IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH

TUGAS AKHIR

Disusun Untuk Memenuhi Syarat Kelulusan Program Strata I pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya



OLEH

AMRULLAH
C2155201113
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) PALANGKARAYA
2025

IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH

TUGAS AKHIR

Disusun Untuk Memenuhi Syarat Kelulusan Program Strata I pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya

Oleh:

AMRULLAH
C2155201113
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) PALANGKARAYA
2025

PERSETUJUAN

IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH

Tugas Akhir Ini Telah Disetujui dan Disahkan

Pembimbing I,	Pembimbing II,
Abdul Hadi, ST., M.Kom.	Lili Ruskiana, M.Kom.
NIK. 198505102021101	NIK. 198707282011007

Mengetahui

Ketua STMIK Palangkaraya,

Ir. Hj. Sri Maryamah, M.M.

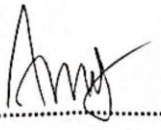
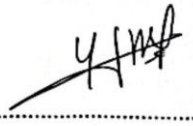
NIK. 196902021995004

PENGESAHAN

IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH

Tugas Akhir ini telah Diujikan, Dinilai, dan Disahkan
Oleh Tim Penguji pada Tanggal 2 Juli 2025

Tim Penguji Tugas Akhir :

1. Sam'ani, S. T., M.Kom. ..... 
   Ketua
2. Elok Faiqotul Himmah, S.Si., M.Sc. ..... 
   Sekretaris
3. Amaya Andri Damaini, S.Kom., M.T. ..... 
   Anggota
4. Abdul Hadi, ST., M.Kom. ..... 
   Anggota
5. Veny Cahya Hardita, M.Kom. ..... 
   Anggota

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : **AMRULLAH**

Nim : **C2155201113**

menyatakan bahwa Tugas Akhir dengan judul :

IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH

adalah hasil karya saya dan bukan merupakan duplikasi sebagian atau seluruhnya dari karya orang lain, kecuali bagian yang sumber informasi dicantumkan.

Pernyataan ini dibuat dengan sebenar-benarnya secara sadar dan bertanggunjawab dan saya bersedia menerima sanksi pembatalan Tugas Akhir apabila terbukti melakukan duplikasi terhadap Tugas Akhir atau karya ilmiah lain yang sudah ada.

Palangka Raya, 2 Juli 2025

Yang Membuat Pernyataan,



AMRULLAH

MOTTO DAN PERSEMBAHAN

MOTTO

"Hidup itu seperti sinyal WiFi - kadang kuat, kadang hilang tanpa sebab. Tapi yang penting, kita tetap terkoneksi dengan harapan, meskipun harus nunggu buffering dulu."

Sebagai ungkapan terima kasih, Tugas Akhir ini penulis persembahkan kepada:

PERSEMBAHAN

- Ayah dan Ibu tercinta, sumber kekuatan dan doa yang tak pernah putus, terima kasih atas cinta, pengorbanan, dan dukungan tanpa syarat dalam setiap langkah hidupku.
- Seluruh dosen STMIK Palangkaraya, yang telah membimbing, menginspirasi, dan membuka wawasan selama perjalanan studi ini. Terima kasih atas ilmu, kesabaran, dan dedikasi Bapak/Ibu dalam membentuk kami menjadi insan yang lebih siap menghadapi masa depan.
- Kepada dosen pembimbing Bapak Abdul Hadi, ST., M.Kom. dan Ibu Lili Rusdiana, M.Kom., atas bimbingan, arahan, dan motivasi yang tak ternilai dalam proses penyusunan tugas akhir ini. Terima kasih telah meluangkan waktu dan tenaga untuk membimbing saya hingga akhir.
- Serta untuk teman-teman seperjuangan angkatan 2021, yang telah menjadi bagian dari cerita indah selama masa kuliah. Kita sudah melewati tawa, stres, begadang, hingga skripsweet bersama dan semua itu akan selalu menjadi kenangan berharga.

INTISARI

Amrullah, C2155201113, 2025. Implementasi Sistem Arsip Surat Keluar Dan Masuk Berbasis Enkripsi Aes Di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah, Pembimbing I Abdul Hadi, S.T., M.Kom., Pembimbing II Lili Rusdiana, M.Kom.

Dalam era digitalisasi, keamanan data menjadi aspek krusial dalam sistem pengelolaan informasi, terutama dalam pengarsipan surat dinas yang bersifat rahasia dan penting. Penelitian ini bertujuan untuk mengimplementasikan sistem arsip surat keluar dan masuk berbasis web yang dilengkapi dengan metode enkripsi *Advanced Encryption Standard* (AES) guna mengamankan data surat pada Dinas Ketahanan Pangan Provinsi Kalimantan Tengah. Sistem ini dirancang untuk memudahkan petugas dalam mengelola surat secara terstruktur dan aman. Metode enkripsi AES digunakan untuk menjaga kerahasiaan isi surat dengan mengenkripsi data sebelum disimpan ke dalam database dan mendekripsinya saat dibutuhkan.

Pengembangan sistem dilakukan menggunakan metode *Research and Development* (R&D), yang mencakup tahapan potensi dan masalah, pengumpulan data, desain produk, validasi desain, revisi desain, uji coba produk, revisi produk, hingga produk akhir. Data diperoleh melalui observasi dan wawancara dengan staf dinas terkait, kemudian dilakukan perancangan sistem menggunakan pendekatan terstruktur serta implementasi menggunakan bahasa pemrograman PHP dan basis data *MySQL*. Validasi sistem dilakukan oleh ahli dan pengguna melalui uji coba langsung untuk mengetahui tingkat keamanannya.

Hasil pengujian *Blackbox* menunjukkan bahwa sistem berhasil mengamankan data surat dan memberikan kemudahan dalam proses pengarsipan serta pencarian dokumen. Dengan implementasi ini, diharapkan keamanan informasi surat di lingkungan dinas dapat ditingkatkan, serta proses manajemen arsip menjadi lebih efektif dan terkontrol.

Kata Kunci: arsip surat, enkripsi aes, keamanan data, pengarsipan digital, metode r&d.

ABSTRACT

Amrullah, C2155201113, 2025. *Implementation of an Incoming and Outgoing Mail Archiving System Based on AES Encryption at the Food Security Agency of Central Kalimantan Province. Supervisor I* Abdul Hadi, S.T., M.Kom. *Supervisor II* Lili Rusdiana, M.Kom.

In the digital era, data security has become a crucial aspect of information management systems, especially in archiving official letters that are confidential and important. This research aims to implement a web-based archiving system for incoming and outgoing letters, equipped with the Advanced Encryption Standard (AES) encryption method to enhance data security at the Food Security Agency of Central Kalimantan Province. The system is designed to assist staff in managing letters in a structured and secure manner. AES encryption is used to maintain the confidentiality of letter contents by encrypting the data before storing it in the database and decrypting it when needed.

The system development follows the Research and Development (R&D) method, which includes stages such as identifying potential and problems, data collection, product design, design validation, design revision, product testing, product revision, and final product. Data were obtained through observation and interviews with relevant agency staff, followed by system design using a structured approach and implementation using PHP programming language and MySQL database. System validation was conducted by experts and users through direct testing to assess its security level.

The Blackbox testing results show that the system successfully secures letter data and facilitates the archiving and retrieval processes. With this implementation, it is expected that the security of letter information within the agency can be improved, and the archive management process becomes more effective, efficient, and well-controlled.

Keywords: mail archiving, aes encryption, data security, digital archiving, r&d method.

KATA PENGANTAR

Alhamdulillah penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena dengan karunia-nya sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH". Tugas Akhir ini disusun untuk memenuhi syarat dalam memperoleh gelar Sarjana Komputer di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya.

Pada kesempatan ini penulis juga menyampaikan terimakasih yang sebesar besarnya kepada semua pihak yang telah memberikan bimbingan, motivasi, semangat, dalam menyelesaikan penulisanTugas Akhir ini, yaitu kepada :

1. Bapak Agus Candra, ST., MT. selaku Kepala Dinas Ketahanan Pangan Provinsi Kalimantan Tengah. Telah menerima dan memberikan izin penelitian sebagai tempat penelitian.
2. Bapak H.Jamni, SE,. MM. selaku Kasubbag Umum dan narasumber di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.
3. Abdul Hadi, S.T., M.Kom. selaku Dosen Pembimbing I yang meluangkan waktunya untuk memberikan bimbingan dalam penyelesaian Tugas Akhir ini.
4. Lili Rusdiana, M.Kom. selaku Dosen Pembimbing II dalam penulisan Tugas Akhir ini, yang juga banyak memberikan saran dan masukan dalam penulisan Tugas Akhir ini.

Penulis mengharapkan masukan,saran dan kritik yang bersifat membangun untuk menyempurnakan Tugas Akhir ini. Semoga Tugas Akhir ini dapat bermanfaat bagi penulis dan pembaca terutama untuk menambah ilmu pengetahuan.

Palangka Raya, 2 Juli 2025

Penulis

DAFTAR ISI

PERSETUJUAN iii
PENGESAHAN iv
PERNYATAAN KEASLIAN v
MOTTO DAN PERSEMBAHAN vi
MOTTO vi
PERSEMBAHAN vi
INTISARI vii
ABSTRACT viii
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR TABEL xiii
DAFTAR GAMBAR vii
DAFTAR LAMPIRAN ix
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Dan Manfaat Penelitian 3
1.5 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 6
2.1 Kajian Teori 6
2.1.1 Implementasi 6
2.1.2 Arsip 6
2.1.3 E-Arsip 6
2.1.4 Manajemen Arsip Elektronik 6
2.1.5 Implementasi E-Arsip 7
2.1.6 Web 8
2.1.7 AES (*Advanced Encryption Standard*)` 8

2.1.8 Pemodelan Berorientasi Objek Menggunakan *Unified Modeling Language* (UML) 10
2.1.9 *MYSQL* 11
2.1.10 *Codeigniter* 12
2.1.11 *Draw.io* 14
2.1.12 Studi pustaka 14
2.1.13 Observasi 15
2.1.14 Wawancara 15
2.1.15 RAD (*Rapid Application Development*) 15
2.1.1 Relasi Antar Tabel 15
2.2 Penelitian yang Relevan 16
BAB III METODOLOGI PENELITIAN 22
3.1 Tinjauan Umum 22
3.2 Jenis Penelitian 22
3.3 Desain Penelitian 23
3.4 Instrumen Penelitian 24
3.5 Analisis Kebutuhan 25
3.6 Analisis Kebutuhan Perangkat Keras Dan Perangkat Lunak Untuk Menjalankan Sistem 26
3.7 Desain Sistem 27
3.7.1 Desain Proses 27
3.7.2 Desain Enkripsi AES 36
3.7.3 Desain Interface 38
BAB IV HASIL DAN PEMBAHASAN 43
4.1 Hasil 43
4.1.1 Gambaran Umum Sistem 43
4.1.2 Implementasi Database 43
4.1.3 Implementasi Hak Pengguna (User) Dan Admin 49
4.1.4 Proses Enkripsi dan Dekripsi Surat (AES) 51
4.1.5 Tampilan Antarmuka Sistem 60

4.1.6 Pengujian Sistem 76
4.2 Pembahasan 79
4.2.1 Evaluasi Sistem 79
4.2.2 Kelebihan Dan Kekurangan Sistem 79
BAB V KESIMPULAN DAN SARAN 81
5.1 Kesimpulan 81
5.2 Saran 81
DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2. 1 Tabel Putaran Algoritma AES tiap blok 8
Tabel 2. 2 *Use Case Diagram* 10
Tabel 2. 3 *Activity diagram* 11
Tabel 2. 4 Penelitian yang Relevan 16
Tabel 3. 1 Kebutuhan Perangkat Lunak 22
Tabel 3. 2 Kebutuhan Perangkat Keras 22
Tabel 3. 2 Kebutuhan Perangkat Keras 33
Tabel 3. 4 Jadwal Penelitian 38

DAFTAR GAMBAR

Gambar 2. 1 Proses Enkripsi Algoritma AES-128 9
Gambar 3. 1 *Use Case Diagram Admin* 24
Gambar 3. 2 *Use Case Diagram User* 25
Gambar 3. 3 *Activity diagram login*.....27
Gambar 3. 3 *Activity diagram surat masuk*.....27
Gambar 3. 3 *Activity diagram surat keluar*.....27
Gambar 3. 3 *Activity diagram laporan surat masuk*.....27
Gambar 3. 3 *Activity diagram laporan surat keluar*.....27
Gambar 3. 3 *Activity diagram pengguna* 27
Gambar 3. 3 *Activity diagram logout*.....27
Gambar 3. 4 *Activity diagram Enkripsi* 28
Gambar 3. 5 *Activity diagram Dekripsi*.....29
Gambar 3. 6 *Flowchart* Enkripsi Data Surat.....30
Gambar 3. 7 *Flowchart* Dekripsi Data Surat 31
Gambar 3. 8 Desain Halaman Login 34
Gambar 3. 9 Desain Halaman *Dashboard*.....35
Gambar 3. 10 Desain Surat Masuk dan Surat Keluar.....35
Gambar 3. 11 Desain Enkripsi File 36
Gambar 3. 12 Desain Dekripsi File.....37
Gambar 4.1 Tabel Utama Database.....44
Gambar 4.2 Tabel Surat Keluar.....45
Gambar 4.3 Tabel Surat Masuk.....46
Gambar 4.4 Tabel *Users*.....47
Gambar 4.5 Tabel Relasi 47
Gambar 4.6 Hak Akses Pengguna (User).....50
Gambar 4.7 Hak Akses Admin.....50
Gambar 4.8 Aturan Enkripsi File Surat Keluar 51
Gambar 4.9 Proses Enkripsi Surat Keluar.....51
Gambar 4.10 Validasi Input Surat Keluar 52
Gambar 4.11 Proses Unduh Surat Keluar.....53
Gambar 4.12 Unduh Enkripsi Surat Keluar 54
Gambar 4.13 Aturan Enkripsi File Surat Masuk 55
Gambar 4.14 Proses Enkripsi Surat Masuk.....56
Gambar 4.15 Validasi Input Surat Masuk 57
Gambar 4.16 Proses Download Surat Masuk.....58
Gambar 4.17 Unduh Enkripsi Surat Masuk.....59
Gambar 4.1.18 Halaman Login 60
Gambar 4.19 Dashboard Pengguna (User).....61
Gambar 4.20 Dashboard Admin.....62
Gambar 4.21 Daftar Surat Masuk.....63

Gambar 4.22 Daftar Surat Keluar.....64
Gambar 4.23 *Form* Input Surat Masuk.....65
Gambar 4.24 *Form* Input Surat Keluar.....66
Gambar 4.25 Deskripsi Dan Download File 68
Gambar 4.26 Detail Surat Masuk 69
Gambar 4.27 Detail Surat Keluar 70
Gambar 4.28 Laporan Surat Masuk.....71
Gambar 4.29 Laporan Surat Keluar.....72
Gambar 4.30 Halaman Manajemen Pengguna 73
Gambar 4.31 Tambah Pengguna 74
Gambar 4.32 Edit Pengguna.....75
Gambar 4.33 Hapus Pengguna 76

DAFTAR LAMPIRAN

Lampiran 1. Source Code Enkripsi Dan Dekripsi Surat
Lampiran 2. Surat Tugas Pembimbing Tugas Akhir
Lampiran 3. Kartu Kegiatan Konsultasi Bimbingan Tugas Akhir
Lampiran 4. Surat Tugas Penguji Seminar Proposal Tugas Akhir
Lampiran 5. Surat Tugas Penguji Tugas Akhir
Lampiran 6. Berita Acara Ujian Tugas Akhir
Lampiran 7. Kartu Kegiatan Seminar Proposal Tugas Akhir
Lampiran 8. Lembar Pengujian Blackbox
Lampiran 9. Surat Ijin Penelitian
Lampiran 10. Dokumentasi Penelitian

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Arsip surat keluar dan masuk memiliki peran penting dalam kelancaran administrasi organisasi, termasuk di instansi pemerintahan seperti Dinas Ketahanan Pangan Provinsi Kalimantan Tengah. Hasil wawancara dengan salah satu staf Dinas Ketahanan Pangan Provinsi Kalimantan Tengah mengungkapkan bahwa pengelolaan arsip surat keluar dan masuk masih dilakukan secara manual, menggunakan map odner dan lemari arsip yang sederhana. Arsip surat berfungsi sebagai dokumen historis, alat evaluasi, dan bukti hukum. Pengelolaan yang baik dapat meningkatkan transparansi dan akuntabilitas organisasi (Widjaya, 2023).

Selain itu, observasi menunjukkan bahwa ruang arsip di instansi tersebut memiliki kapasitas terbatas, sehingga seringkali arsip menumpuk secara tidak terorganisir. Ketika dilakukan audit internal, ditemukan bahwa sekitar 15% dokumen sulit ditemukan atau tidak dapat diverifikasi keberadaannya. Hal ini memperlihatkan risiko kehilangan data yang nyata.

Dalam era digital, keamanan data menjadi perhatian utama, terutama ketika dokumen mengandung informasi sensitif yang memengaruhi kebijakan strategis, seperti surat-surat resmi terkait program ketahanan pangan. Salah satu metode yang dapat

mengamankan sistem adalah dengan menerapkan teknologi enkripsi. Algoritma *Advanced Encryption Standard* (AES) dikenal sebagai metode enkripsi yang sangat aman untuk melindungi data dari akses yang tidak sah.

Dalam sistem arsip surat keluar dan masuk, penting mengamankan file untuk mencegah kehilangan atau penyalahgunaan informasi yang mengancam kerahasiaan dan integritas arsip. Penelitian ini berfokus pada enkripsi file surat, termasuk surat perintah, keputusan, undangan, laporan resmi, serta dokumen komunikasi internal dan eksternal. Perlindungan mencakup keamanan akses, enkripsi data, dan cadangan (*backup*).

Dengan adanya sistem ini, diharapkan Dinas Ketahanan Pangan Provinsi Kalimantan Tengah dapat lebih baik dalam melaksanakan tugas dan fungsinya, serta memberikan layanan publik yang lebih berkualitas kepada masyarakat.

1.2 Perumusan Masalah

Bagaimana merancang dan mengembangkan sistem arsip surat keluar dan masuk berbasis enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah untuk keamanan data surat?

1.3 Batasan Masalah

Agar lebih terfokus dan mencapai tujuan yang diinginkan, pembahasan dibatasi pada hal-hal berikut :

a. Pengguna sistem arsip surat online terbatas pada pegawai Dinas Ketahanan Pangan Provinsi Kalimantan Tengah yang memiliki hak akses untuk mengelola arsip surat keluar dan masuk.

b. Sistem hanya mencakup proses pengarsipan surat masuk dan keluar, termasuk pencatatan, pengarsipan, pencarian, dan pengamanan dokumen.

c. Sistem akan dikembangkan menggunakan bahasa pemrograman *Codeigniter*, database *MySQL* dan enkripsi AES (*Advanced Encryption Standard*).

1.4 Tujuan Dan Manfaat Penelitian

a. Tujuan Penelitian

Merancang dan mengembangkan sistem arsip surat masuk dan keluar berbasis web dengan enkripsi AES (*Advanced Encryption Standard*) yang dapat diimplementasikan pada Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.

b. Manfaat Penelitian

1. Manfaat bagi Dinas Ketahanan Pangan Provinsi

   Kalimantan Tengah Membantu mengamankan pengelolaan keamanan arsip surat keluar dan masuk, serta mendukung trans*form*asi digital dalam administrasi Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.

2. Manfaat bagi Penulis

   Sebagai pengalaman praktis dalam mengembangkan dan menerapkan sistem berbasis teknologi enkripsi AES, serta menambah wawasan dalam bidang keamanan data dan manajemen arsip.

3. Manfaat bagi STMIK Palangkaraya

   Mengetahui kemampuan mahasiswa dalam mengusai materi yang diperoleh saat kuliah dan kemampuan mahasiswa dalam menerapkan pengetahuannya sebagai bahan evaluasi. Memberikan kesempatan bagi mahasiswa untuk terlibat langsung dalam pengembangan sistem yang aman, sehingga mereka dapat memahami lebih dalam tentang pengelolaan data yang sensitif serta penerapan teknologi enkripsi dalam dunia nyata.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan tugas akhir ini terdiri dari beberapa bab dan masing-masing bab membahas dan menguraikan pokok permasalahan yang berbeda, sebagai Gambaran disini penulis menyertakan garis-garis besarnya yaitu :

BAB I PENDAHULUAN

Bab ini berisikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan tinjauan pustaka yang diambil dari penelitian yang relevan beserta susunan kajian teori yang disesuaikan dengan tema Tugas Akhir.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan tentang tahapan yang dilakukan peneliti dalam mengumpulkan informasi atau data yang dibutuhkan.

BAB IV PEMBAHASAN

Bab ini berisikan tentang hasil dari penelitian dan pembahasan dari hasil yang didapat.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan tentang kesimpulan dan saran yang diberikan untuk pengembangan selanjutnya

BAB II

TINJAUAN PUSTAKA

2.1 Kajian Teori

2.1.1 Implementasi

Implementasi adalah sebagai langkah nyata untuk merealisasikan rencana, memastikan tujuan tercapai, dan mengevaluasi hasil agar sesuai dengan yang diharapkan. Implementasi merupakan suatu proses mendapatkan suatu hasil yang sesuai dengan tujuan atau sasaran kebijakan itu sendiri. Pelaksana kebijakan melakukan suatu aktivitas atau kegiatan yang terkait dengan pelaksanaan kebijakan tersebut (Syaputra, D. S., & Saputri, L. 2022).

2.1.2 Arsip

Arsip merupakan hal yang paling utama dan mendasar yang harus diperhatikan dalam segala jenis kegiatan administrasi, manajemen dalam suatu organisasi dikarenakan arsip merupakan data informasi yang tersimpan mengenai segala hal yang kita kerjakan dalam rutinitas harian. Dalam administrasi dan manajemen arsip berperan sangat vital sebagai bahan untuk perencanaan, bahan pengawasan dan pelaporan, bahan utama pengambilan keputusan dalam suatu organisasi dan tanpa arsip tidak mungkin suatu organisasi dapat beroperasi dengan tertib, teratur dan lancar (Widya, R. & Abdul, K. B. 2024).

2.1.3 E-Arsip

E-Arsip merupakan sistem yang dirancang untuk mengelola dokumen dan informasi secara digital. E-arsip adalah sebuah sistem kearsipan secara elektronis yang dapat digunakan oleh staf atau pegawai instansi pemerintahan sebagai suatu alat yang berguna dalam memantau dan mengelola hal-hal yang berkaitan dengan sistem kearsipan baik berbentuk berkas, folder, audio, visual (Kominfo. 2024).

2.1.4 Manajemen Arsip Elektronik

Menurut (Santoso, A. B., & Prabowo, T. T. 2022), Manajemen arsip elektronik adalah untuk mengelola, menyimpan, dan mengakses dokumen digital secara aman, dan terorganisir agar informasi dapat ditemukan dengan mudah saat dibutuhkan. beberapa manfaat penggunaan sistem pengelolaan secara elektonik yang mendorong sebagian besar organisasi untuk mengimplementasikan manajemen arsip elektronik diantaranya adalah:

a. Cepat ditemukan dokumen tanpa meninggalkan meja kerja dan memungkinkan pemanfaatan arsip.
b. Pengindeksan yang fleksibel dan Pencarian dengan mencari file berdasarkan kata kunci maupun nama file dan ditemukan nya dalam bentuk *full text* dokumen secara *full-text*.

c. Kita hanya dapat melihat dilayar monitor atau print-nya tanpa dapat mengubahnya. Sehingga kecil kemungkinan file akan hilang.

d. Resiko rusak nya dokumen kertas atau buram karena usia dapat diminimalisir karena tersimpan secara digital.

2.1.5 Implementasi E-Arsip

Implementasi arsip elektronik adalah untuk menerapkan sistem pengelolaan arsip digital yang aman, memastikan dokumen disimpan, diatur, dan diakses dengan mudah serta aman. Sistem kearsipan adalah untuk kepentingan operasional dengan asas bahwa hanya informasi yang tepat digunakan oleh orang yang tepat dan untuk kepentingan tepat pada waktu yang tepat dengan biaya serendah mungkin dengan rangkaian subsistem dalam manajemen kearsipan yang bekerja sama untuk mencapai tujuan agar arsip tertata dalam unit-unit informasi siap pakai (Harisanty, D., & Anugrah, E. P. 2022),

Sistem kearsipan harus bisa mencakup semua subsistem dalam manajemen kearsipan. Manajemen kearsipan dimaknai sebagai pelaksanaan fungsi-fungsi manajeman di dalam rangka mengelola keseluruhan daur hidup arsip. Pengertian implementasi e-arsip dapat suatu proses yang dinamis dalam melakukan kegiatan kearsipan untuk memantau dan mengelola hal-hal yang berkaitan dengan sistem kearsipan.

