

Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
<https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index>
 Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
 Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
 e-ISSN: [2685-0893](https://doi.org/10.35889/jutisi.v15i1.3511)

Implementasi *Laravel* dan AES-256 untuk Keamanan Arsip Digital PMB

DOI: <http://dx.doi.org/10.35889/jutisi.v15i1.3511>

Creative Commons License 4.0 (CC BY – NC)



Yunita Adelia Oktoreza^{1*}, Th. Dwiati Wismarini²

Teknologi Informasi, Universitas Stikubank, Semarang, Indonesia
 *e-mail *Corresponding Author*: yunitaadelia3002@mhs.unisbank.ac.id

Abstract

Operational obstacles in document retrieval and significant data security risks within the STIE BPD Jateng PMB Unit served as the primary motivation for this study. The researcher proposed a web-based archiving platform developed using the Laravel framework, reinforced by the Advanced Encryption Standard (AES-256) encryption scheme. The development procedure followed the Waterfall methodology, encompassing requirements identification, structural design, and the coding phase. Research findings indicated that utilizing the MVC pattern in Laravel produced a more organized system, while the integration of the AES-256 algorithm effectively protected documents from unauthorized access. Based on black-box testing results, all functional components of the system were proven to operate optimally. It was concluded that the implementation of this technology not only significantly accelerated administrative management but also ensured document privacy through an automated data security system.

Keywords: *Digital Archive; Laravel; Document Security; AES-256; Information Systems.*

Abstrak

Hambatan dalam efisiensi penemuan kembali dokumen serta tingginya risiko keamanan data pada Unit PMB STIE BPD Jateng menjadi latar belakang dilakukannya penelitian ini. Peneliti mengusulkan sebuah solusi berupa platform kearsipan berbasis web yang dikembangkan menggunakan *framework Laravel* dan diperkuat dengan skema enkripsi *Advanced Encryption Standard (AES-256)*. Prosedur pengembangan sistem ini mengacu pada metodologi Waterfall yang meliputi fase identifikasi kebutuhan, perancangan struktur, hingga tahap pengkodean. Temuan penelitian menunjukkan bahwa pemanfaatan pola MVC pada *Laravel* mampu menghasilkan sistem yang lebih terorganisir, sementara integrasi algoritma AES-256 secara efektif memproteksi dokumen dari akses yang tidak memiliki otoritas. Berdasarkan hasil pengujian *black-box*, seluruh komponen fungsional sistem terbukti beroperasi dengan optimal. Dapat disimpulkan bahwa implementasi teknologi ini tidak hanya mempercepat tata kelola administrasi secara signifikan, tetapi juga menjamin aspek privasi dokumen melalui sistem pengamanan data yang otomatis.

Kata kunci: *Arsip Digital; Laravel; Keamanan Dokumen; AES-256; Sistem Informasi.*

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi digital dalam tata kelola organisasi, termasuk di lingkungan perguruan tinggi [1]. Digitalisasi administrasi menjadi strategi penting untuk meningkatkan efisiensi, transparansi, dan akuntabilitas pengelolaan dokumen institusi. Tingginya penetrasi internet di Indonesia pada tahun 2024 menunjukkan bahwa aktivitas pendidikan semakin bergantung pada sistem berbasis digital [2]. Dalam hal tersebut, arsip tidak hanya berfungsi sebagai sumber informasi administratif, tetapi juga sebagai bukti hukum yang menjamin legitimasi kegiatan akademik dan keuangan. Regulasi kearsipan nasional menegaskan bahwa pengelolaan arsip harus dilakukan secara efektif, efisien, dan berkelanjutan untuk menjamin ketersediaan informasi yang autentik, utuh, dan terpercaya [3]. Pengembangan model sistem keamanan arsip digital menjadi isu strategis yang relevan untuk

diteliti, khususnya dalam menghadapi meningkatnya risiko kebocoran dan penyalahgunaan data di sektor pendidikan [4]. Penerapan sistem arsip digital tidak hanya menjadi kebutuhan teknis, tetapi juga merupakan tuntutan regulasi dan tata kelola institusi yang baik [5].

Analisis situasi pada Unit Penerimaan Mahasiswa Baru (PMB) STIE BPD Jateng menunjukkan adanya permasalahan dalam pengelolaan arsip digital. Pada tahun akademik 2023/2024 tercatat 1.327 calon mahasiswa dengan rata-rata enam dokumen per orang, sehingga jumlah arsip mencapai lebih dari 7.900 dokumen per tahun dan dapat melebihi 10.000 berkas jika digabungkan dengan dokumen administratif lainnya. Sistem penyimpanan yang masih tersebar pada beberapa perangkat dan belum terintegrasi menyebabkan proses pencarian dokumen memerlukan waktu 10–15 menit per berkas, serta meningkatkan risiko duplikasi, inkonsistensi, dan kehilangan data. Selain itu, sebagian dokumen masih disimpan dalam format terbuka tanpa mekanisme enkripsi, padahal memuat data sensitif seperti Nomor Induk Kependudukan, nilai akademik, dan bukti pembayaran. Kondisi ini menunjukkan adanya kesenjangan antara kebutuhan keamanan informasi dan sistem pengelolaan arsip yang saat ini diterapkan, sehingga diperlukan solusi yang tidak hanya meningkatkan efisiensi, tetapi juga menjamin perlindungan data secara komprehensif

Sejumlah penelitian terdahulu telah berupaya mengatasi permasalahan pengelolaan arsip digital. Prahoro (2023) mengembangkan sistem pengarsipan dokumen berbasis web menggunakan *framework Laravel* dengan metode *Software Development Life Cycle (SDLC)* dan pengujian *black-box*, yang menghasilkan peningkatan efisiensi serta kemudahan temu kembali arsip [6]. Prayogie *et al* (2025) merancang aplikasi pengarsipan surat berbasis *Laravel* melalui pendekatan rekayasa perangkat lunak terstruktur dan pengujian fungsional sistem, yang terbukti meningkatkan efektivitas kerja administrasi [7]. Putra *et al* (2025) mengembangkan sistem *E-Arsip* berbasis *web* menggunakan metode *waterfall* dengan hasil sistem mampu mengurangi risiko kehilangan dokumen dan meningkatkan kerapian pengelolaan arsip [8]. Di sisi lain, penelitian di bidang keamanan data oleh Sari *et al* (2021) menggunakan metode eksperimen kriptografi untuk menguji algoritma AES-256 dan menyimpulkan bahwa algoritma tersebut memiliki ketahanan tinggi terhadap serangan *brute force* [9]. Jannah *et al* (2023) melalui pendekatan implementatif dan pengujian keamanan sistem membuktikan bahwa enkripsi AES-256 mampu menjaga kerahasiaan dokumen meskipun terjadi akses tidak sah terhadap media penyimpanan [10]. Namun demikian, penelitian-penelitian tersebut masih terpisah antara aspek pengembangan sistem arsip dan aspek keamanan kriptografi. Belum terdapat penelitian yang mengintegrasikan *framework Laravel* dengan penerapan enkripsi AES-256 secara langsung pada level file arsip, khususnya dalam konteks pengelolaan arsip PMB perguruan tinggi yang memiliki karakteristik data sensitif dan volume dokumen yang tinggi. Gap inilah yang menjadi dasar dilakukannya penelitian ini.

