_i
2C		47		6B
FA		41		BB
F9	⊕	54	=	AD
E1		4C		AD

2C = 0 0 1 0 1 1 0 0

47 = 0 1 0 0 0 1 1 1 ⊕

6B= 0 1 1 0 1 0 1 1

W_{i-1}		W_{i-4}		W_i
6B		55		3E
BB		4C		F7
AD	⊕	55	=	F8
AD		53		FE

6B = 0 1 1 0 1 0 1 1

55 = 0 1 0 1 0 1 0 1 ⊕

3E= 0 0 1 1 1 1 1 0

Ketika semua langkah diulang-ulang sampai banyaknya putaran, maka akan menghasilkan skedul kunci sebagai berikut:

41	45	47	55
4B	4D	41	4C
55	41	54	55
53	4E	4C	53

Ronde 0

69	2C	6B	3E
B7	FA	BB	F7
B8	F9	AD	F8
AF	E1	AD	FE

Ronde 1

03	2F	44	7A
F6	0C	B7	40
03	FA	57	AF
1D	FC	51	AF

Ronde 2

0E	21	65	1F
8F	83	34	74
7A	80	D7	78
C7	3B	6A	C5

Ronde 3

94	B5	D0	CF
33	B0	84	F0
DC	5C	8B	F3
07	3C	56	93

Ronde 4

08	BD	6D	A2
3E	8E	0A	FA
00	5C	D7	24
8D	B1	E7	74

Ronde 5

05	B8	D5	77
08	86	8C	76
92	CE	19	3D
B7	06	E1	95

Ronde 6

7D	C5	10	67
2F	A9	25	53
B8	76	6F	52
42	44	A5	30

Ronde 7

10	D5	C5	A2
2F	86	A3	F0
BC	CA	A5	F7
C7	83	26	16

Ronde 8

87	52	97	35
47	C1	62	92
FB	31	94	63
FD	7E	58	4E

Ronde 9

FE	AC	3B	0E
BC	7D	1F	8D
D4	E5	71	12
6B	15	4D	03

Ronde 10

3.6.2 Initial Round

Langkah ketiga merupakan proses enkripsi menggunakan algoritma kriptografi Advanced Encryption Standard. Dalam proses ini terdapat beberapa langkah transformasi yang dilakukan secara bertahap, yaitu sebagai berikut:

Melakukan transformasi *AddRoundKey* dengan cara melakukan operasi XOR antara *plaintext* dengan *cipherkey* seperti contoh berikut ini :

55	55	55	52	⊕	41	45	47	55	=	14	10	12	07
4D	4E	4C	44		4B	4D	41	4C		06	03	0D	08
53	47	43	41		55	41	54	55		06	06	17	14
55	47	45	53		53	4E	4C	53		06	09	09	00
Plaintext					*Cipherkey*					Initial Round			

Proses perhitungan nilai *AddRoundKey* dilakukan dengan melakukan operasi pada setiap baris dan kolom yang sama

55 = 0 1 0 1 0 1 0 1
41 = 0 1 0 0 0 0 0 1 ⊕

14 = 0 0 0 1 0 1 0 0

3.6.3 Round 1 Sampai 9

1. *SubBytes*

   Tahap selanjutnya pada round 1 dilakukan proses transformasi *SubBytes* dengan cara melakukan operasi substitusi tak linear yang beroperasi secara mandiri pada setiap *byte* dengan menggunakan tabel S-box seperti contoh berikut:

14	10	12	07
06	03	0D	08
06	06	17	14
06	09	09	00

FA	CA	C9	C5
6F	7B	D7	30
6F	6F	F0	FA
6F	01	01	63

2. ShifRows

Tahap selanjutnya adalah transformasi *ShiftRows*, yaitu proses pergeseran *byte* pada setiap baris state secara melingkar. Baris pertama tidak mengalami pergeseran, sementara baris lainnya digeser ke kiri sesuai dengan aturan pada algoritma AES, seperti ditunjukkan pada contoh berikut.

FA	CA	C9	C5
6F	7B	D7	30
6F	6F	F0	FA
6F	01	01	63

Tidak mengalami Pergeseran

Digeser 1 *byte* ke kiri.

Digeser 2 *byte* ke kiri.

Digeser 3 *byte* ke kiri.

FA	CA	C9	C5
7B	D7	30	6F
F0	FA	6F	6F
63	6F	01	01
After ShiftRows			

3. MixColumns

Tahap selanjutnya adalah transformasi *MixColumns*, yaitu proses yang bekerja pada setiap kolom state dengan menganggap setiap kolom sebagai polinomial. Proses transformasi ini digambarkan melalui operasi matriks seperti pada contoh berikut.

2	3	1	1		FA	CA	C9	C5		F1	78	B7	4E
1	2	3	1	x	7B	D7	30	6F	=	64	05	19	AB
1	1	2	3		F0	FA	6F	6F		DF	43	24	77
3	1	1	2		63	6F	01	01		58	B6	1D	56
					Hasil Shiftrows					Hasil Mixcolumns			

Nilai F1 pada proses *MixColumns* diperoleh dari hasil perkalian setiap elemen dengan konstanta matriks, yaitu (02 x FA) ⊕ (03 x 7B) ⊕ (01 x F0) ⊕ (01 x 63), kemudian dijumlahkan menggunakan operasi XOR, proses pencarian MixColumn sebagai berikut :

(02 FA) ⊕ (03 x 7B) ⊕ (01 x F0) ⊕ (01 x 63)

a. (02 x FA) = $x+(x^7 + x^6 + x^5 + x^4 + x^3 + x^1)$

$= x^8 + x^7 + x^6 + x^5 + x^4 + x^2$

$= \cancel{x^4} + x^3 + x^1 + x^0 + x^7 + x^6 + x^5 + \cancel{x^4} + x^2$

= 1110 1111 (EF)

b. (03 x 7B) = (02 x 7B) ⊕ (01 x 7B)

(02 x 7B) = $x+(x^6 + x^5 + x^4 + x^3 + x^1 + x^0)$

$= x^7 + x^6 + x^5 + x^4 + x^2 + x^1$

= 1111 0110 (F6)

0111 1011 (7B) ⊕

= 1000 1101 (8D)

c. (01 x F0) = $x^7 + x^6 + x^5 + x^4$

= 1111 00000 (F0)

d. (01 x 63) = $x^6 + x^5 + x^1 + x^0$

= 0110 0011 (63)

EF = 1 1 1 0 1 1 1 1

8D = 1 0 0 0 1 1 0 1 ⊕

= 0 1 1 0 0 0 1 0

F0 = 1 1 1 1 0 0 0 0 ⊕

= 1 0 0 1 0 0 1 0

63 = 0 1 1 0 0 0 1 1 ⊕

F1 = 1 1 1 1 0 0 0 1

4. AddRoundKey

Tahap selanjutnya adalah *AddRoundKey*, yaitu proses menggabungkan hasil *MixColumns* dengan kunci ronde (round key) menggunakann operasi XOR. Pada tahap ini, setiap elemen hasil *MixColumns* diXOR kan dengan elemen kunci yang sesuai sehingga menghasilkan state baru.

F1	78	B7	4E		69	2C	6B	3E		98	54	DC	70
64	05	19	AB	x	B7	FA	BB	F7	=	D3	FF	A2	5C
DF	43	24	77		B8	F9	AD	F8		67	BA	89	8F
58	B6	1D	56		AF	E1	AD	FE		F7	57	B0	A8
Hasil Mixcolumns					Round Key 1					Hasil			

F1 = 1 1 1 1 0 0 0 1

69 = 0 1 1 0 1 0 0 1 ⊕

98= 1 0 0 1 1 0 0 0

Selanjutnya proses dilanjutkan ke round 2 sampai round 9 dengan tahapan yang sama, dengan hasil sebagai berikut