2.1.6 Web

Web adalah sebagai *platform* untuk menyampaikan informasi, berinteraksi, dan menyediakan berbagai layanan secara online melalui jaringan internet. Web adalah salah satu aplikasi yang berisikan dokumen- dokumen multimedia didalamnya yang menggunakan protokol *HTTP (hyper text transfer protocol)* dan dalam mengunakan perangkat lunak yang disebut *browser*. *Browser* (perambah) adalah aplikasi yang mampu menjalankan dokumen-dokumen web dengan cara diterjemahkan. Beberapa jenis *browser* yang populer saat ini di antaranya : *Internet Exspoler* yang diperoduksi oleh *Microsoft*, *Mozila Firefox*, *Opera* dan *Safari* yang diperoduksi oleh *Apple* (Nur, M., Soedijono, B., & Arief, M. R. 2021) .

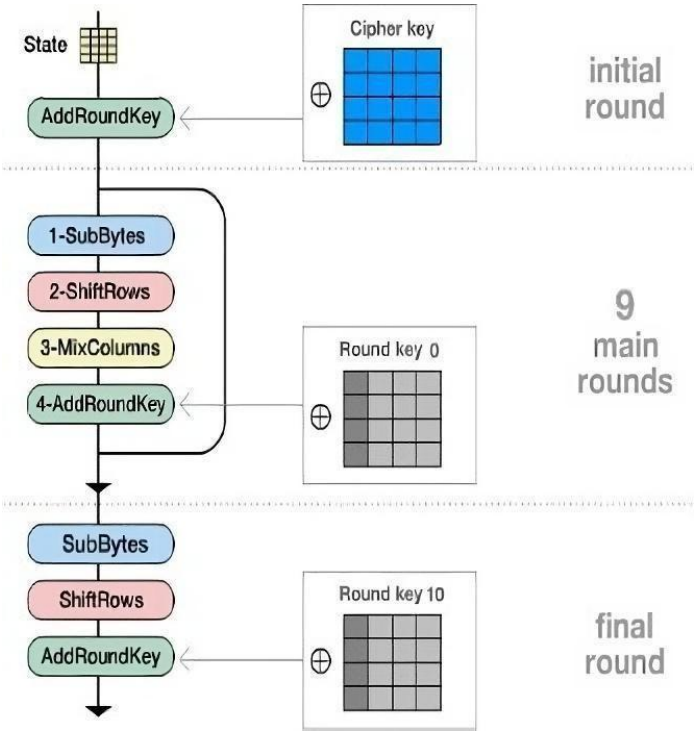
2.1.7 AES (*Advanced Encryption Standard*)`

Advanced Encryption Standard (AES) merupakan algoritma kriptografi modern yang dapat digunakan untuk mengamankan data. Blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi disebut algoritma AES. *Chipertext* adalah data yang tidak dapat dikenal, dan proses mengubah data asli menjadi *chipertext* adalah enkripsi. Sebaliknya dekripsi mengubah *ciphertext* data menjadi bentuk asli, yang dikenal sebagai *plaintext*. Algoritma aes memiliki beberapa macam kunci enkripsi dan dekripsi pertama 128 bit, kedua 192 bit, dan yang ketiga 256 bit.

Tabel 2. 1 Tabel Putaran Algoritma AES tiap blok

Tipe	Kunci	Blok Input	Jumlah n
AES – 128	128-bit	128-bit	10
AES – 192	192-bit	128-bit	12
AES – 256	256-bit	128-bit	14

Pada penelitian ini digunakan AES-128 *bit* yang dilakukan terhadap *state* atau *array of byte* dua dimensi. Sebuah proses penyandian *plaintext* menjadi *ciphertext* adalah penjelasan teknis proses enkripsi atau secara umum enkripsi adalah sebuah proses mengonversikan data normal menjadi data rahasia yang dapat dilihat pada Gambar 2. 1.



Gambar 2.1 Proses Enkripsi Algoritma AES-128

Proses enkripsi algoritma AES-128 akan melakukan beberapa Trans*form*asi bytes yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *Mixcolumns* yang dipisahkan menjadi 3 bagian, yaitu *Initial Round*, *Main Rounds*, dan *Final Round*.

2.1.8 Pemodelan Berorientasi Objek Menggunakan Unified Modeling Language (UML)

Menurut (Pratama, E. B., & Saparingga, U. 2021), UML (*Unified Modeling Language*) adalah untuk membantu dalam merancang, menggambarkan, dan mendokumentasikan sistem perangkat lunak dengan cara yang jelas dan terstruktur. UML merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem. UML juga merupakan Bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membanngun perangkat lunak. Alat bantu yang digunakan dalam perancangan berorientasi objek berbasiskan UML adalah sebagai berikut:

a) *Use Case Diagram*

Use case digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi- fungsi tersebut. *Use case* diagram merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat (Purnasari, et al, 2022).

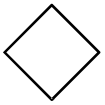
Tabel 2.2 Simbol - Simbol Pada *Use Case Diagram*

Simbol	Notasi	Keterangan
	*Actor*	Mewakili pengguna atau sistem lain yang berinteraksi dengan sistem.
	*Use Case*	Menggambarkan fungsi atau layanan yang disediakan oleh sistem.
	Assocation	Menghubungkan aktor dengan use case yang menunjukkan interaksi.
	Relasi	Sebagai penghubung antara *actor use case*, *use case – use case* dll
<<include>>	*Include*	Menunjukkan bahwa suatu use case memerlukan atau menyertakan fungsi lain.
<<extend>>	*Extend*	Mengindikasikan bahwa fungsi tambahan dapat terjadi dalam kondisi tertentu.

b) Activity diagram

Activity diagram adalah salah satu jenis diagram yang digunakan dalam *Unified Modeling Language* (UML) untuk memodelkan alur kerja atau aktivitas dalam sebuah sistem. Diagram ini menggambarkan urutan langkah-langkah atau aktivitas yang dilakukan, termasuk pengambilan keputusan dan paralelisme, sehingga memberikan gambaran proses secara visual (Ardhana, V. Y. P. 2021).

Tabel 2.3 Simbol - Simbol Pada *Activity diagram*

Simbol	Notasi	Keterangan
	*Initial State*	Titik awal untuk memulai suatu aktivitas
	*Final State*	Titik akhir untuk mengakhiri suatu aktivitas
	*Activity*	Menandakan sebuah aktivitas
	*Decision*	Pilihan untuk pengambilan keputusan
	*Control Flow*	Arus aktivitas

2.1.9 *MYSQL*

MySQL adalah sebuah sistem manajemen basis data sederhana yang digunakan untuk mengelola dan mengakses data dalam basis data. Fungsinya adalah untuk melakukan operasi dasar seperti menyimpan, mengubah, mengambil, dan menghapus data menggunakan perintah SQL dengan fokus pada kemudahan untuk aplikasi kecil atau terdistribusi. MSQL sistem managemen *database* SQL yang bersifat *Open Source* dan paling populer saat ini. *Database* ini dibuat untuk keperluan sistem database yang cepat, handal dan mudah digunakan. Sistem *database MySQL* mendukung beberapa fitur seperti *multithreaded, multi-user* dan SQL *database* manajemen sistem (DBMS). (Praba, A. D., & Safitri, M. 2020).

2.1.10 *Codeigniter*

Codeigniter adalah *framework* PHP yang berfungsi untuk mempermudah pengembangan aplikasi web dengan menyediakan berbagai fitur siap pakai, seperti manajemen database, keamanan, dan pengelolaan URL, sehingga proses coding menjadi lebih cepat dan terstruktur.*Codeigniter* adalah kerangka kerja PHP: *Hypertext Preprocessor* yang dapat membantu mempercepat *developer* dalam pengembangan aplikasi *website (web)* berbasis PHP daripada menulis semua kode program dariawal (Kurniadi, et al., 2022).

2.1.11 *Draw.io*

Draw io adalah *website* dan *software* yang digunakan untuk membuat *flowchat*, *draw io* berguna untuk merancang *Use Case diagram* maupun *Activity diagram* (Marthiawati, N., Kurniawansyah, K., Nugraha, H., & Khairunnisa, F. 2024).

2.1.12 Studi pustaka

Studi pustaka adalah metode pengumpulan data dengan menelaah berbagai literatur, dokumen, atau publikasi ilmiah yang relevan dengan topik penelitian. Studi pustaka berfungsi untuk memperoleh dasar teori, memperluas wawasan, serta memahami konteks penelitian secara mendalam. Studi pustaka dilakukan untuk mengidentifikasi gap penelitian sebelumnya, menemukan kerangka berpikir, serta membangun argumen yang kuat dalam penelitian (Sukmawati, S. & Nasran, N. 2021).

2.1.13 Observasi

Observasi adalah metode pengumpulan data melalui pengamatan langsung terhadap objek atau fenomena di lapangan. Teknik ini bertujuan untuk memahami situasi nyata dan perilaku subjek penelitian dalam konteks tertentu. Observasi dipandang sebagai cara efektif untuk menangkap data perilaku yang tidak dapat terungkap melalui wawancara atau survei (Nikmah, K. 2023).

2.1.14 Wawancara

Wawancara adalah teknik pengumpulan data dengan melakukan interaksi langsung antara peneliti dan narasumber untuk menggali informasi mendalam. Menyatakan bahwa wawancara membantu peneliti mendapatkan data yang subjektif dan kontekstual, terutama dalam penelitian (Harmawan, R., & Setiawan, A. 2022).

2.1.15 RAD (*Rapid Application Development*)

RAD adalah metodologi pengembangan sistem yang menekankan pada kecepatan pengembangan dengan kualitas yang baik. Metode ini sangat cocok untuk proyek-proyek yang memerlukan waktu pengembangan yang singkat dan fleksibilitas tinggi dalam merespon perubahan kebutuhan pengguna. RAD adalah model pengembangan perangkat lunak yang menekankan pada pembuatan prototipe dan iterasi cepat. Tujuannya adalah untuk memenuhi kebutuhan pengguna dengan lebih baik dan lebih cepat

dibandingkan dengan metode tradisional seperti *System Development Life Cycle* (SDLC) . Model ini memungkinkan pengguna untuk terlibat langsung dalam proses pengembangan, sehingga menghasilkan sistem yang lebih sesuai dengan harapan mereka (Sondang, 2024).

2.1.16 Relasi Antar Tabel

Relasi antar tabel adalah hasil dari model *entity relationship diagram*. Relasi ini akan memperlihatkan rancangan fisik basis data dan juga akan menghasilkan tabel-tabel yang nantinya dapat digunakan dalam proses implementasi sistem (Muhammad Riza Alifi et al. 2022).

2.2 Penelitian yang Relevan

Penelitian relevan adalah penelitian yang sudah pernah dilakukan sebelumnya dan dianggap relevan atau berkaitan dengan topik penelitian yang akan dilakukan. Penelitian relevan bermanfaat untuk menghindari pengulangan penelitian dengan topik yang sama.

Tabel 2.4 menunjukkan bahwa salah satu manfaat utama dari penelitian relevan adalah membantu peneliti memposisikan penelitiannya dalam konteks yang lebih luas. Dengan mengetahui penelitian-penelitian yang

telah dilakukan sebelumnya, peneliti dapat mengidentifikasi celah-celah pengetahuan yang belum terungkap dan merumuskan pertanyaan penelitian yang orisinal.

Selain itu, penelitian relevan juga dapat berfungsi sebagai sumber inspirasi bagi peneliti. Dengan mempelajari metode penelitian yang digunakan oleh peneliti lain, peneliti dapat memperoleh ide-ide baru untuk penelitiannya sendiri.

Tabel 2.4 Penelitian Yang Relevan

No	Penulis/ Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
1	(Ravi Octian Nafis,Mochamad Sidqon,Universitas 17 Agustus 1945 Surabaya, 2024)	Rancang Bangun Sistem E-Arsip Berbasis Website Menggunakan Metode Enkripsi *AES (Advanced Encryption Standard)* Studi Kasus KPU Sidoarjo	Waterfall	Merancang dan mengimplementasikan Sistem E-Arsip berbasis web di Komisi Pemilihan Umum (KPU) Sidoarjo	Studi ini bertujuan untuk merancang dan mengimplementasikan Sistem Informasi E-Arsip berbasis website di lingkungan Komisi Pemilihan Umum (KPU) Sidoarjo, dengan menerapkan metode pengembangan perangkat lunak Waterfall. Pusat perhatian utama penelitian adalah penerapan algoritma enkripsi AES dalam konteks manajemen arsip elektronik.
2	(Re Riski Dwi Andika , Sri Mulyati, 2022)	Penerapan Algoritma AES-128 Untuk Aplikasi Pengarsipan Dokumen Berbasis Web Pada Pt Studio Inovasi Teknologi	*Advanced Encryption Standard* (AES) 128 bit	Sistem pengolahan file dengan mengenkripsi file Pada Pt Studio Inovasi Teknolog	aplikasi managemen file menggunakan sistem berbasis web dengan keamanan menggunakan metode *Advanced Encryption Standard*-128 sangat diperlukan, dikarenakan file atau dokumen lebih tertata rapi dan terjaga keamanannya dibandingkan dengan penyimpanan manual, selain itu dokumen lebih mudah dicari. Dokumen yang telah tersimpan akan terenkripsi dengan sempurna sehingga dokumen aman dari penyalahgunaan serta terjaga keasliannya.

No	Penulis/ Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
3	(Yesi Puspita Dewi , Wulandari , Nofiyani, 2023)	Sistem Penyimpanan Dokumen Digital Dengan Enkripsi Menggunakan Metode Algoritma *Advanced Encryption Standard* Pada Pt Xyz	*Advanced Encryption Standard* (AES) 128	Sistem penyimpanan dokumen digital yang menerapkan enkripsi dengan metode algoritma AES (Advanced Encryption System)	Penelitian ini membangun sebuah aplikasi sistem penyimpanan dokumen digital untuk menyelesaikan masalah PT XYZ dimana dokumen digital yang berisi informasi sensitif tidak memiliki penyimpanan dan prosedur yang aman, sehingga apabila terjadi kebocoran keamanan dapat digunakan oleh pihak yang tidak diharapkan.

No	Penulis/ Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
4	(Dio Rachma Putra, Mochamad Sidqon, 2023)	Rancang Bangun Sistem Informasi E-Arsip Berbasis Website Untuk Pengamanan Dokumen Menggunakan Metode Advance Encryption Standard (AES) DKPP Kota Surabaya	Waterfall	merancang dan mengimplementasikan sistem e-arsip berbasis web di Dinas Ketahanan Pangan dan Pertanian (DKPP) Kota Surabaya dengan menerapkan metode *Advanced Encryption Standard* (AES)	Pengembangan sistem e-arsip berbasis website dengan menggunakan AES tidak hanya meningkatkan keamanan dan efisiensi pengelolaan dokumen, tetapi juga memberikan fondasi yang kokoh bagi DKPP Kota Surabaya untuk mendukung operasional mereka dengan lebih baik di masa depan.

No	Penulis/ Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
5	(Yusuf Jordan El Anwar , Roni Habibi , Noviana Riza, 2022)	Penerapan Metode Kriptografi AES Untuk Mengamankan File Dokumen	*Advanced Encryption Standard* (AES)	perkembangan perusahaan x saat ini belum memiliki suatu media untuk melakukan pengamanan file dokumen. Oleh karena itu, tujuan utama penelitian ini adalah membuat model pengamanan file dokumen.	Sistem pengamanan dokumen elektronik berbasis web dapat mengenkripsi dan mendekripsi dokumen elektronik menggunakan metode kriptografi *Advanced Encryption Standard*.

BAB III

METODOLOGI PENELITIAN

3.1 Tinjauan Umum

Dinas Ketahanan Pangan Provinsi Kalimantan Tengah sebagai salah satu instansi pemerintah memiliki kebutuhan untuk mengelola dokumen secara sistematis, aman, dan mudah diakses. Namun, pengelolaan arsip secara manual atau sistem yang kurang terintegrasi sering kali menghadapi berbagai kendala, seperti risiko kehilangan data, akses yang lambat, dan kerentanan terhadap ancaman keamanan data.

Untuk mengatasi permasalahan tersebut, implementasi sistem arsip berbasis digital dengan menggunakan teknologi enkripsi *Advanced Encryption Standard* (AES) menjadi solusi yang relevan. Enkripsi AES merupakan salah satu algoritma kriptografi yang diakui secara luas karena tingkat keamanannya yang tinggi, mampu melindungi informasi sensitif dari akses yang tidak sah. Dengan memanfaatkan sistem ini, Dinas Ketahanan Pangan Provinsi Kalimantan Tengah dapat memastikan keamanan data surat masuk dan keluar sekaligus mengamankan proses administrasi.

3.2 Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah *Research and Development* (R&D) karena metode penelitian R&D ini adalah jenis penelitian yang tahapannya meliputi penelitian awal

untuk memahami masalah, pengembangan solusi atau produk, pengujian, serta penyempurnaan hingga produk siap digunakan atau diterapkan

3.3 Desain Penelitian

Pada penelitian ini penulis menggunakan desain penelitian RAD (*Rapid Application Development*). Dan berikut tahapan yang peneliti lakukan antara lain :

a. Analisis kebutuhan

Untuk memahami alur surat, dilakukan wawancara dengan pegawai atau pengguna sistem di Dinas Ketahanan Pangan, disertai analisis dokumen arsip surat sebelumnya guna mengetahui struktur data surat yang digunakan. Selanjutnya, dilakukan identifikasi kebutuhan teknis, termasuk perangkat keras, perangkat lunak, dan kebutuhan keamanan seperti enkripsi AES. Hasil dari tahapan tersebut dituangkan dalam dokumen spesifikasi kebutuhan atau *System Requirements Specification* (SRS).

b. Design Sistem

Tahap ini mencakup perancangan arsitektur sistem, desain database, dan antarmuka pengguna. Proses enkripsi menggunakan algoritma AES dirancang untuk menjamin keamanan data surat keluar dan masuk.

c. Implementasi Sistem

Implementasi dilakukan dengan membangun sistem berbasis web menggunakan bahasa pemrograman PHP dan *framework* Laravel. Database menggunakan *MySQL* untuk menyimpan data arsip surat, sementara proses enkripsi AES diintegrasikan untuk melindungi data.

d. Pengujian Sistem

Pengujian dilakukan untuk memastikan sistem berfungsi sesuai dengan kebutuhan. Metode pengujian yang digunakan adalah *Black Box Testing*, yang difokuskan pada pengujian fungsi-fungsi sistem.

e. Evaluasi Sistem

Evaluasi sistem dilakukan melalui penyusunan laporan yang mencakup hasil pengujian performa dan keamanan sistem secara menyeluruh, dengan tujuan untuk menilai efektivitas implementasi fitur-fitur utama, seperti kecepatan proses, serta tingkat perlindungan terhadap potensi ancaman keamanan, sehingga dapat memberikan gambaran menyeluruh mengenai keandalan dan kelayakan sistem yang telah dirancang.

3.4 Instrumen Penelitian

Teknik pengumpulan data dalam kegiatan penelitian ini dilakukan dengan studi pustaka, observasi, dan wawancara yaitu :

a. Studi Pustaka

Penelitian yang dilakukan dengan cara membaca dan mempelajari buku-buku atau referensi dari internet,dan lainnya yang berhubungan dengan masalah yang akan di teliti sebagai tinjauan pustaka.

b. Observasi

Pengumpulan data dengan melakukan pengamatan langsung kelapangan untuk memperoleh data yang akurat untuk kebutuhan sistem arsip surat keluar dan masuk dengan enkripsi AES yang akan dibangun.

c. Wawancara

Pengumpulan data dengan cara melakukan komunikasi dan wawancara secara langsung dengan pihak-pihak terkait yaitu, pegawai Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.

3.5 Analisis Kebutuhan

Adapun dalam pengembangan sistem ini, agar sistem yang dibangun dapat berjalan dengan baik maka dibutuhkan suatu analis sebagai berikut. Berikut kebutuhan perangkat lunak dapat di lihat pada Tabel 3.1

Tabel 3.1 Kebutuhan Perangkat Lunak

Perangkat Lunak	Spesifikasi
Windows 11 Home 64-Bit	Sebagai sistem operasi
PHP versi 8 dan HTML versi 5	Sebagai bahasa pemrograman
Codeigniter 4 dan Bootstrap 4	Sebagai Framework sistem
Xampp versi 3.2.4	Sebagai *web server* lokal / *localhost*
MySQL	Sebagai database
Visual studio code	Sebagai kode editor untuk proses pembuatansistem informasi
Canva	Sebagai perancang desain antarmuka dan alat
Draw.io	Sebagai perancang flowchart

Pada penelitian ini penulis juga menggunakan perangkat keras komputer dalam pembuatan sistem.

Berikut kebutuhan perangkat keras dapat dilihat pada Tabel 3.2

Tabel 3.2 Kebutuhan Perangkat Keras

Perangkat Keras	Spesifikasi
Type	Lenovo IdeaPad Gaming 3 15ARH05
Processor	AMD Ryzen 5 4600H with Radeon Graphics 3.00 GHz
Memory	8,00 GB

3.6 Desain Sistem

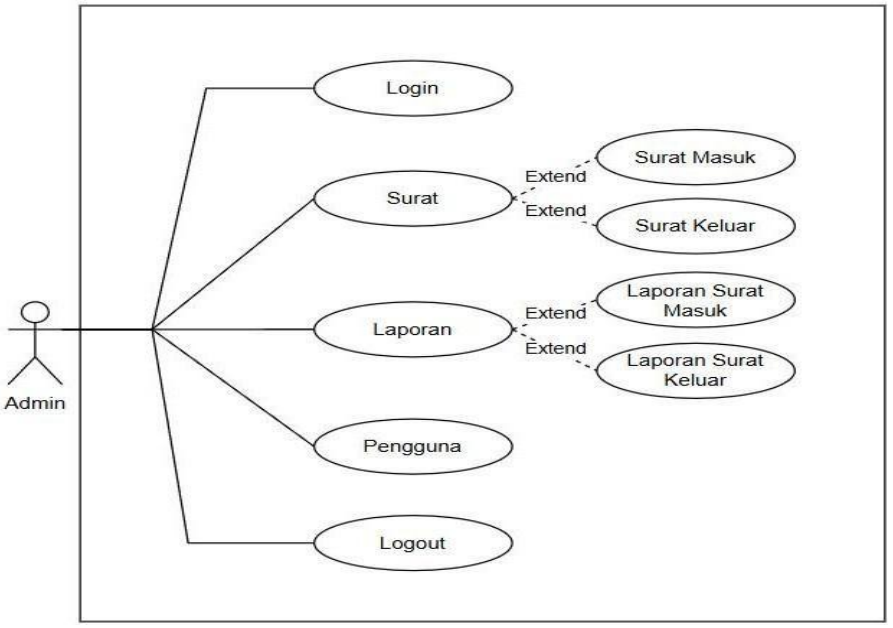
Pada bagian ini, akan diuraikan secara jelas rancangan dan desain yang bertujuan untuk menggambarkan struktur sistem yang akan bertujuan untuk menggambarkan struktur sistem yang akan dibuat oleh penulis.

3.6.1 Desain Proses

Dalam desain sistem, disini penulis menggunakan diagram UML (*Unified Modeling Languange)* dan *Flowchart.* Adapun diagram yang digunakan adalah *UseCase Diagram*, *Activity diagram* juga *Flowchart*.