Berdasarkan gap tersebut, penelitian ini mengusulkan model sistem keamanan arsip digital berbasis *web* menggunakan *framework Laravel* yang terintegrasi dengan algoritma enkripsi AES-256 pada level file serta mekanisme kontrol akses berbasis peran (*role-based access control*). *Laravel* dipilih karena memiliki arsitektur *Model-View-Controller (MVC)* yang mendukung pengembangan sistem yang terstruktur, modular, dan mudah dipelihara, serta menyediakan fitur keamanan seperti autentikasi, validasi input, dan proteksi CSRF. Integrasi enkripsi AES-256 dilakukan sebelum file disimpan ke server, sehingga dokumen tidak dapat dibaca tanpa kunci dekripsi yang sah. Pendekatan ini dipandang efektif karena memberikan perlindungan tidak hanya pada basis data, tetapi juga pada file arsip secara langsung, sehingga meminimalkan risiko kebocoran data meskipun terjadi akses tidak sah terhadap penyimpanan. Kebaruan (*novelty*) penelitian ini terletak pada integrasi komprehensif antara sistem arsip digital berbasis *Laravel*, penerapan enkripsi AES-256 pada level file, dan pengaturan hak akses berbasis peran yang disesuaikan dengan struktur organisasi PMB. Dengan demikian, penelitian ini menawarkan model sistem keamanan arsip digital yang lebih terintegrasi, kontekstual, dan aplikatif di lingkungan perguruan tinggi.

2. Metodologi

Penelitian ini merupakan penelitian *Research and Development (R&D)* yang berfokus pada pengembangan sistem arsip digital Penerimaan Mahasiswa Baru (PMB) dengan menerapkan *framework Laravel* dan algoritma enkripsi AES-256 sebagai mekanisme pengamanan data. Metode pengembangan sistem yang digunakan adalah metode *Waterfall*, karena metode ini menyediakan tahapan kerja yang sistematis dan terstruktur mulai dari

analisis kebutuhan hingga pengujian sistem. Tahapan penelitian meliputi analisis kebutuhan sistem, perancangan sistem, implementasi sistem, pengujian sistem, dan analisis hasil pengujian, di mana setiap tahapan menghasilkan luaran yang menjadi dasar bagi tahapan berikutnya [11].

2.1 Analisis Kebutuhan Sistem

Seluruh desain sistem disajikan pada bagian ini sebagai hasil transformasi dari tahap analisis kebutuhan. Perancangan diawali dengan penyajian Model Arsitektur Sistem yang menggambarkan hubungan antara pengguna, aplikasi berbasis Laravel, modul enkripsi dan dekripsi AES-256, serta media penyimpanan data. Model arsitektur ini menunjukkan alur interaksi sistem secara menyeluruh, mulai dari proses autentikasi pengguna, pengelolaan arsip digital, hingga mekanisme pengamanan file pada saat penyimpanan dan akses dokumen.

Selanjutnya, disajikan desain proses sistem yang memodelkan alur pengelolaan arsip secara operasional. Proses dimulai dari unggah dokumen oleh pengguna yang telah terautentikasi, kemudian sistem melakukan enkripsi menggunakan algoritma AES-256 sebelum file disimpan ke server. Pada saat dokumen diakses kembali, sistem melakukan proses dekripsi secara otomatis sehingga file hanya dapat ditampilkan kepada pengguna yang memiliki hak akses sesuai peran yang ditetapkan. Selain itu, disusun pula desain logis sistem yang menjelaskan mekanisme kerja algoritma AES-256 pada level file, termasuk proses pembangkitan kunci, enkripsi data, dan dekripsi saat proses akses. Luaran dari tahap ini berupa model arsitektur sistem, diagram alur proses, serta rancangan mekanisme pengamanan arsip digital yang menjadi dasar implementasi sistem.

2.2 Perancangan Sistem

Tahap perancangan sistem dilakukan berdasarkan hasil analisis kebutuhan dengan tujuan memodelkan struktur dan alur kerja sistem secara konseptual dan teknis. Perancangan meliputi desain arsitektur sistem yang menggambarkan hubungan antara pengguna, aplikasi berbasis Laravel, proses enkripsi dan dekripsi AES-256, serta media penyimpanan data.

Selain itu, dirancang pula desain proses sistem yang menggambarkan alur pengelolaan arsip, mulai dari proses unggah dokumen yang diikuti dengan enkripsi sebelum disimpan ke server, hingga proses akses dokumen yang diawali dengan dekripsi sebelum ditampilkan kepada pengguna yang berwenang. Desain logis sistem juga disusun untuk menjelaskan mekanisme kerja algoritma AES-256 dalam proses enkripsi dan dekripsi data pada level file. Luaran dari tahap ini berupa model arsitektur sistem, diagram alur proses, serta rancangan mekanisme pengamanan data arsip digital.

2.3 Implementasi Sistem

Tahap implementasi sistem merupakan realisasi dari hasil perancangan ke dalam bentuk aplikasi yang dapat dijalankan. Implementasi dilakukan menggunakan framework Laravel sebagai basis pengembangan aplikasi web, serta mengintegrasikan algoritma AES-256 untuk mengamankan file arsip digital.

Pada tahap ini dikembangkan beberapa modul utama, yaitu modul autentikasi pengguna, modul pengelolaan arsip digital, modul enkripsi file saat proses unggah, modul dekripsi file saat proses akses, modul *reader* dokumen, serta modul dashboard sistem. Setiap file yang diunggah ke sistem akan terlebih dahulu diproses menggunakan algoritma AES-256 sehingga file yang tersimpan di server berada dalam bentuk terenkripsi dan tidak dapat dibaca secara langsung tanpa melalui proses dekripsi oleh sistem yang sah.

2.4 Pengujian Sistem

Tahap pengujian sistem dilakukan untuk memastikan bahwa seluruh fungsi sistem berjalan sesuai dengan kebutuhan yang telah ditetapkan pada tahap analisis. Pengujian dilakukan menggunakan metode *black-box testing*, yaitu pengujian yang berfokus pada fungsi sistem tanpa melihat struktur kode program.

Pengujian dilakukan terhadap fungsi-fungsi utama sistem, seperti login pengguna, proses unggah dokumen, proses enkripsi file, proses akses dokumen, proses dekripsi file, dan fungsi *reader* dokumen. Selain itu, pengujian keamanan dilakukan dengan memeriksa file yang tersimpan di server untuk memastikan bahwa file berada dalam kondisi terenkripsi dan tidak dapat dibaca secara langsung di luar sistem aplikasi.

2.5 Analisis Hasil Pengujian

Tahap analisis hasil pengujian dilakukan secara deskriptif dengan membandingkan hasil pengujian sistem terhadap kebutuhan fungsional yang telah ditetapkan pada tahap analisis kebutuhan. Analisis ini bertujuan untuk menilai tingkat keberhasilan sistem dalam menjalankan seluruh fungsi yang dirancang serta efektivitas penerapan algoritma AES-256 dalam mengamankan data arsip digital PMB.

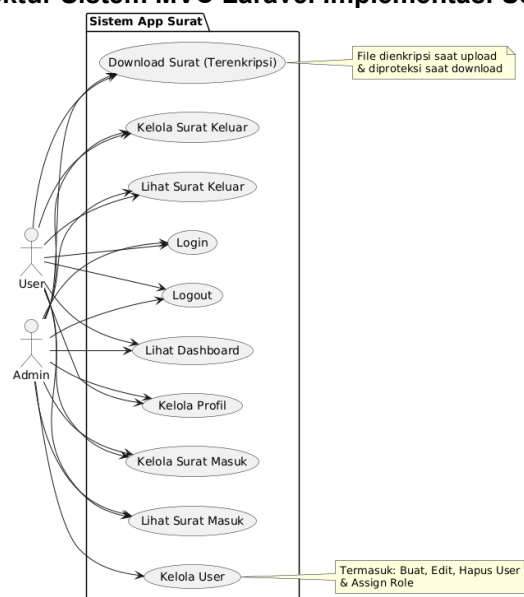
Sistem dinyatakan berhasil apabila seluruh fitur dapat berfungsi sesuai spesifikasi, proses enkripsi dan dekripsi berjalan dengan benar, serta file arsip yang tersimpan di server berada dalam kondisi terenkripsi dan hanya dapat diakses oleh pengguna yang memiliki hak akses melalui mekanisme autentikasi dan kontrol peran yang telah ditentukan.