a. Round 2

46	20	86	51
66	16	3A	4A
85	F4	A7	73
68	5B	E7	C2
After Sub*Byte*s			

46	20	86	51
16	3A	4A	66
A7	73	85	F4
C2	68	5B	E7
After Shiftrows			

D3	15	17	1B
5A	A9	DD	7D
58	44	30	F6
E4	F9	E8	B4
After MixColumns			

D0	3A	53	61
AC	A5	6A	3D
5B	BE	67	59
F9	05	B9	1B
After AddRoundKey			

b. Round 3

70	80	ED	EF
91	06	02	27
39	AE	85	CB
99	6B	56	AF
After Sub*Byte*s			

70	80	ED	EF
06	02	27	91
85	CB	39	AE
AF	99	6B	56
After Shiftrows			

30	4F	FA	95
47	5B	83	69
8D	BF	05	C3
56	7B	E4	B9
After MixColumns			

CE	6E	9F	8A
C8	D8	B7	1D
F7	3F	D2	BB
91	40	8E	7C
After AddRoundKey			

c. Round 4

8B	9F	DB	7E
E8	61	A9	A4
68	75	B5	EA
81	09	19	10
After Sub*Byte*s			

8B	9F	DB	7E
61	A9	A4	E8
B5	EA	68	75
10	81	09	19
After Shiftrows			

0B	AE	3B	B3
9D	72	39	33
AB	61	B4	57
72	E0	A8	2D
After MixColumns			

9F	1B	EB	7C
AE	C2	BD	C3
77	3D	3F	A4
75	DC	FE	BE
After AddRoundKey			

d. Round 5

DB	AF	E9	10
E4	25	7A	2E
F5	27	75	49
9D	86	BB	AE
After Sub*Byte*s			

DB	AF	E9	10
25	7A	2E	E4
75	49	F5	27
AE	9D	86	BB
After Shiftrows			

19	1F	C8	8B
A0	1D	37	11
FD	FB	A7	6C
61	F8	EC	9E
After MixColumns			

11	A2	A5	29
9E	93	3D	EB
FD	A7	70	48
EC	49	0B	EA
After AddRoundKey			

e. Round 6

82	3A	06	A5
0B	DC	27	E9
54	5C	51	52
CE	3B	2B	87
After Sub*Byte*s			

82	3A	06	A5
DC	27	E9	0B
51	52	54	5C
87	CE	3B	2B
After Shiftrows			

B6	81	43	3B
55	4C	08	7C
6E	F0	0A	6B
05	BC	C1	F5
After MixColumns			

B3	39	96	4C
5D	CA	84	0A
FC	3E	13	56
B2	BA	20	60
After AddRoundKey			

f. Round 7

6D	12	90	29
4C	74	5F	67
B0	B2	7D	B1
37	F4	B7	D0

After Sub*Byte*s

6D	12	90	29
74	5F	67	4C
7D	B1	B0	B2
D0	37	F4	B7

After Shiftrows

EB	43	D6	83
D2	53	61	CB
88	6D	8B	D8
05	B6	8F	F0

After MixColumns

96	86	C6	E4
FD	FA	44	98
30	1B	E4	8A
47	F2	2A	C0

After AddRoundKey

g. Round 8

90	44	B4	69
54	2D	1B	46
04	AF	69	7E
A0	89	E5	BA

After Sub*Byte*s

90	44	B4	69
2D	1B	46	54
69	7E	04	AF
BA	A0	89	E5

After Shiftrows

9F	7B	34	64
CB	50	BD	CE
BA	58	7A	4C
80	F2	8C	91
After MixColumns			

8F	AE	F1	C6
E4	D6	1E	3E
06	92	DF	BB
47	71	AA	87
After AddRoundKey			

h. Round 9

73	E4	A1	B4
69	F6	72	B2
6F	4F	9E	EA
A0	A3	AC	17
After Sub*Byte*s			

73	E4	A1	B4
F6	72	B2	69
9E	EA	6F	4F
17	A0	A3	AC
After Shiftrows			

6E	0F	58	2B
2A	85	CC	1B
9B	A2	33	AC
D3	F4	78	A2
After MixColumns			

E9	5D	CF	1E
6D	44	AE	89
60	93	A7	CF
2E	8A	20	EC
After AddRoundKey			

3.6.4 Final Round

Pada round ke-10 sebagai round terakhir, terdapat sedikit perbedaan pada tahapan proses yang dilakukan, hanya melalui tiga tahapan, yaitu *SubBytes*, *ShiftRows*, dan *AddRoundKey*

1E	4C	8A	72
3C	1B	E4	A7
D0	DC	5C	8A
31	7E	B7	CE
After Sub*Byte*s			

1E	4C	8A	72
1B	E4	A7	3C
5C	8A	D0	DC
CE	31	7E	B7
After Shiftrows			

E0	E0	B1	7C
A7	99	B8	B1
88	6F	A1	CE
A5	24	33	B4
After AddRoundKey			

Final Chipertext : EOA788A5E0996F24B1B8A1337CB1CEB4

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Kebutuhan Sistem

Kebutuhan sistem merupakan hal yang paling penting untuk diperhatikan agar sistem yang dikembangkan dapat berjalan dengan baik dan optimal. Pada tahap ini dilakukan pengidentifikasian seluruh kebutuhan yang mendukung proses implementasi sistem, baik dari sisi perangkat keras (hardware) maupun perangkat lunaak (software). Penyusunan kebutuhan ini bertujuan untuk memastikan bahwa sistem pengamanan arsip dokumen digital berbasis web dengan pengamanan data menggunakan algoritma AES-128 dapat beroperasi secara efektif, efisien, dan tetap stabil saat digunakan

4.1.1 Kebutuhan Perangkat Keras (Hardware)

Perangkat keras yang digunakan dalam penelitian ini adalah sebuah laptop dengan spesifikasi sebagai berikut:

a. Prossesor: intel Core i5
b. RAM: 8GB
c. Penyimpanan: 256 GB
d. Kartu Grafis: NVIDIA GeForce GTX 1650
e. Layar: 15,6 inci Full HD
f. Sistem Operasi: Windows

4.1.2 Kebutuhan Perangkat Lunak (Software)

Perangkat lunak yang digunakan dalam pengembangan dan pengujian sistem pengamanan arsip dokumen digital adalah sebagai berikut:

a. Visual Studio Code
b. XAMPP
c. MySQL
d. PHP
e. HTML
f. Google Chrome

4.2 Implementasi Sistem

Implementasi sistem merupakan tahapan lanjutan dari proses perancangan yang bertujuan untuk merealisasikan sistem ke dalam bentuk aplikasi yang dapat digunakan secara langsung. Pada tahap ini, sistem dibangun berdasarkan kebutuhan yang telah ditentukan sebelumnya, dengan fokus utama pada pengamanan arsip dokumen digital. Seluruh fungsi yang dirancang diimplementasikan agar dapat berjalan sesuai dengan kebutuhan pengguna, sehingga sistem mampu memberikan kinerja yang optimal dalam menjaga keamanan data.

Sistem yang dikembangkan merupakan sistem pengamanan arsip dokumen digital dengan menerapkan algoritma AES-128 sebagai metode perlindungan data. Proses enkripsi dilakukan saat dokumen dikirim kebagian keuangan dan saat dokumen disimpan ke dalam sistem sehingga data tersimpan dalam benruk yang tidak dapat dibaca secara langsung, sedangkan proses dekripsi dilakukan ketika dokumen diakses oleh pihak yang berwenang. Implementasi sistem mencakup pembuatan tampilan antarmuka, pembangunan fitur pengelolaan arsip, serta intergrasi dengan database.

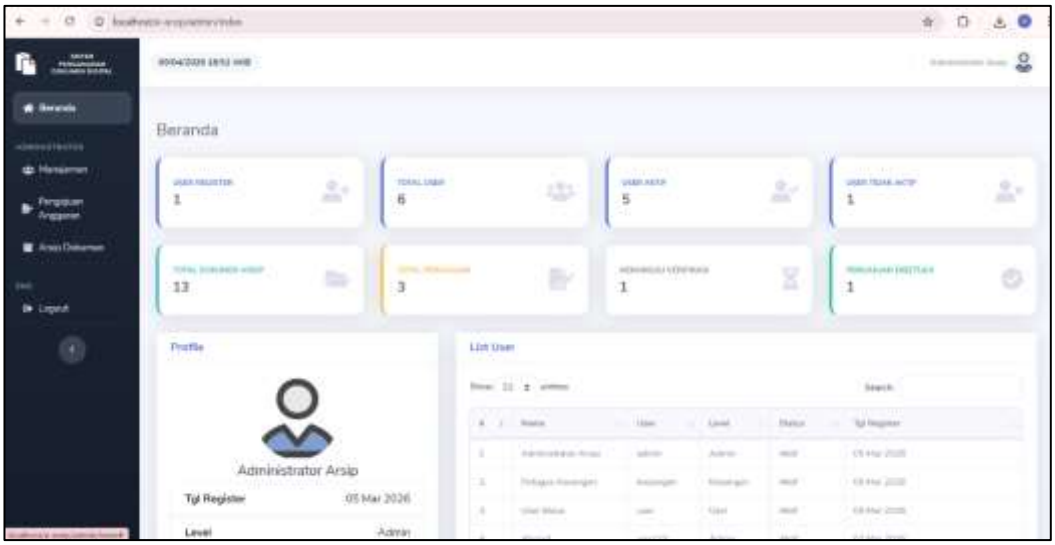
4.2.1 Halaman Login

Halaman login merupakan tampilan awal yang digunakan oleh pengguna untuk masuk ke dalam sistem. Pada halaman ini, pengguna diminta untuk memasukan username dan password yang telah terdaftar. Sistem akan melakukan proses validasi terhadap data yang dimasukkan. Jika data yang dimasukkan benar, maka pengguna akan diarahkan ke halaman utama sesuai dengan hak aksesnya. Sebaliknya, jika data tidak sesuai, maka sistem akan menampilkan pesan kesalahan.

Gambar 4. 1 Halaman Login

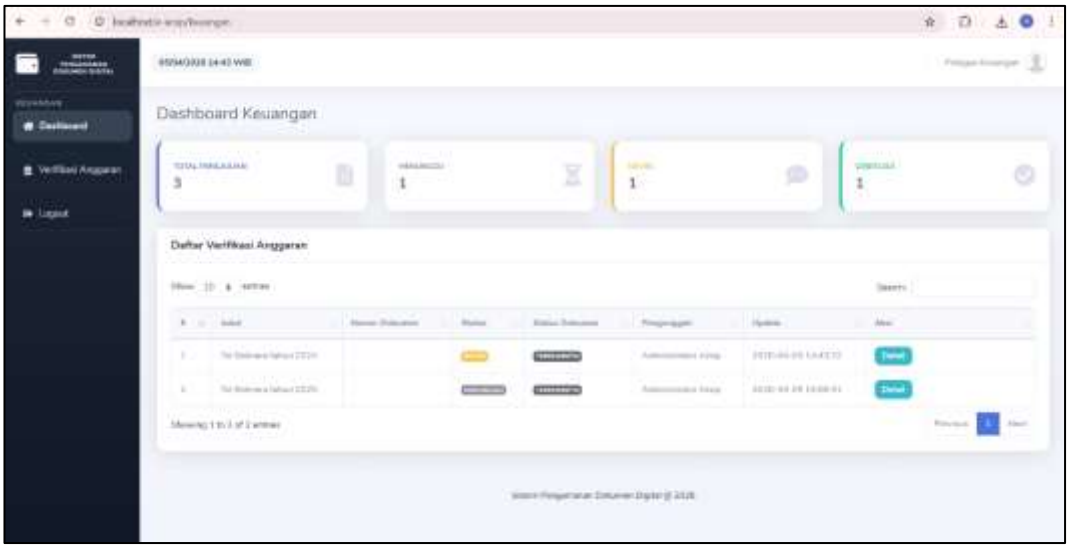
4.2.2 Halaman Dashboard

Halaman dashboard merupakan halaman utama yang ditampilkan setelah pengguna berhasil melakukan prosses login ke dalam sistem. Halaman ini berfungsi sebagai pusat navigasi yang menyediakan berbagai menu dan fitur sesuai dengan hak akses masing-masing pengguna. Pada sistem ini, halaman dashboard dibagi menjadi bebarapa jenis berdasarkan peran pengguna, yaitu admin, keuangan dan user. Perbedaan peran ini bertujuan untuk membatasi akses serta menjaga keamanaan dan pengelolaan data agar lebih terstruktur.



