

**RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN
DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA
AES-256 BERBASIS WEB**

SKRIPSI

DISUSUN OLEH

MUHAMMAD ASRIL AZMI

NPM. 2209010100



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

MEDAN

2026

**RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN
DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA
AES-256 BERBASIS WEB**

SKRIPSI

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

MUHAMMAD ASRIL AZMI

NPM. 2209010100

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

MEDAN

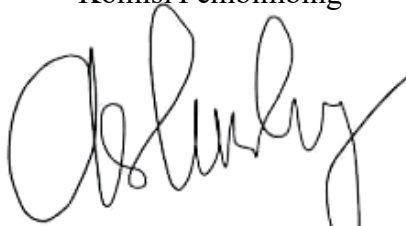
2026

LEMBAR PENGESAHAN

Judul Skripsi : Rancang Bangun Sistem Keamanan
Penyimpanan Dokumen Digital Menggunakan
Algoritma AES-256 Berbasis Web
Nama Mahasiswa : Muhammad Asril Azmi
NPM : 2209010100
Program Studi : Sistem Informasi

Menyetujui

Komisi Pembimbing



(Rizaldy Khair, S.Kom., M.Kom.)

NIDN. 0116098802

Ketua Program Studi



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

NIDN. 0117088902

Dekan



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

NIDN. 0127099201

PERNYATAAN ORISINALITAS

RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB

SKRIPSI

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

Medan, 27 Agustus 2026

Yang membuat pernyataan



Muhammad Asril Azmi

NPM. 2209010100

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

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

Nama	: Muhammad Asril Azmi
NPM	: 2209010100
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

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

**RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN
DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA
AES-256 BERBASIS WEB**

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

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 27 Agustus 2026

Yang membuat pernyataan



Muhammad Asril Azmi

NPM. 2209010100

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	:	Muhammad Asril Azmi
Tempat dan Tanggal Lahir	:	Medan, 26 Mei 2003
Alamat Rumah	:	Jl. Bhayangkara No. 424
Telefon/Faks/HP	:	082213899406
E-Mail	:	asrilazmi25@gmail.com
Instansi Tempat Kerja	:	-
Alamat Kantor	:	-

DATA PENDIDIKAN

SD	:	SDS Pertiwi Medan	TAMAT	:	2009-2015
SMP	:	SMP Negeri 11 Medan	TAMAT	:	2015-2018
SMA	:	SMA Dharmawangsa Medan	TAMAT	:	2018-2021

KATA PENGANTAR



Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Akrim, M.Pd., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Dr. Firahmi Rizky, S.Kom., M.Kom., Wakil Dekan I Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
4. Bapak Muhammad Basri, S.Si., M.Kom., Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
5. Bapak Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom. Ketua Program Studi Sistem Informasi UMSU.
6. Bapak Mulkan Azhari, S.Kom., M.Kom. Sekretaris Program Studi Sistem Informasi UMSU.
7. Bapak Rizaldi Khair, S.Kom., M.Kom. selaku Dosen Pembimbing yang telah memberikan bimbingan serta arahan kepada penulis selama proses penyelesaian Tugas Akhir ini.
8. Bapak Martiano, S.Kom., M.Kom. selaku Dosen Pembimbing I yang telah memberikan saran, koreksi, dan masukan kepada penulis dalam proses penyelesaian Tugas Akhir ini.
9. Ibu Fatma Sari Hutagalung, S.Kom., M.Kom, selaku Dosen Pembimbing II yang telah memberikan saran, koreksi, dan masukan kepada penulis dalam proses penyelesaian Tugas Akhir ini.

10. Kedua orang tua tercinta, Papa dan Mama, yang senantiasa memberikan doa, dukungan, kasih sayang, serta pengorbanan yang tiada henti kepada penulis.
11. Kak Nadia dan Bang Lucky yang senantiasa memberikan semangat, bantuan, serta dorongan positif dalam setiap proses yang dilalui.
12. Putri Nabila selaku pacar penulis yang telah memberikan dukungan, perhatian, serta membantu penulis dalam pengerjaan skripsi ini.
13. Seluruh pihak yang telah memberikan bantuan, baik secara langsung maupun tidak langsung, yang tidak dapat penulis sebutkan satu per satu dalam penyelesaian skripsi ini.

RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB

ABSTRAK

Keamanan dokumen digital merupakan salah satu aspek yang perlu diperhatikan untuk mencegah informasi diakses oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk mengembangkan sistem penyimpanan dokumen digital berbasis web yang menerapkan algoritma Advanced Encryption Standard (AES-256-CBC) sebagai mekanisme pengamanan. Sistem dibangun dengan menggunakan framework Laravel, bahasa pemrograman PHP, basis data SQLite, serta pustaka OpenSSL untuk mendukung proses enkripsi dan dekripsi dokumen. Pengujian sistem dilakukan menggunakan metode Black Box Testing untuk mengetahui kesesuaian fungsi sistem dengan kebutuhan yang telah ditentukan. Pengujian mencakup fitur login, unggah dokumen, enkripsi, dekripsi, pengunduhan, dan penghapusan dokumen. Hasil penelitian menunjukkan bahwa algoritma AES-256-CBC dapat diterapkan pada sistem untuk memberikan perlindungan terhadap dokumen digital. Setiap dokumen yang diunggah diproses melalui enkripsi secara otomatis sebelum disimpan, sedangkan pengambilan dokumen ke bentuk semula memerlukan Encryption Key yang dimiliki pengguna. Sistem juga menggunakan Initialization Vector (IV) yang dihasilkan secara acak pada setiap proses enkripsi sebagai bagian dari mekanisme pengamanan data. Hasil pengujian menggunakan metode Black Box menunjukkan bahwa seluruh fungsi utama sistem telah berjalan sesuai dengan kebutuhan fungsional. Dengan demikian, sistem yang dikembangkan dapat digunakan untuk mendukung keamanan penyimpanan dokumen digital berbasis web.

Kata Kunci: keamanan dokumen digital, AES-256-CBC, kriptografi, Laravel, Black Box Testing.

DESIGN AND DEVELOPMENT OF A WEB-BASED DIGITAL DOCUMENT STORAGE SECURITY SYSTEM USING THE AES-256 ALGORITHM

ABSTRACT

Security of digital documents is an important aspect in preventing information from being accessed by unauthorized parties. This study aims to develop a web-based digital document storage system that applies the Advanced Encryption Standard (AES-256-CBC) algorithm as a security mechanism. The system was developed using the Laravel framework, PHP programming language, SQLite database, and OpenSSL library to support document encryption and decryption processes. System testing was conducted using the Black Box Testing method to determine whether the system functions meet the specified requirements. The testing covered login, document upload, encryption, decryption, document download, and document deletion features. The results showed that the AES-256-CBC algorithm can be implemented in the system to provide protection for digital documents. Each uploaded document is automatically encrypted before being stored, while restoring the document to its original form requires an Encryption Key owned by the user. The system also uses an Initialization Vector (IV) that is randomly generated for each encryption process as part of the data security mechanism. The results of Black Box Testing indicated that all main system functions operated according to the specified functional requirements. Therefore, the developed system can be used to support the security of web-based digital document storage.

Keywords: digital document security, AES-256-CBC, cryptography, Laravel, Black Box Testing.