3. Hasil dan Pembahasan

3.1 Lingkungan Implementasi Sistem

Lingkungan implementasi sistem mencakup perangkat keras, perangkat lunak, serta framework dan tools pendukung yang digunakan dalam pembangunan dan pengujian sistem arsip digital berbasis *website* pada Unit PMB STIE BPD Jateng. Perangkat keras yang digunakan memiliki spesifikasi minimal prosesor Intel Core i3 atau setara, RAM 4 GB, media penyimpanan HDD/SSD 256 GB, serta perangkat input-output berupa keyboard, mouse, dan monitor, yang sudah memadai untuk mendukung proses pengembangan dan operasional sistem. Perangkat lunak yang digunakan meliputi sistem operasi Windows sebagai platform pengembangan, Apache sebagai web server, MySQL sebagai sistem manajemen basis data untuk mengelola data arsip dan pengguna, serta Google Chrome sebagai browser pengujian sistem. Adapun framework dan tools pendukung yang digunakan adalah bahasa pemrograman PHP dengan framework Laravel yang menerapkan arsitektur MVC serta menyediakan fitur keamanan dan pengelolaan basis data terintegrasi, Composer sebagai dependency manager, dan Visual Studio Code sebagai text editor/IDE untuk membantu penulisan serta pengelolaan kode program.

3.2 Implementasi Arsitektur Sistem MVC Laravel Implementasi Use Case Diagram

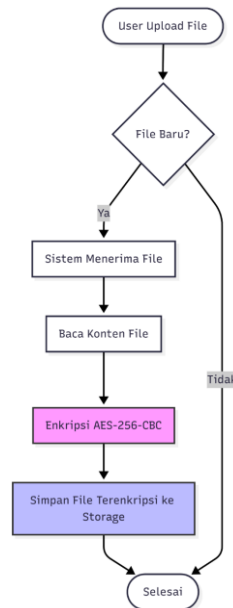


Gambar 1. Use Case Diagram Sistem Arsip Digital Unit PMB STIE BPD Jateng

Use Case Diagram menggambarkan interaksi antara dua aktor utama, yaitu Admin sebagai pihak yang memiliki hak akses penuh untuk mengelola pengguna, arsip, dan sistem, serta User sebagai staf Unit PMB dengan hak akses terbatas sesuai perannya, yang menjadi acuan dalam implementasi fitur menggunakan framework Laravel. Sistem menyediakan fungsi utama berupa login dan logout untuk autentikasi dan keamanan sesi, melihat dashboard sebagai ringkasan informasi arsip dan aktivitas pengguna, serta pengelolaan profil untuk memperbarui data pribadi. Selain itu, sistem mendukung pengelolaan dan peninjauan surat

masuk serta surat keluar yang meliputi proses tambah, ubah, hapus, unggah dokumen, dan pengelolaan metadata surat, di mana setiap proses unggah otomatis menerapkan mekanisme keamanan dokumen. Pengguna juga dapat mengunduh surat dalam kondisi aman melalui proses dekripsi dan proteksi tambahan seperti *password* pada PDF atau ZIP. Khusus Admin, tersedia use case kelola user yang mencakup pembuatan, pengeditan, penghapusan akun, serta pengaturan role dan hak akses, sehingga keseluruhan sistem mampu mengelola arsip digital secara terstruktur, aman, dan sesuai dengan kebutuhan Unit PMB STIE BPD Jateng.

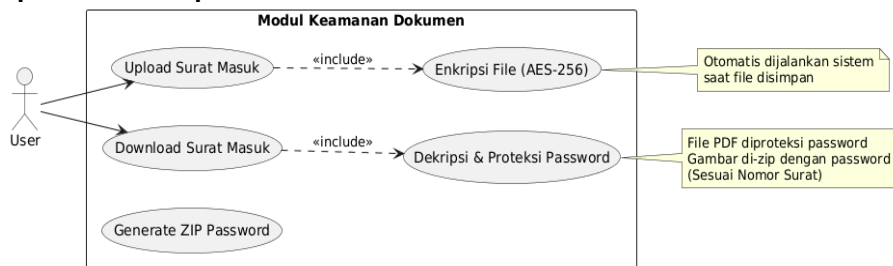
1) Implementasi Controller



Gambar 2. Flowchart Proses Upload dan Enkripsi Dokumen

Proses upload file dimulai ketika Admin atau User mengunggah dokumen arsip melalui antarmuka sistem dengan melengkapi data pendukung surat dan memilih file yang sesuai, kemudian request diterima oleh controller yang bertugas memvalidasi tipe, ukuran, dan kelengkapan data file. Setelah validasi berhasil, controller membaca konten file untuk memperoleh data biner tanpa langsung menyimpannya dalam bentuk asli, lalu menjalankan proses enkripsi menggunakan algoritma AES-256-CBC dengan kunci rahasia yang tersimpan aman pada konfigurasi Laravel. Hasil enkripsi berupa file terenkripsi yang tidak dapat dibaca secara langsung, sehingga menjamin keamanan dokumen dari akses tidak sah. Selanjutnya, file terenkripsi tersebut disimpan ke dalam storage sistem melalui mekanisme Laravel yang tidak dapat diakses secara publik, sementara database hanya menyimpan metadata file seperti nama dan lokasi penyimpanan, sehingga arsip tetap terlindungi dan hanya dapat diakses melalui sistem yang sah.