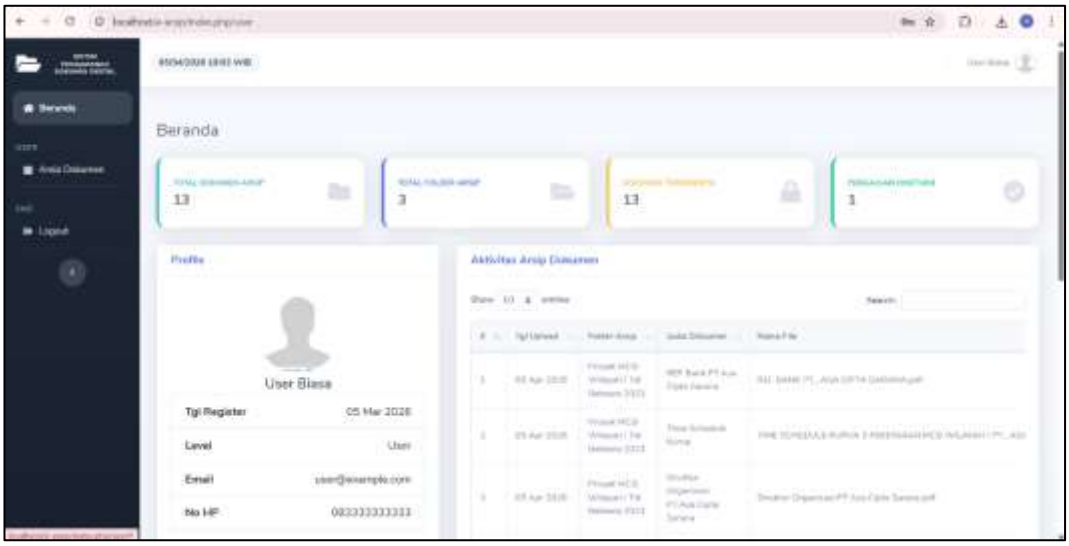
Gambar 4. 2 Halaman Dashboard Admin

Dashboard admin merupakan halaman utama dengan akses penuh terhadap seluruh fitur sistem yang berperan dalam pengelolaaan dan pengendalian secara menyeluruh. Melalui dashboard ini, admin dapat mengelola data pengguna seperti menambah, mengubah dan menghapus user. Admin dapat melihat seluruh data dokumen yang tersimpan dalam sistem dan memiliki kewenangan untuk mengenkripsi dan mendekripsi dokumen untuk menjaga keamanan data. Selain itu, Admin juga melakukan pengajuan anggaran dan menunggu proses verifikasi sebelum diproses lebih lanjut, serta memantau seluruh aktivitas sistem.



Gambar 4. 3 Halaman Dashboard Keuangan

Dashboard keuangan merupakan halaman bagi pengguna dengan peran keuangan yang memiliki akses terbatas. Pada halaman ini, keuangan dapat membuka dokumen untuk ditindaklannjuti, melakukan verifikasi terhadap pengajuan anggaran dari admin, serta memberikan komentar atau catataan apabila diperlukan revisi. Dengan demikian, proses pengelolaan dokumen dan anggaran dapat berjalan secara terarah dan sesuai dengan tugas yang telah diberikan.

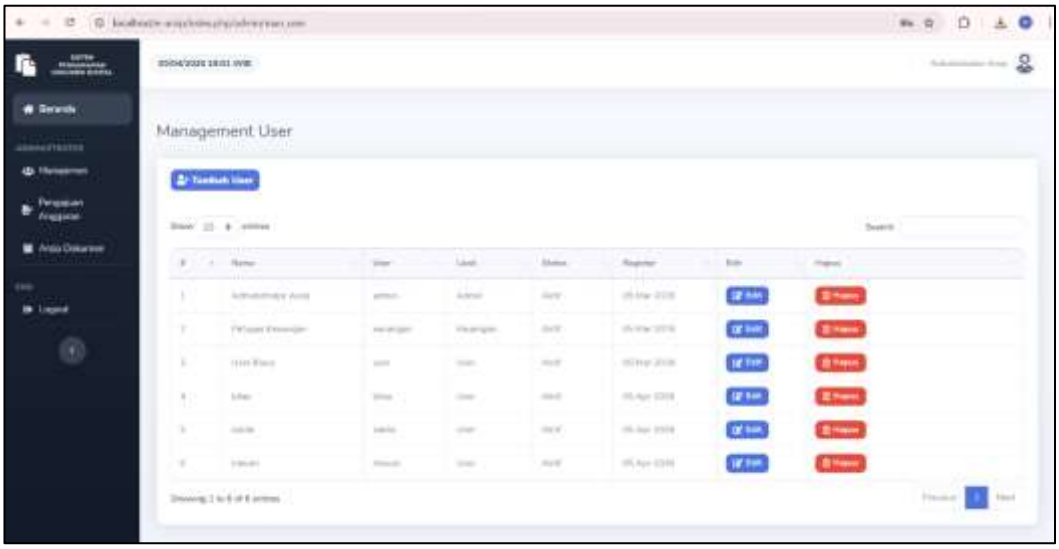


Gambar 4. 4 Halaman Dashboard User

Dashboard User merupakan halaman yang diperuntukkan bagi pengguna umum dengan akses yang sangat terbatas. Pada halaman ini, pengguna hanya dapat melihat daftar arsip dokumen yang memiliki status terbuka, tanpa memiliki hak untuk menambah, mengubah, mengunduh, maupun menghapus data. Dengan pembatasan tersebut, sistem dapat menjaga keamanan dan keteraturan data sesuai dengan peran pengguna.

4.2.3 Halaman Management User

Halaman Management User merupakan fitur yang digunakan oleh admin untuk mengelola data pengguna dalam sistem. Pada halaman ini, admin dapat menambahkan, mengubah, dan menghapus data user sesuai dengan kebutuhan. Selain itu, admin juga dapat mengatur peran (role) pengguna seperti admin, keuangan dan user agar hak akses setiap pengguna sesuai dengan fungsinya.

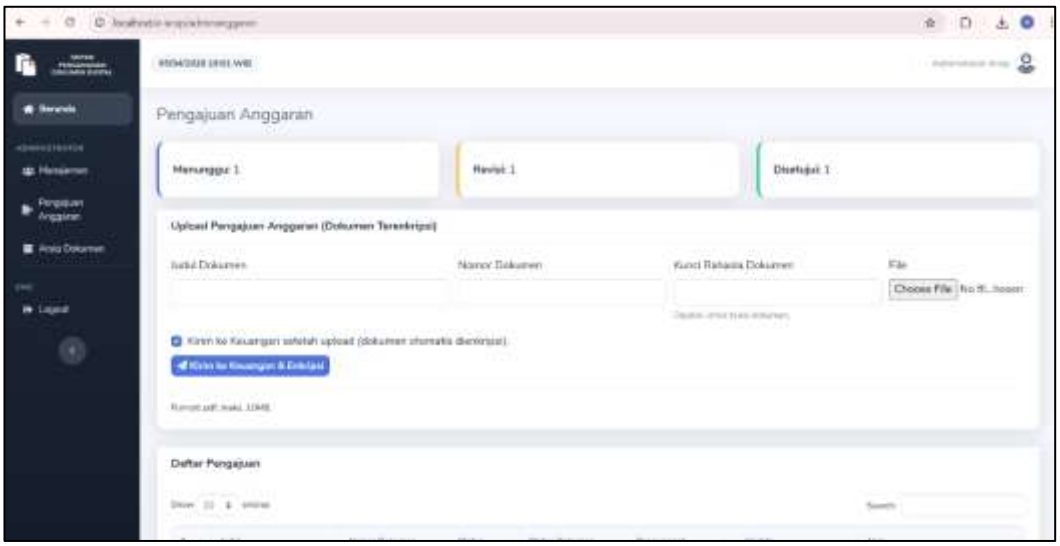


Gambar 4. 5 Halaman Management User

4.2.4 Halaman Pengajuan Anggaran

Halaman Pengajuan Anggaran merupakan fitur yang digunakan oleh admin untuk mengajukan anggaran yang akan diproses dalam sistem. Pada

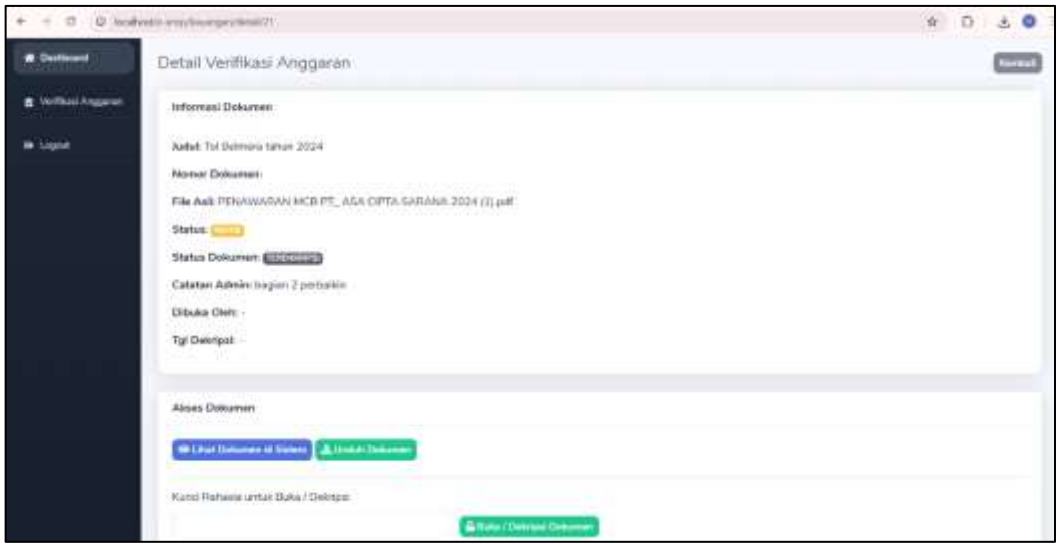
halaman ini, admin dapat mengupload data pengajuan seperti rincian anggaran, jumlah dana, serta keterangan pendukung lainnya. Setelah pengajuan dikirim, data akan diteruskan ke bagian keuangan untuk dilakukan proses verifikasi.