DAFTAR ISI

LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS	iii
RIWAYAT HIDUP	v
KATA PENGANTAR	vi
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	4
BAB II LANDASAN TEORI	6
2.1 Sistem Keamanan Informasi.....	6
2.1.1 Confidentiality (Kerahasiaan)	6
2.1.2 Integrity (Keutuhan).....	7
2.2.1 Jenis-Jenis Dokumen Digital.....	10
2.2.2 Risiko Keamanan Dokumen Digital	11
2.3 Kriptografi	12
2.3.2 Dekripsi	13
2.3.3 Jenis-Jenis Kriptografi.....	14
2.4 Algoritma Advanced Encryption Standard (AES-256).....	15
2.4.1 AES-256	15
2.4.3 Perbandingan Algoritma Kriptografi.....	18
2.4.4 Kelebihan AES-256.....	20
2.5 Sistem Berbasis Web	21

2.5.1 Arsitektur Sistem Berbasis Web.....	22
2.5.2 Kelebihan Sistem Berbasis Web	23
2.5.3 Keterkaitan dengan Penelitian.....	24
2.6 <i>Flowchart</i>	25
2.6.1 Fungsi <i>Flowchart</i>	26
2.6.2 Simbol-Simbol <i>Flowchart</i>	26
2.7 UML (Unified Modeling Language).....	27
2.7.1 Fungsi UML.....	28
2.7.2 Use Case Diagram.....	28
2.7.4 Simbol-Simbol UML	29
2.7.5 Keterkaitan UML dengan Penelitian	30
2.8 Enkripsi dan Dekripsi Dokumen dalam Sistem	31
2.8.1 Proses Enkripsi Dokumen	31
2.8.2 Proses Dekripsi Dokumen.....	32
2.9 Penelitian Terdahulu	33
2.10 Kerangka Pemikiran	36
BAB III ANALISA DAN PERANCANGAN SISTEM.....	39
3.1 Analisis Permasalahan	39
3.2 Analisis Kebutuhan Sistem	40
3.2.1 Kebutuhan Fungsional	41
3.2.2 Kebutuhan Non-Fungsional	41
3.3 Algoritma Sistem	42
3.3.1 Algoritma Enkripsi Dokumen	43
3.3.2 Algoritma Dekripsi Dokumen.....	44
3.3.3 Integrasi Algoritma dalam Sistem.....	45
3.3.4 Mekanisme Pengelolaan Kunci (<i>Key Management</i>)	45
3.3.5 <i>Flowchart</i> Sistem	46
3.4 Pemodelan dan Perancangan Sistem.....	48
3.4.1 Arsitektur Sistem.....	49
3.4.2 Use Case Diagram.....	50
3.4.3 <i>Activity</i> Diagram	52
BAB IV HASIL DAN PEMBAHASAN	55

4.1 Implementasi Sistem.....	55
4.1.1 Lingkungan Implementasi.....	56
4.1.2 Basis Data.....	56
4.2 Implementasi Algoritma AES-256.....	65
4.2.1 Proses Enkripsi.....	66
4.2.2 Proses Dekripsi.....	66
4.2.3 Pengelolaan Kunci.....	67
4.3 Pengujian Sistem	67
4.3.1 Metode Pengujian.....	68
4.3.2 Pengujian Login	69
4.3.3 Pengujian Upload	69
4.3.4 Pengujian Enkripsi	70
4.3.5 Pengujian Dekripsi	71
4.3.6 Pengujian Penghapusan Dokumen	72
BAB V KESIMPULAN DAN SARAN.....	73
5.1 Kesimpulan	73
5.2 Saran	74
DAFTAR PUSTAKA.....	76
LAMPIRAN.....	79

DAFTAR TABEL

Tabel 2.1 Perbandingan Algoritma Kriptografi	19
Tabel 2.2 Simbol Flowchart	26
Tabel 2.3 Simbol UML	30
Tabel 2.4 Penelitian Terdahulu	34
Tabel 4.1 Detail Environment	56
Tabel 4.2 Pengujian Login	69
Tabel 4.3 Pengujian Upload	69
Tabel 4.4 Pengujian Enkripsi	70
Tabel 4.5 Pengujian Dekripsi	71
Tabel 4.6 Pengujian Penghapusan Dokumen	72