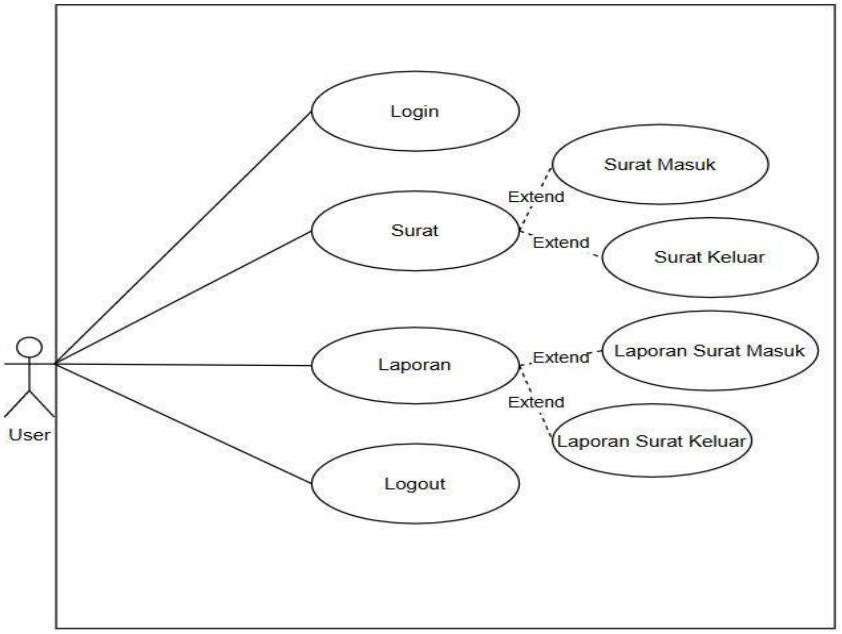
a. Use Case Diagram

Use Case Diagram adalah salah satu jenis *diagram* dalam pemodelan perangkat lunak yang digunakan untuk menggambarkan interaksi antara sistem perangkat lunak dengan berbagai aktor atau entitas yang terlibat. Tujuannya adalah untuk mengidentifikasi, menggambarkan, dan memahami bagaimana pengguna atau aktor eksternal berinteraksi dengan system perangkat lunak, serta menentukan fungsionalitas utama yang akan disediakan oleh sistem. Gambar 3. 1 merupakan *use case diagram* dari user administrator, menu yang dapat diakses, serta proses yang dialami oleh admin ketika aplikasi dijalankan.



Gambar 3.1 *Use Case Diagram Admin*

Gambar 3. 2 merupakan *use case diagram* dari *user*, menu yang dapat diakses, serta proses yang dialami oleh umum ketika aplikasi dijalankan.



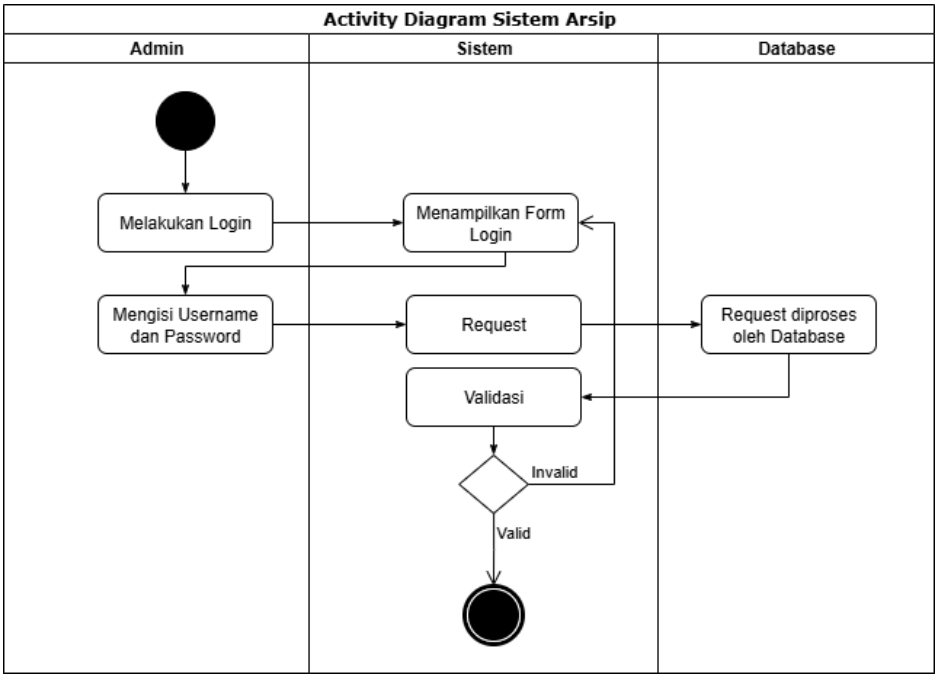
Gambar 3.2 *Use Case Diagram User*

b. Activity diagram

Pada pemodelan UML, diagram aktivitas (*Activity diagram)* adalah jenis diagram dalam pemodelan perangkat lunak yang digunakan untuk menggambarkan alur kerja atau aktivitas yang terjadi dalam suatu proses atau sistem. Tujuannya adalah untuk memberikan pandangan visual tentang bagaimana tugas, aktivitas, dan perubahan satus berlangsung dalam suatu prosesatau interaksi.

a) Activity diagram login

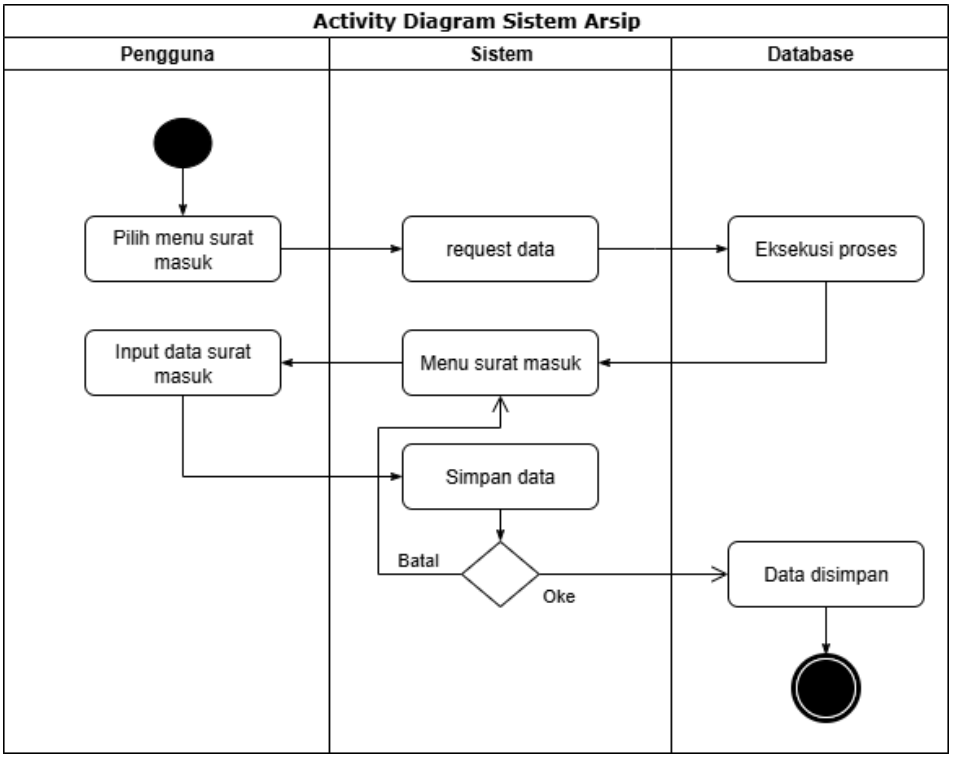
Gambar 3. 3 *A*merupakan *Activity diagram* yang menunjukkan alur *login admin* pada sistem arsip, mulai dari mengisi *username* dan *password*, memproses ke *database, h*ingga validasi berhasil atau gagal.



Gambar 3.3 *Activity Diagram Login*

b) *Activity diagram* surat masuk

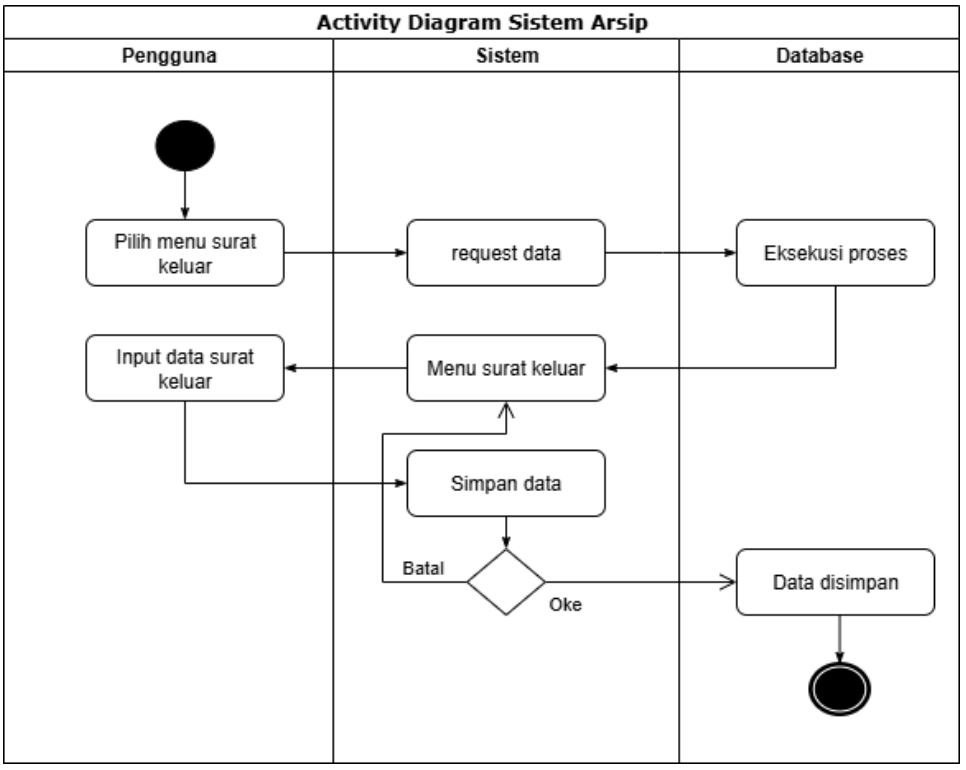
Gambar 3. 4 merupakan *Activity diagram* yang menggambarkan alur proses surat masuk pada sistem arsip, dimulai dari pengguna memilih menu surat masuk, sistem meminta data ke *database*, lalu pengguna menginput data surat masuk. Setelah itu, sistem menyimpan data dan memverifikasi apakah lanjut menyimpan (oke) atau dibatalkan, kemudian data disimpan dalam *database*.



Gambar 3. 4 *Activity Diagram* Surat Masuk

c) *Activity diagram* surat keluar

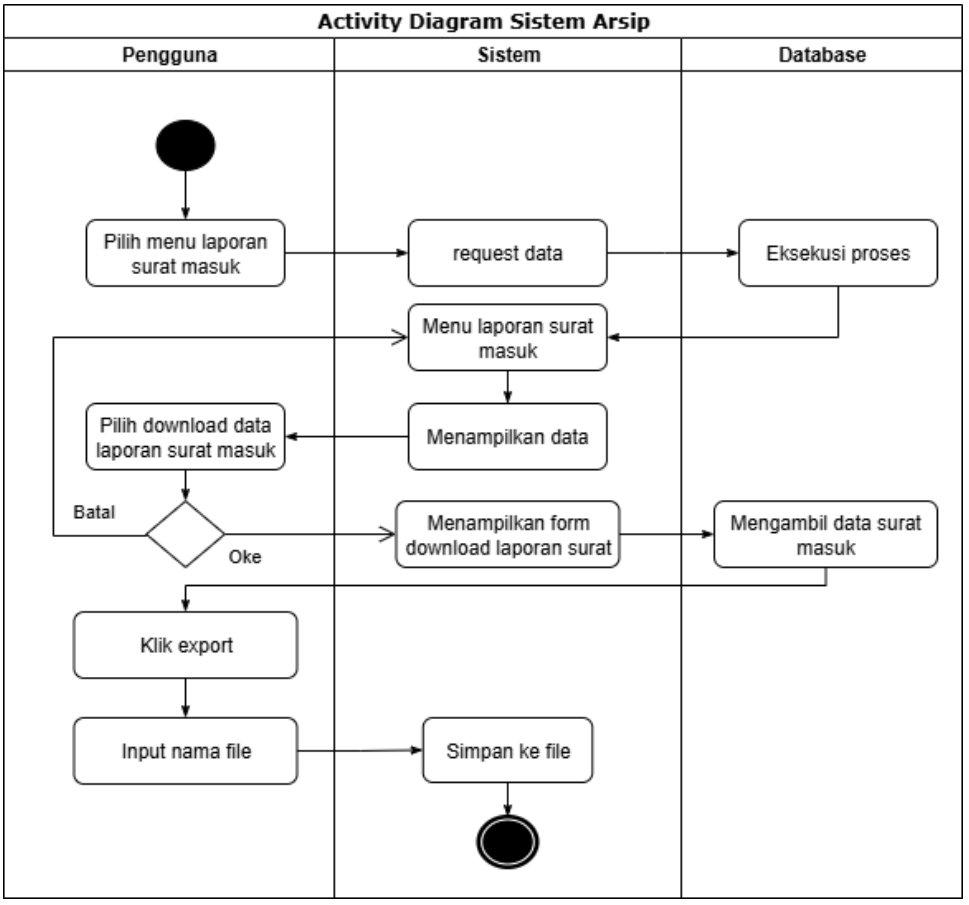
Gambar 3. 5 merupakan *Activity diagram* yang menunjukkan alur proses surat keluar pada sistem arsip, di mana pengguna memilih menu surat keluar, sistem melakukan permintaan data ke *database*, lalu pengguna menginput data surat keluar. Setelah itu, sistem menyimpan data dan memverifikasi apakah lanjut menyimpan (oke) atau dibatalkan, kemudian data disimpan dalam *database*.



Gambar 3. 5 *Activity Diagram* Surat Keluar

d) *Activity diagram l*aporan surat masuk

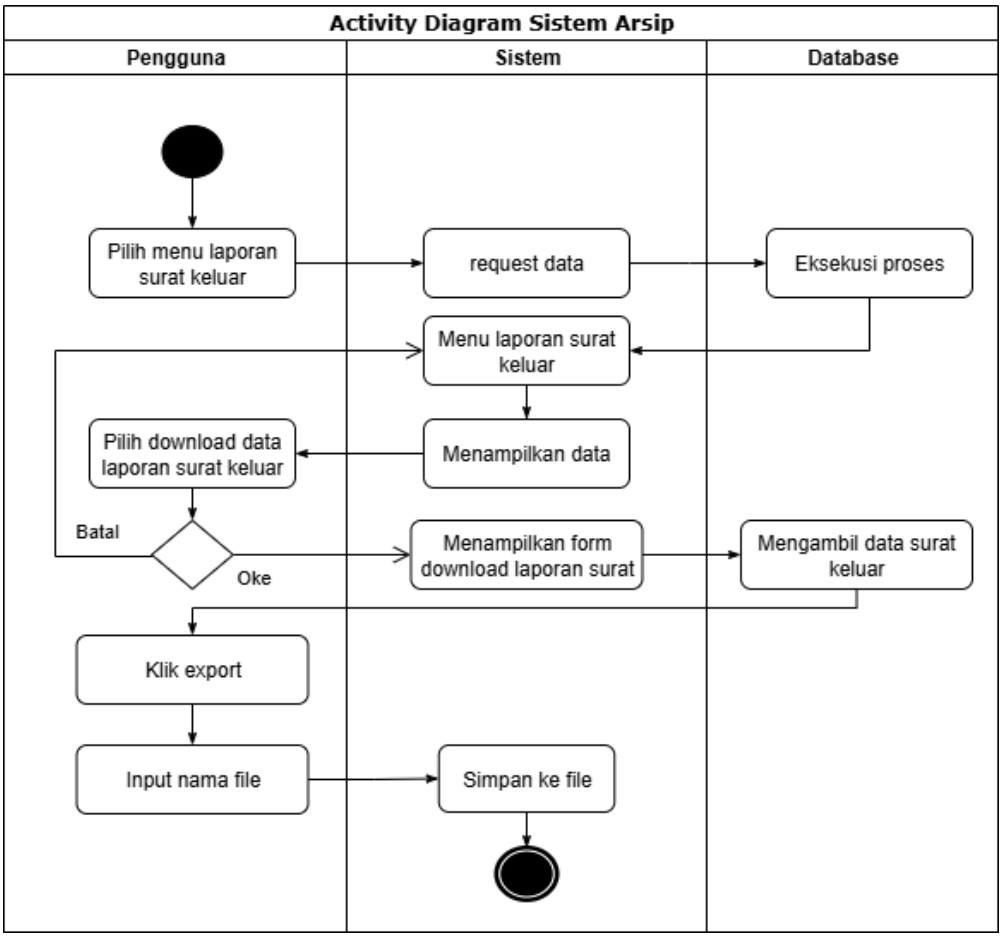
Gambar 3. 6 merupakan *Activity diagram* yang *menggambarkan alur pembuatan laporan surat masuk, dimulai dari pengguna memilih menu laporan, sistem mengambil dan menampilkan data dari database, lalu pengguna memilih untuk mengunduh laporan. Jika disetujui, pengguna klik ekspor, memasukkan nama file, dan sistem menyimpan laporan ke file.*



Gambar 3. 6 *Activity Diagram* Laporan Surat Masuk

e) *Activity diagram* Laporan Surat keluar

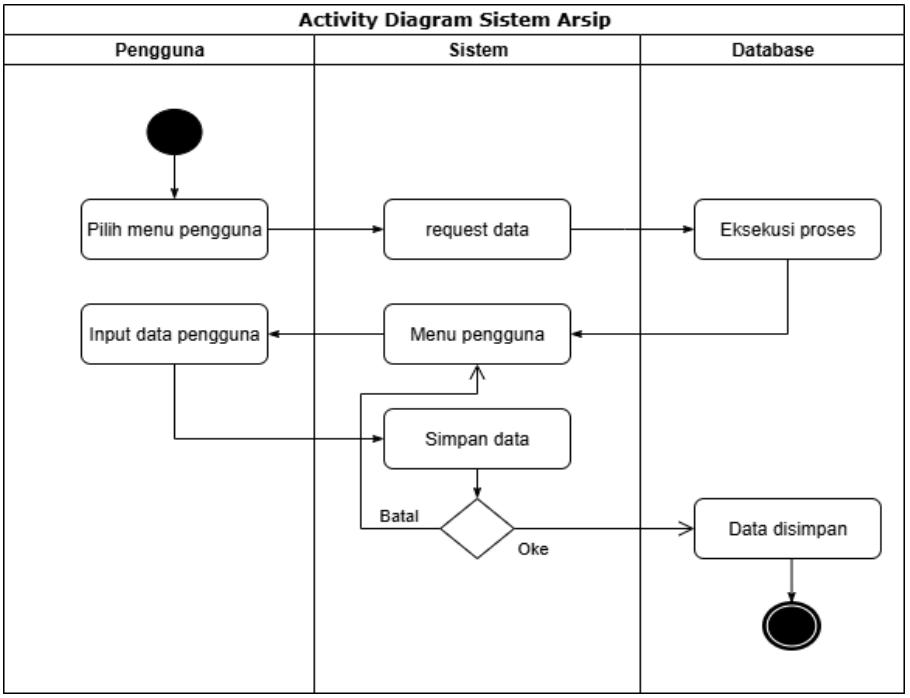
Gambar 3. 7 merupakan *Activity diagram* yang menjelaskan alur pembuatan laporan surat keluar, dimulai dari pengguna memilih menu laporan, sistem mengambil dan menampilkan data dari *database*, lalu pengguna memilih *download* laporan. Jika disetujui, pengguna klik ekspor, memasukkan nama file, dan sistem menyimpan data ke file.



Gambar 3. 7 *Activity Diagram* Laporan Surat Keluar

f) *Activity diagram* pengguna

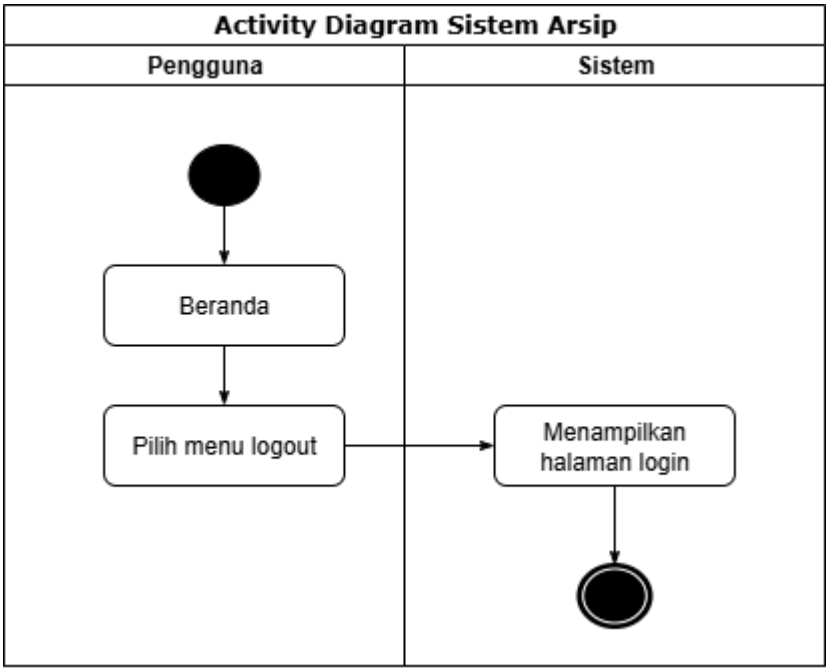
Gambar 3. 8 merupakan *Activity diagram* yang menggambarkan alur aktivitas pengguna saat memilih menu, menginput data, dan menyimpan data. Proses dimulai dari pengguna yang memilih menu, sistem melakukan permintaan data ke database, lalu menampilkan menu pengguna. Setelah pengguna menginput data, sistem mencoba menyimpan data; jika berhasil, data disimpan di database, jika batal maka proses berhenti. Diagram ini menunjukkan interaksi antara pengguna, sistem, dan database dalam pengelolaan arsip.



Gambar 3. 8 *Activity Diagram* Pengguna

g) Activity diagram logout

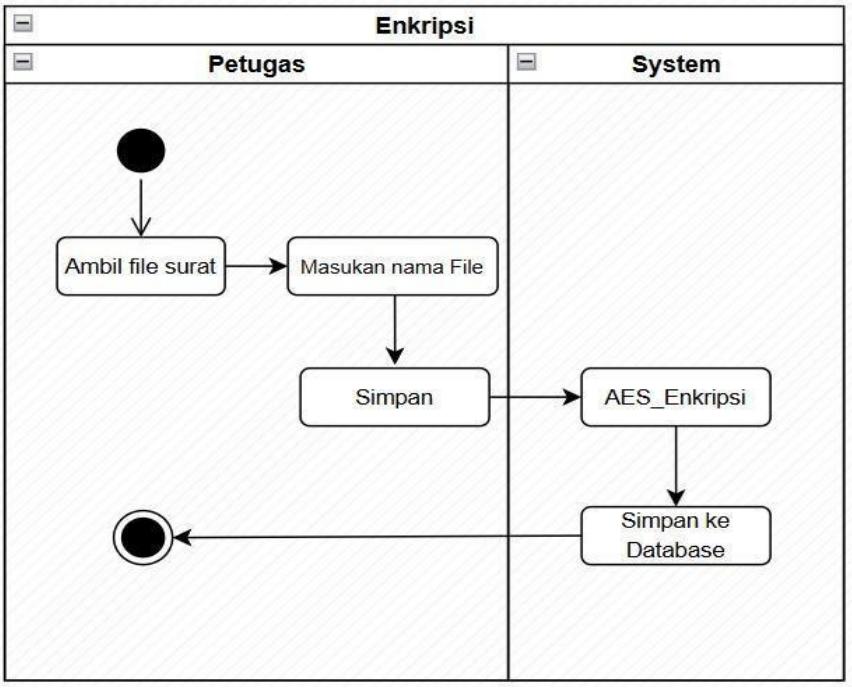
Gambar 3. 9 merupakan *Activity diagram* yang menggambarkan proses *logout* pada sistem arsip. Dimulai dari pengguna berada di halaman Beranda, lalu memilih menu *logout.* Setelah itu, sistem akan merespons dengan menampilkan halaman *login,* yang menandai akhir aktivitas.



Gambar 3.9 *Activity Diagram Logout*

h) Activity diagram Enkripsi

Gambar 3.10 Merupakan *Activity diagram* enkripsi yang menggambarkan proses enkripsi file surat yang melibatkan dua aktor, yaitu Petugas dan System. Proses dimulai dengan petugas mengambil file surat dan memasukkan nama file ke dalam sistem. Selanjutnya, petugas memasukkan kunci (*key*) enkripsi yang diperlukan untuk proses keamanan data. Setelah itu, file dan kunci enkripsi disimpan, dan sistem secara otomatis menjalankan proses enkripsi menggunakan algoritma *AES (Advanced Encryption Standard)*. File yang sudah terenkripsi kemudian disimpan ke dalam database, dan proses berakhir. Diagram ini menampilkan alur komunikasi dan aktivitas yang terjadi antara petugas dan sistem secara jelas, dengan pembagian tugas yang terstruktur.