Gambar 4. 6 Halaman Pengajuan Anggaran

4.2.5 Halaman Verifikasi Anggaran

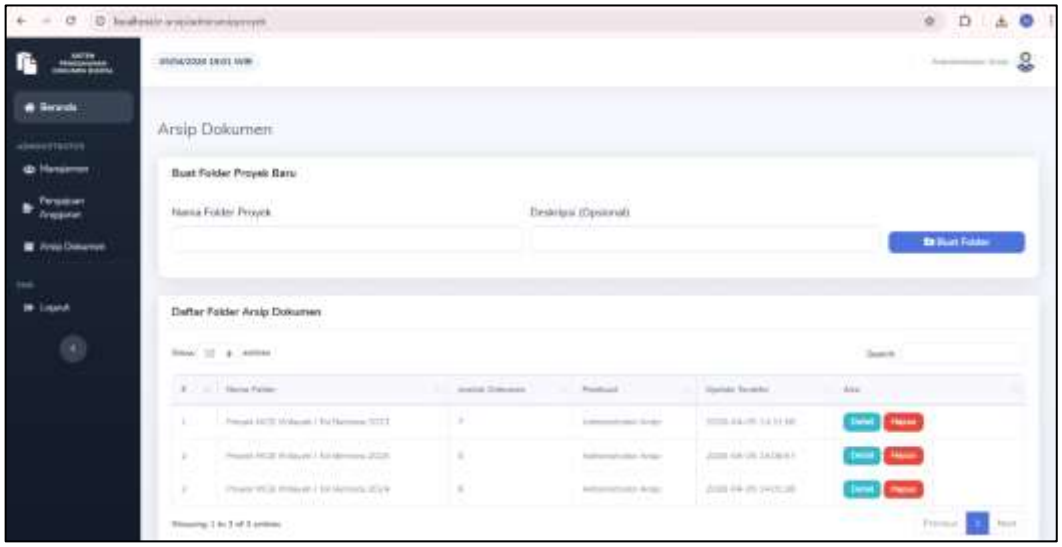
Halaman Verifikasi Anggaran merupakan fitur yang digunakan oleh bagian keuangan untuk memeriksa dan mindaklanjuti pengajuan anggaran yang diajukan oleh admin. Pada halaman ini, keuangan dapat melihat detail pengajuan, melakukan pengecekan, serta menentukan apakah pengajuan disetujui atau perlu direvisi. Selain itu, keuangan juga dapat memberikan catatan atau komentar sebagai bahan perbaikan.



Gambar 4. 7 Halaman Verifikasi Anggaran

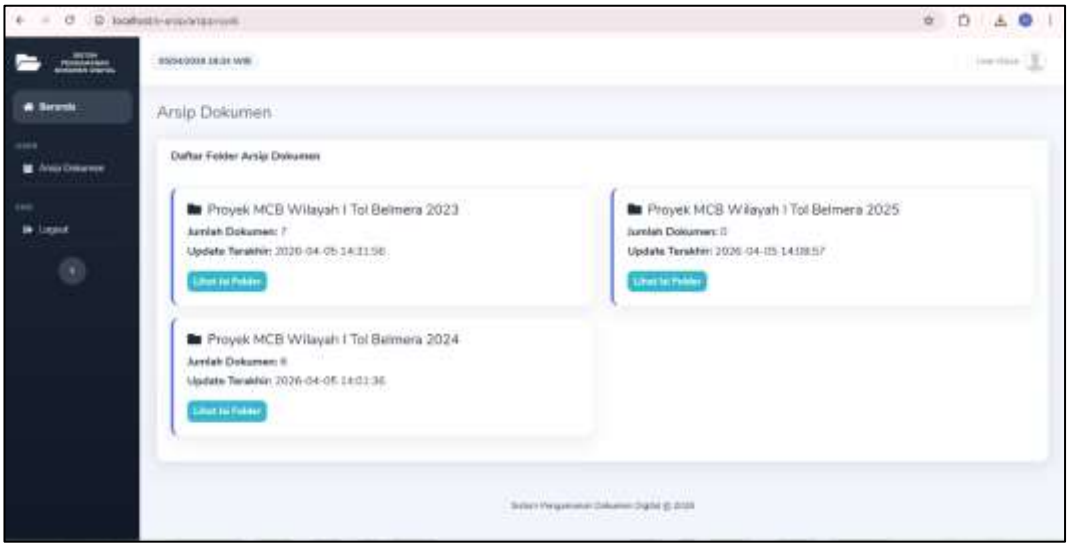
4.2.6 Halaman Arsip Dokumen

Halaman Arsip Dokumen merupakan fitur yang digunakan untuk menyimpan dan menampilkan seluruh dokumen yang telah diproses dalam sistem, baik dokumen yang telah dienkripsi maupun yang masih dalam bentuk asli. Halaman ini berfungsi sebagai pusat penyimpanan data sehingga memudahkan pengguna dalam mencari, melihat, dan mengelola dokumen sesuai kebutuhan.



Gambar 4. 8 Halaman Arsip Dokumen Admin

Halaman Arsip Dokumen Admin memiliki akses penuh dalam pengelolaan dokumen. Admin dapat membuat folder baru, menambahkan dokumen, serta melakukan proses enkripsi dan dekripsi. Selain itu, admin juga dapat melihat, menghapus, dan mengunduh dokumen sesuai dengan kebutuhan.



Gambar 4. 9 Halaman Arsip Dokumen User

Sementara itu, Halaman Arsip Dokumen User memiliki hak akses terbatas yaitu dapat melihat daftar dokumen dengan status dekripsi. User tidak dapat menambahkan, mengubah, maupun menghapus dokumen, sehingga keamanan dan keteraturan data tetap terjaga sesuai dengan hak akses yang diberikan.

4.2.7 Implementasi Enkripsi Dokumen

Implementasi enkripsi dokumen pada sistem ini ditunjukkan melalui perbandingan data sebelum dan sesudah dilakukan proses enkripsi menggunakan algoritma AES-128. Perbandingan ini bertujuan untuk melihat perubahan bentuk sebagai upaya pengamanan dokumen. Pada tahap ini, dokumen yang awalnya masih dalam bentuk asli (*plaintext*) dan dapat dibaca dengan jelas diproses

menggunakan algoritma AES-128 sehinngga berubah menjadi bentuk yang tidak dapat dipahami, untuk menjaga kerahasiaan data yang tersimpan dalam sistem.

Gambar 4. 10 Dokumen Sebelum Enkripsi

Berdasarkan gambar tersebut, terlihat bahwa isi dokumen masi berupa data asli yang dapat dipahami oleh pengguna tanpa adanya proses pengamanan. Selanjutnya, dokumen tersebut diproses menggunakan algoritma AES-128 sehingga menghasilkan dokumen dalam bentuk terenkripsi (*ciphertext*)

Gambar 4. 11 Gambar Setelah Enkripsi

Pada gambar tersebut, terlihat bahwa isi dokumen telah berubah menjadi karakter acak yang tidak dapat dibaca. Hal ini menunjukkan bahwa proses

enkripsi telah berhasil dilakukan dan mampu melindungi data dari akses yang tidak berwenang.

4.3 Pengujian Sistem

Proses pengujian sistem merupakan tahap penting dalam pengembangan sistem pengamanan dokumen yang bertujuan untuk menilai kesesuaian antara rancangan sistem dengan hasil implementasi yang telah dibangun. Pengujian sistem dilakukan untuk memastikan seluruh fitur yang telah dibuat dapat berjalan dengan baik sesuai dengan kebutuhan.

Pada tahap ini, dilakukan pengujian terhadap setiap fitur dalam sistem, seperti proses login, pengelolaan data pengguna, pengajuan dan verifikasi anggaran, serta pengelolaan dokumen termasuk enkripsi dan dekripsi. Pengajuan dilakukan dengan memberikan berbagai kondisi input untuk melihat respons sistem dan kesesuaian output yang dihasilkan. Selain itu, pengujian juga bertujuan untuk menemukan kemungkinan kesalahan atau kekurangan sehingga dapat dilakukan perbaikan agar sistem dapat berjalan secara optimal, aman, dan sesuai dengan alur yang telah dirancang

NO	Fitur	Skenario Pengujian	Aktor	Output Yang Diharapkan	Hasil
1	Login	Pengguna input username dan password valid	Semua Pengguna	Masuk ke dashboard sesuai role	Berhasil
2	Login Gagal	Pengguna input username dan password tidak valid	Semua Pengguna	Muncul notifikasi gagal login	Berhasil
3	Login Field	Pengguna tidak mengisi username dan password	Semua Pengguna	Sistem menolak proses login	Berhasil

4	Tambah User	Input data user baru	Admin	Data user berhasil ditambahkan	Berhasil
5	Edit User	Mengubah data user	Admin	Data User diperbarui	Berhasil
6	Hapus User	Menghapus User	Admin	Data user terhapus	Berhasil
7	Buat Folder	Menginput nama folder	Admin	Folder berhasil dibuat	Berhasil
8	Upload Dokumen	Menginput Dokumen	Admin	Dokumen tersimpan di sistem	Berhasil
9	Enkripsi	Menginput kunci enkripsi	Admin & keuangan	Dokumen terenkripsi	Berhasil
10	Dekripsi	Menginput kunci dekripsi	Admin & keuangan	Dokumen kembali kebentuk asli	Berhasil
11	Pengajuan Anggaran	Mengajukan anggaran dan kirim kebagian keuangan	Admin	Data tersimpan dengan status menunggu verifikasi	Berhasil
12	Verifikasi Anggaran	Keuangan memverifikasi pengajuan	Keuangan	Status berubah disetujui/revisi	Berhasil
13	Revisi	Keuangan memberikan komentar	Keuangan	Status revisi dan komentar tersimpan	Berhasil
14	Setujui	Keuangan menyetujui anggaran	Keuangan	Status menjadi disetujui	Berhasil
15	Buat folder	Menginput nama folder	Admin	Folder tersimpan	Berhasil
16	Rename	Mengubah nama Folder	Admin	Nama Folder berubah	Berhasil
16	Hapus dokumen	Klik menu hapus	Admin	Dokumen terhapus	Berhasil
17	Unduh dokumen	Klik menu unduh	Admin	Dokumen berhasil terunduh	Berhasil
18	Lihat dokumen	Klik menu lihat	Admin & User	Dokumen berhasil terbuka	Berhasil
19	Logout	Klik menu logout	Semua Pengguna	Keluar dari sistem	Berhasil

4.4 Analisis Hasil

Berdasarkan hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa sistem pengamanan dokumen yang dibangun sudah berjalan dengan baik sesuai dengan fungsi yang dirancang. Setiap fitur dalam sistem, seprti login, pengelolaan data pengguna, pengajuan dan verifikasi anggaran, serta pengelolaan dokumen termasuk proses enkripsi dan dekripsi, mampu memberikan hasil yang sesuai dengan yang diharapkan

Selain itu, sistem juga telah menerapkan pembagian hak akses dengan jelas, dimana admin memiliki kendali penuh terhadap sistem, bagian keuangan bertugas melakukan verifikasi dan menindaklanjuti dokumen, sedangkan user hanya dapat melihat dokumen dengan status tertentu. Pembagian ini menunjukkan bahwa sistem mampu menjaga keamanan sekaligus keteraturan data sesuai dengan peran masing-masing pengguna.