DAFTAR GAMBAR

Gambar 2.1 CIA Triad Dalam Keamanan Informasi	8
Gambar 2.2 Proses Enkripsi dan Dekripsi.....	13
Gambar 2.3 Proses Enkripsi Algoritma AES-256	18
Gambar 2.4 Arsitektur Sistem Berbasis Web	22
Gambar 2.5 Proses Enkripsi Dokumen	32
Gambar 2.6 Proses Dekripsi Dokumen	33
Gambar 2.7 Kerangka Pemikiran	38
Gambar 3.1 Flowchart Sistem	47
Gambar 3.2 Arsitektur Sistem	49
Gambar 3.3 Use Case Diagram	51
Gambar 3.4 Activity Diagram	53
Gambar 4.1 Struktur Tabel Users	57
Gambar 4.2 Struktur Tabel Documents	58
Gambar 4.3 Tampilan Halaman Login	59
Gambar 4.4 Tampilan Halaman Dashboard	60
Gambar 4.5 Tampilan Halaman Upload	61
Gambar 4.6 Tampilan Modal Box Private Key	63
Gambar 4.7 Tampilan Modal Box Input Private Key Dekripsi	64

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang sangat cepat telah mendorong transisi dalam pengelolaan berkas dari format tradisional menjadi digital. Pemanfaatan dokumen digital memberikan berbagai manfaat, seperti penyimpanan yang lebih efisien, akses yang mudah, dan fleksibilitas dalam penyebaran data. Namun, manfaat tersebut juga menghadirkan tantangan baru dalam hal keamanan, terutama yang berkaitan dengan perlindungan kerahasiaan data sensitif (*Putra et al., 2024*).

Permasalahan utama yang diangkat dalam studi ini adalah masih terdapat banyak sistem penyimpanan dokumen digital yang tidak menerapkan metode perlindungan data yang efektif, terutama dalam hal enkripsi. Dokumen sering kali disimpan dalam bentuk asli, sehingga mudah terpapar pada berbagai risiko seperti akses ilegal, kebocoran informasi, dan perubahan data (Widodo dan Purnomo, 2020). Situasi ini menunjukkan adanya perbedaan antara tuntutan keamanan data dan implementasinya pada sistem yang tersedia saat ini.

Program Studi Sistem Informasi di Universitas Muhammadiyah Sumatera Utara (UMSU) bertanggung jawab atas pengelolaan berbagai jenis dokumen digital, termasuk rekaman administrasi akademik, komunikasi tertulis, informasi mahasiswa, dokumentasi acara, skripsi, serta dokumen penting lainnya. Dokumen-dokumen ini memiliki relevansi informasi yang tinggi sehingga memerlukan sistem penyimpanan yang dapat menjamin kerahasiaan, integritas, dan ketersediaan data. Dengan demikian, penerapan mekanisme keamanan dalam penyimpanan dokumen

dianggap sebagai faktor penting untuk memastikan bahwa pengelolaan dokumen dilakukan dengan aman dan teratur (*Kaaffah et al.*, 2025; NIST, 2023).

Untuk memperkuat perlindungan penyimpanan dokumen digital dalam program studi Sistem Informasi di Universitas Muhammadiyah Sumatera Utara (UMSU), diperlukan suatu sistem keamanan untuk menjaga dokumen dari akses yang tidak diinginkan. Salah satu strategi yang mungkin efektif adalah penerapan teknik kriptografi menggunakan algoritma Advanced Encryption Standard (AES-256), yang telah terbukti memberikan tingkat perlindungan yang tinggi dan banyak diterapkan dalam berbagai sistem keamanan informasi terkini (NIST, 2023).