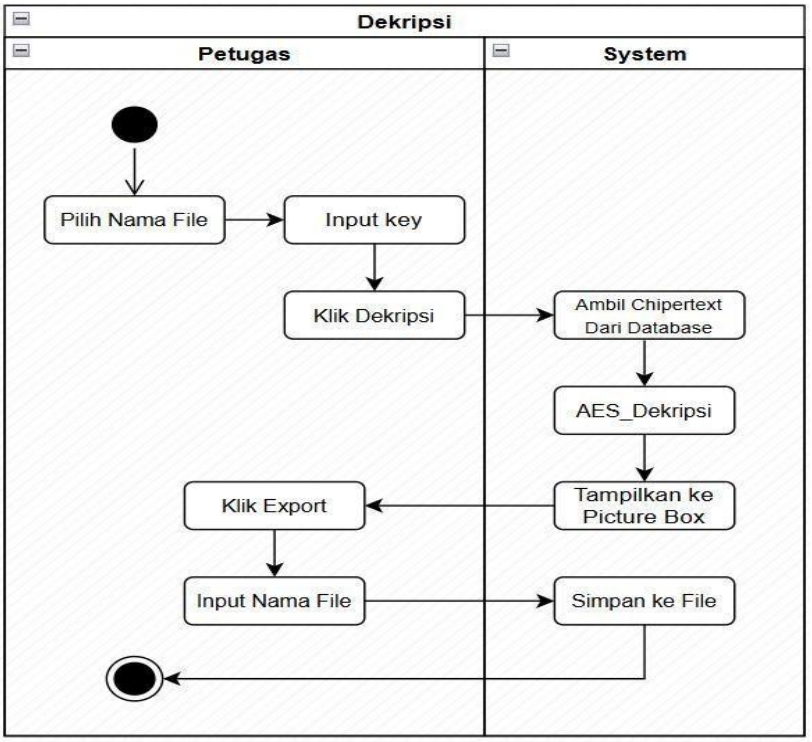


Gambar 3.10 *Activity diagram Enkripsi*

i) Activity diagram Dekripsi

Gambar 3.11 Merupakan *Activity diagram* dekripsi yang menggambarkan proses dekripsi file yang dilakukan oleh Petugas dengan bantuan System. Proses dimulai dengan petugas memilih nama file yang akan didekripsi, kemudian memasukkan kunci (*key*) yang sesuai. Setelah itu, petugas mengklik tombol "Dekripsi", dan sistem mengambil data terenkripsi (*ciphertext*) dari database. Sistem kemudian menjalankan algoritma dekripsi AES (*AES_Decrypt*) untuk mengembalikan data ke bentuk aslinya dan menampilkannya ke dalam Picture Box. Petugas kemudian dapat mengekspor file hasil dekripsi dengan

memasukkan nama file baru, dan system menyimpannya ke file yang diinginkan. Proses ini memastikan bahwa data yang didekripsi aman dan terstruktur dengan baik.



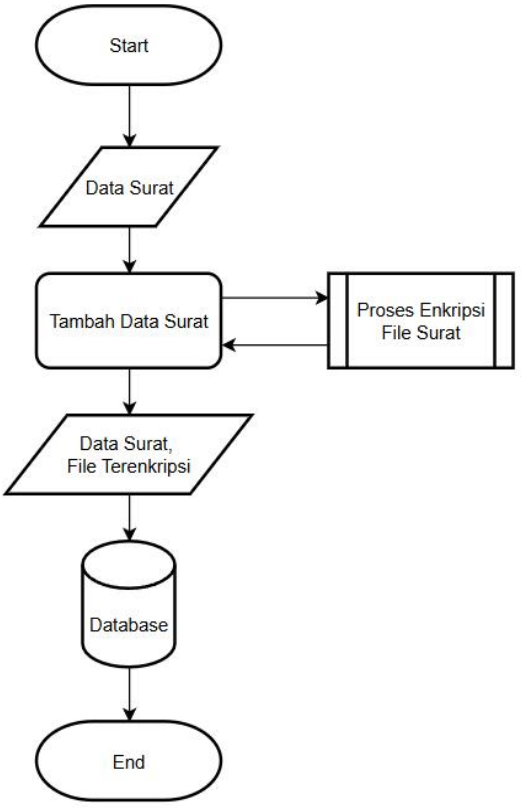
Gambar 3.11*Activity diagram Dekripsi*

c. Flowchart

Algoritma AES-128 akan diimplementasikan pada bagian tambah data surat, baik surat masuk dan surat keluar, adapun yang akan diamankan ialah file dokumen surat yang akan disimpan kedalam database. Sehingga file dokumen surat aman di simpan ke database dan terhindar dari sql injection. Berikut diagram alur dari proses enkripsi tambah data surat dan tambah data user:

a) Flowchart enkripsi data file surat

Gambar 3. 1 2 merupakan gambaran alur dari data surat yang ditambahkan oleh user kemudian dienkripsi lalu disimpan kedalam database.

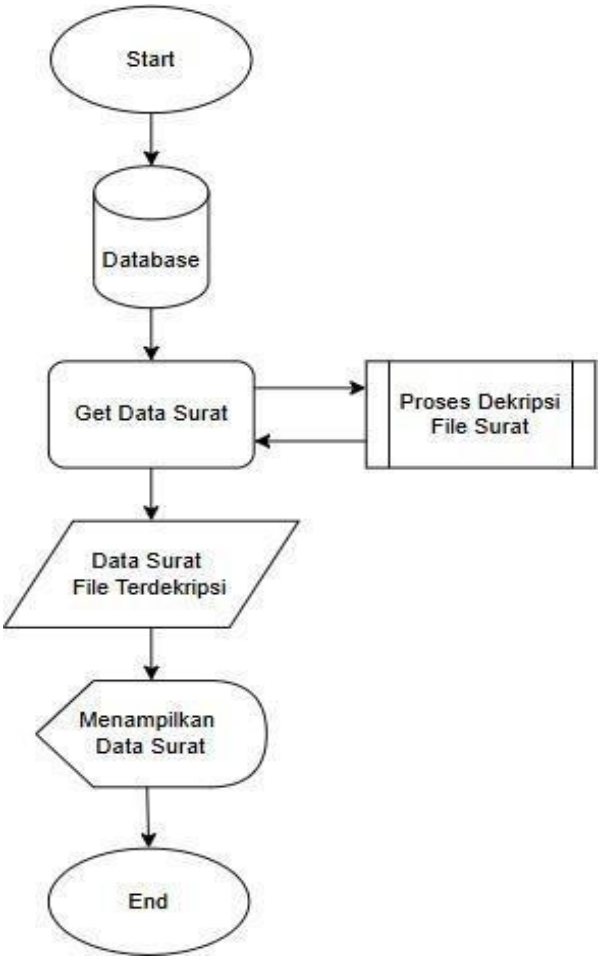


Gambar 3.12 Flowchart Enkripsi Data Surat

Selain alur dari enkripsi data surat, juga terdapat alur proses dekripsi data surat. Proses dimulai dengan mengambil data dari database, kemudian dilakukan Get Data Surat yang mengarah pada proses dekripsi file surat. Hasil dari proses dekripsi berupa data surat dan nama file yang telah terdekripsi. Selanjutnya, data surat ditampilkan dan proses berakhir. Agar lebih jelas berikut flowchart dari alur dekripsi data surat.

b) Flowchart proses dekripsi data surat

Gambar 3. 1 3 alur dari proses dekripsi data surat kemudian ditampilkan ke *interface* Ketika *menu* administrasi di akses.



Gambar 3.13 *Flowchart* Dekripsi Data Surat

3.6.2 Desain Enkripsi AES

Enkripsi *Advanced Encryption Standard* (AES) adalah salah satu algoritma simetris yang sering digunakan karena keamanannya yang tinggi. Dalam konteks Sistem Arsip Surat Keluar dan Masuk Berbasis Enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah, algoritma AES dapat diterapkan untuk melindungi data sensitif, seperti isi surat, identitas pengirim, dan penerima surat.

a. Desain Arsitektur Sistem
   a) Frontend: Sistem berbasis web dengan *Codeigniter*4.Backend: API menggunakan Node.js atau PHP yang akan menangani proses enkripsi dan dekripsi.
   b) Database: *MySQL* sebagai media penyimpanan.

b. Data yang Akan Dienkripsi

   Berikut adalah data sensitif yang akan diamankan menggunakan AES:

   a) Isi Surat:
      1) Tujuan: Melindungi isi dokumen dari akses tidak sah.
      2) Format: Plain text atau dokumen yang diunggah.
   b) Identitas Pengirim dan Penerima:

      Nama, jabatan, dan instansi yang terkait.

c) Nomor Surat:

Nomor penting yang digunakan untuk penelusuran.

d) Lampiran:

File lampiran surat PDF dienkripsi sebelum disimpan di server.

c. Proses Kerja AES pada Aplikasi

a) Penyimpanan Data

1) Input Data: Pengguna mengisi *form*ulir atau mengunggah dokumen melalui frontend.

2) Enkripsi: Data yang diterima backend dienkripsi menggunakan AES (dengan kunci rahasia yang hanya diketahui oleh sistem).

3) Penyimpanan: Data yang telah dienkripsi disimpan di database atau penyimpanan cloud.

b) Pengambilan Data

1) Query: Data dienkripsi diambil dari database.

2) Dekripsi: Sistem mendekripsi data menggunakan kunci rahasia.

3) Output: Data ditampilkan kembali dalam bentuk asli (plaintext) kepada pengguna yang berhak.

d. Struktur Database yang Terenkripsi

Tabel 3.3 Tabel Database yang Terenkripsi

Tabel	Kolom	Enkripsi	Keterangan
surat_masuk	id_surat	Tidak	ID unik untuk identifikasi.
	isi_surat	AES (128-bit key)	Isi surat dienkripsi.
	pengirim	Tidak	Identitas pengirim tidak dienkripsi
	tanggal_terima	Tidak	Informasi tanggal tidak dienkripsi
surat_keluar	id_surat	Tidak	ID unik untuk identifikasi.
	isi_surat	AES (128-bit key)	Isi surat dienkripsi.
	penerima	Tidak	Identitas penerima tidak dienkripsi
	tanggal_kirim	Tidak	Informasi tanggal tidak dienkripsi

3.6.3 Desain *Interface*

Pada tahap ini akan dijelaskan desain *interface* pada halaman –

halaman didalam media pembelajaran ini nantinya. Adapun rancangan desain *interface* adalah sebagai berikut:

a. Desain *Login*

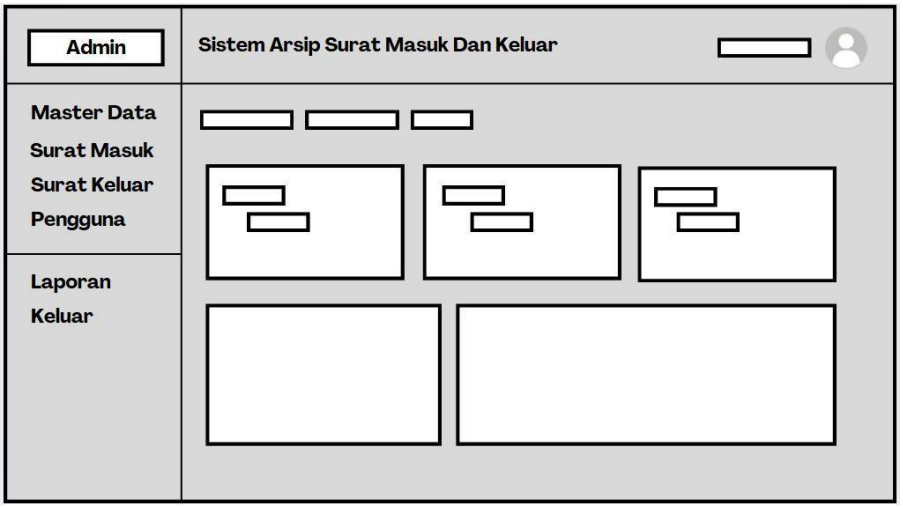
Tampilan Desain *login* adalah rancangan yang akan ditampilkan saat *admin* atau *operator* ingin masuk kedalam halaman *dashboard*. Halaman ini berisi *form* untuk memverifikasi apakah *admin* atau operator memasukkan data yang valid. Tampilan halaman login dapat dilihat pada Gambar 3.14.



Gambar 3.14 Desain Halaman Login

b. Desain *Dashboard*

Tampilan Desain *dasboard* adalah rancangan yang akan ditampilkan ketika admin atau operator berhasil *login*. Halaman ini berisikan master data, surat masuk, surat keluar, pengguna, laporan dan keluar/logout. Tampilan halaman *dasboard* dapat dilihat pada Gambar 3.15.

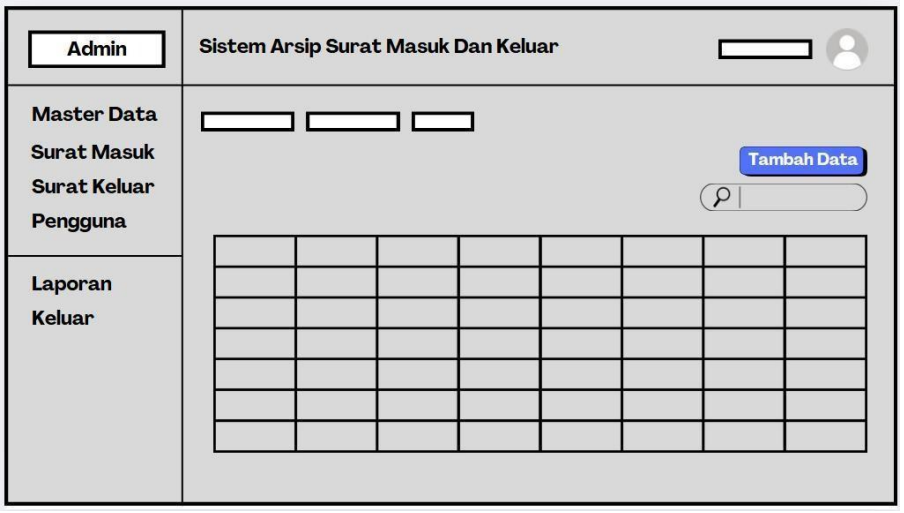


Gambar 3.15 Desain Halaman *dashboard*

c. Desain Surat Masuk dan Surat Keluar

Tampilan surat masuk dan surat keluar memilik kegunaan yang sama yaitu untuk menampilkan data surat masuk dan surat keluar yang di simpan di dalam data base. Secara fitur dapat melakukan *insert*, *preview*, *delete* dan *download* data surat. Komponen yang digunakan pada tampilan data surat masuk dan surat keluar antara lain komponen tombol, komponen teks, komponen *card*, komponen tabel untuk menampung data yang akan

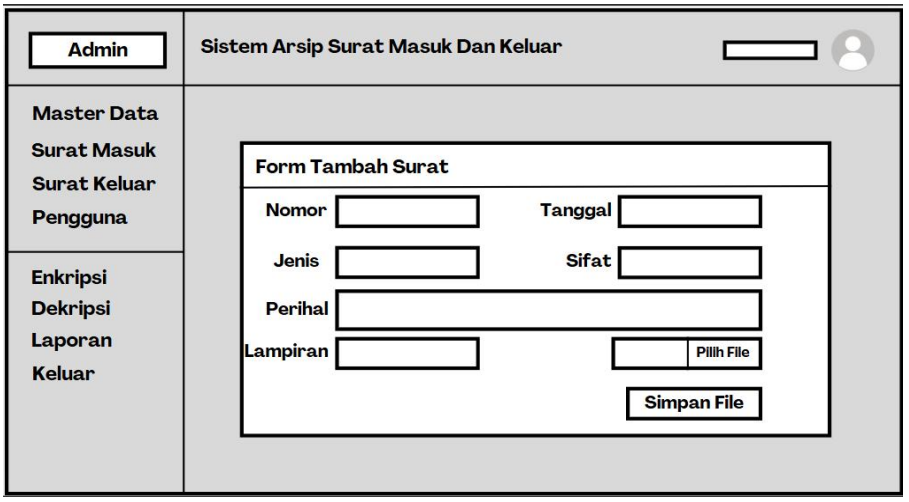
ditampilkan ke *user*. Tampilan desain bisa dilihat pada Gambar 3.16.



Gambar 3.16 Desain Surat Masuk dan Surat Keluar

d. Desain Enkripsi File

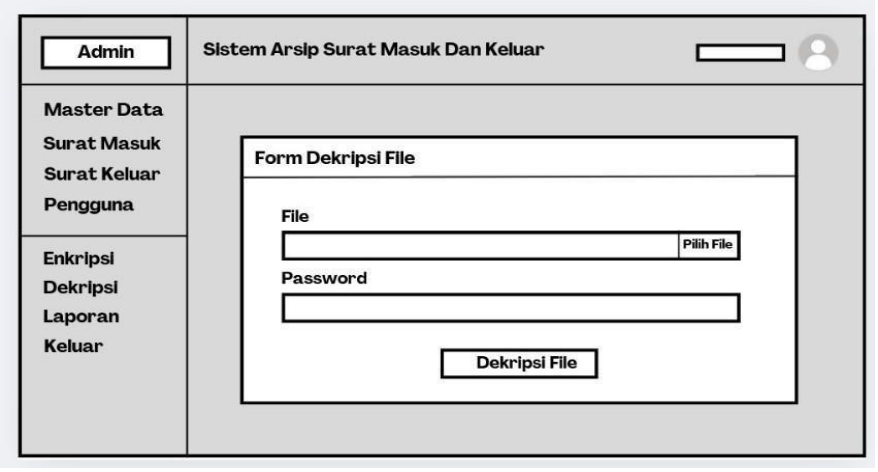
Tampilan desain ini merupakan antarmuka *Form* Tambah Surat pada sistem arsip surat masuk dan keluar, yang dilengkapi fitur penyimpanan file secara langsung. Saat pengguna mengisi data surat dan mengunggah lampiran, tombol "Simpan File" akan secara otomatis memicu proses enkripsi terhadap file yang diunggah menggunakan metode seperti AES sebelum disimpan ke sistem. Meskipun proses enkripsi tidak ditampilkan secara eksplisit di antarmuka, namun sistem dirancang untuk mengamankan lampiran secara otomatis saat penyimpanan guna menjaga kerahasiaan dan integritas data surat.. Tampilan desain bisa dilihat pada Gambar 3.17.



Gambar 3.17 Desain Enkripsi File

e. Desain Dekripsi File

Halaman dekripsi file merupakan halaman untuk melakukan dekripsi file yang terenkripsi. User wajib memasukkan file/dokumen yang terenkripsi dengan menekan tombol choose file setelah itu user juga harus memasukkan password dari file enkripsi tersebut. Tampilan desain bisa dilihat pada Gambar 3.18.



Gambar 3.18 Desain Dekripsi File

BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil

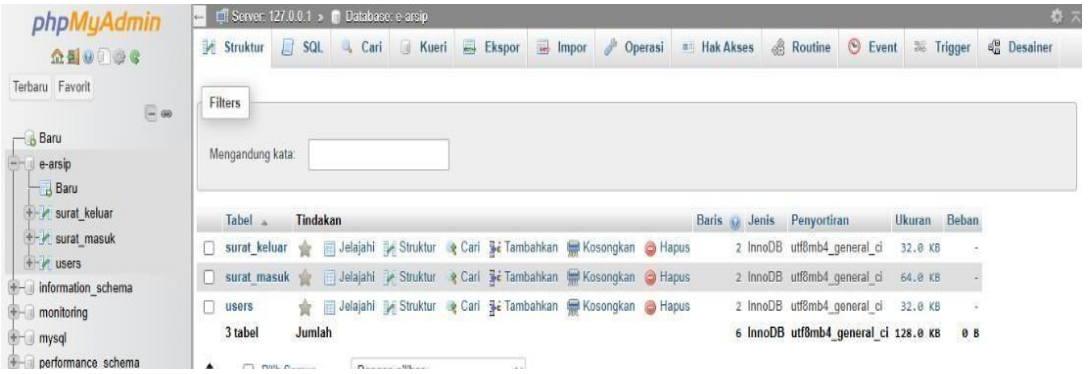
4.1.1 Gambaran Umum Sistem

Sistem e-arsip surat keluar dan masuk yang dikembangkan merupakan sebuah aplikasi berbasis web yang dirancang untuk membantu proses digitalisasi, pengelolaan, dan pengamanan arsip surat di lingkungan Dinas Ketahanan Pangan Provinsi Kalimantan Tengah. Sistem ini memungkinkan pengguna untuk menginput, menyimpan, mencari, serta mengakses arsip surat baik yang masuk maupun yang keluar. Salah satu keunggulan utama dari sistem ini adalah penerapan algoritma *Advanced Encryption Standard* (AES) pada file surat yang diunggah, sehingga informasi penting dalam dokumen dapat terlindungi dari akses tidak sah. Sistem dibangun menggunakan teknologi pemrograman web seperti PHP dan *MySQL* sebagai basis data. Terdapat dua jenis pengguna dalam sistem, yaitu admin dan user.

4.1.2 Implementasi Database

a. Tabel Utama Database

Database yang digunakan dalam sistem arsip surat keluar dan masuk ini diberi nama e-arsip dan dibangun menggunakan sistem manajemen basis data *MySQL*, tampilan tabel utama database bisa dilihat pada Gambar 4.1.

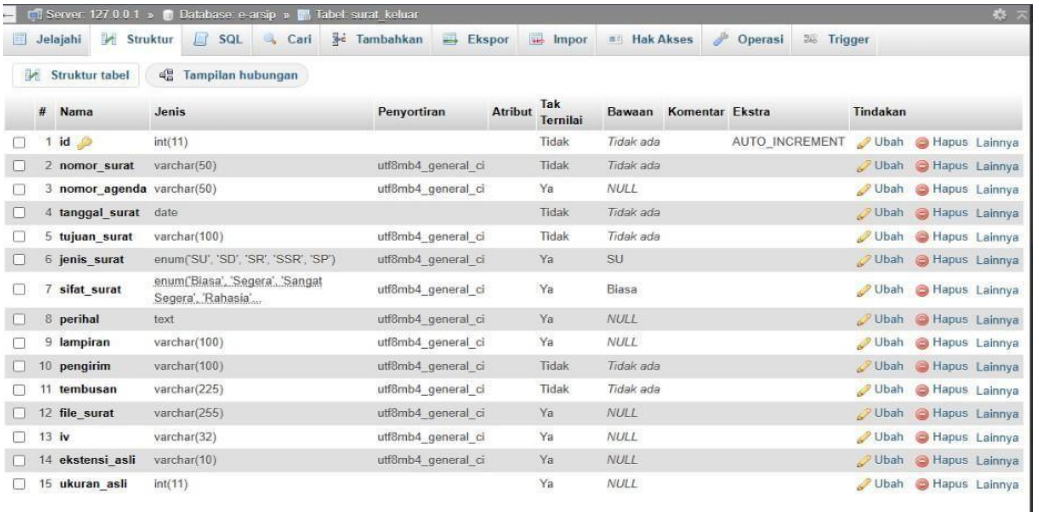


Gambar 4.1 Tabel Utama Database

Dalam database ini terdapat tiga tabel utama, yaitu users, surat_masuk, dan surat_keluar. Tabel users menyimpan data pengguna sistem, baik admin maupun user biasa, yang terdiri dari informasi seperti username, password (telah di-hash), dan level akses. Tabel ini sangat penting untuk mengatur hak akses masing-masing pengguna dalam sistem. Selanjutnya, tabel surat_masuk berfungsi untuk menyimpan seluruh data surat yang diterima instansi, termasuk nomor surat, pengirim, tanggal surat, dan isi surat yang telah dienkripsi menggunakan algoritma AES guna menjaga kerahasiaan informasi. Sementara itu, tabel surat_keluar menyimpan data surat yang dikirim oleh instansi kepada pihak lain, dengan struktur data yang hampir serupa dengan surat masuk, yakni mencakup nomor surat, penerima, tanggal, dan isi surat yang juga dienkripsi. Ketiga tabel ini membentuk dasar penyimpanan dan pengelolaan data dalam sistem, sehingga mendukung proses digitalisasi arsip secara aman, dan cepat di lingkungan Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.

b. Tabel Surat Keluar

Tabel surat_keluar dalam database e-arsip digunakan untuk menyimpan data surat yang dikeluarkan oleh instansi, tampilan tabel surat keluar database bisa dilihat pada Gambar 4.1.2.