Dari sisi keamanan, penggunaan enkripsi dan dekripsi pada dokumen terbukti dapat melindungi data dari akses yang tidak berwenang. Dokumen yang telah dienkripsi tidak dapat dibaca tanpa proses dekripsi yang sesuai, sehingga kerahasiaannya tetap terjaga. Selain itu, selama proses pengujian, sistem juga menunjukkan kinerja yang stabil tanpa adanya kendala yang berarti. Dengan demikian, sistem yang telah dibangun dapat dikatakan telah memenuhi kebutuhan pengguna dan dapat digunakan untuk membantu pengelolaan dokumen secara lebih aman, terstuktur, dan efektif.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perancangan sistem pengamanan arsip dokumen digital di PT. Asa Cipta Sarana telah berhasil dibangun sesuai dengan kebutuhan pengguna. Sistem yang dikembangkan mampu mengelola dokumen secara terstuktur melalui berbagai fitur seperti pengelolaan pengguna, pengarsipan dokumen, serta proses pengajuan dan verifikasi anggaran, sehingga mendukung pengelolaan data menjadi lebih tertata dan mudah diakses sesuai dengan hak pengguna.

Penerapan algoritma AES-128 dalam sistem telah berhasil diimplementasikan sebagai metode utama dalam pengamanan dokumen. Setiap dokumen yang disimpan dalam sistem akan melalui proses enkripsi sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang. Dokumen tersebut hanya dapat diakses kembali melalui proses dekripsi yang sesuai, sehingga kerahasiaan dan keamanan data dapat terjaga dengan baik.

Selain itu, hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan baik sesuai dengan yang diharapkan. Sistem mampu mengolah data secara stabil tanpa mengalami kesalahan yang signifikan, serta dokumen yang telah dienkripsi dapat dikembalikan ke bentuk semula tanpa perubahan isi. Hal ini menunjukkan bahwa sistem tidak hanya mampu menjaga keamanan, tetapi juga mempertahankan keutuhan data selama proses penyimpanan dan pengambilan dokumen. Dengan demikian, sistem yang

dibangun dapat digunakan sebagai solusi dalam meningkatkan keamanan dan pengelolaan arsip dokumen digital.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan dalam penelitian ini, terdapat beberapa saran yang dapat diberikan sebagai bahan pengembangan selanjutnya:

1. Sistem dapat dikembangkan lebih lanjut difokuskan dengan menambahkan fitur yang lebih beragam dan sesuai dengan kebutuhan pengguna, sehingga dapat meningkatkan kemudahan pengguna serta mendukung pengoperasian sistem secara lebih efektif.
2. Pada pengembangan selanjutnya, sistem diharapkan tidak hanya mendukung dokumen berformat PDF, tetapi juga dapat mengakomodasi berbagai format dokumen digital lainnya seperti doc, docx, dan xls/xlsx, untuk meningkatkan fleksibilitas dalam pengelolaan dan penyimpanan arsip
3. Pengembangan berikutnya dapat mempertimbangkan penggunaan atau penggabungan algoritma kriptografi lain sebagai alternatif untuk meningkatkan metode pengamanan dokumen.

DAFTAR PUSTAKA

Akbar Ridho, & Moh. Ali Romli. (2024). *SISTEM PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256)*.

Al-Khowarizmi, S. Kom. , M. Kom. (2021). *PENGANTAR TEKNOLOGI INFORMASI (Dalam Perkembangan Data Science)* (M. P. Muhammad Arifin, Ed.; Vol. 280).

Ardiyansa, M., Efitra, & Baharsyah, B. (2025). Perancangan Sistem Informasi Pengarsipan Data Internal Berbasis Web Dengan Fitur Keamanan Enkripsi Di BPSIP Jambi. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(2), 677–686. https://doi.org/10.62712/juktisi.v4i2.504

Dedi Saputra, Weiskhy Steven Dharmawan, Muhammad Syarif, & Deni Risdiansyah. (2023). *Analisis & Perancangan Sistem Informasi*.

Dr. Budi Raharjo, S. K. M. K. MM. (2025). *Pengembangan Web PHP (Hypertext Preprocessor) Language*.

Ferdi Riza, Muhammad Haris, Farid Akbar Siregar, Mahardika Abdi Prawira Tanjung, Andi Zulherry, Zuli Agustina Gultom, Okvi Nugroho, Mhd Basri, Amrullah, Mulkan Azhari, Fatma Sari Hutagalung, & Hevlie Winda Nazry. (2025). *Kriptografi Dan Sekuriti Sistem*.

Kusuma Nugraha, A., Puspita Dewi, Y., Priscila, L., Ciledug Raya, J., Utara, P., Pesanggrahan, K., Jakarta Selatan, K., & Khusus Ibukota Jakarta, D. (2023). *SISTEM PENYIMPANAN DOKUMEN DIGITAL DENGAN ENKRIPSI*

MENGGUNAKAN METODE ALGORITMA RSA PADA PT INFOMEDIA SOLUSI HUMANIKA. *4*(1), 87–96.

Malik, S., & Saifudin, A. (2023). Implementasi Algoritma Advanced Encryption Standart - 128 Berbasis Dekstop pada Teks dan Dokumen. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *6*(2), 147–153. https://doi.org/10.32493/jtsi.v6i2.22694

Manullang, S., Allwine, & Jakaria Sembiring. (2023). Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *17*(1), 53–67. https://doi.org/10.35457/antivirus.v17i1.2811

Maulida, R., Haryono, W., & Maulana, A. E. (2023). *JAMAIKA: Jurnal Abdi Masyarakat Program Studi Teknik Informatika Universitas Pamulang*.

Nisfu Melati Sukma, W., Reynata, A., Auzini Yasmine, D., & Maulana Putra Pratama, D. (2023). *SYSTEMATIC LITERATURE REVIEW (SLR) : KEAMANAN DALAM SISTEM INFORMASI*. *2*(6). https://www.google.com/

Penulis, T., Permata Putri, M., Nadeak, E., Rahmi, N., Rini, A., Novita Sari, D., Kusmiati, H., & Almaheri Adhi Pratama, R. (2023). *SISTEM MANAJEMEN BASIS DATA MENGGUNAKAN MySQL*. www.freepik.com

Putra Pratama, B., & Haryono, W. (2020). *PERANCANGAN APLIKASI KRIPTOGRAFI PADA DOKUMEN PENGARSIPAN DENGAN MENGGUNAKAN ALGORITMA TRIPLE DES BERBASIS WEB*. *1*(4). http://openjournal.unpam.ac.id/index.php/JOAIIA/index204

Qadriah, L., Achmady, S., & Husaini. (2023). Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA). *Jurnal Sains Dan Informatika*, 29–35. https://doi.org/10.34128/jsi.v9i1.519

Sahal, A., & Winardi, S. (2021). Penerapan Sistem Pengarsipan Digital Sebagai Pendukung Pengelolaan Arsip Digital Pada Program Studi (Studi Kasus: Program Studi D3 Manajemen Informatika Fakultas Sains dan Teknologi Universitas Respati Yogyakarta). *Jurnal Teknologi Informasi*, *3*.

Santoso, J. T., Kom, S., & Kom, M. (2022). *P Y YAYASAN PRIMA AGUS TEKNIK PHP Pengembangan Web*.

LAMPIRAN

Lampiran 1. Surat Penetapan Dosen Pembimbing

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No.

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

KEPUTUSAN DEKAN
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
Nomor : 1074/KEP/II.3.AU/UMSU-09/F/2025

Tentang :
PENGANGKATAN DOSEN PEMBIMBING SKRIPSI
PRODI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

بسم الله الرحمن الرحيم

Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara, setelah:

Menimbang :
1. Bahwa sehubungan dengan pelaksanaan Tugas Akhir Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara;
2. Bahwa untuk memenuhi maksud tersebut perlu diterbitkan surat keputusan Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara.

Mengingat :
1. Undang-undang Republik Indonesia No. 12 Tahun 2012 tentang Pendidikan Tinggi;
2. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi;
3. Pedoman Perguruan Tinggi Muhammadiyah;
4. Statuta Universitas Muhammadiyah Sumatera Utara
5. Keputusan Rektor No. 1001/KEP/II.3-AU/UMSU/D/2025 tanggal 25 Oktober 2025 tentang Dekan Fakultas Ilmu Komputer dan Teknologi Informasi UMSU Masa Jabatan 2025-2029
6. Keputusan Rektor No. 624/KEP/II.3.AU/UMSU/D/2025 tentang Prodi Fakultas Ilmu Komputer dan Teknologi Informasi UMSU Masa Jabatan 2025-2029

MEMUTUSKAN

Menetapkan :

KESATU : Menetapkan nama-nama dalam lampiran surat keputusan ini sebagai Dosen Pembimbing Prodi Sistem Informasi Fakultas Ilmu Komputer dan Teknologi Informasi UMSU.

KEDUA : Keputusan ini berlaku sejak tanggal ditetapkan, dan akan ditinjau serta diperbaiki kembali jika terdapat kekeliruan di kemudian hari.