2) Implementasi Implementasi Keamanan Dokumen

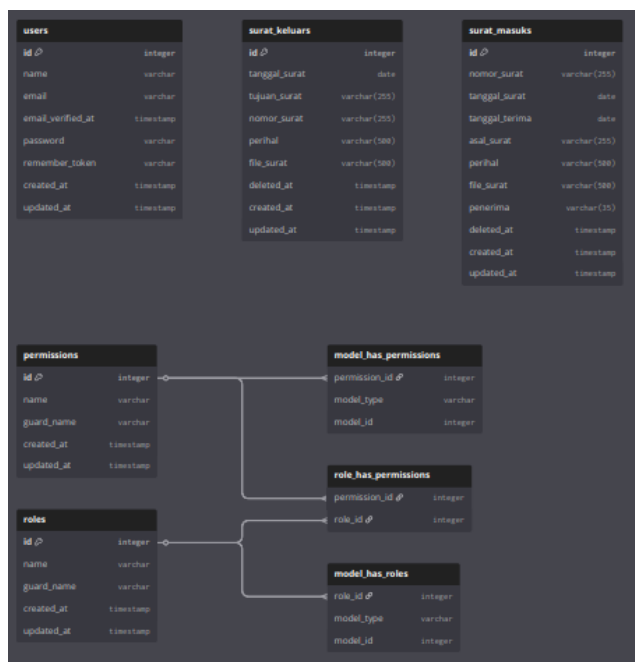


Gambar 3. Use Case Diagram Modul Keamanan Dokumen

Keamanan dokumen merupakan fitur utama dalam sistem arsip digital berbasis *website* pada Unit PMB STIE BPD Jateng yang diterapkan sejak proses unggah hingga pengunduhan dokumen untuk melindungi arsip dari akses tidak sah dan menjaga kerahasiaan data. Pada saat unggah, sistem terlebih dahulu memeriksa apakah file merupakan file baru untuk mencegah duplikasi, kemudian membaca konten file dan melakukan enkripsi menggunakan algoritma AES-256-CBC di sisi server sehingga file asli tidak pernah disimpan dalam bentuk terbuka, melainkan hanya dalam bentuk terenkripsi beserta metadata pendukungnya di database. Proses ini berjalan otomatis tanpa melibatkan pengguna secara langsung. Pada saat pengunduhan, sistem memverifikasi hak akses pengguna, melakukan dekripsi file secara sementara, lalu menerapkan proteksi tambahan berupa password pada dokumen PDF atau ZIP berpassword untuk jenis file lainnya dengan password yang disesuaikan dengan nomor surat. File kemudian dikirimkan melalui mekanisme streaming agar tidak tersimpan secara terbuka di server. Dengan mekanisme ini, keamanan dokumen tetap terjaga meskipun file berhasil diunduh, sehingga modul keamanan dokumen menjadi komponen inti sistem arsip digital dan sejalan dengan tujuan penelitian, yaitu mengembangkan sistem arsip digital berbasis website dengan penambahan fitur keamanan dokumen.

3.3 Implementasi Basis Data

1) Struktur Tabel Basis Data



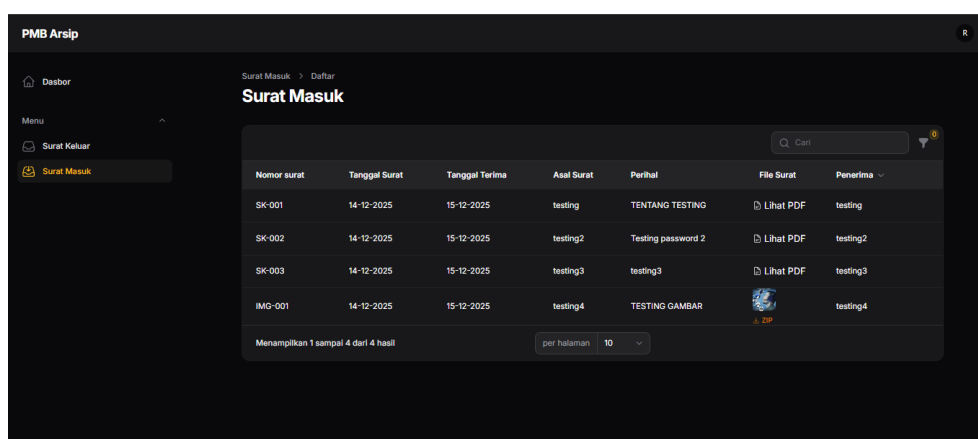
Gambar 4. Database

Implementasi basis data pada sistem arsip digital berbasis website di Unit PMB STIE BPD Jateng menggunakan MySQL yang terintegrasi dengan framework Laravel melalui Eloquent ORM untuk menyimpan, mengelola, dan mengamankan data secara terstruktur. Basis data dirancang untuk mendukung pengelolaan surat masuk, surat keluar, manajemen pengguna, serta pengaturan hak akses dan keamanan dokumen. Tabel utama yang digunakan meliputi tabel *users* untuk menyimpan data pengguna dan kebutuhan autentikasi, tabel *surat_masuks* untuk mengelola arsip surat masuk, tabel *surat_keluars* untuk pengarsipan surat keluar, tabel *roles* untuk menyimpan peran pengguna seperti admin dan petugas PMB, serta tabel *permissions* untuk mendefinisikan hak akses setiap fitur sistem. Selain itu, digunakan tabel relasi seperti *role_has_permissions*, *model_has_roles*, dan *model_has_permissions* guna mendukung mekanisme *Role-Based Access Control* (RBAC), sehingga setiap pengguna hanya dapat mengakses fitur sesuai peran dan izin yang diberikan. Dengan struktur ini, basis

data tidak hanya mendukung kerapian dan keterpaduan pengelolaan arsip digital, tetapi juga memperkuat aspek keamanan dan kontrol akses dalam sistem.

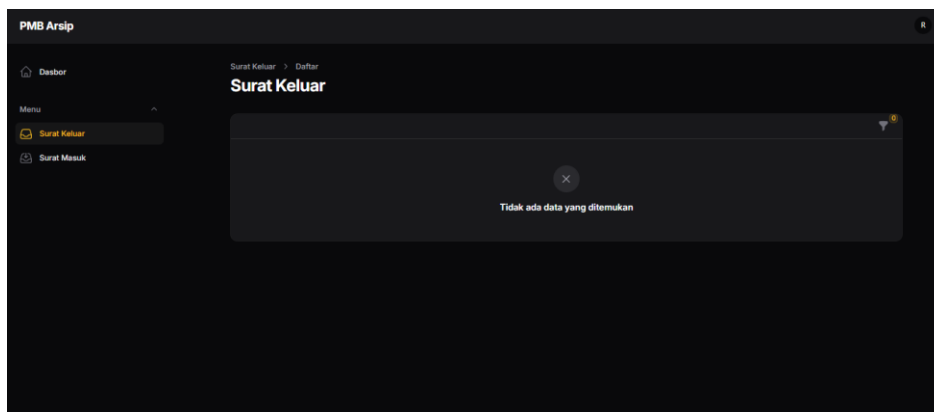
Relasi antar tabel pada basis data diimplementasikan untuk mendukung integrasi data dan keamanan sistem melalui hubungan antara tabel users dengan roles menggunakan tabel model_has_roles, relasi antara roles dengan permissions melalui tabel role_has_permissions, serta relasi antara users dengan permissions melalui tabel model_has_permissions, sehingga pengaturan hak akses pengguna dapat diterapkan secara fleksibel, terstruktur, dan aman sesuai kebutuhan Unit PMB STIE BPD Jateng. Basis data diintegrasikan dengan framework Laravel menggunakan *Eloquent ORM*, di mana setiap tabel direpresentasikan dalam bentuk model sehingga proses pengelolaan data dapat dilakukan tanpa menuliskan perintah SQL secara langsung, serta didukung oleh fitur migration untuk pengelolaan struktur tabel dan seeder untuk pengisian data awal seperti role dan permission, yang memudahkan proses pengembangan, pemeliharaan, dan pengujian sistem. Dari sisi keamanan, basis data dilengkapi dengan mekanisme enkripsi kata sandi pengguna, pembatasan akses data berdasarkan role, validasi input sebelum penyimpanan data, serta pengamanan file dokumen yang tersimpan dalam sistem, sehingga mampu menjaga kerahasiaan, integritas, dan ketersediaan data arsip secara optimal.