#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	id	int(11)			Tidak	*Tidak ada*		AUTO_INCREMENT	Ubah Hapus Lainnya
2	nomor_surat	varchar(50)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
3	nomor_agenda	varchar(50)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
4	tanggal_surat	date			Tidak	*Tidak ada*			Ubah Hapus Lainnya
5	tujuan_surat	varchar(100)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
6	jenis_surat	enum('SU', 'SD', 'SR', 'SSR', 'SP')	utf8mb4_general_ci		Ya	SU			Ubah Hapus Lainnya
7	sifat_surat	enum('Biasa', 'Segera', 'Sangat Segera', 'Rahasia'...	utf8mb4_general_ci		Ya	Biasa			Ubah Hapus Lainnya
8	perihal	text	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
9	lampiran	varchar(100)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
10	pengirim	varchar(100)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
11	tembusan	varchar(225)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
12	file_surat	varchar(255)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
13	iv	varchar(32)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
14	ekstensi_asli	varchar(10)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
15	ukuran_asli	int(11)			Ya	*NULL*			Ubah Hapus Lainnya

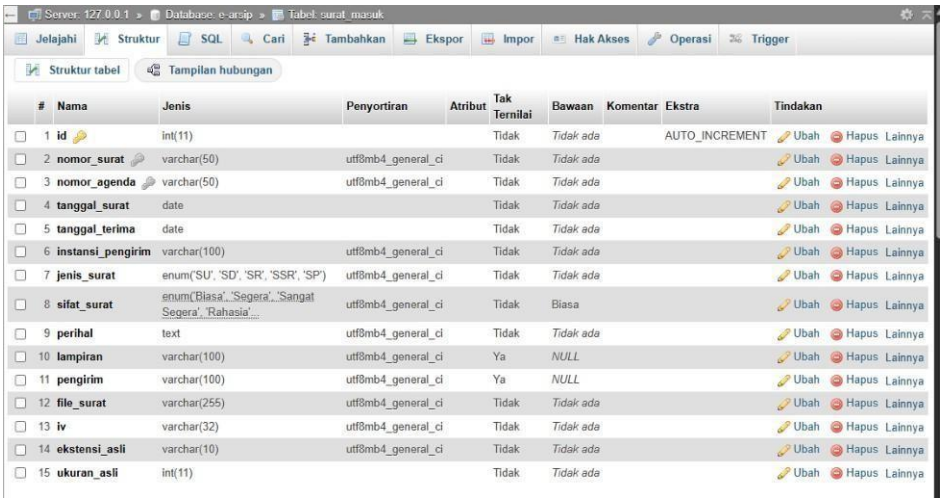
Gambar 4.2 Tabel Surat Keluar

Tabel ini terdiri dari beberapa kolom penting seperti id sebagai identitas unik surat, nomor_surat dan nomor_agenda sebagai penanda administratif, serta tanggal_surat, tujuan_surat, jenis_surat, dan sifat_surat yang menjelaskan karakteristik surat. Kolom perihal, lampiran, pengirim, dan tembusan digunakan untuk mencatat isi ringkas surat, file pendukung, pengirim surat, serta pihak-pihak yang ditembuskan. Untuk menjamin keamanan data, sistem menyimpan file surat dalam bentuk terenkripsi pada kolom file_surat, dengan nilai iv (*Initialization Vector*) untuk proses enkripsi AES, serta mencatat ekstensi_asli

dan ukuran_asli file. Struktur ini mendukung pengelolaan arsip digital surat keluar secara aman, dan mudah diakses oleh pengguna sesuai hak aksesnya.

c. Tabel Surat Masuk

Tabel surat_masuk pada database e-arsip digunakan untuk menyimpan data surat yang diterima oleh instansi, tampilan tabel surat masuk database bisa dilihat pada Gambar 4.1.3.



#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	id	int(11)			Tidak	Tidak ada		AUTO_INCREMENT	Ubah Hapus Lainnya
2	nomor_surat	varchar(50)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
3	nomor_agenda	varchar(50)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
4	tanggal_surat	date			Tidak	Tidak ada			Ubah Hapus Lainnya
5	tanggal_terima	date			Tidak	Tidak ada			Ubah Hapus Lainnya
6	instansi_pengirim	varchar(100)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
7	jenis_surat	enum('SU', 'SD', 'SR', 'SSR', 'SP')	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
8	sifat_surat	enum('Biasa', 'Segera', 'Sangat Segera', 'Rahasia'...	utf8mb4_general_ci		Tidak	Biasa			Ubah Hapus Lainnya
9	perihal	text	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
10	lampiran	varchar(100)	utf8mb4_general_ci		Ya	NULL			Ubah Hapus Lainnya
11	pengirim	varchar(100)	utf8mb4_general_ci		Ya	NULL			Ubah Hapus Lainnya
12	file_surat	varchar(255)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
13	iv	varchar(32)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
14	ekstensi_asli	varchar(10)	utf8mb4_general_ci		Tidak	Tidak ada			Ubah Hapus Lainnya
15	ukuran_asli	int(11)			Tidak	Tidak ada			Ubah Hapus Lainnya

Gambar 4.3 Tabel Surat Masuk

Tabel ini memiliki kolom id sebagai kunci utama yang bersifat auto-increment, serta nomor_surat dan nomor_agenda sebagai identifikasi administratif surat. Informasi tanggal disimpan melalui kolom tanggal_surat dan tanggal_terima, sedangkan kolom instansi_pengirim mencatat asal surat. Jenis dan sifat surat ditentukan melalui kolom jenis_surat dan sifat_surat dengan tipe enum yang membatasi pilihan seperti SU, SD, SR, hingga kategori kerahasiaan seperti Biasa atau

Rahasia. Untuk mendeskripsikan isi dan detail dokumen, digunakan kolom perihal, lampiran, dan pengirim. File surat yang diterima disimpan secara terenkripsi di kolom file_surat, dengan nilai iv sebagai *Initialization Vector* untuk proses enkripsi AES. Selain itu, sistem juga mencatat format file asli dalam kolom ekstensi_asli dan ukuran file melalui ukuran_asli, sehingga seluruh data arsip surat masuk dapat dikelola secara digital dengan aman

d. Tabel Users

Tabel users pada database e-arsip berfungsi untuk menyimpan data pengguna sistem, baik sebagai admin maupun pengguna biasa, yang memiliki peran penting dalam proses autentikasi dan manajemen hak akses, tampilan tabel user database bisa dilihat pada Gambar 4.1.4.



#	Nama	Jenis	Penyortiran	Atribut	Tak Ternilai	Bawaan	Komentar	Ekstra	Tindakan
1	id	int(11)			Tidak	*Tidak ada*		AUTO_INCREMENT	Ubah Hapus Lainnya
2	nama	varchar(100)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
3	email	varchar(100)	utf8mb4_general_ci		Ya	*NULL*			Ubah Hapus Lainnya
4	username	varchar(100)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
5	password	varchar(255)	utf8mb4_general_ci		Tidak	*Tidak ada*			Ubah Hapus Lainnya
6	role	enum('admin', 'pengguna')	utf8mb4_general_ci		Ya	admin			Ubah Hapus Lainnya
7	status	enum('aktif', 'nonaktif')	utf8mb4_general_ci		Ya	aktif			Ubah Hapus Lainnya

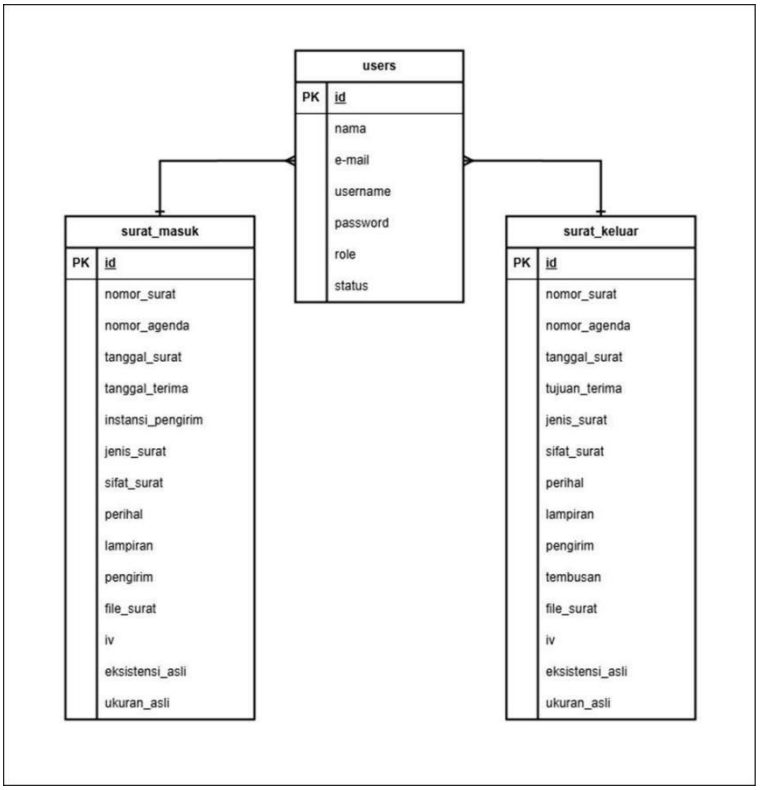
Gambar 4.4 Tabel Users

Tabel ini terdiri dari beberapa kolom utama, antara lain id sebagai primary key yang diatur auto-increment, nama dan

email untuk mencatat identitas pengguna, serta username dan password yang digunakan saat proses login, di mana password biasanya dienkripsi atau di-hash untuk menjaga keamanan. Kolom role berisi tipe data enum yang menentukan peran pengguna, yaitu antara 'admin' dan 'pengguna', yang akan memengaruhi fitur-fitur sistem yang dapat diakses. Selain itu, kolom status mencatat apakah akun pengguna dalam kondisi 'aktif' atau 'nonaktif', sehingga administrator dapat mengatur izin akses tanpa harus menghapus akun. Struktur tabel ini memungkinkan sistem berjalan secara aman dan terkontrol dengan baik, serta mendukung pengelolaan pengguna dalam aplikasi arsip surat.

e. Tabel Relasi

Sistem e-Arsip dirancang untuk mengelola surat masuk dan keluar secara digital. Untuk mendukung kebutuhan tersebut, digunakan tiga tabel utama dalam basis data, yaitu: users, surat_keluar, dan surat_masuk.



Gambar 4.5 Tabel Relasi

Gambar tersebut merupakan diagram relasi antar tabel dalam sebuah sistem arsip surat berbasis database, yang terdiri dari tiga tabel utama: User, Surat Masuk, dan Surat Keluar. Tabel User menyimpan data pengguna sistem seperti nama, email, username, password, role, dan status. Tabel ini memiliki relasi satu ke banyak (*one-to-many*) dengan tabel Surat Masuk dan Surat Keluar, yang ditunjukkan dengan garis panah. Artinya,satu pengguna dapat menginput atau menangani banyak surat masuk dan surat keluar.

Tabel Surat Masuk menyimpan informasi terkait surat yang diterima, seperti nomor surat, nomor agenda, tanggal surat,

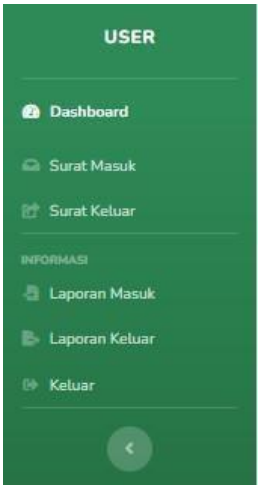
tanggal terima, instansi pengirim, jenis dan sifat surat, perihal, lampiran, pengirim, file surat, level keamanan (iv), eksistensi asli, serta ukuran dokumen asli. Sedangkan tabel Surat Keluar menyimpan data surat yang dikirim keluar oleh instansi, meliputi informasi yang hampir serupa dengan Surat Masuk, namun ditambah dengan kolom tujuan_surat dan tembusan.

4.1.3 Implementasi Hak Pengguna (User) Dan Admin

Dalam sistem e-arsip yang dikembangkan, terdapat dua jenis pengguna utama, yaitu Admin dan User (Pengguna).

a. Pengguna (User)

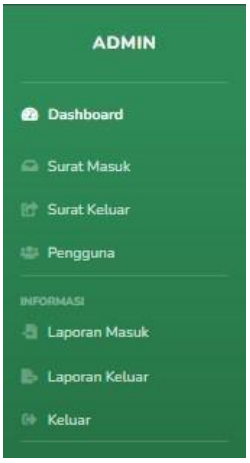
Pengguna (user) memiliki akses terhadap fitur utama sistem seperti input dan pengelolaan surat masuk dan surat keluar, melihat daftar surat masuk dan keluar, melihat laporan surat masuk dan keluar, serta proses enkripsi dan dekripsi file surat, tampilan halaman user bisa dilihat pada Gambar 4.6.



Gambar 4.6 Hak Akses Pengguna (User)

b. Admin

Admin memiliki akses terhadap fitur utama sistem namun terdapat akses tambahan untuk mengelola data pengguna, yang mencakup menambahkan user baru, mengedit data pengguna, mengubah status akun (aktif/nonaktif), dan menentukan peran pengguna (admin atau user), tampilan halaman admin bisa dilihat pada Gambar 4.7.



Gambar 4.7 Hak Akses Admin

4.1.4 Proses Enkripsi dan Dekripsi Surat (AES)

Sistem e-arsip ini menerapkan algoritma *Advanced Encryption Standard* (AES) untuk menjaga kerahasiaan file surat yang diunggah ke dalam sistem, baik surat masuk maupun surat keluar.

a. Enkripsi dan Dekripsi Surat Keluar

1. Enkripsi Surat

```
1 reference
protected const UKURAN_MAKSIMAL_FILE = 10240; // 10MB dalam KB
1 reference
protected const JENIS_FILE_DIIZINKAN = ['pdf', 'doc', 'docx'];
2 references
protected const ITERASI_PBKDF2 = 10000;
2 references
protected const PANJANG_KUNCI_AES = 32;
1 reference
protected const PANJANG_IV = 16; // Untuk AES-128
1 reference
protected const STATIC_PASSWORD = 'Dishanpang'; // Ganti dengan password kuat
9 references
protected $suratKeluarModel;
1 reference
protected $enkripsi;
3 references
protected $validasi;
```

Gambar 4.8 Aturan Enkripsi File Surat Keluar

Password statis “Dishampang” digunakan sebagai dasar enkripsi file. Sistem juga membatasi jenis file yang diizinkan untuk diunggah hanya pada format PDF, DOC, dan DOCX, serta membatasi ukuran file maksimal hingga 10 MB (10240

```
0 references | 0 overrides
public function simpan_surat(): RedirectResponse
{
    if (!$this->validasiInput()) {
        return $this->redirectDenganError();
    }

    $file = $this->request->getFile(fileID: 'fileSurat');
    // $password = $this->request->getPost('passwordSurat');
    $iv = $this->generateIV();

    try {
        $dataFile = $this->prosesFileUpload(file: $file, password: self::STATIC_PASSWORD, iv: $iv);
        $this->simpanDataSurat(dataFile: $dataFile, iv: $iv);
    } catch (RuntimeException $e) {
        $this->bersihkanUploadGagal(filename: $dataFile['nama_aman'] ?? null);
        return $this->redirectDenganError(pesan: $e->getMessage());
    }
    return redirect()->to(uri: base_url(relativePath: 'surat-keluar'))
        ->with(key: 'sukses', message: 'Surat berhasil disimpan! File telah dienkripsi dengan password.');
}
```

Gambar 4.9 Proses Enkripsi Surat Keluar

Fungsi simpan_surat() yang menangani proses unggah dan penyimpanan file surat pada aplikasi web. Fungsi ini pertama-tama memvalidasi input, lalu mengambil file yang diunggah dari *form* dengan nama fileSurat dan menghasilkan nilai IV (*Initialization Vector*) untuk enkripsi. File kemudian diproses dan dienkripsi menggunakan password statis (STATIC_PASSWORD) melalui metode prosesFileUpload, lalu hasilnya disimpan menggunakan simpanDataSurat. Jika terjadi kesalahan selama proses, error ditangani melalui blok catch, dan pengguna diarahkan kembali dengan pesan kesalahan. Jika berhasil, pengguna akan diarahkan ke halaman surat- keluar dengan pesan sukses bahwa file telah disimpan dan dienkripsi.

```
1 reference
private function validasiInput(): bool
{
    $aturan = [
        'fileSurat' => [
            'uploaded[fileSurat]',
            'max_size[fileSurat,' . self::UKURAN_MAKSIMAL_FILE . ']',
            'ext_in[fileSurat,' . implode(separator: ',', array: self::JENIS_FILE_DIIZINKAN) . ']'
        ],
        'nomorSurat' => 'required',
        'tanggalSurat' => 'required|valid_date'

    ];

    return $this->validasi->setRules(rules: $aturan)->run(data: $this->request->getPost());
}
```

Gambar 4.10 Validasi Input Surat Keluar

Fungsi validasiInput() ini berfungsi untuk memvalidasi data input dari *form* sebelum diproses lebih lanjut. Validasi dilakukan terhadap tiga elemen: fileSurat harus diunggah, tidak

melebihi ukuran maksimum yang ditentukan (UKURAN_MAKSIMAL_FILE), dan memiliki ekstensi yang diizinkan (JENIS_FILE_DIIZINKAN); nomorSurat wajib diisi; dan tanggalSurat juga wajib diisi serta harus berupa format tanggal yang valid. Aturan-aturan ini diterapkan menggunakan method setRules() dan dijalankan dengan run(), yang kemudian mengembalikan true jika validasi berhasil dan false jika gagal.

2. Deskripsi Surat

```php
0 references | 0 overrides
public function proses_unduh(): RedirectResponse|ResponseInterface
{
    try {
        $this->bersihkanOutputBuffer();

        $id = $this->request->getPost(index: 'id');
        $password = $this->request->getPost(index: 'password');
        $this->validasiInputUnduh(id: $id, password: $password);

        $surat = $this->dapatkanSuratValid(id: $id);
        $pathFile = $this->dapatkanPathFileValid(filename: $surat['file_surat']);

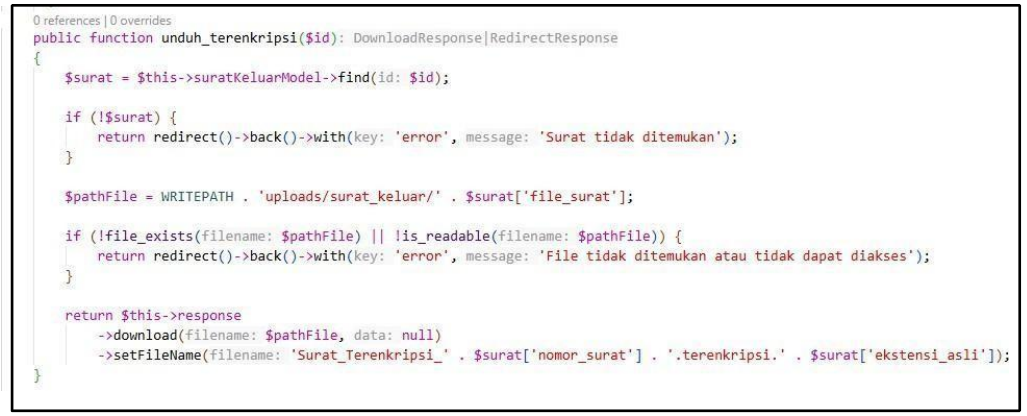
        // Dekripsi file
        $kontenTerdekripsi = $this->dekripsiFile(
            pathFile: $pathFile,
            password: $password,
            iv: base64_decode(string: $surat['iv'])
        );

        // Kirim file terdekripsi dalam base64 untuk AJAX
        if ($this->request->isAJAX()) {
            return $this->response->setJSON(body: [
                'success'   => true,
                'url'       => 'data:application/octet-stream; base64,' . base64_encode(string: $kontenTerdekripsi),
                'nama_file' => 'Surat_' . $surat['nomor_surat'] . '.' . $surat['ekstensi_asli']
            ]);
        } else {
            // Untuk request biasa, lakukan download langsung
            return $this->persiapkanResponseUnduh(
                konten: $kontenTerdekripsi,
                nomorSurat: $surat['nomor_surat'],
                ekstensi: $surat['ekstensi_asli']
            );
        }
    } catch (RuntimeException $e) {
        if ($this->request->isAJAX()) {
            return $this->response->setJSON(body: [
                'success' => false,
                'pesan' => $e->getMessage()
            ]);
        } else {
            return $this->redirectDenganError(pesan: $e->getMessage());
        }
    }
}
```

Gambar 4.11 Proses Unduh Surat Keluar

Fungsi proses_unduh() pada kode di atas bertugas untuk memproses permintaan unduhan file yang telah

dienkripsi. Pertama- tama, sistem mengambil id dan password dari input POST, lalu memvalidasinya. Jika surat ditemukan dan path file valid, maka file didekripsi menggunakan fungsi dekripsiFile() dengan path, password, dan IV (*Initialization Vector*) yang didekode dari base64. Jika permintaan dilakukan melalui *AJAX*, sistem akan mengirimkan file dalam bentuk base64 string dan metadata nama file sebagai respons JSON. Jika bukan *AJAX*, maka file akan langsung diunduh menggunakan fungsi siapkanResponUnduh(). Jika terjadi kesalahan, akan ditangani dengan mengembalikan pesan error dalam format JSON (untuk *AJAX*) atau diarahkan kembali dengan error message untuk permintaan biasa.



```
0 references | 0 overrides
public function unduh_terenkripsi($id): DownloadResponse|RedirectResponse
{
    $surat = $this->suratKeluarModel->find(id: $id);

    if (!$surat) {
        return redirect()->back()->with(key: 'error', message: 'Surat tidak ditemukan');
    }

    $pathFile = WRITEPATH . 'uploads/surat_keluar/' . $surat['file_surat'];

    if (!file_exists(filename: $pathFile) || !is_readable(filename: $pathFile)) {
        return redirect()->back()->with(key: 'error', message: 'File tidak ditemukan atau tidak dapat diakses');
    }

    return $this->response
        ->download(filename: $pathFile, data: null)
        ->setFileName(filename: 'Surat_Terenkripsi_' . $surat['nomor_surat'] . '.terenkripsi.' . $surat['ekstensi_asli']);
}
```

Gambar 4.12 Unduh Enkripsi Surat Keluar

Fungsi unduh_terenkripsi($id) pada kode di atas digunakan untuk mengunduh file surat terenkripsi berdasarkan ID-nya. Pertama, sistem mencari data surat dari database menggunakan model suratKeluarModel. Jika data tidak

ditemukan, pengguna diarahkan kembali dengan pesan error. Selanjutnya, path file disusun berdasarkan direktori penyimpanan dan nama file dari database. Fungsi kemudian memeriksa apakah file benar-benar ada dan dapat dibaca. Jika tidak, pengguna juga akan diarahkan kembali dengan pesan kesalahan. Jika file valid, sistem mengunduh file tersebut dan menamai file yang diunduh dengan format Surat_Terenkripsi_<nomor_surat>.

terenkripsi.<ekstensi_asli>.

b. Enkripsi dan Dekripsi Surat Masuk

1. Enkripsi Surat

```
1 reference
protected const MAX_FILE_SIZE = 10240; // 10MB in KB
1 reference
protected const ALLOWED_FILE_TYPES = ['pdf', 'doc', 'docx'];
2 references
protected const PBKDF2_ITERATIONS = 10000;
2 references
protected const AES_KEY_LENGTH = 32;
1 reference
protected const IV_LENGTH = 16; // For AES-128
1 reference
protected const STATIC_PASSWORD = 'Dishanpang'; // Ganti dengan password kuat
9 references
protected $suratMasukModel;
1 reference
protected $encrypter;
3 references
protected $validation;
```

Gambar 4.13 Aturan Enkripsi File Surat Masuk

MAX_FILE_SIZE membatasi ukuran maksimal file yang diunggah sebesar 10MB, sementara *ALLOWED_FILE_TYPES* menentukan jenis file yang diizinkan (PDF dan dokumen Word).