Ditetapkan di : Medan
Pada tanggal : 13 Jumadil Akhir 1447 H
03 Desember 2025 M

Dekan

Dr. Al-Khowarizmi., M.Kom
NIDN : 0127099201

Tembusan:
1. Yth. Wakil Dekan I & III UMSU di Medan,-
2. Ka. Prodi SI dan Sek. Prodi SI,-
3. Pertinggal.

BAN-PT MQA STARS

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
umsumedan umsumedan umsumedan umsumedan

Lampiran Dosen Pembimbing Prodi Sistem Informasi
Nomor : 1074/KEP/II.3.AU/UMSU-09/F/2025
Tanggal : 13 Jumadil Akhir 1447 H /03 Desember 2025 M

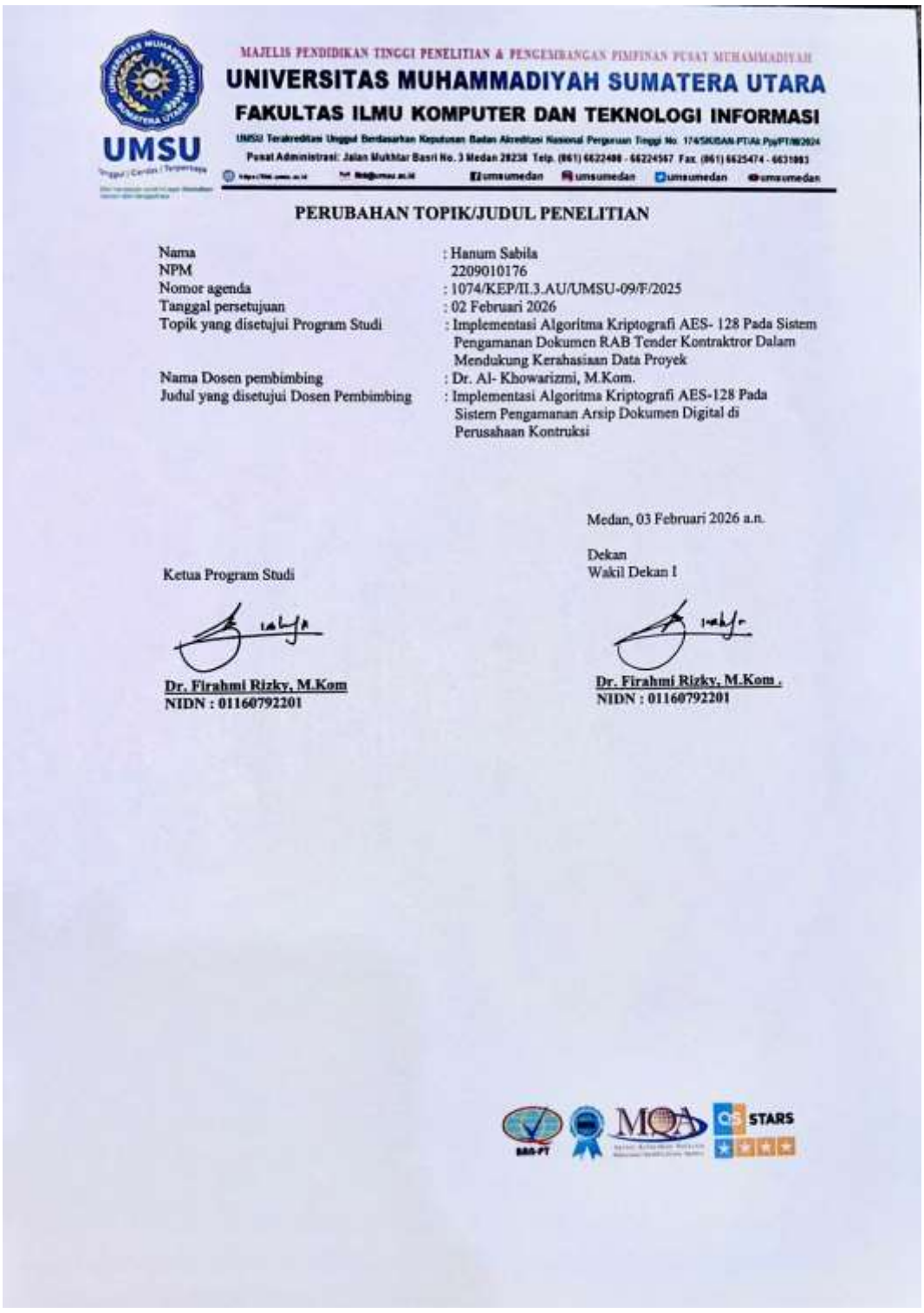
PENGANGKATAN DOSEN PEMBIMBING SKRIPSI
PRODI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

NO	NAMA	NPM	JUDUL	DOSEN
1	Nabila Sofiani	2209010261	Implementasi Algoritma Random Forest Untuk Deteksi File Pdf Fishing Berbasis Metadata Dokumen	Mulkan Azhari, S.Kom.,M.Kom.
2	Muhammad Fikrie Ar-Rasyid	2209010144	Penerapan Data Mining untuk Klasifikasi penyakit Migrain berdasarkan gejala klinis menggunakan algoritma K-Nearest Neighbor (KNN)	Rizaldy Khair, M.Kom
3	Mega Kumala Sari	2209010237	Sistem Informasi Geografis Pencarian Jarak Terdekat Lokasi Fasilitas Layanan Kesehatan di Kabupaten Labuhan Batu Utara Menggunakan Algoritma Dijkstra Berbasis Web	Dr. Al-Khowarizmi, M.Kom.
4	Nursaid Fatahillah	2209010164	Analisis Sentimen Keluhan Pelanggan PLN Menggunakan Algoritma Naïve Bayes untuk Meningkatkan Kinerja Pelayanan	Dr. Al-Khowarizmi, M.Kom.
5	Hanum Sabila	2209010176	Implementasi Kriptografi AES-128 pada sistem Pengamanan Dokumen RAB Tender Kontraktor dalam Mendukung Kerahasiaan Data Proyek	Dr. Al-Khowarizmi, M.Kom.
6	Najwa Ajrina	2209010293	sistem pakar diagnosa dini gangguan membaca pada anak sekolah dasar menggunakan metode certainty factor	Dr. Firahuni Rizky, M.Kom
7	Muhammad Dzaki Fauzi	2209010114	Deteksi Manipulasi Citra digital (tentukan objeknya) Berbasis ELA dan Histogram Color Shift Berbasis Web	Mahardika Prawira Tanjung, S.Kom.,M.Kom.

Dekan

Dr. Al-Khowarizmi., M.Kom
NIDN : 0127099201

Lampiran 2. Surat Perubahan Judul Penelitian



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak-PPJ/PT/III/2024

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

PERUBAHAN TOPIK/JUDUL PENELITIAN

Nama	: Hanum Sabila
NPM	2209010176
Nomor agenda	: 1074/KEP/II.3.AU/UMSU-09/F/2025
Tanggal persetujuan	: 02 Februari 2026
Topik yang disetujui Program Studi	: Implementasi Algoritma Kriptografi AES- 128 Pada Sistem Pengamanan Dokumen RAB Tender Kontraktror Dalam Mendukung Kerahasiaan Data Proyek
Nama Dosen pembimbing	: Dr. Al- Khowarizmi, M.Kom.
Judul yang disetujui Dosen Pembimbing	: Implementasi Algoritma Kriptografi AES-128 Pada Sistem Pengamanan Arsip Dokumen Digital di Perusahaan Kontruksi

Medan, 03 Februari 2026 a.n.

Dekan
Wakil Dekan I

Ketua Program Studi

Dr. Firahmi Rizky, M.Kom
NIDN : 01160792201

Dr. Firahmi Rizky, M.Kom .
NIDN : 01160792201

Lampiran 3. Surat Izin Penelitian

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
umsumedan umsumedan umsumedan umsumedan

Nomor : 533/II.3-AU/UMSU-09/F/2026
Lampiran : -
Perihal : **IZIN PENELITIAN**

Medan, 19 Syawwal 1447 H
07 April 2026 M

Kepada Yth.
Bapak/Ibu Pimpinan
PT. Asa Cipta Sarana
Jl. STM Komplek Artha Vista No. 17 B Medan

Di Tempat

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan hormat, sehubungan mahasiswa kami akan menyelesaikan studi,untuk itu kami memohon kesediaan Bapak / Ibu untuk memberikan kesempatan pada mahasiswa kami melakukan riset di **Perusahaan / Instansi** yang Bapak / Ibu pimpin, guna untuk penyusunan skripsi yang merupakan salah satu persyaratan dalam menyelesaikan Program **Studi Strata Satu (S-1)**

Adapun Mahasiswa/i di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara tersebut adalah:

Nama	**: Hanum Sabila**
Npm	**: 2209010176**
Jurusan	**: Sistem Informasi**
Semester	**: VIII (Delapan)**
Judul	**: IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONTRUKSI**
Email	**: hanumsabila07@gmail.com**
Hp/Wa	**: 08992900295**

Demikianlah surat kami ini, atas perhatian dan kerjasama yang Bapak / Ibu berikan kami ucapkan terimaksih