2) Implementasi Antarmuka Pengguna *Reader*



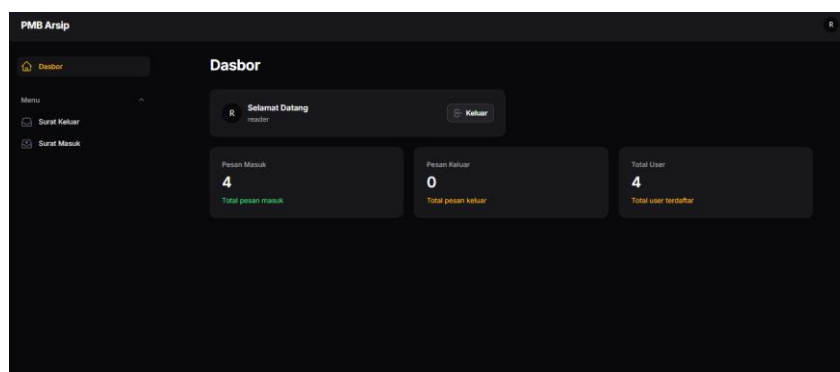
Gambar 5. Surat Masuk Pengguna *Reader*

Pengguna dengan peran reader merupakan salah satu tipe pengguna dalam sistem arsip digital Unit PMB STIE BPD Jateng yang memiliki hak akses terbatas dan dirancang khusus hanya untuk kebutuhan membaca serta melihat arsip dokumen tanpa kewenangan melakukan pengelolaan data. Reader tidak diperbolehkan untuk menambahkan, mengubah, maupun menghapus data surat, serta tidak memiliki akses untuk mengelola pengguna dan pengaturan hak akses sistem. Akses yang dimiliki hanya terbatas pada halaman dashboard, surat masuk, dan surat keluar dalam bentuk tampilan daftar arsip. Pada halaman Surat Masuk, pengguna reader dapat melihat informasi arsip yang meliputi nomor surat, tanggal surat, tanggal diterima, asal surat, perihal, file surat, dan penerima surat. Reader hanya memiliki hak untuk melihat dan mengunduh dokumen melalui tombol "Lihat PDF" atau file ZIP, di mana seluruh file yang diunduh telah melalui proses pengamanan, yaitu file PDF dilindungi dengan password dan file gambar dikompresi dalam bentuk ZIP yang juga menggunakan password, dengan password disesuaikan berdasarkan nomor surat sehingga hanya pihak yang memiliki informasi surat yang dapat membuka dokumen tersebut. Selain itu, halaman ini juga menyediakan fitur pencarian data surat dan pengaturan jumlah data yang ditampilkan per halaman, namun seluruh fitur bersifat read-only tanpa adanya tombol tambah, edit, atau hapus data, sehingga secara tegas menunjukkan keterbatasan hak akses pengguna *reader* dalam sistem.



Gambar 6. Surat Keluar Pengguna *Reader*

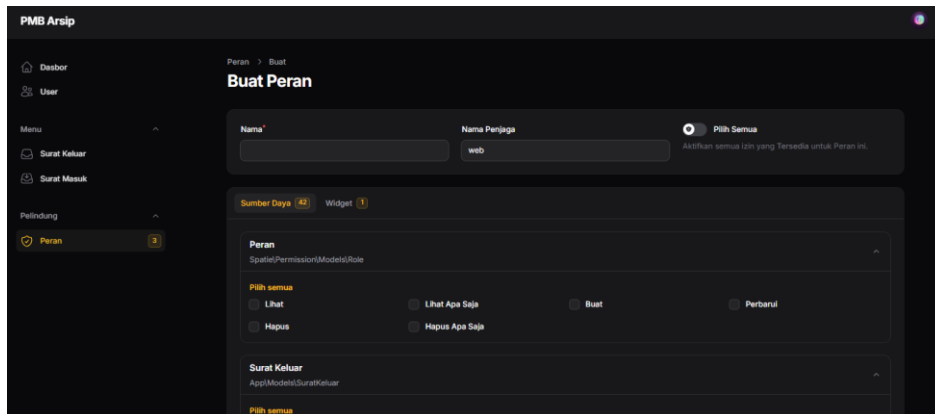
Halaman Surat Keluar pada pengguna reader berfungsi untuk menampilkan daftar arsip surat keluar yang telah dikelola oleh admin atau petugas PMB, di mana pengguna reader hanya dapat melihat data surat keluar yang tersedia di dalam sistem tanpa memiliki kewenangan untuk melakukan pengelolaan data. Apabila tidak terdapat data surat keluar yang dapat diakses, sistem secara otomatis akan menampilkan pesan “Tidak ada data yang ditemukan”, yang menunjukkan bahwa tampilan sistem menyesuaikan dengan ketersediaan data serta hak akses pengguna. Pada halaman ini, pengguna reader tidak dapat menambahkan surat keluar, tidak dapat mengedit data, dan tidak dapat menghapus arsip, sehingga seluruh interaksi pengguna dibatasi hanya pada aktivitas melihat informasi arsip. Pembatasan ini bertujuan untuk menjaga keamanan, keutuhan, dan integritas data arsip agar tetap terpelihara dengan baik dalam sistem.



Gambar 7. *Dasboard* Pengguna *Reader*

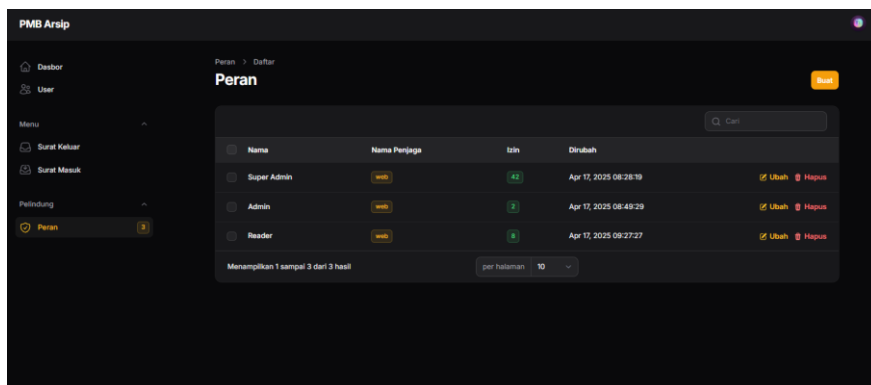
Dashboard pengguna Reader menampilkan informasi utama dalam bentuk beberapa kartu ringkasan yang bersifat informatif dan hanya dapat dibaca (*read-only*). Pada bagian atas terdapat kartu sambutan yang memuat teks “Selamat Datang” sebagai tanda bahwa pengguna berhasil terautentikasi, identitas role “*reader*” yang menunjukkan hak akses terbatas, ikon profil berupa inisial nama pengguna sebagai identitas akun, serta tombol “Keluar” (logout) yang berfungsi untuk mengakhiri sesi demi menjaga keamanan akun. Selain itu, terdapat kartu Pesan Masuk yang menampilkan jumlah total arsip surat masuk yang tersimpan dalam sistem sebagai informasi ketersediaan data arsip aktif dengan indikator warna hijau, kartu Pesan Keluar yang menunjukkan jumlah arsip surat keluar yang tercatat dengan indikator warna oranye untuk membedakan jenis data, serta kartu Total User yang menampilkan jumlah keseluruhan pengguna terdaftar dalam sistem. Seluruh informasi tersebut hanya dapat dilihat oleh pengguna Reader tanpa hak untuk melakukan perubahan data, sehingga dashboard berfungsi sebagai sarana pemantauan kondisi arsip dan penggunaan sistem secara ringkas, informatif, dan aman.