PBKDF2_ITERATIONS, *AES_KEY_LENGTH*, dan *IV_LENGTH* adalah parameter untuk proses enkripsi AES-128. *STATIC_PASSWORD* adalah password statis yang digunakan untuk enkripsi. Selain itu, terdapat properti $suratMasukModel, $encrypter, dan $validation yang kemungkinan digunakan dalam proses manajemen surat masuk, enkripsi file, dan validasi input.



```
1 reference
private function processUploadedFile($file, string $password, string $iv): array
{
    if (!$file->isValid() || $file->hasMoved()) {
        throw new RuntimeException(message: 'File upload tidak valid');
    }
    $originalName = $file->getClientName();
    $originalExt = $file->getClientExtension();
    $originalSize = $file->getSize();
    $safeName = $this->generateSafeFilename(originalName: $originalName);
    $fileContent = file_get_contents(filename: $file->getTempName());
    $encryptedContent = $this->encryptWithPassword(data: $fileContent, password: $password, iv: $iv);

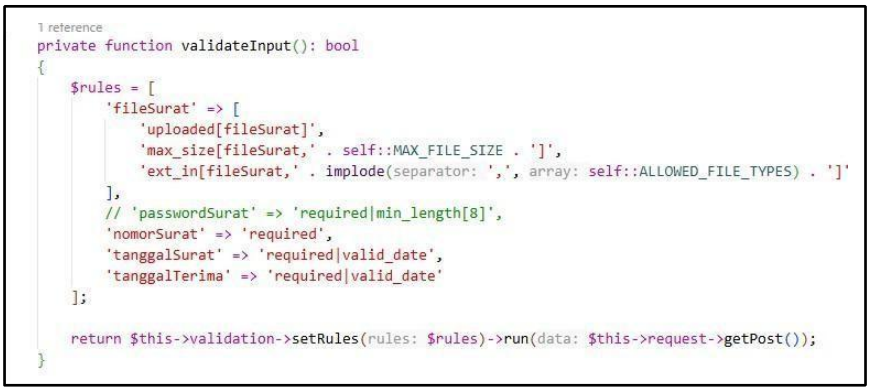
    $this->saveEncryptedFile(filename: $safeName, content: $encryptedContent);

    return [
        'safe_name' => $safeName,
        'original_ext' => $originalExt,
        'original_size' => $originalSize
    ];
}
```

Gambar 4.14 Proses Enkripsi Surat Masuk

Fungsi processUploadedFile() ini digunakan untuk memproses file yang diunggah oleh pengguna dengan cara mengenkripsi isi file tersebut. Fungsi terlebih dahulu memeriksa apakah file valid dan telah dipindahkan; jika tidak, akan memunculkan *exception*. Selanjutnya, fungsi mengambil nama asli, ekstensi, dan ukuran file, serta menghasilkan nama file yang aman untuk penyimpanan. Isi file dibaca, lalu dienkripsi menggunakan password dan IV (*Initialization Vector*) melalui metode

encryptWithPassword(). Hasil enkripsi kemudian disimpan dengan nama file yang aman menggunakan fungsi *saveEncryptedFile()*. Fungsi ini mengembalikan informasi dasar file asli, seperti nama, ekstensi, dan ukuran.



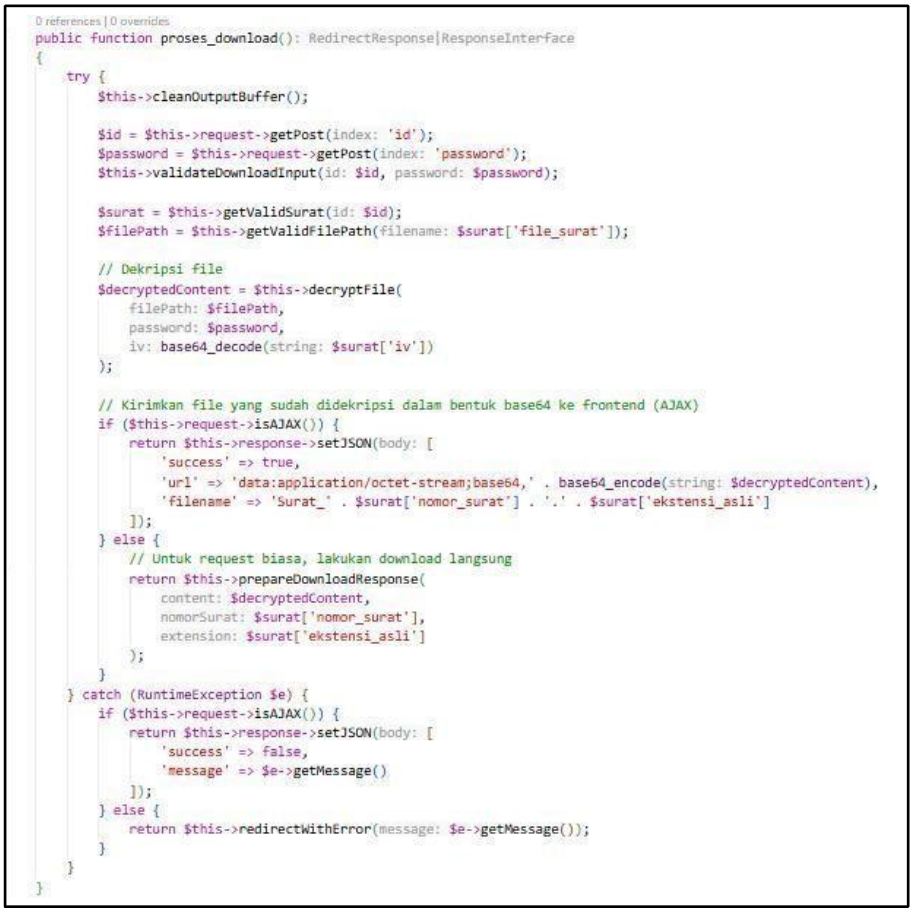
```
1 reference
private function validateInput(): bool
{
    $rules = [
        'fileSurat' => [
            'uploaded[fileSurat]',
            'max_size[fileSurat,' . self::MAX_FILE_SIZE . ']',
            'ext_in[fileSurat,' . implode(separator: ',', array: self::ALLOWED_FILE_TYPES) . ']'
        ],
        // 'passwordSurat' => 'required|min_length[8]',
        'nomorSurat' => 'required',
        'tanggalSurat' => 'required|valid_date',
        'tanggalTerima' => 'required|valid_date'
    ];

    return $this->validation->setRules(rules: $rules)->run(data: $this->request->getPost());
}
```

Gambar 4.15 Validasi Input Surat Masuk

Fungsi *validateInput()* yang bertugas memvalidasi inputan *form*. Fungsi ini mendefinisikan aturan validasi (*$rules*) untuk beberapa field, seperti fileSurat yang harus diunggah, tidak melebihi ukuran maksimum (*MAX_FILE_SIZE*), dan memiliki ekstensi yang diizinkan (*ALLOWED_FILE_TYPES*). Selain itu, *field* nomorSurat, tanggalSurat, dan tanggalTerima juga divalidasi agar wajib diisi dan memiliki format tanggal yang valid. Setelah semua aturan ditentukan, fungsi menjalankan validasi menggunakan $this->*validation* terhadap data yang diperoleh dari *$this->request->getPost()*.

2. Deskripsi Surat



```
0 references | 0 overrides
public function proses_download(): RedirectResponse|ResponseInterface
{
    try {
        $this->cleanOutputBuffer();

        $id = $this->request->getPost(index: 'id');
        $password = $this->request->getPost(index: 'password');
        $this->validateDownloadInput(id: $id, password: $password);

        $surat = $this->getValidSurat(id: $id);
        $filePath = $this->getValidFilePath(filename: $surat['file_surat']);

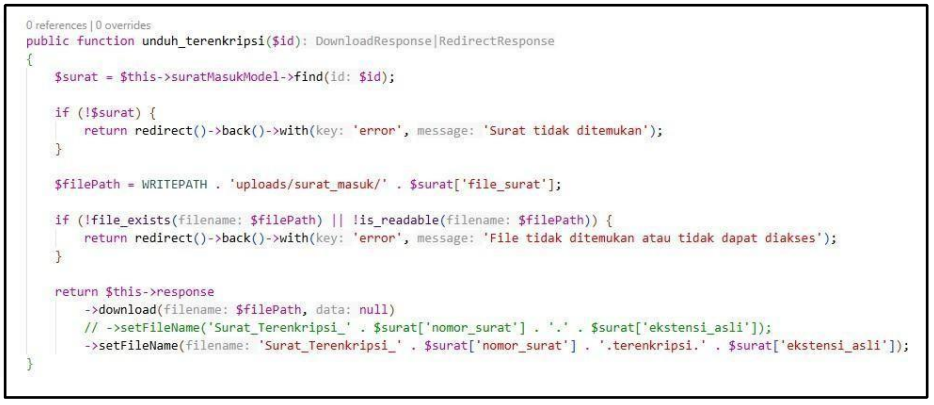
        // Dekripsi file
        $decryptedContent = $this->decryptFile(
            filePath: $filePath,
            password: $password,
            iv: base64_decode(string: $surat['iv'])
        );

        // Kirimkan file yang sudah didekripsi dalam bentuk base64 ke frontend (AJAX)
        if ($this->request->isAJAX()) {
            return $this->response->setJSON(body: [
                'success' => true,
                'url' => 'data:application/octet-stream; base64,' . base64_encode(string: $decryptedContent),
                'filename' => 'Surat_' . $surat['nomor_surat'] . '.' . $surat['ekstensi_asli']
            ]);
        } else {
            // Untuk request biasa, lakukan download langsung
            return $this->prepareDownloadResponse(
                content: $decryptedContent,
                nomorSurat: $surat['nomor_surat'],
                extension: $surat['ekstensi_asli']
            );
        }
    } catch (RuntimeException $e) {
        if ($this->request->isAJAX()) {
            return $this->response->setJSON(body: [
                'success' => false,
                'message' => $e->getMessage()
            ]);
        } else {
            return $this->redirectWithError(message: $e->getMessage());
        }
    }
}
```

Gambar 4.16 Proses Download Surat Masuk

Fungsi proses_download() yang menangani proses dekripsi dan pengunduhan file terenkripsi berdasarkan input id dan password. Fungsi ini memulai dengan membersihkan *output buffer*, mengambil data id dan password dari request POST, serta memvalidasi input tersebut. Setelah mendapatkan data surat dan path file, file kemudian didekripsi menggunakan password dan IV (*Initialization Vector*) dari surat. Jika permintaan berasal

dari *AJAX*, file didekripsi dan dikembalikan dalam format Base64 bersama nama file-nya. Jika bukan *AJAX*, file didekripsi dan langsung dikembalikan sebagai respons unduhan. Jika terjadi error, maka akan dikembalikan pesan kesalahan dalam format JSON (untuk *AJAX*) atau diarahkan dengan pesan error (untuk non-*AJAX*).



```
0 references | 0 overrides
public function unduh_terenkripsi($id): DownloadResponse|RedirectResponse
{
    $surat = $this->suratMasukModel->find(id: $id);

    if (!$surat) {
        return redirect()->back()->with(key: 'error', message: 'Surat tidak ditemukan');
    }

    $filePath = WRITEPATH . 'uploads/surat_masuk/' . $surat['file_surat'];

    if (!file_exists(filename: $filePath) || !is_readable(filename: $filePath)) {
        return redirect()->back()->with(key: 'error', message: 'File tidak ditemukan atau tidak dapat diakses');
    }

    return $this->response
        ->download(filename: $filePath, data: null)
        // ->setFileName('Surat_Terenkripsi_' . $surat['nomor_surat'] . '.' . $surat['ekstensi_asli']);
        ->setFileName(filename: 'Surat_Terenkripsi_' . $surat['nomor_surat'] . '.terenkripsi.' . $surat['ekstensi_asli']);
}
```

Gambar 4.17 Unduh Enkripsi Surat Masuk

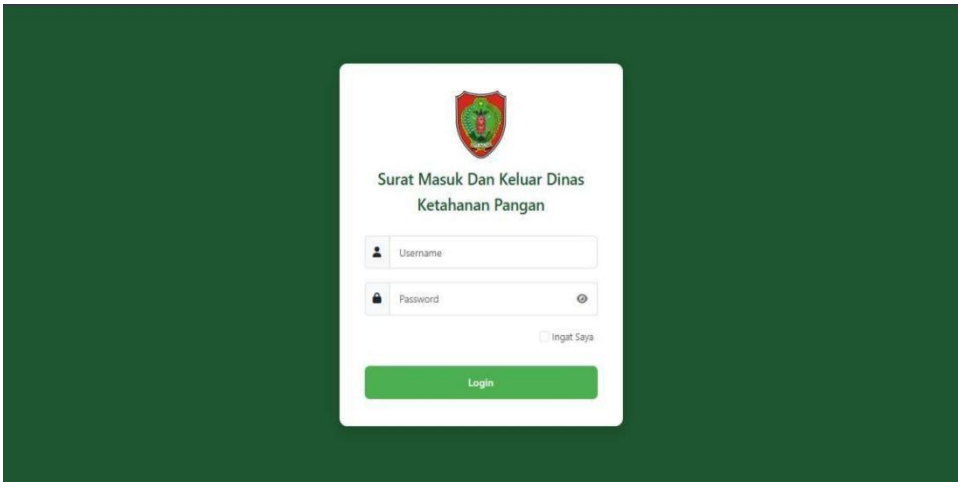
Fungsi unduh_terenkripsi($id) yang digunakan untuk mengunduh file surat terenkripsi berdasarkan ID-nya. Fungsi ini pertama-tama mencari data surat di database menggunakan model suratMasukModel. Jika data tidak ditemukan, pengguna akan diarahkan kembali dengan pesan error. Jika data ditemukan, sistem membentuk path file berdasarkan direktori *WRITEPATH* dan nama file dari data surat. Selanjutnya, dilakukan pengecekan apakah file tersebut ada dan dapat dibaca. Jika tidak, pengguna juga akan diarahkan kembali dengan pesan error. Jika valid, file

akan diunduh menggunakan *$this->response->download()* dan diberi nama baru sesuai dengan format Surat_Terenkripsi_[nomor_surat]. terenkripsi.[ekstensi_asli].

4.1.5 Tampilan Antarmuka Sistem

a. Halaman Login

Halaman login dari sistem informasi Surat Masuk dan Keluar Dinas Ketahanan Pangan. Terdapat *form* login yaitu dua input field untuk Username dan Password. Halaman ini memverifikasi identitas pengguna melalui kombinasi username dan password yang dimasukkan. Jika cocok dengan data di database, maka akses diberikan. Dalam sistem Surat Masuk dan Keluar Dinas Ketahanan Pangan, peran (role) admin dan pengguna (user), tampilan halaman login bisa dilihat pada Gambar 4.1.18.

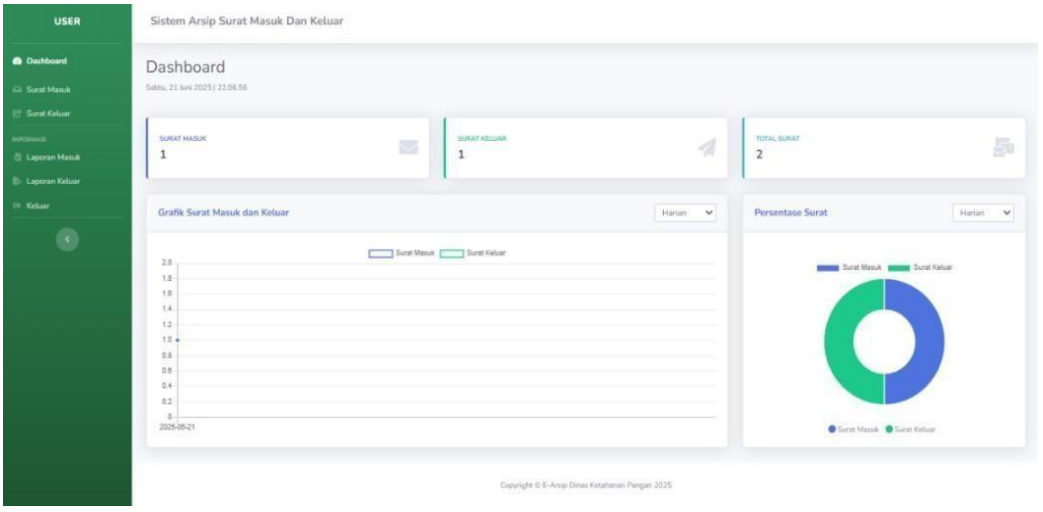


Gambar 4.18 Halaman Login

b. Dashboard

1. Dashboard Pengguna (User)

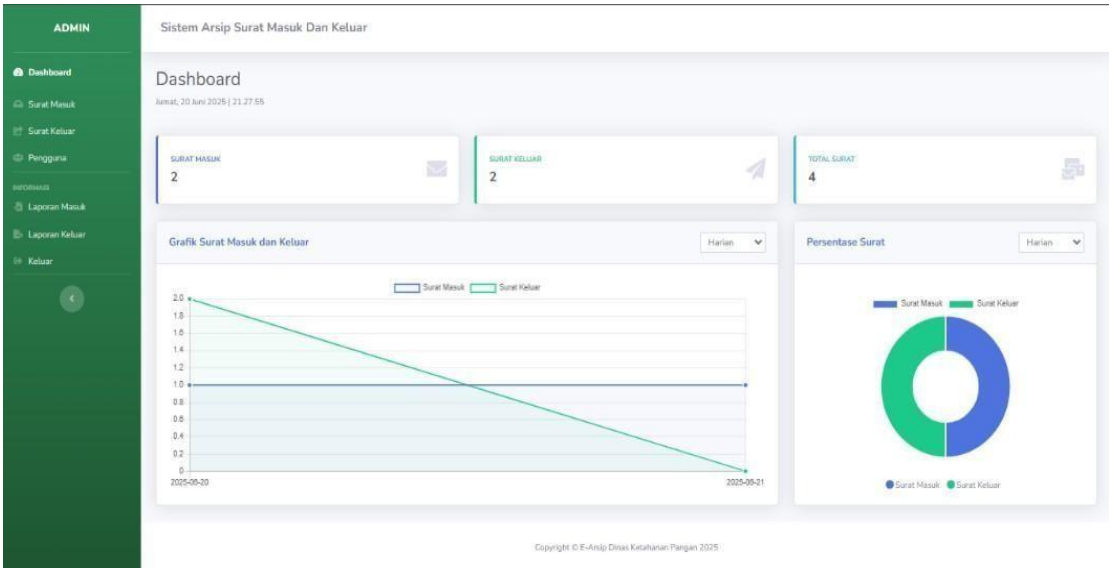
Sistem menampilkan jumlah surat masuk, surat keluar, serta total keseluruhan surat yang telah tercatat dalam database. Dalam sistem ini, pengguna (user) yang telah login dapat menginput surat, melihat data surat, mengunduh file dengan memasukkan password enkripsi yang sesuai, serta mengakses laporan masuk dan keluar, tampilan halaman dasboard User bisa dilihat pada Gambar 4.1.19.



Gambar 4.19 Dashboard Pengguna (User)

2. Dashboard Admin

Menampilkan rekap data jumlah surat masuk, surat keluar, dan total keseluruhan surat yang telah diarsipkan, Memiliki hak akses tambahan ke menu "Pengguna" yang hanya tersedia di dashboard admin. Selain itu, admin juga dapat melihat data surat, mengunduh file dengan memasukkan password enkripsi yang sesuai, serta mengakses laporan masuk dan keluar, tampilan halaman dasboard admin bisa dilihat pada Gambar 4.20.

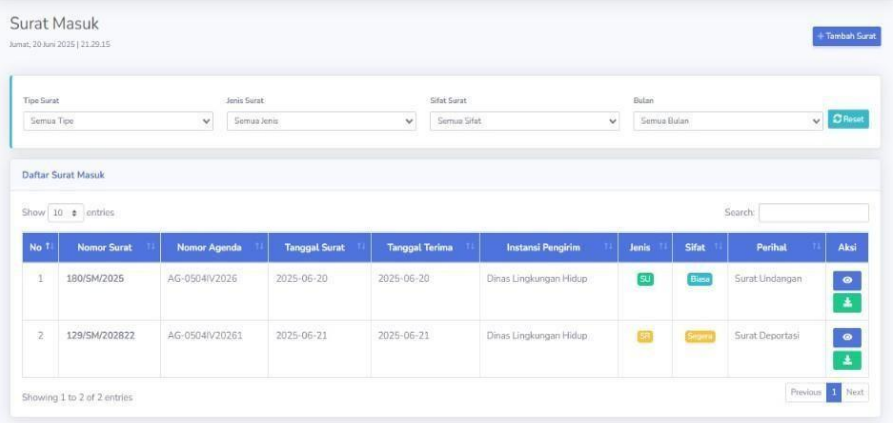


Gambar 4.20 Dashboard Admin

c. Halaman Daftar Surat

1. Daftar Surat Masuk

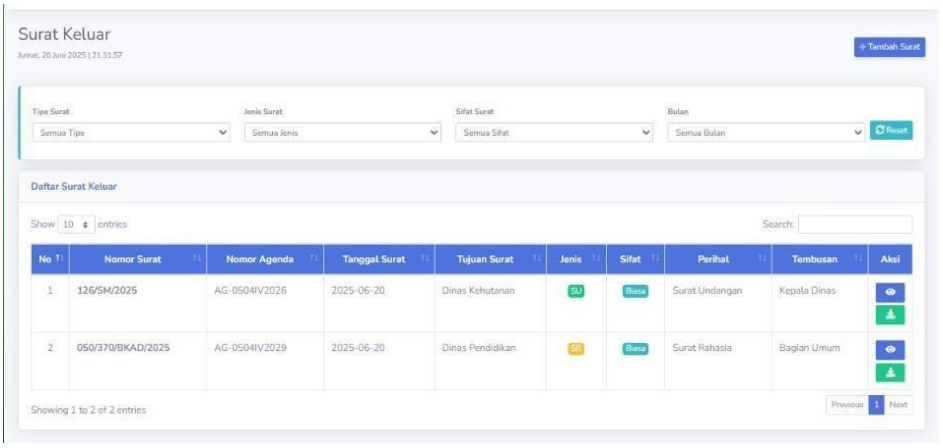
Di bagian atas halaman, terdapat tombol untuk tambah surat, filter pencarian berdasarkan Tipe Surat, Jenis Surat, Sifat Surat, dan Bulan, yang memudahkan pengguna untuk menyaring data sesuai kebutuhan. Tepat di bawahnya terdapat tabel Daftar Surat Masuk yang menampilkan informasi lengkap dari masing- masing surat, termasuk Nomor Surat, Nomor Agenda, Tanggal Surat, Tanggal Terima, Instansi Pengirim, Jenis Surat, Sifat Surat, Perihal, dan kolom Aksi. Di kolom aksi terdapat dua tombol: ikon mata untuk melihat detail surat dan ikon unduh untuk mengunduh dokumenterkait, tampilan halaman surat masuk bisa dilihat pada



Gambar 4.21 Daftar Surat Masuk

2. Daftar Surat Keluar

Halaman Surat Keluar dalam sistem E-Arsip Surat Masuk dan Keluar. Di bagian atas, tersedia tombol untuk tambah surat, filter pencarian berdasarkan Tipe Surat, Jenis Surat, Sifat Surat, dan Bulan, yang berguna untuk menyaring data sesuai kriteria tertentu. Di bawahnya terdapat tabel Daftar Surat Keluar yang memuat informasi penting seperti Nomor Surat, Nomor Agenda, Tanggal Surat, Tujuan Surat, Jenis, Sifat, Perihal, dan Tembusan. Kolom Aksi menyediakan dua ikon, yaitu ikon mata untuk melihat detail surat dan ikon unduh untuk mengakses dokumen surat yang terenkripsi, tampilan halaman surat keluar bisa dilihat pada Gambar 4.1.22.

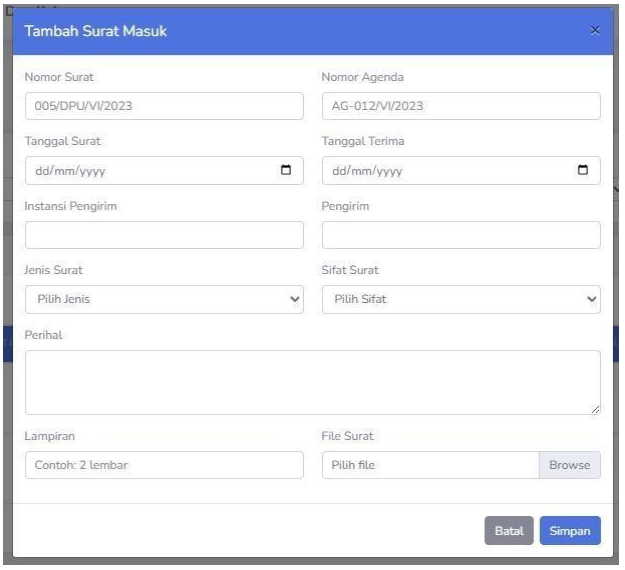


Gambar 4.22 Daftar Surat Keluar

d. *Form* Tambah Surat

1. Tambah Surat Masuk

Halaman ini berfungsi untuk menambahkan atau memasukan file surat masuk ke sistem, file surat akan otomatis terenkripsi dan disimpan di database, tampilan halaman tambah surat bisa dilihat pada Gamba 4.1.23.