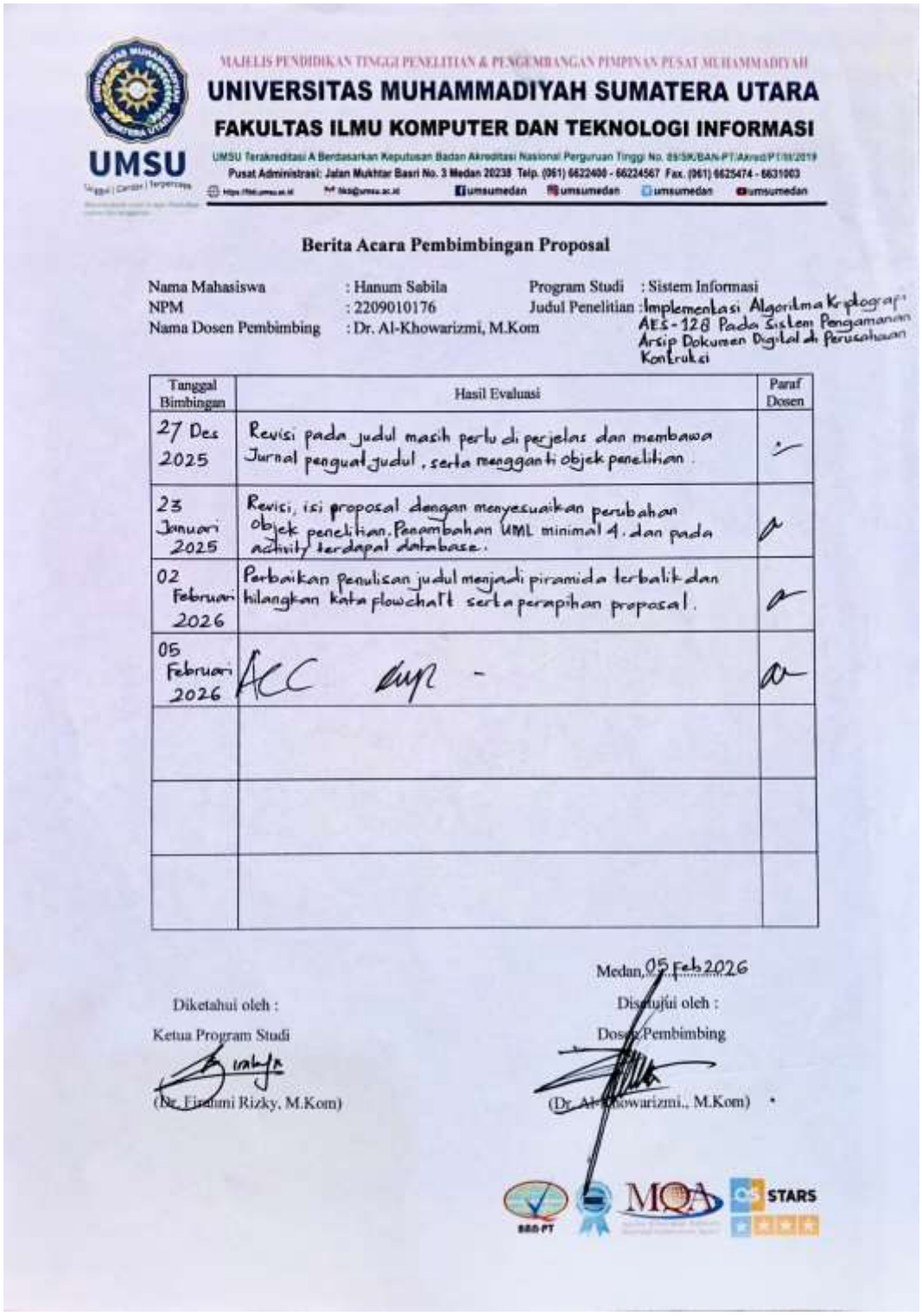
Wassalamu 'alaikum Warahmatullahi Wabarakatuh

Dekan

Assoc. Prof. Dr. Al-Khowarizmi,M.Kom.
NIDN : 0127099201

Cc.File

Lampiran 4. Berita Acara Pembimbingan Proposal



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Hanum Sabila
NPM : 2209010176
Nama Dosen Pembimbing : Dr. Al-Khowarizmi, M.Kom
Program Studi : Sistem Informasi
Judul Penelitian : Implementasi Algoritma Kriptografi AES-128 Pada Sistem Pengamanan Arsip Dokumen Digital di Perusahaan Konstruksi

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
27 Des 2025	Revisi pada judul masih perlu di perjelas dan membawa Jurnal penguat judul, serta menggant objek penelitian.	
23 Januari 2025	Revisi, isi proposal dengan menyesuaikan perubahan objek penelitian. Penambahan UML minimal 4. dan pada activity terdapat database.	
02 Februari 2026	Perbaikan penulisan judul menjadi piramida terbalik dan hilangkan kata flowchart serta perapihan proposal.	
05 Februari 2026	ACC dup -	

Medan, 05 Feb 2026

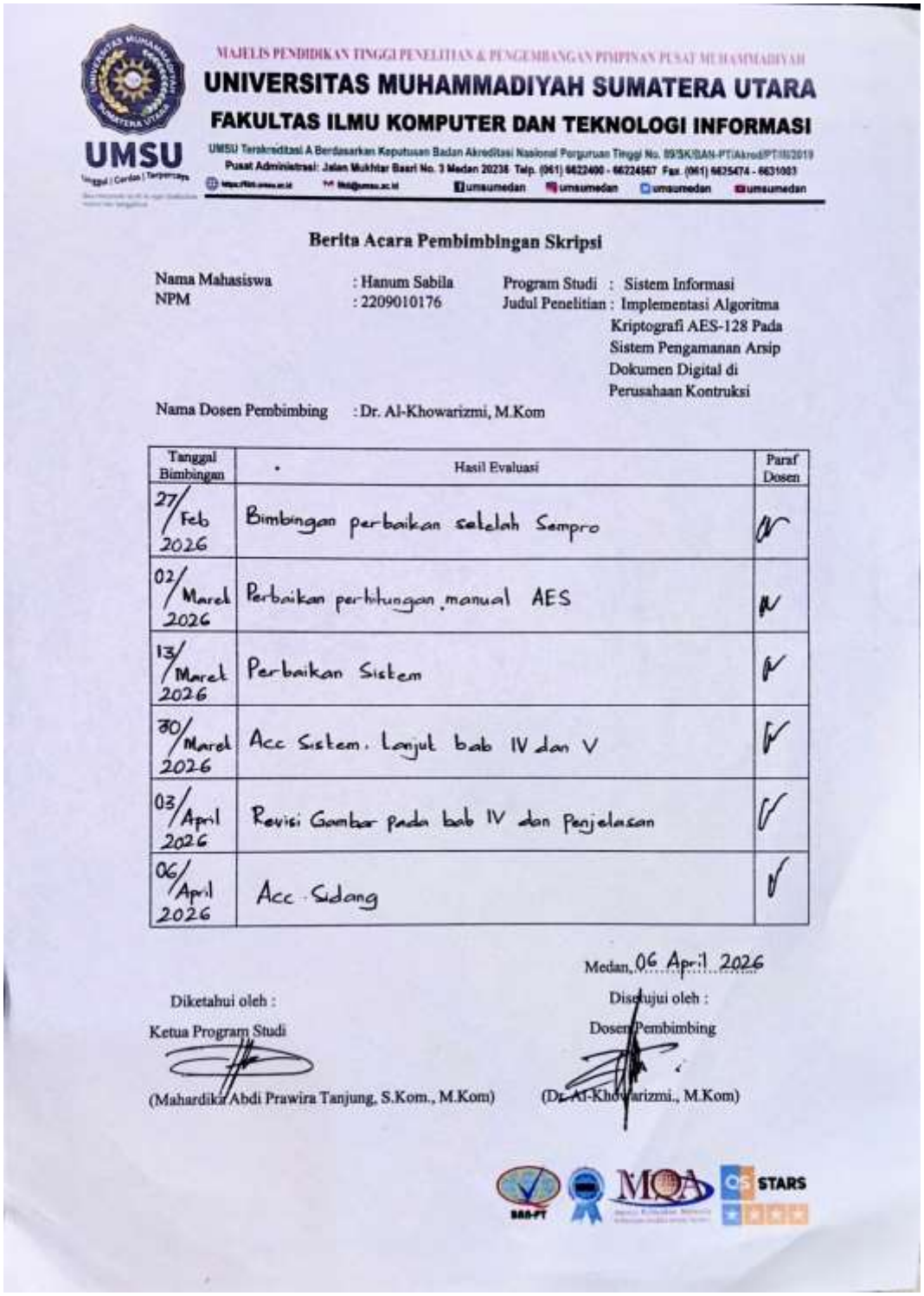
Diketahui oleh :
Ketua Program Studi

(Dr. Fatahmi Rizky, M.Kom)

Disetujui oleh :
Dosen Pembimbing

(Dr. Al-Khowarizmi., M.Kom)

Lampiran 5. Berita Acara Pembimbingan Skripsi



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

Berita Acara Pembimbingan Skripsi

Nama Mahasiswa : Hanum Sabila
NPM : 2209010176
Program Studi : Sistem Informasi
Judul Penelitian : Implementasi Algoritma Kriptografi AES-128 Pada Sistem Pengamanan Arsip Dokumen Digital di Perusahaan Kontruksi

Nama Dosen Pembimbing : Dr. Al-Khowarizmi, M.Kom

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
27/Feb/2026	Bimbingan perbaikan setelah Sempro	
02/Maret/2026	Perbaikan perhitungan manual AES	
13/Maret/2026	Perbaikan Sistem	
30/Maret/2026	Acc Sistem. Lanjut bab IV dan V	
03/April/2026	Revisi Gambar pada bab IV dan Penjelasan	
06/April/2026	Acc Sidang	