3) Implementasi Antarmuka Pengguna Admin

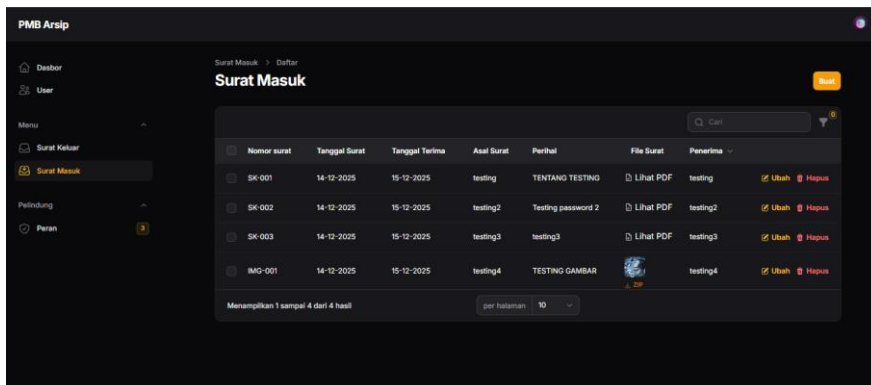


Gambar 8. Buat Peran Pengguna Admin

Halaman Buat Peran pada pengguna admin berfungsi untuk menambahkan peran baru sekaligus mengatur hak akses (izin) dalam sistem arsip digital PMB STIE BPD Jateng. Melalui halaman ini, admin dapat menentukan nama peran, guard name yang secara default menggunakan web, serta memilih izin sesuai tingkat kewenangan pengguna, termasuk fitur Pilih Semua untuk mengaktifkan seluruh izin secara otomatis. Pengaturan izin dikelompokkan berdasarkan sumber daya sistem seperti peran, surat masuk, dan surat keluar dengan opsi melihat, menambah, memperbarui, dan menghapus data, sehingga memudahkan pengelolaan akses secara terstruktur. Dengan adanya fitur ini, admin dapat membatasi atau memberikan hak akses sesuai kebutuhan, sekaligus menerapkan mekanisme *Role-Based Access Control (RBAC)* secara efektif guna menjaga keamanan dan ketertiban pengelolaan arsip digital.

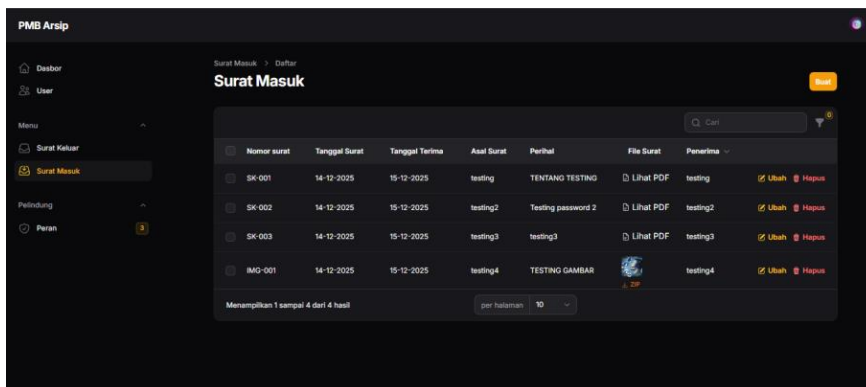


Gambar 9. Peran Pengguna Admin



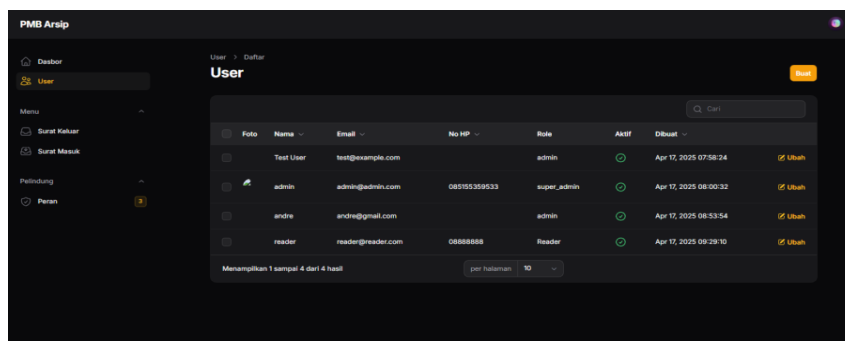
Gambar 10. Surat Masuk Pengguna Admin

Halaman Daftar Peran pada pengguna admin berfungsi untuk menampilkan seluruh peran yang terdaftar dalam sistem arsip digital PMB STIE BPD Jateng dalam bentuk tabel yang memuat nama peran, guard name, jumlah izin, serta waktu terakhir perubahan data. Pada halaman ini ditampilkan peran utama seperti Super Admin, Admin, dan Reader dengan jumlah izin yang berbeda sesuai tingkat kewenangannya, yang menunjukkan penerapan pembatasan akses untuk menjaga keamanan dokumen arsip. Selain itu, tersedia fitur pencarian dan pengaturan jumlah data per halaman untuk memudahkan pengelolaan, serta aksi ubah dan hapus peran yang dapat dilakukan oleh admin. Dengan demikian, halaman ini mendukung penerapan *Role-Based Access Control (RBAC)* secara terstruktur sehingga pengaturan hak akses pengguna dapat dikelola dengan efektif dan aman.



Gambar 11. Surat Keluar Pengguna Admin

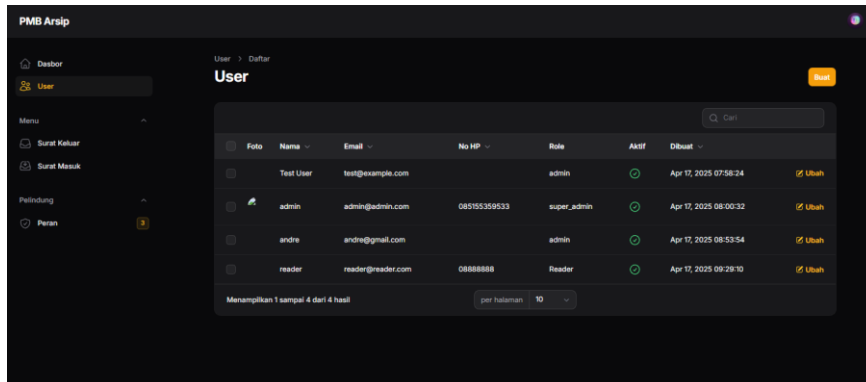
Halaman Surat Masuk pengguna Admin pada Gambar 11. menampilkan sistem dengan desain antarmuka dark mode yang modern dan nyaman di mata, dilengkapi navigasi sidebar yang konsisten untuk mengakses dasbor, manajemen user, pengelolaan surat masuk dan keluar, serta pengaturan peran sebagai bagian dari fitur keamanan. Modul Surat Masuk menunjukkan sistem telah berjalan dengan baik melalui penyajian data dalam tabel terstruktur yang memuat nomor surat, tanggal surat, tanggal terima, asal, perihal, dan penerima, serta mendukung manajemen berkas dalam berbagai format seperti PDF dan ZIP. Fitur CRUD telah tersedia secara lengkap melalui tombol “Buat”, aksi “Ubah” dan “Hapus”, serta dilengkapi dengan fitur pencarian, filter, dan pagination untuk memudahkan pengelolaan arsip dalam jumlah besar. Sementara itu, Modul Surat Keluar menampilkan kondisi empty state dengan pesan “Tidak ada data yang ditemukan”, yang menandakan bahwa logika sistem telah berfungsi meskipun belum terdapat data, dan tetap mempertahankan elemen kontrol seperti tombol “Buat” serta filter, sehingga konsistensi fungsi antar modul tetap terjaga.



Gambar 12. Tampilan User Pengguna Admin

Halaman User pada pengguna Admin berfungsi sebagai fitur keamanan untuk mengontrol dan memantau siapa saja yang dapat berinteraksi dengan sistem arsip digital, di mana tabel pengguna menampilkan identitas seperti foto, nama, email, dan nomor HP. Penerapan *Role-Based Access Control (RBAC)* terlihat dari kolom role yang membedakan hak akses pengguna menjadi super_admin, admin, dan reader sesuai tingkat kewenangannya

terhadap dokumen. Selain itu, kolom status “Aktif” dengan ikon centang hijau menunjukkan bahwa akun berada dalam kondisi valid dan diizinkan mengakses sistem, sementara kolom “Dibuat” berfungsi sebagai audit trail sederhana yang mencatat waktu pembuatan akun untuk kebutuhan pengawasan dan administrasi.