Gambar 4.23 *Form* Input Surat Masuk

fungsi halaman ini adalah untuk memasukkan data surat masuk ke dalam sistem.

a). Nomor Surat dan Nomor Agenda: sebagai identifikasi unik

surat.

b). Tanggal Surat dan Tanggal Terima: mencatat waktu

surat dibuat dan diterima.

c). Instansi Pengirim & Pengirim: mencatat asal surat.

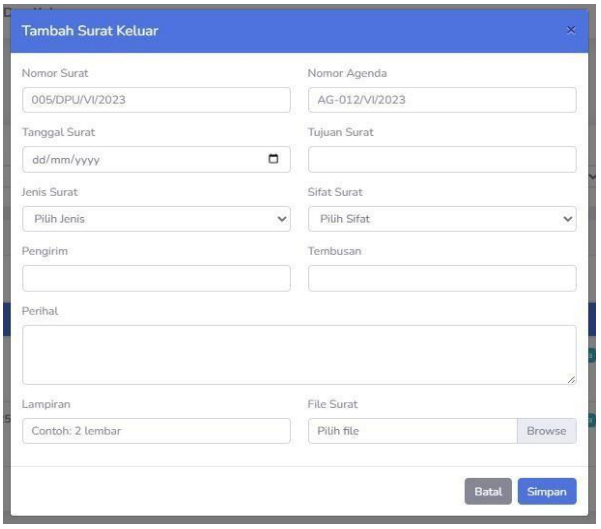
d). Jenis Surat & Sifat Surat: dipilih dari dropdown untuk mengelompokkan surat.

e). Perihal: menjelaskan isi atau topik surat.

f). Lampiran dan File Surat: informasi pelengkap dan unggahan file asli surat.

2. Tambah Surat Keluar

Halaman ini berfungsi untuk menambahkan atau memasukan file surat keluar ke sistem, file surat akan otomatis terenkripsi dan disimpan di database, tampilan halaman tambah surat bisa dilihat pada Gambar 4.24.



Gambar 4.24 *Form* Input Surat Keluar

Form Tambah Surat Keluar dalam sistem arsip surat Dinas Ketahanan Pangan.

a). Nomor Surat & Nomor Agenda: sebagai identifikasi unik surat keluar.

b). Tanggal Surat: tanggal surat dibuat.

c). Tujuan Surat: instansi atau pihak yang menerima surat.

d). Jenis & Sifat Surat: kategori dan urgensi surat, dipilih dari *dropdown*.

e). Pengirim & Tembusan: nama pihak pengirim dan siapa saja yang menerima tembusan.

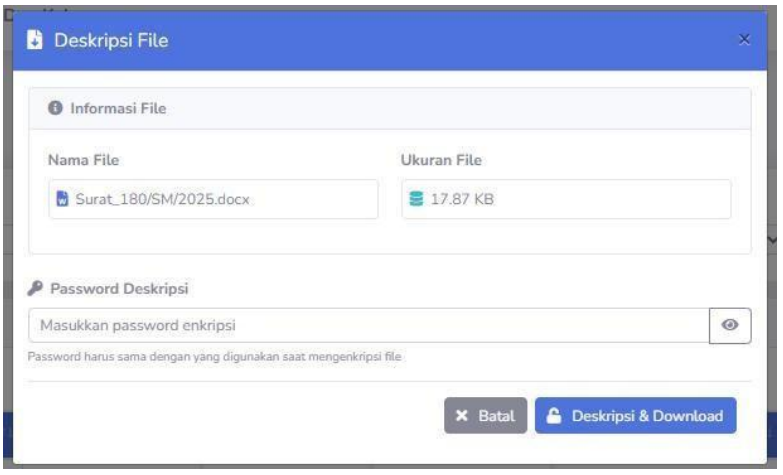
f). Perihal: isi ringkasan atau topik utama surat.

g). Lampiran & File Surat: detail tambahan dan unggahan file surat resmi yang akan dikirim.

e. *Form* Dekripsi dan Download File

Ketika klik tombol unduh pada salah satu surat masuk atau keluar, akan muncul pop-up “Dekripsi File” yang berisi informasi nama file dan ukuran file. Sebelum file bisa diunduh, pengguna diwajibkan memasukkan password dekripsi sebagai langkah keamanan untuk membuka file yang telah dienkripsi. Terdapat kolom isian password dengan ikon mata untuk melihat atau menyembunyikan karakter. Dua tombol tersedia di bagian bawah pop-up, yaitu

tombol Batal untuk membatalkan proses dan tombol Dekripsi & Download untuk melanjutkan proses setelah memasukkan password enkripsi yang benar, tampilan halaman dekripsi dan download surat bisa dilihat pada Gambar 4.25.



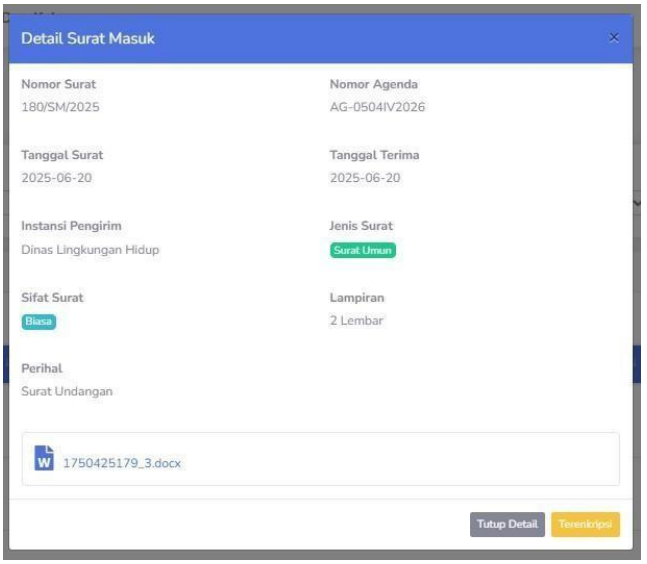
Gambar 4.25 Dekripsi Dan Download File

f. Halaman Detail Surat

1. Detail Surat Masuk

Pada detail surat masuk dapat melihat informasi lengkap mengenai surat masuk yang dipilih. Detail yang ditampilkan meliputi Nomor Surat, Nomor Agenda, Tanggal Surat dan Tanggal Terima, serta Instansi Pengirim. Selain itu, ditampilkan juga Jenis Surat, Sifat Surat, jumlah Lampiran, dan Perihal. Status file ini ditandai sebagai Terenkripsi, yang mengindikasikan bahwa file tersebut dilindungi dan memerlukan proses

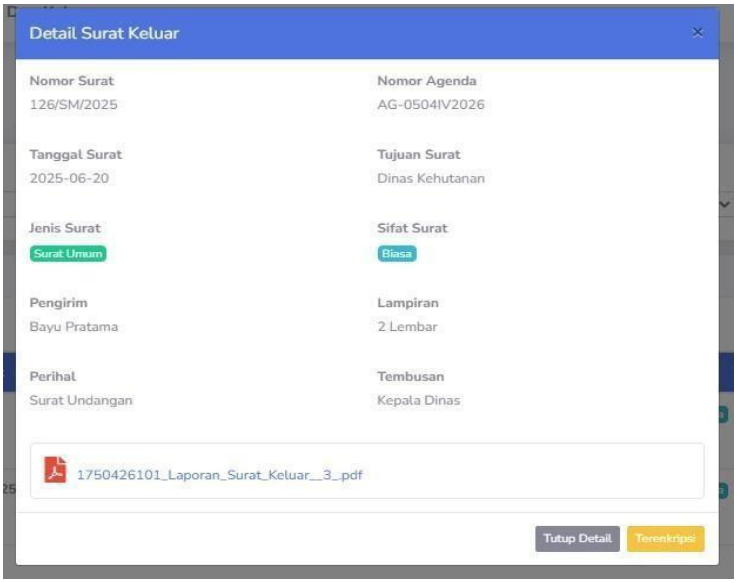
deskripsi untuk diakses, tampilan halaman detail surat masuk bisa dilihat pada Gambar 4.26.



Gambar 4.26 Detail Surat Masuk

2. Detail Surat Keluar

Di dalam jendela ini, informasi lengkap terkait surat keluar antara lain Nomor Surat, Nomor Agenda, Tanggal Surat, Tujuan Surat, dan Jenis Surat. Selain itu, surat ini memiliki Sifat Surat, Pengirim, Perihal, Lampiran serta Tembusan surat. Status surat ditandai sebagai Terenkripsi, yang berarti dokumen tersebut dilindungi dengan sistem keamanan dan memerlukan proses deskripsi sebelum dapat diakses, tampilan halaman detail surat keluar bisa dilihat pada Gambar 4.27.

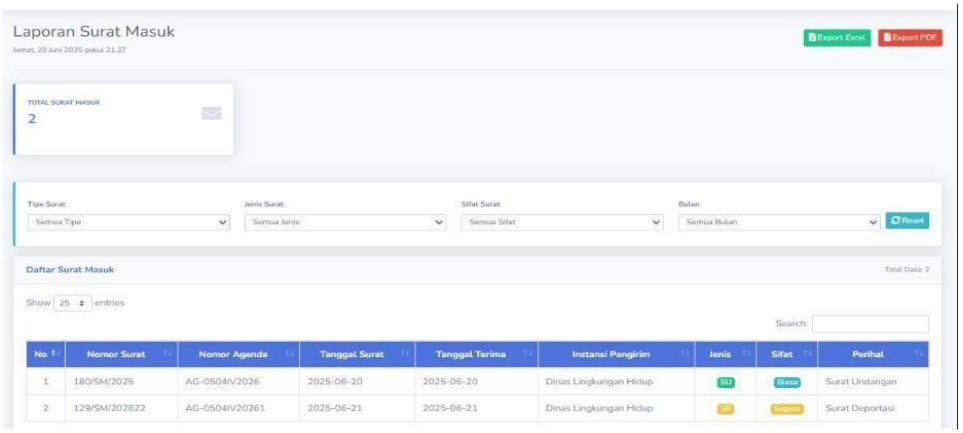


Gambar 4.27 Detail Surat Keluar

g. Halaman Laporan Surat

1. Laporan Surat Masuk

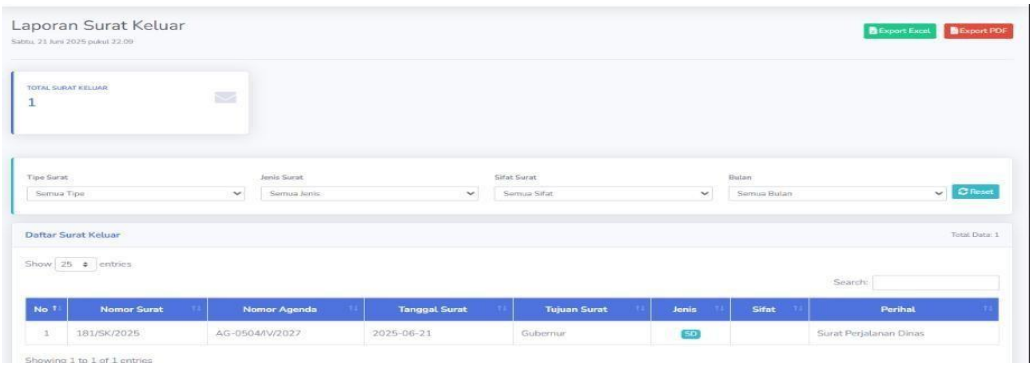
Halaman ini berfungsi menampilkan rekapitulasi data surat masuk yang telah tercatat dalam sistem, lengkap dengan fitur filter dan ekspor, melihat jumlah total surat masuk, memfilter data berdasarkan tipe, jenis, sifat, dan bulan surat, serta menelusuri detail setiap surat seperti nomor, tanggal, pengirim, dan perihal. Tersedia pula fitur ekspor ke format Excel dan PDF yang memudahkan proses pelaporan atau pencetakan arsip, berikut gambar laporan surat masuk pada Gambar 4.28.



Gambar 4.28 Laporan Surat Masuk

2. Laporan Surat Keluar

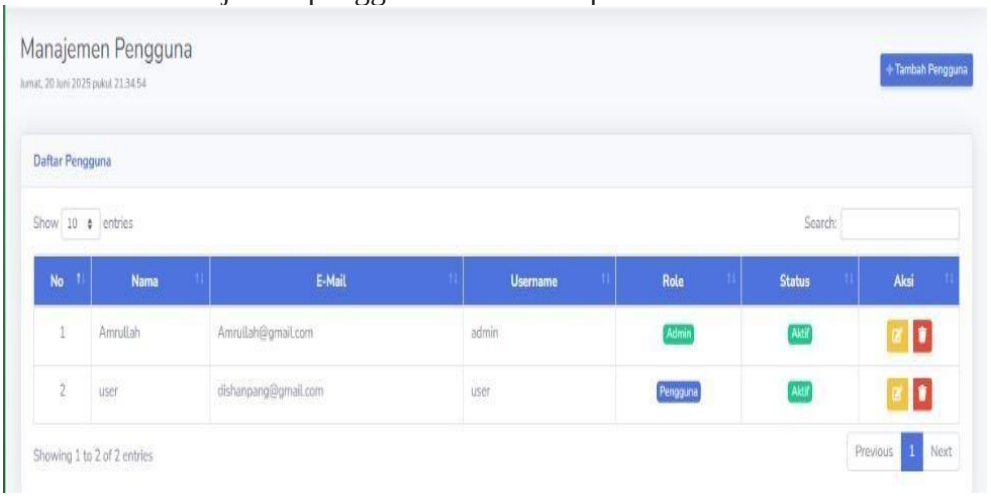
Memberikan akses dalam melihat daftar surat keluar yang telah terdata, dapat memfilter data berdasarkan tipe, jenis, sifat, dan bulan surat untuk mempersempit pencarian. Di bagian tabel, dapat melihat informasi lengkap surat seperti nomor surat, tanggal, instansi pengirim, jenis, sifat, dan perihal surat. Tersedia tombol untuk melihat detail surat dan ekspor atau mengunduh file, tampilan halaman laporan surat masuk bisa dilihat pada Gambar 4.29.



Gambar 4.29 Laporan Surat Keluar

h. Halaman Managemen Pengguna (Dashboard Admin)

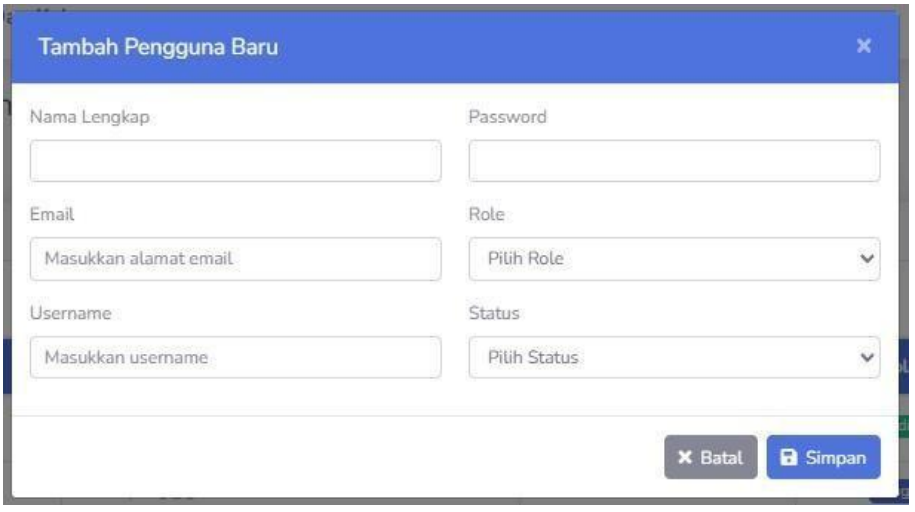
Halaman "Pengguna" dari sistem arsip surat masuk dan keluar yang hanya dapat diakses oleh admin, terdapat daftar pengguna yang terdaftar dalam sistem, lengkap dengan informasi seperti nama, email, username, peran (role), dan status. Di bagian kanan tabel, terdapat kolom aksi dengan dua tombol: ikon pensil untuk mengedit data pengguna dan ikon tempat sampah untuk menghapus pengguna. Di pojok kanan atas halaman juga tersedia tombol "+ Tambah Pengguna" untuk menambahkan pengguna baru, tampilan halaman manajemen pengguna bisa dilihat pada Gambar 4.30.



Gambar 4.30 Halaman Manajemen Pengguna

1. Tambah Pengguna

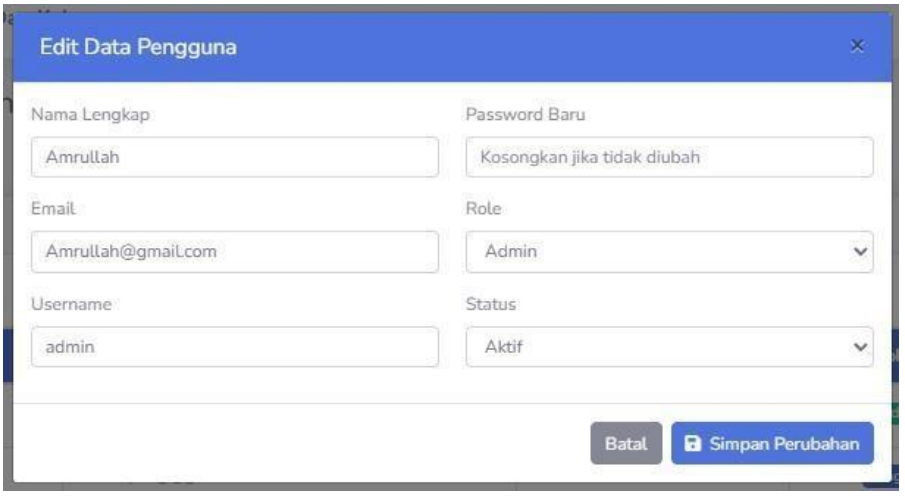
Formulir ini digunakan oleh admin untuk menambahkan akun pengguna ke dalam sistem. Terdapat enam isian yang harus dilengkapi, yaitu: Nama Lengkap, Email, Username, Password, Role (peran pengguna seperti Admin atau Pengguna biasa), dan Status (aktif atau nonaktif). Di bagian bawah terdapat dua tombol: Batal untuk membatalkan proses input dan Simpan untuk menyimpan data pengguna baru yang telah diisi, tampilan halaman tambah pengguna bisa dilihat pada Gambar 4.31.



Gambar 4.31 Tambah Pengguna

2. Edit Pengguna

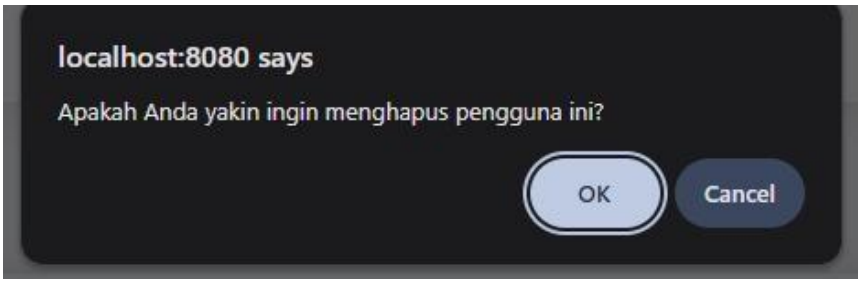
Admin dapat memperbarui informasi pengguna yang sudah terdaftar. Beberapa data yang bisa diubah meliputi Nama Lengkap, Email, Username, Role (peran seperti Admin atau Pengguna biasa), dan Status (Aktif atau Nonaktif). Terdapat juga kolom Password Baru, yang bisa dikosongkan jika tidak ingin mengubah kata sandi. Di bagian bawah, tersedia dua tombol yaitu Batal untuk membatalkan perubahan dan Simpan Perubahan untuk menyimpan update data, tampilan halaman edit pengguna bisa dilihat pada Gambar 4.32.



Gambar 4.32 Edit Pengguna

3. Hapus Pengguna

Menampilkan kotak dialog konfirmasi dari *browser* dengan pesan: “Apakah Anda yakin ingin menghapus pengguna ini?”. Pesan ini muncul saat admin mengklik tombol hapus pada data pengguna di sistem arsip surat masuk dan keluar. Dialog ini memiliki dua pilihan: tombol OK untuk melanjutkan proses penghapusan, dan tombol Cancel untuk membatalkan aksi tersebut, tampilan halaman hapus pengguna bisa dilihat pada Gambar 4.33.



Gambar 4.33 Hapus Pengguna

4.1.6 Pengujian Sistem

Pada penelitian kali ini penulis melakukan pengujian menggunakan metode *blackbox. Blackbox* testing dilakukan dikampus STMIK Palangkaraya pada tanggal 21 Juni 2025 dengan penguji Ibu Amaya Andri Damaini, S.Kom.,M.T. Pengujian Blackbox dapat dilihati ditabel 4.1.

Tabel 4.1 Pengujian *Blackbox*

SKENARIO UJI	HASIL YANG DIHARAPKAN	KESIMPULAN
Memilih halaman login admin/user	Sistem menampilkan halaman login admin/user	Valid
Memasukan data login username dan password jika salah	Sistem kembali kehalaman login dan memberi pesan (Username atau password salah.)	Valid
Memasukan data login username dan password jika benar	Sistem masuk ke halaman beranda admin	Valid
Masuk halaman Dashboard admin/user	Sistem menampilkan halaman dashbaord admin/user	Valid
Memilih halaman surat masuk dan keluar	Sistem menampilkan halaman surat masuk dan keluar yang terdapat fitur tambah, filter, cari, lihat, dan download surat.	Valid
Memilih tombol tambah surat	Sistem menampilkan *form* tambah surat, admin/user dapat menambahkan dan mengenkripsi surat	Valid
Memilih tombol filter surat	Sistem menampilkan filter dan admin/user dapat mencari surat yang diinginkan	Valid
Memilih tombol cari surat	Sistem menampilkan *form* cari dan admin/user dapat mencari surat yang diinginkan	Valid
Memilih tombol lihat surat(logo mata)/cek hasil enkripsi	Sistem menampilkan *form* lihat surat, admin/user dapat melihat surat yang terenkripsi.	Valid
Memilih tombol download surat/ dekripsi	Sistem menampilkan *form* download surat, admin/user dapat	Valid

SKENARIO UJI	HASIL YANG DIHARAPKAN	KESIMPULAN
surat	mendownload dan dekripsi surat.	
Memilih halaman pengguna	Sistem menampilkan halaman pengguna yang terdapat fitur tambah, cari, edit, dan hapus pengguna.	Valid
Memilih tombol tambah pengguna	Sistem menampilkan *form* tambah pengguna dan admin dapat menambahkan data pengguna	Valid
Memilih tombol cari pengguna	Sistem menampilkan *form* cari dan admin dapat mencari data pengguna yang diinginkan	Valid
Memilih tombol edit Pengguna	Sistem menampilkan *form* edit pengguna dan admin dapat mengubah data pengguna	Valid
Memilih tombol hapus pengguna	Sistem menampilkan alert konfirmasi untuk hapus, lalu admin bisa memilih untuk menghapus data	Valid
Memilih halaman laporan surat masuk dan keluar	Sistem menampilkan halaman laporan surat masuk dan keluar yang terdapat fitur filter, cari, dan download laporan surat.	Valid
Memilih tombol filter laporan surat	Sistem menampilkan filter laporan dan admin/user dapat mencari laporan surat yang diinginkan	Valid
Memilih tombol cari laporan surat	Sistem menampilkan *form* cari laporan dan admin/user dapat mencari laporan surat yang diinginkan	Valid

SKENARIO UJI	HASIL YANG DIHARAPKAN	KESIMPULAN
Memilih tombol download laporan surat	Sistem menampilkan *form* download laporan surat, admin/user dapat mendownload dalam bentuk pdf atau excel.	Valid
Memilih halaman logout admin/user	Sistem menampilkan kembali halaman login admin/user	Valid

4.2 Pembahasan

4.2.1 Evaluasi Sistem

Evaluasi sistem dilakukan untuk menilai sejauh mana sistem e- arsip surat keluar dan masuk berbasis enkripsi AES ini dapat memenuhi kebutuhan pengguna di lingkungan Dinas Ketahanan Pangan Provinsi Kalimantan Tengah. Berdasarkan hasil uji coba dan tanggapan dari pengguna terbatas (admin dan user), sistem dinilai memiliki antarmuka yang cukup mudah digunakan, serta mampu mengelola dokumen arsip secara sistematis. Proses enkripsi dan dekripsi berjalan dengan lancar tanpa mengganggu performa sistem. Selain itu, struktur penyimpanan dan pengelolaan surat melalui dashboard terbukti mempermudah pelacakan surat masuk dan keluar.