Medan, 06 April 2026

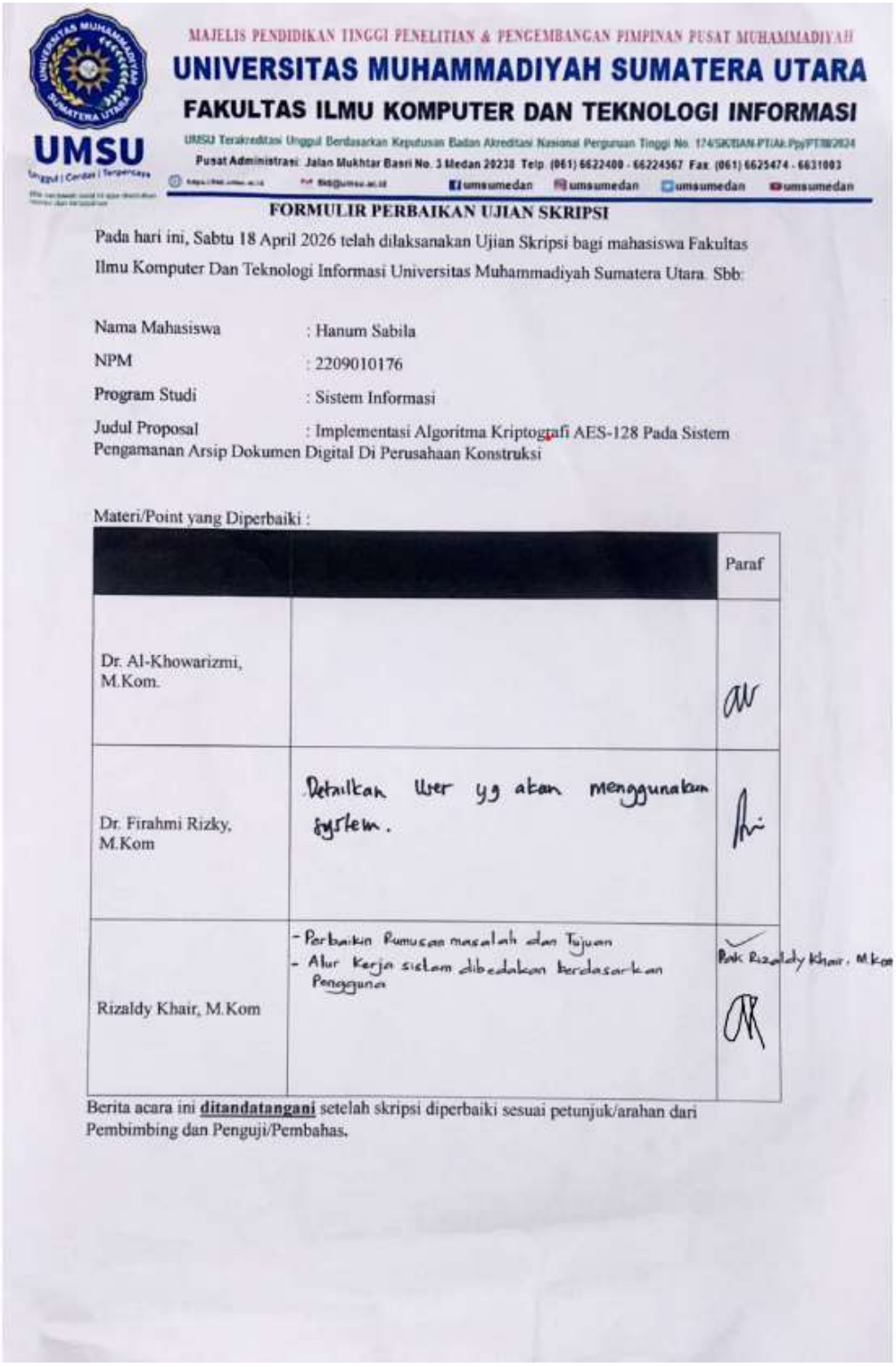
Diketahui oleh :
Ketua Program Studi

(Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom)

Disetujui oleh :
Dosen Pembimbing

(Dr. Al-Khowarizmi., M.Kom)

Lampiran 6. Formulir Perbaikan Ujian Skripsi



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

FORMULIR PERBAIKAN UJIAN SKRIPSI

Pada hari ini, Sabtu 18 April 2026 telah dilaksanakan Ujian Skripsi bagi mahasiswa Fakultas Ilmu Komputer Dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Sbb:

Nama Mahasiswa : Hanum Sabila

NPM : 2209010176

Program Studi : Sistem Informasi

Judul Proposal : Implementasi Algoritma Kriptografi AES-128 Pada Sistem Pengamanan Arsip Dokumen Digital Di Perusahaan Konstruksi

Materi/Point yang Diperbaiki :

		Paraf
Dr. Al-Khowarizmi, M.Kom.		
Dr. Firahmi Rizky, M.Kom	Detailkan User yg akan menggunakan system.	
Rizaldy Khair, M.Kom	- Perbaikin Rumusan masalah dan Tujuan - Alur kerja sistem dibedakan berdasarkan Pengguna	Pak Rizaldy Khair, M.Kom

Berita acara ini **ditandatangani** setelah skripsi diperbaiki sesuai petunjuk/arahan dari Pembimbing dan Penguji/Pembahas.

Lampiran 7. LOA

KOHESI
JURNAL SAINS DAN TEKNOLOGI

CAHAYA ILMU BANGSA INSTITUTE
Biro Penelitian, Publikasi, dan Pengabdian Kepada Masyarakat
KEMENKUMHAM AHU-0018913-AH.01.14
Perum Puri Kartika Asri Blok 2 A2 Malang
e-mail: admin @cahayailmubangsa.institute

LETTER OF ACCEPTANCE

NO: 2026/CIB013/LOA1012

Assalamualaikum Wr. Wb.
Bersama surat ini, kami menerangkan bahwa artikel dengan keterangan naskah berikut

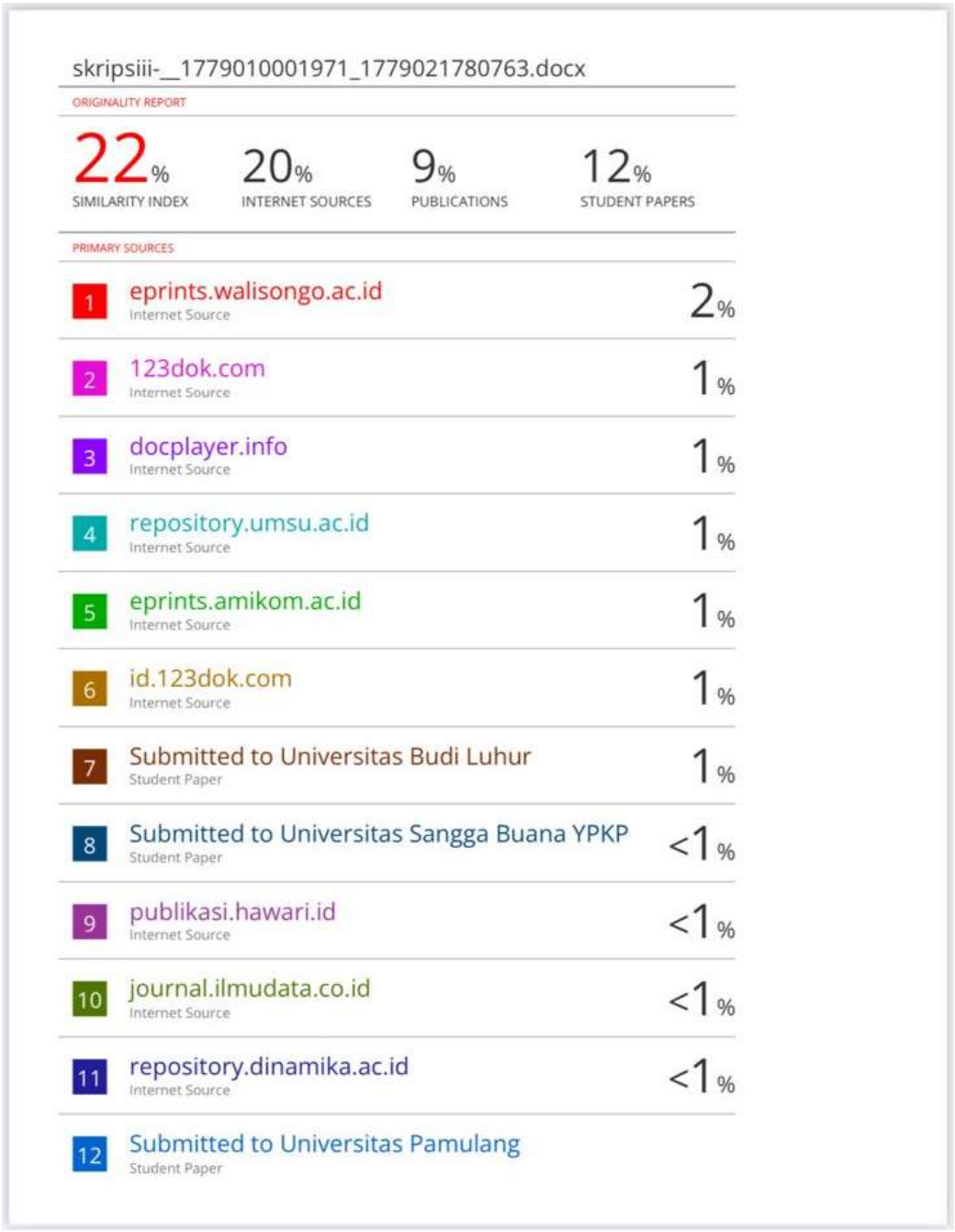
Judul	IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 PADA SISTEM PENGAMANAN ARSIP DOKUMEN DIGITAL DI PERUSAHAAN KONSTRUKSI
Author	Hanum Sabila, Al-Khowarizmi
Instansi	Universitas Muhammadiyah Sumatera Utara
Korespondensi	hanumsabila07@gmail.com
Jurnal	Kohesi: Jurnal Sains dan Teknologi
Volume	Vol. 10 No. 12 (2026)
Link Terbitan	https://cibangsa.com/index.php/kohesi/article/view/10355

Berstatus ACCEPTED untuk dipublish. Keputusan ini dibuat sebagai tanda bahwa naskah yang bersangkutan telah lolos plagiarism checker. Dan LoA ini dibuat sebagai bukti bahwa author telah menyelesaikan APC yang telah ditetapkan oleh pengelola jurnal. LOA Berlaku jika dilengkapi link dan pdf publish. Hubungi kami di **admin_jurnal@cahayailmubangsa.institute** jika ada pertanyaan lebih lanjut, terima kasih.

Malang, 20 May 2026

Dr. Umam Rofiq, M.Pd., Ph.D
Director

Lampiran 8. Turnitin



skripsiii-__1779010001971_1779021780763.docx

ORIGINALITY REPORT

22%	20%	9%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	eprints.walisongo.ac.id Internet Source	2%
2	123dok.com Internet Source	1%
3	docplayer.info Internet Source	1%
4	repository.umsu.ac.id Internet Source	1%
5	eprints.amikom.ac.id Internet Source	1%
6	id.123dok.com Internet Source	1%
7	Submitted to Universitas Budi Luhur Student Paper	1%
8	Submitted to Universitas Sangga Buana YPKP Student Paper	<1%
9	publikasi.hawari.id Internet Source	<1%
10	journal.ilmudata.co.id Internet Source	<1%
11	repository.dinamika.ac.id Internet Source	<1%
12	Submitted to Universitas Pamulang Student Paper	