Gambar 13. Tampilan *Dasboard* Pengguna Admin

Halaman Dasbor berfungsi sebagai pusat informasi yang menampilkan ringkasan statistik sistem secara real-time, seperti jumlah pesan masuk, pesan keluar, dan total pengguna, serta dilengkapi panel sambutan “Selamat Datang” dan tombol logout untuk menjaga keamanan sesi. Modul Manajemen Pengguna menerapkan *Role-Based Access Control* (RBAC) dengan peran *super_admin*, *admin*, dan *reader*, dilengkapi data identitas pengguna serta status akun aktif sebagai fondasi utama keamanan sistem. Sementara itu, modul Surat Masuk menjadi pusat pengelolaan arsip digital yang terorganisir melalui pencatatan metadata surat, dukungan berbagai format file seperti PDF dan ZIP, fitur pratinjau dokumen, serta kontrol data lengkap melalui fungsi tambah, ubah, dan hapus.

3.4 Pengujian Fungsional (*Blackbox Testing*)

Tabel 1. Pengujian Fungsional (*Blackbox Testing*)

No	Fitur	Input	Langkah Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	Login / Logout	<i>Username & Password</i> valid	Masuk ke sistem, klik logout	<i>Dashboard</i> tampil, sesi berakhir saat logout	Sesuai	Valid
2	Unggah Dokumen	File PDF/ZIP	Pilih file, isi metadata, klik unggah	File terenkripsi otomatis, metadata tersimpan	Sesuai	Valid
3	Unduh Dokumen	Arsip tersimpan	Pilih file, klik unduh	File terdekripsi sementara, password aktif	Sesuai	Valid
4	Pencarian Arsip	Nomor surat / tanggal	Masukkan kriteria pencarian	Data arsip sesuai filter muncul	Sesuai	Valid
5	CRUD Surat Masuk (Admin)	Data surat baru	Tambah, ubah, hapus surat	Data tersimpan / terupdate / terhapus sesuai perintah	Sesuai	Valid
6	CRUD User & Role (Admin)	Data user / role baru	Tambah, ubah, hapus, atur hak akses	Data tersimpan / terupdate / terhapus, hak akses sesuai	Sesuai	Valid

4. Pembahasan

Penelitian ini mengusulkan pengembangan sistem arsip digital PMB berbasis website dengan penerapan Laravel dan algoritma enkripsi AES-256-CBC untuk mengatasi beberapa masalah utama yang diidentifikasi pada awal penelitian, yaitu pengelolaan arsip yang masih manual dan tidak terintegrasi, risiko kehilangan serta kebocoran dokumen, dan ketiadaan mekanisme keamanan data yang kuat. Berdasarkan hasil pengujian fungsional, semua fitur utama sistem, seperti pengelolaan surat masuk dan keluar, unggah dokumen, enkripsi otomatis saat unggah, dekripsi sementara saat unduh, pencarian arsip berbasis metadata, serta pembatasan hak akses berbasis peran (*role-based access control*), berhasil berjalan sesuai kebutuhan yang telah dianalisis [12]. Hal ini menunjukkan bahwa konsep sistem yang diusulkan berpotensi secara efektif menyelesaikan masalah yang dihadapi, khususnya dalam hal integrasi pengelolaan arsip dan perlindungan dokumen secara kriptografis. Penerapan enkripsi AES-256-CBC pada setiap dokumen memastikan bahwa file disimpan dalam bentuk terenkripsi, sehingga meskipun terjadi akses tidak sah ke server, isi dokumen tetap terlindungi tanpa kunci dekripsi yang valid [13]. Penambahan proteksi berupa password pada file PDF atau ZIP saat pengunduhan semakin memperkuat keamanan, sehingga hanya pengguna yang memiliki informasi arsip yang sah dapat mengakses isi dokumen. Dengan arsitektur MVC Laravel, pengelolaan data, kontrol proses enkripsi-dekripsi, dan tampilan antarmuka pengguna dapat dipisahkan secara jelas, sehingga keamanan informasi diterapkan secara sistematis dan terintegrasi [14].

Hasil penelitian ini memperkuat temuan penelitian terdahulu terkait efektivitas penggunaan AES-256 dalam pengamanan dokumen digital. Ridho & Romli (2024) menunjukkan bahwa AES-256 mampu menjaga kerahasiaan dokumen pada sistem berbasis web [15], sedangkan Nizamuddin & Sakti (2025) menggabungkan AES-256 dengan kompresi Huffman untuk pengamanan file berbasis web, tetapi penelitian mereka tidak mengintegrasikan kontrol akses berbasis peran, sehingga hanya fokus pada keamanan file tanpa mempertimbangkan alur kerja pengguna [16]. Putri *et al* (2025) membuktikan bahwa AES-256-CBC efektif menjaga data akademik sensitif tanpa mengurangi performa sistem, namun sistem mereka belum memanfaatkan integrasi enkripsi dengan workflow manajemen arsip secara menyeluruh [17]. Penelitian ini menegaskan dan memperluas temuan tersebut dengan menggabungkan enkripsi dokumen, pengelolaan arsip, dan kontrol akses berbasis peran dalam satu sistem terstruktur. Selain itu, penggunaan password dinamis berbasis metadata surat menambah lapisan perlindungan yang jarang dibahas pada penelitian terdahulu, sehingga memberikan kontribusi baru dalam pengembangan sistem arsip digital yang aman.

Beberapa penelitian lain menunjukkan pendekatan berbeda yang dapat dianggap bertentangan atau kurang komprehensif dibanding penelitian ini. Misalnya, penelitian oleh Surya *et al* (2025) menggunakan AES-256 dikombinasikan dengan hashing SHA-256 untuk menjaga integritas dokumen di *cloud storage*, namun pendekatan ini lebih kompleks dan memerlukan manajemen kunci tambahan sehingga belum tentu praktis untuk sistem manajemen arsip di lingkungan perguruan tinggi [18]. Dengan demikian, penelitian ini menawarkan solusi alternatif yang lebih terintegrasi dan sederhana dalam konteks pengelolaan arsip pendidikan, sekaligus mempertahankan keamanan tingkat tinggi.

Secara praktis, penelitian ini memberikan model sistem arsip digital yang dapat direplikasi pada unit kerja lain di lingkungan perguruan tinggi atau institusi serupa yang membutuhkan pengamanan dokumen tingkat tinggi. Temuan ini menguatkan tren pemanfaatan algoritma AES-256 dalam pengamanan informasi digital dan memperluas aplikasinya pada konteks sistem arsip pendidikan, dengan integrasi penuh antara manajemen arsip, kriptografi, dan kontrol akses. Dengan demikian, penelitian ini tidak hanya relevan secara teoritis, tetapi juga efektif secara praktis dalam menghadapi risiko keamanan dokumen modern, sekaligus memperkaya literatur ilmiah tentang penerapan kriptografi pada sistem informasi berbasis web.

5. Simpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem, dapat disimpulkan bahwa penelitian berhasil menghasilkan sistem arsip digital berbasis website yang mampu menjawab permasalahan utama dalam pengelolaan arsip di Unit PMB STIE BPD Jateng, yaitu keterbatasan efisiensi, kesulitan pencarian dokumen, serta rendahnya tingkat keamanan data arsip. Penerapan framework Laravel dengan arsitektur *Model-View-Controller* (MVC) terbukti mampu membangun sistem yang terstruktur, modular, dan mudah

dikembangkan, sehingga mendukung pengelolaan arsip secara terintegrasi dan tertib administrasi. Sementara itu, implementasi algoritma AES-256-CBC sebagai mekanisme enkripsi dokumen menjadikan keamanan sebagai fitur inti sistem, yang diperkuat dengan proses dekripsi terkontrol, proteksi password pada file hasil unduhan, serta pengaturan hak akses berbasis peran, sehingga kerahasiaan dan integritas arsip digital dapat terjaga secara optimal. Keterpaduan antara Laravel sebagai platform pengembangan aplikasi dan AES-256 sebagai metode pengamanan dokumen menunjukkan bahwa sistem tidak hanya berfungsi sebagai media penyimpanan, tetapi juga sebagai sistem manajemen arsip yang aman dan andal. Dengan demikian, sistem ini mampu mendukung pengelolaan arsip PMB secara modern, efektif, dan aman, sekaligus membuka peluang pengembangan lebih lanjut seperti integrasi dengan sistem akademik kampus, penerapan audit log aktivitas pengguna, serta penguatan mekanisme *backup* dan *recovery* untuk meningkatkan keandalan dan keamanan arsip digital di masa mendatang.

Daftar Referensi

- [1] A. Almadira, Y. Pratama, Dan F. Purwani, "Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data," *Jurnal Scientech Research and Development.*, Vol. 6, No. 2, pp. 540–549, Des 2024, doi: 10.56670/Jsr.V6i2.608.
- [2] We Are Social, "Laporan Khusus Digital 2024," We Are Social. [Daring]. Tersedia Pada: <https://wearesocial.com/id/blog/2024/01/digital-2024/>
- [3] Badan Pemeriksa Keuangan Republik Indonesia, "Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 7 Tahun 2017 Tentang Gerakan Nasional Sadar Tertib Arsip," Badan Pemeriksa Keuangan Republik Indonesia. [Daring]. Tersedia Pada: <https://peraturan.bpk.go.id/details/194504/perka-arsip-nasional-no-7-tahun-2017>
- [4] A. Anisah, D. Wahyuningsih, E. Helmud, T. Suwanda, P. Romadiana, Dan D. Irawan, "Rancang Bangun Sistem Informasi Manajemen Arsip Digital," *Jurnal Sisfokom (Sistem Inf. Dan Komputer)*, Vol. 10, No. 3, pp. 419–425, Des 2021, Doi: 10.32736/Sisfokom.V10i3.1300.
- [5] S. Surahman, M. T. Hidayatullah, A. Widawati, Dan D. Agustin, "Strategi Pengelolaan Informasi Dan Kearsipan Di Lembaga Pendidikan," *Jurnal Pendidikan Dan Studi Islam*, Vol. 6, No. 1, pp. 292–298, 2025. <https://doi.org/10.55623/au.v6i1.394>
- [6] D. G. Prahoro, "Sistem Informasi Pengarsipan Dokumen Berbasis Web Menggunakan Framework Laravel Di PT Kereta Commuter Indonesia," *Skrpsi Universitas Semarang*, 2023.
- [7] A. Prayogie, S. Auliana, Dan B. Rakhim Setya Permana, "Perancangan Aplikasi Pengarsipan Surat Berbasis Web Menggunakan Framework Laravel Pada Skpd Terpadu Provinsi Banten," *Jati (Jurnal Mahasiswa Teknik Informatika.)*, Vol. 9, No. 5, pp. 9171–9175, 2025, doi: 10.36040/Jati.V9i5.15130.
- [8] C. H. A. Putra, A. A. Soni, I. G. A. Sudandi, Dan I. K. A. Surya, "E-Arsip Ukm Paskamras Berbasis Web Menggunakan Framework Laravel," *Innovative : Journal Social Science Research*, Vol. 5, pp. 406–415, 2025. <https://doi.org/10.31004/innovative.v5i2.17993>
- [9] M. Sari, H. D. Purnomo, Dan I. Sembiring, "Review : Cryptographic Algorithm For Sms Security System On Android," *Jifotech:Journal Information Technology*, Vol. 2, No. 1, 2022, pp. 11-20, doi: <https://doi.org/10.46229/Jifotech.V2i1.292>.
- [10] A. F. Jannah, M. Tahir, M. S. S. Q. Aini, Dan T. W. Hermawan, "Penggunaan Algoritma Aes (Advanced Encryption Standard) Pada Veracrypt Untuk Mengamankan Data Pada Perangkat Penyimpanan," *Jati:Jurnal Mahasiswa Teknik Informasi*, Vol. 9, No. 4, pp. 101-120, 2025. <https://doi.org/10.36040/jati.v9i4.14318>
- [11] V. Z. Kamila Dan E. Subastian, "Analisis Dan Perancangan Sistem Evaluasi Pelatihan Tenaga Kependidikan," *Sebatik*, Vol. 10, No. 2, pp. 159–164, 2020.
- [12] P. A. Pratama, "Pengembangan Sistem Arsip Digital Berbasis Website Dengan Framework Laravel Untuk Efisiensi Penyimpanan Website-Based Digital Archiving System Development With Laravel Framework For Storage Efficiency And Data Security," *Jurnal Komputer Dan Teknologi Sains*, Vol. 3, No. 2, pp. 9–12, 2024. doi: <https://doi.org/10.37637/komteks.v3i2.2167>
- [13] W. T. Ramdan Dan D. Yusuf, "Rancang Bangun Portal Document Management System Berbasis Web Untuk Digitalisasi Arsip Menggunakan Frawework Laravel (Studi Kasus : Pt . Bridgestone Tire Indonesia)," *Jati: Jurnal Mahasiswa Teknik Informatika*, Vol. 8, No.

- 4, pp. 8091–8097, 2024. <https://doi.org/10.36040/jati.v8i4.10499>
- [14] A. Hidayatullah Dan D. Yusuf, “Pengembangan Backend Sistem Kearsipan Dokumen Menggunakan Framework Laravel Di Cv . Nakula Sadewa,” *Journal Software Development Digital Business Intelligence and Computer Engineering*, Vol. 02, No. 02, pp. 61–68, 2024, Doi: 10.57203/Session.V2i02.2024.61-68.
- [15] A. Ridho Dan M. A. Romli, “Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (Aes-256),” *Jurnal Informatika Teknologi Dan Sains*, Vol. 10, No 10, pp. 1044–1052, 2024.
- [16] N. A. Kafa, D. Virgian, Dan S. Yudha, “Implementasi Kriptografi Berbasis Web Dengan Algoritma Advanced Encryption Standard (Aes) 256 Dan Kompresi Huffman Untuk Pengamanan File Di Smk Satria,” *Jurnal Ticom: Technology of Information and Communication*, Vol. 12, pp. 50–55, 2024. DOI: <https://doi.org/10.70309/ticom.v12i2.109>
- [17] Z. Hayat, A. Putri, Y. A. Yustraini, R. Ariansyah, Dan N. C. Nisa, “Pengamanan Data Akademik Berbasis Web Dengan Enkripsi Aes-256 (Studi Kasus Pada Pendataan Digital Sma Xyz),” *Jurnal Nasaional Teknologi Informasi Dan Aplikasi*, Vol. 3, pp. 707–716, 2025.
- [18] J. Surya, A. Louis, F. Rini, Dan S. Mulyati, “Cryptographic Framework For Cloud-Based Document Storage Using Aes-256 And Sha-256 Hybrid Systems,” *Junal Ilmu Pengetahuan Dan Teknolgi Komputer.*, Vol. 11, No. 2, pp. 807-817, 2025, Doi: 10.33480/Jitk.V11i2.7132.Cryptographic.