4.2.2 Kelebihan Dan Kekurangan Sistem

a. Kelebihan

Sistem e-arsip ini memiliki beberapa kelebihan yaitu: Pertama, penggunaan algoritma AES memberikan jaminan keamanan pada file surat yang disimpan di dalam sistem. Kedua, antarmuka sistem yang sederhana dan intuitif memudahkan pengguna dalam melakukan input dan pelacakan surat. Ketiga, Fitur-fitur seperti unggah file, proses enkripsi otomatis, dan akses data berdasarkan hak pengguna juga berjalan sesuai fungsinya.

b. Kekurangan

Sistem ini masih memiliki beberapa kekurangan. Salah satu kekurangan utama adalah belum adanya fitur notifikasi otomatis untuk surat yang belum dibaca, sehingga informasi baru tidak dapat terpantau secara langsung tanpa memeriksa daftar surat satu per satu. Selain itu, sistem masih berjalan secara lokal (*localhost*) dan belum *di-deploy* ke server online atau jaringan internal instansi, sehingga aksesibilitasnya terbatas hanya pada perangkat pengembang, dan password atau secret key dekripsi masih statis belum dinamis.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem, maka diperoleh beberapa kesimpulan sebagai berikut:

1. Penelitian ini telah berhasil menghasilkan sistem arsip surat keluar dan masuk berbasis enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah.
2. Sistem e-arsip surat keluar dan masuk berhasil dibangun menggunakan teknologi berbasis web dengan menerapkan algoritma enkripsi AES (*Advanced Encryption Standard*) untuk menjamin keamanan file surat yang diunggah.
3. Sistem mampu melakukan proses input, penyimpanan, pencarian, dan pengelolaan surat secara digital dengan antarmuka yang sederhana, ramah pengguna, dan sesuai dengan kebutuhan instansi.
4. Proses enkripsi dilakukan secara otomatis saat file surat diunggah ke sistem, dan proses dekripsi hanya dapat dilakukan oleh pengguna yang memiliki hak akses yang sah.
5. Pembagian hak akses antara admin dan user telah diterapkan, di mana perbedaan utama terletak pada hak admin dalam mengelola data pengguna.

5.2 Saran

Untuk pengembangan sistem e-arsip ke depan, beberapa saran yang dapat dipertimbangkan adalah sebagai berikut:

1. Menambahkan fitur notifikasi surat belum dibaca, agar pengguna dapat segera mengetahui adanya surat baru tanpa harus memeriksa daftar secara manual.
2. Mendeploy sistem ke server online atau jaringan lokal instansi, sehingga dapat digunakan secara real-time oleh seluruh pegawai yang berwenang dan tidak terbatas hanya di localhost.
3. Mengembangkan fitur log aktivitas pengguna, agar setiap tindakan penting (seperti unggah, unduh, dan dekripsi file) dapat terekam dan diaudit.
4. Menambahkan sistem backup otomatis dan periodik, untuk menjaga keberlangsungan data jika terjadi kerusakan atau kehilangan file di server.

DAFTAR PUSTAKA

Ardhana,V.Y.P.(2021).Pemodelan Activity Diagram untuk Perancangan Sistem Informasi Rekam Medis pada Klinik – *Jurnal Kesehatan Qamarul Huda*, Vol. 9 No. 2, hlm. 106–109. https://doi.org/10.37824/jkqh.v9i2.2021.310

Direktorat Jenderal Aplikasi Informatika – Kominfo. (2024). *Implementasi Sistem e-Arsip dalam Mendukung Tata Kelola Pemerintahan Digital*. Halaman: artikel online (tanpa nomor halaman) https://aptika.kominfo.go.id/tag/e-arsip

Harisanty, D., & Anugrah, E. P. (2022). *Legality of electronic archive management in realizing Indonesia E-government*. Digital Library Perspectives, Vol. 38 No. 1, hlm. 88–103.
https://www.emerald.com/insight/content/doi/10.1108/dlp-12-2020- 0123/full/html

Harmawan, R., & Setiawan, A. (2022). *Metode Wawancara Mendalam dalam Penelitian Sosial: Studi Kasus di Kota X*. Jurnal Metodologi Sosial, Vol. 5 No. 1, hlm. 45–60.

Marthiawati, N., Kurniawansyah, K., Nugraha, H., & Khairunnisa, F. (2024). *Pelatihan Pembuatan UML (Unified Modelling Language) Menggunakan Aplikasi Draw.io Pada Prodi Sistem Informasi Universitas Muhammadiyah Jambi*. Transformasi Masyarakat : Jurnal Inovasi Sosial dan Pengabdian, Vol. 1 No.2, Hlm.225-33 https://doi.org/10.62383/transformasi.v1i2.109

Muhammad Riza Alifi et al. (2022). *Pemodelan Data Relasional pada NoSQL Berorientasi Dokumen*. Jurnal Nasional Teknik Elektro dan Teknologi Informasi,Vol.11No.3,hlm.183–191
https://www.researchgate.net/publication/363140746_Pemodelan_Data_Relasional_pada_NoSQL_Berorientasi_Dokumen

Nikmah, K. (2023). *Penerapan Metode Pembelajaran Observasi Lapangan pada Mata Kuliah Studi Arsip untuk Meningkatkan Kemampuan Berpikir Kritis Mahasiswa*. ASANKA: Journal of Social Science and Education, Vol. 4 No. 1, hlm. 26–33.
https://doi.org/10.21154/asanka.v4i1.5912 (jurnal.iainponorogo.ac.id)

Nur, M., Soedijono, B., & Arief, M. R. (2021). *Perencanaan Strategis Sistem Informasi untuk Meningkatkan Keunggulan Bersaing (Studi Kasus: Universitas XYZ)*. Jurnal Teknologi Informasi Respati, Vol. 16 No. 1. https://jti.respati.ac.id/index.php/jurnaljti/article/view/391/339

Pangestu, H. A., Kurniadi, D., & Septiana, Y. (2022). *Aplikasi Pengelolaan Data Pegawai Berbasis REST API untuk Transfer Data Real Time dengan Framework CodeIgniter*. Jurnal Algoritma, Vol. 19 No. 1, hlm. 313–322. https://doi.org/10.33364/algoritma/v.19-1.1090

Praba, A. D., & Safitri, M. (2020). *Studi Perbandingan Performansi antara MySQL dan PostgreSQL*. Jurnal Khatulistiwa Informatika, Vol. 8 No. 2, https://doi.org/10.31294/jki.v8i2.8851.g4533

Pratama, E. B., & Saparingga, U. (2021). *Pemodelan UML Sistem Informasi Administrasi Kependudukan Untuk Kantor Desa*. Jurnal Ilmiah Media Sisfo, Vol. 15 o. 2, hlm. 107–118. https://doi.org/10.33998/mediasisfo.2021.15.2.1085

Purnasari, M., Hartiwi, Y., & Nurhayati, N. (2022). *Perancangan Sistem Informasi Pengelolaan Dana Masjid Berbasis Web Menggunakan Unified Modeling Language (UML)*. Resolusi: Rekayasa Teknik Informatika dan Informasi, Vol. 2 No. 6 (Juli 2022), hlm. 258–264. https://doi.org/10.30865/resolusi.v2i6.416

Santoso, A. B., & Prabowo, T. T. (2022). *Analisis Manajemen Arsip Elektronik di Kantor Kementerian Agama Kabupaten Bantul Yogyakarta*. Khazanah: Jurnal Pengembangan Kearsipan, Vol. 15 No. 2 (November 2022), hlm.74–87. https://www.researchgate.net/publication/365073511_Analisis_Manajemen_Arsip_Elektronik_di_Kantor_Kementerian_Agama_Kabupaten_Bantul_Yogyakarta

Sondang, S. (2024). *Penerapan Metode RAD Dalam Pengembangan Sistem Informasi Pemesanan Jasa Percetakan Berbasis Web pada Percetakan Karya Sehati Jaya*. REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer, Vol. 8 No. 3, hlm. 871–881. https://doi.org/10.33395/remik.v8i3.13944

Sukmawati, S. & Nasran, N. (2021). *Studi Pustaka Penggunaan Metode Pembelajaran Jarak Jauh Berbasis E-Learning pada Mahasiswa PPKn Masa New Normal*. Jurnal Pendidikan Tambusai, Vol. 5 No. 3, hlm. 7188–7191. https://doi.org/10.31004/jptam.v5i3.2110

Syaputra, D. S., & Saputri, L. (2022). *Implementasi permainan tradisional Rimau untuk membentuk nilai-nilai karakter dalam pembelajaran PJOK di MTS Negeri Binjai*. Serunai: Jurnal Ilmiah Ilmu Pendidikan, 8(1), 56–63. https://ejournal.stkipbudidaya.ac.id/index.php/ja/article/view/1524

Widya, R. & Abdul. K. B. (2024). Sistem Pengelolaan Arsip Aktif di Dinas Kependudukan dan Catatan Sipil Kota Medan. Jurnal Ilmiah Dinamika Sosial, Vol. 8, No. 2, hlm.141-159.

LAMPIRAN

```php
/**
 * Menyimpan surat terenkripsi
 */
public function simpan_surat()
{
    if (!$this->validasiInput()) {
        return $this->redirectDenganError();
    }

    $file = $this->request->getFile('fileSurat');
    // $password = $this->request->getPost('passwordSurat');
    $iv = $this->generateIV();

    try {
        $dataFile = $this->prosesFileUpload($file, $this->password, $iv);

        $this->simpanDataSurat($dataFile, $iv);
    } catch (RuntimeException $e) {
        $this->bersihkanUploadGagal($dataFile['nama_aman'] ?? null);
        return $this->redirectDenganError($e->getMessage());
    }
    return redirect()->to(base_url('surat-keluar'))
        ->with('sukses', 'Surat berhasil disimpan! File telah dienkripsi dengan password.');
}

/**
 * Menampilkan prompt password untuk download
 */
public function unduh($id)
{
    $surat = $this->suratKeluarModel->find($id);

    if (!$surat) {
        return redirect()->back()->with('error', 'Surat tidak ditemukan');
    }
```

```
    return view('password_prompt', [
        'id' => $id,
        'nomor_surat' => $surat['nomor_surat']
    ]);
}

/**
 * Proses download dengan validasi password
 */
public function proses_unduh()
{
    try {
        $this->bersihkanOutputBuffer();

        $id = $this->request->getPost('id');
        $password = $this->request->getPost('password');
        $this->validasiInputUnduh($id, $password);

        $surat = $this->dapatkanSuratValid($id);
        $pathFile = $this->dapatkanPathFileValid($surat['file_surat']);

        // Dekripsi file
        $kontenTerdekripsi = $this->dekripsiFile(
            $pathFile,
            $password,
            base64_decode($surat['iv'])
        );

        // Kirim file terdekripsi dalam base64 untuk AJAX
        if ($this->request->isAJAX()) {
            return $this->response->setJSON([
                'success'   => true,
                'url'       => 'data:application/octet-stream; base64,' . base64_encode($kontenTerdekripsi),
                'nama_file' => 'Surat_' . $surat['nomor_surat'] . '.' . $surat['ekstensi_asli']
            ]);
        } else {
            // Untuk request biasa, lakukan download langsung
            return $this->persiapkanResponseUnduh(
                $kontenTerdekripsi,
                $surat['nomor_surat'],
                $surat['ekstensi_asli']
            );
        }
    } catch (RuntimeException $e) {
        if ($this->request->isAJAX()) {
            return $this->response->setJSON([
                'success' => false,
                'pesan' => $e->getMessage()
            ]);
        } else {
            return $this->redirectDenganError($e->getMessage());
        }
    }
}
```

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS

No.355/STMIK-3.C.2/KP/XII/2024

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama- nama tersebut di bawah ini :

1. Nama : Abdul Hadi, S.T., M.Kom.
   NIK : 198505102021101
   Sebagai Pembimbing I Dalam Pembuatan Program
2. Nama : Lili Rusdiana, M.Kom.
   NIK : 198707282011007
   Sebagai Pembimbing II Dalam Penulisan Tugas Akhir

Untuk membimbing Tugas Akhir mahasiswa :

Nama	:	Amrullah
NIM	:	C2155201113
Program Studi	:	TEKNIK INFORMATIKA (55201)
Tanggal Daftar	:	06 September 2024
Judul Tugas Akhir	:	Implementasi Sistem Arsip Surat Keluar dan Masuk Berbasis Enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 2 Desember 2024
Ketua Program Studi Teknik Informatika,

Lili Rusdiana, M.Kom.
NIK. 198707282011007

Tembusan :
1. Pembimbing I dan II
2. Mahasiswa yang bersangkutan
3. Arsip

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI
TUGAS AKHIR

Nama Mahasiswa : Amrullah
NIM : C2155201113
Tanggal Persetujuan Judul : 2 Desember 2024
Judul Tugas Akhir : Implementasi Sistem Arsip Surat Kaluar dan Masuk Berbasis Enkripsi AES di Dinas Ketahanan Pangan Provinsi KALTENG

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	2/12/2024	3/12/2024	Memperbaiki: Latar belakang dan Penulisan	
	6/12/2024	8/12/2024	Memperbaiki Daftar isi dan Batasan masalah	
	12/12/2024	14/12/2024	Cek pedoman untuk penulisan bab dan lainnya	
	13/12/2024	14/12/2024	Menambahkan data yang diamankan dan teori alur AES (pada bab 2)	
	21/12/2024	22/12/2024	Tambah Paparan kerja AES, tambah gambar Alur AES, dan Melengkapi daftar pustaka	
	22/12/2024	24/12/2024	Perbaiki jarak penulisan, Menambahkan teori dan sumber, juga perbaiki jadwal penelitian	
	29/12/2024	29/12/2024	Mempergelaskan kalimat use Case diagram dan menambahkan paragraf baru kesimpulan peneliti	
	31/12/2024	2/12/2024	Memaparkan data yang perlu diamankan, Menambahkan Activity diagram proses enkripsi, memperbaiki Flowchart, dan menambahkan desain	
	9/1/2025	4/1/2025	Acc Seminar	
	9/1/2025	9/1/2025	ACC Seminar	

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	20/6/2025		Penambahan Abstrak dan tabel Kelasi.	
	23/6/2025		desain bab 3 pada bagian peg database Sesuaikan dengan bab 4	
	24/6/2025		revisi abstrak pembaca dan perbaikan kalimat kesimpulan masalah dan tujuan penelitian	
	25/6/2025		perbaiki narasi pada blackbox.	
	25/6/2025		Acc Sidang	
	25/1/2025		Lanjutkan ke bab 4	
	23/3/2025		Sesuaikan penulisan dengan laporan / template	
	24/6/2025		cek kembali penulisan sesuai laporan / template	
	25/6/2025		lengkapi laporan	
	25/6/2025		Acc Sidang	

Menyetujui :

Dosen Pembimbing I,

Abdul Hadi

Dosen Pembimbing II,

Lili Rahman S

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS
PENGUJI SEMINAR PROPOSAL TUGAS AKHIR

No.003/STMIK-3.C.2/KP/I/2025

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan kepada nama-nama berikut :

1. Nama : Amaya Andri Damaini, S.Kom., M.T
   NIK : 199309042018001
   Sebagai Ketua
2. Nama : Abdul Hadi, S.T., M.Kom.
   NIK : 198505102021101
   Sebagai Sekretaris
3. Nama : Lili Rusdiana, M.Kom.
   NIK : 198707282011007
   Sebagai Anggota

Tim Penguji Seminar Proposal Tugas Akhir :

Nama	:	Amrullah
NIM	:	C2155201113
Hari/Tanggal	:	Kamis, 16 Januari 2025
Waktu	:	08.30 WIB
Judul Proposal	:	Implementasi Sistem Arsip Surat Keluar dan Masuk Berbasis Enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 15 Januari 2025
Ketua Program Studi Teknik Informatika

Lili Rusdiana, M.Kom
NIK. 198707282011007

Tembusan :
1. Dosen Penguji
2. Mahasiswa yang Bersangkutan
3. Arsip Prodi

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS PENGUJI TUGAS AKHIR

No.151/STMIK-3.C.2/AU/VI/2025

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan kepada nama- nama berikut :

1. Nama : Sam'ani, S.T., M.Kom.
   NIK : 197703252005105
   Sebagai Ketua
2. Nama : Elok Faiqotul Himmah, S.Si., M.Sc
   NIK : 198503092009003
   Sebagai Sekretaris
3. Nama : Amaya Andri Damaini, S.Kom., M.T
   NIK : 199309042018001
   Sebagai Anggota
4. Nama : Ir. Abdul Hadi, S.T., M.Kom
   NIK : 198505102021101
   Sebagai Anggota
5. Nama : Veny Cahya Hardita, M.Kom
   NIK : 199504302020002
   Sebagai Anggota

Untuk menguji Tugas Akhir mahasiswa :

Nama Mahasiswa	:	Amrullah
N I M	:	C2155201113
Hari / Tanggal Ujian	:	Rabu, 2 Juli 2025
Waktu	:	08.30 WIB
Judul TA	:	IMPLEMENTASI SISTEM ARSIP SURAT KELUAR DAN MASUK BERBASIS ENKRIPSI AES DI DINAS KETAHANAN PANGAN PROVINSI KALIMANTAN TENGAH
Ruang	:	Kelas TI 2

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 28 Juni 2025

Ketua Program Studi Teknik Informatika,

28 Juni 2025

Ir. ABDUL HADI, S.T., M.Kom
NIK. 198505102021101

Tembusan :
1. Dosen Penguji
2. Mahasiswa yang Bersangkutan
3. Arsip

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN SEMINAR PROPOSAL TUGAS AKHIR

Nama Mahasiswa : AMRULLAH
N I M : C2155201113
Program Studi : Teknik Informatika

No.	Hari/ Tanggal	Judul	Mahasiswa Penyaji	Nama Tim Dosen	Tanda Tangan
1.	Jum'at 22-11-2024	Sistem Pengiraman Tanaman Pada Rumah Tangga Berbasis IOT Menggunakan ESP8266	APRIANSON	Hotmian Sitohang Herkules, S.kom. Elia Zakharia	
2.	Jum'at 22-11-2024	Prototype Sistem Penghitung Otomatis Jumlah Jemaat berbasis IOT Pada Gereja Ewanggelion	Imanuel Natalis Timisela	Herkules, S.kom. Amnya. A.D. S.kom. Hotmian S. S.kom.	
3	Sabtu 23-11-2024	Analisis Jaringan Hostpot dgn Parameter Quality of service (QOS) Pada Kantor wilayah kementerian agama provinsi kalimantan tengah	Taufikur Rahman	Ir. Hj. Siti Maryamah Sulistyoarti, S.kom Rudini, M.pd.	
4	Sabtu 23-11-2024	Implementasi Teknologi IOT pada budidaya Ikan Lele Bioflok untuk Monitoring kualitas Air	AHMAD Husaini	Samani, ST., M.kom Herkules, S.kom., M.cs. Lili Rusdiana, M.kom	
5	Jum'at 20-12-2024	Prototype pendeteksi Hujan Pada atap otomatis untuk Lingkungan Rumah menggunakan Esp0266 dan Blynk	STEVEN WINATA	Elia zakharia, MT. HERKULES, S.kom. DR. MAURA Widyaningsih	

Palangka Raya, 22 NOVEMBER 2024
Mahasiswa ybs,

AMRULLAH

Keterangan :
- *) Coret yang tidak perlu
- Harap kartu jangan sampai hilang, digunakan sebagai syarat seminar
- Minimal 5 (lima) kali mengikuti seminar

LEMBAR BERITA ACARA PENGUJIAN BLACK BOX

Uji Coba "***Implementasi Sistem Arsip Surat Keluar dan Masuk Berbasis Enkripsi AES di Dinas Ketahanan Pangan Provinsi Kalimantan Tengah***"

Nama : AMRULLAH

NIM : C2155201113

Jurusan : Teknik Informatika

Jika hasil pengujian sesuai dengan yang diharapkan maka kolom hasil pengujian diisi dengan simbol "centang"(√), jika tidak maka isi dengan simbol "strip"(-).

PENGUJIAN	HASIL YANG DIHARAPKAN	HASIL PENGUJIAN
Memilih halaman login admin/user	Sistem menampilkan halaman login admin/user	√
Memasukan data login username dan password jika salah	Sistem kembali kehalaman login dan memberi pesan (Username atau password salah.)	√
Memasukan data login username dan password jika benar	Sistem masuk ke halaman beranda admin	√
Masuk halaman Dashboard admin/user	Sistem menampilkan halaman dashbaord admin/user	√
Memilih halaman surat masuk dan keluar	Sistem menampilkan halaman surat masuk dan keluar yang terdapat fitur tambah, filter, cari, lihat, dan download surat.	√
Memilih tombol tambah surat	Sistem menampilkan form tambah surat, admin/user dapat menambahkan dan mengenkripsi surat	√
Memilih tombol filter surat	Sistem menampilkan filter dan admin/user dapat mencari surat yang diinginkan	√
Memilih tombol cari surat	Sistem menampilkan form cari dan admin/user dapat mencari surat yang diinginkan	√
Memilih tombol lihat surat(logo mata)/cek hasil enkripsi	Sistem menampilkan form lihat surat, admin/user dapat melihat surat yang terenkripsi.	√

Memilih tombol download surat/ dekripsi surat	Sistem menampilkan form download surat, admin/user dapat mendownload dan dekripsi surat.	✓
Memilih halaman pengguna	Sistem menampilkan halaman pengguna yang terdapat fitur tambah, cari, edit, dan hapus pengguna.	✓
Memilih tombol tambah pengguna	Sistem menampilkan form tambah pengguna dan admin dapat menambahkan data pengguna	✓
Memilih tombol cari pengguna	Sistem menampilkan form cari dan admin dapat mencari data pengguna yang diinginkan	✓
Memilih tombol edit Pengguna	Sistem menampilkan form edit pengguna dan admin dapat mengubah data pengguna	✓
Memilih tombol hapus pengguna	Sistem menampilkan alert konfirmasi untuk hapus, lalu admin bisa memilih untuk menghapus data	✓
Memilih halaman laporan surat masuk dan keluar	Sistem menampilkan halaman laporan surat masuk dan keluar yang terdapat fitur filter, cari, dan download laporan surat.	✓
Memilih tombol filter laporan surat	Sistem menampilkan filter laporan dan admin/user dapat mencari laporan surat yang diinginkan	✓
Memilih tombol cari laporan surat	Sistem menampilkan form cari laporan dan admin/user dapat mencari laporan surat yang diinginkan	✓
Memilih tombol download laporan surat	Sistem menampilkan form download laporan surat, admin/user dapat mendownload dalam bentuk pdf atau excel.	✓
Memilih halaman logout admin/user	Sistem menampilkan kembali halaman login admin/user	✓

Palangkaraya, 21 Juni 2025

Dosen Penguji,

Amaya Andri Damanni, S.Kom., MT.

NIK. 199304092016006

PEMERINTAH PROVINSI KALIMANTAN TENGAH
DINAS KETAHANAN PANGAN
Jl. Willem AS No. 09 Palangkaraya 73111
Telp/WA 081253235363 email : dinasketahananpanganprov@gmail.com

Palangka Raya, 16 Juni 2025

Nomor : 408 /Um.150/DKP/06/2025.
Lampiran : -
Hal : Persetujuan penelitian dan pengumpulan data untuk tugas akhir an. AMRULLAH

Yth. Ketua STMIK Palangkaraya
di-
PALANGKA RAYA.

Menindak lanjuti Surat Saudara Nomor 442/STMIK-C-2/AK/VI/2025 tanggal 12 Juni 2025 Perihal : Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir an. AMRULLAH, kami sampaikan bahwa pada prinsifnya Dinas Ketahanan Pangan Provinsi Kalimantan Tengah dapat memberi izin dan memfasilitasi dalam pengumpulan data yang diperlukan. Silahkan berkomumikasi langsung ke Subbag Keuangan, Umum dan kepegawaian.

Demikian kami sampaikan, atas perhatian diucapkan terima kasih.

An. Kepala Dinas,
Sekretaris,

Hj. BASTIAH, SE
NIP. 19670706 199003 2 010

Tembusan :
Kasubbag Keuangan, Umum dan Kepegawaian