Berangkat dari permasalahan tersebut, studi ini memiliki tujuan untuk merancang serta membangun sistem keamanan berbasis web yang dapat menyimpan dokumen digital dalam program studi Sistem Informasi di Universitas Muhammadiyah Sumatera Utara (UMSU) dengan menggunakan algoritma AES-256. Sistem ini dikembangkan untuk melindungi dokumen digital melalui proses enkripsi dan dekripsi, serta menjamin bahwa dokumen tersebut hanya dapat diakses oleh pengguna yang memiliki izin akses yang tepat.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah disampaikan, penelitian ini merumuskan beberapa permasalahan sebagai berikut:

1. Bagaimana merancang sistem keamanan penyimpanan dokumen digital berbasis web menggunakan algoritma AES-256 pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU)?
2. Bagaimana mengimplementasikan algoritma AES-256 pada proses enkripsi dan dekripsi dokumen digital dalam sistem keamanan penyimpanan

dokumen di Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU)?

3. Bagaimana menghasilkan sistem keamanan penyimpanan dokumen digital berbasis web yang mampu meningkatkan keamanan dokumen dari risiko akses tidak sah dan kebocoran data pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU)?

1.3 Batasan Masalah

Untuk menjaga agar penelitian tetap terarah dan sesuai dengan tujuan yang telah ditetapkan, ruang lingkup penelitian ini dibatasi pada hal-hal berikut:

1. Penelitian ini berfokus pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU) sebagai objek penelitian dalam penggunaan sistem keamanan untuk penyimpanan dokumen digital.
2. Sistem yang dibangun merupakan sistem keamanan penyimpanan dokumen digital berbasis web pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU).
3. Proses yang dibahas meliputi enkripsi dan dekripsi dokumen digital dalam sistem.
4. Jenis dokumen yang digunakan dalam penelitian ini dibatasi pada file dokumen digital tertentu (seperti PDF atau dokumen teks).
5. Sistem yang dibangun tidak membahas aspek keamanan jaringan secara mendalam, seperti serangan *hacking*, *penetration testing*, atau keamanan server tingkat lanjut.
6. Pengujian sistem difokuskan pada fungsi enkripsi, dekripsi, dan penyimpanan dokumen, bukan pada performa sistem secara keseluruhan.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang serta mengembangkan sistem keamanan berbasis web untuk penyimpanan dokumen digital dengan menerapkan algoritma AES-256 pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU).
2. Menerapkan algoritma AES-256 pada proses enkripsi dan dekripsi dokumen digital guna meningkatkan keamanan dalam penyimpanan dokumen pada Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU).
3. Menguji fungsionalitas sistem keamanan penyimpanan dokumen digital yang dibangun agar proses unggah (upload), enkripsi, penyimpanan, dekripsi, dan pengunduhan (download) dokumen dapat berjalan sesuai dengan kebutuhan pengguna di Program Studi Sistem Informasi Universitas Muhammadiyah Sumatera Utara (UMSU).

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan kontribusi, baik secara teoritis maupun praktis, sebagai berikut:

1. Manfaat Teoritis

Secara teoritis, studi ini memiliki tujuan untuk memberikan manfaat pada kemajuan ilmu pengetahuan dalam sektor teknologi informasi, terutama mengenai aspek perlindungan data dan kriptografi. Di samping itu,

penelitian ini mungkin berfungsi sebagai acuan bagi peneliti berikutnya yang berminat pada penggunaan algoritma *Advanced Encryption Standard (AES-256)* dalam sistem keamanan untuk dokumen digital (Surya et al., 2025).

2. Manfaat Praktis

a. Bagi Kampus

Penelitian ini diharapkan bisa berfungsi sebagai rujukan dan sumber informasi tambahan bagi pelajar serta komunitas akademik dalam mengembangkan penelitian selanjutnya dalam bidang keamanan informasi, terutama yang berkaitan dengan perlindungan dokumen digital.

b. Bagi Penulis

Khususnya terkait dengan pengembangan sistem berbasis web dan penerapan algoritma kriptografi AES-256, proyek penelitian ini dapat memperluas wawasan, pengetahuan, dan pengalaman penulis dalam menerapkan keterampilan yang mereka pelajari selama studi.

c. Bagi Masyarakat

Penelitian ini diharapkan dapat menghadirkan solusi untuk meningkatkan keamanan penyimpanan dokumen digital, sehingga masyarakat dapat menyimpan dan mengelola informasi penting dengan lebih aman.

BAB II

LANDASAN TEORI

2.1 Sistem Keamanan Informasi

Sistem keamanan informasi merupakan upaya yang dilakukan untuk menjaga data dan informasi dari berbagai ancaman yang dapat memengaruhi kerahasiaan, integritas, serta ketersediaan informasi (Kaaffah et al., 2025). Seiring dengan perkembangan era digital, kebutuhan terhadap keamanan informasi semakin meningkat karena teknologi terus berkembang dalam mendukung proses penyimpanan dan pengolahan data, terutama pada dokumen digital (Putra et al., 2024).

Keamanan informasi diperlukan untuk menjaga data agar tidak dapat diakses, diubah, maupun disalahgunakan oleh pihak yang tidak memiliki kewenangan (Permana et al., 2025). Berbagai ancaman dapat memengaruhi keamanan informasi, baik yang berasal dari serangan siber, kesalahan pengguna, maupun kelemahan dalam sistem yang digunakan (Reddy Penubadi et al., 2023). Dengan demikian, diperlukan sistem keamanan yang mampu memberikan perlindungan terhadap data secara menyeluruh.

Dalam keamanan informasi, terdapat tiga prinsip dasar yang dikenal sebagai CIA Triad, yaitu *Confidentiality*, *Integrity*, dan *Availability*. Ketiga prinsip tersebut menjadi dasar dalam pengembangan sistem keamanan informasi yang kuat serta memiliki keterkaitan satu sama lain (NIST, 2023).

2.1.1 Confidentiality (Kerahasiaan)

Confidentiality adalah prinsip yang menjamin informasi hanya dapat diakses oleh pihak yang memiliki kewenangan. Prinsip tersebut bertujuan

untuk melindungi data dan mencegah terjadinya akses dari pihak yang tidak mempunyai hak untuk mengaksesnya (Ridho & Ali Romli, 2024). Aspek *confidentiality* menjadi sangat penting dalam penyimpanan dokumen secara digital karena informasi yang tersimpan di dalamnya dapat berupa data yang bersifat sensitif dan rahasia (Indriyawati *et al.*, 2021).

Upaya untuk melindungi kerahasiaan data dapat dilakukan dengan memanfaatkan kriptografi, salah satunya melalui proses enkripsi data (Randy Fachrezi *et al.*, 2026). Penelitian ini menerapkan *Advanced Encryption Standard* (AES-256) sebagai metode pengamanan dokumen digital, sehingga akses terhadap dokumen hanya dapat dilakukan oleh pihak yang mempunyai kunci yang tepat (Baso & Anriani L, 2024).

2.1.2 Integrity (Keutuhan)

Integrity berkaitan dengan kondisi data yang tetap utuh dan terjaga dari perubahan maupun manipulasi tanpa izin. Penerapan prinsip ini memastikan bahwa informasi yang diterima pengguna tetap sesuai dengan data yang sebelumnya dikirimkan atau disimpan (Hayat Arka Putri *et al.*, 2025).

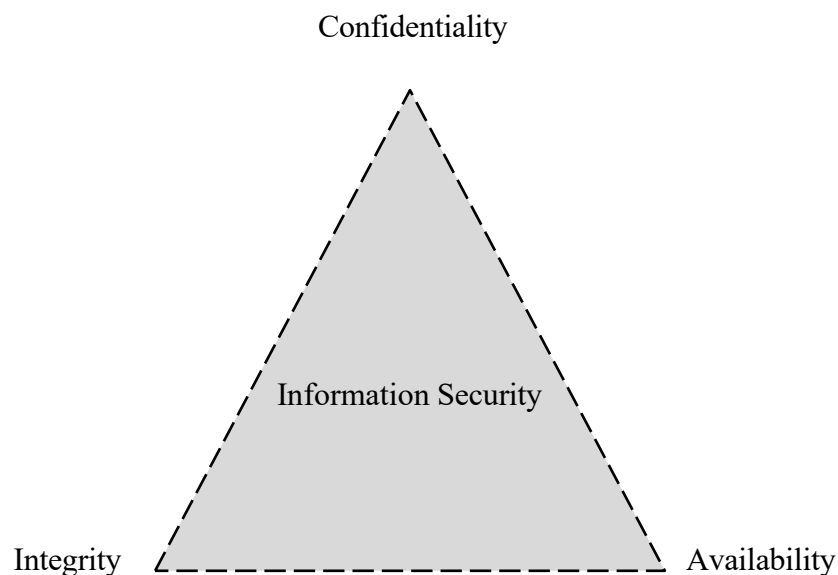
Dalam sistem penyimpanan dokumen digital, *integrity* sangat penting untuk menjaga keaslian dan keakuratan data. Perubahan data yang tidak sah dapat menyebabkan kesalahan informasi dan merugikan pengguna. Oleh karena itu, sistem keamanan harus mampu mendeteksi dan mencegah adanya perubahan data yang tidak diinginkan.

2.1.3 Availability (Ketersediaan)

Availability merujuk pada kemampuan suatu sistem dalam menjaga ketersediaan informasi agar tetap dapat digunakan oleh pihak yang memiliki

hak akses pada waktu yang diperlukan. Sistem yang baik harus mampu menyediakan akses yang cepat, stabil, dan berkelanjutan tanpa mengganggu aspek keamanan (Ayu Pramesthi Wardhani & Asriningtias, 2023).

Ketersediaan data sangat penting dalam mendukung aktivitas pengguna, terutama dalam sistem berbasis web yang mengandalkan akses secara *online* (Purba, 2025). Oleh karena itu, sistem harus dirancang agar tetap dapat diakses dengan baik meskipun terdapat gangguan atau beban penggunaan yang tinggi.



Gambar 2.1 CIA Triad Dalam Keamanan Informasi

Sumber: Diolah oleh penulis

Berdasarkan Gambar 2.1, terdapat tiga komponen utama dalam keamanan informasi, yaitu *confidentiality*, *integrity*, dan *availability* yang memiliki keterkaitan satu dengan lainnya. Ketiga komponen ini harus diterapkan secara seimbang agar sistem keamanan informasi dapat berjalan dengan optimal.

2.2 Dokumen Digital

Dokumen digital merupakan segala bentuk dokumen yang disimpan, dikelola, dan diproses dalam format elektronik menggunakan perangkat computer (*Indriyawati et al., 2021*). Dokumen ini dapat berupa tulisan, visual, rekaman suara, video, ataupun perpaduan beberapa jenis format. Penggunaan dokumen digital terus mengalami peningkatan sejalan dengan kemajuan teknologi informasi yang menyediakan kemudahan dalam penyimpanan serta penyebaran data dibandingkan dokumen konvensional (*Aditya & Romli, 2025*).

Dokumen digital memiliki berbagai keunggulan, di antaranya kemudahan dalam penyimpanan, pengolahan, pencarian, serta distribusi. Selain itu, dokumen digital juga memungkinkan integrasi dengan sistem informasi berbasis web yang dapat diakses oleh pengguna tanpa terbatas oleh waktu dan tempat. (*Naqiyah et al., 2025*). Hal ini menjadikan dokumen digital sebagai komponen penting dalam mendukung aktivitas organisasi maupun individu (*Kaaffah et al., 2025*).

Namun demikian, di balik keunggulan tersebut, dokumen digital juga memiliki berbagai risiko, terutama dalam aspek keamanan. Penggunaan dokumen digital dapat menghadapi berbagai ancaman, seperti akses tidak sah, pengambilan data tanpa izin, manipulasi informasi, serta kerusakan data akibat kesalahan sistem atau serangan siber (*Putra et al., 2024*). Risiko tersebut dapat berdampak pada hilangnya kerahasiaan, keutuhan, maupun ketersediaan data.

Oleh sebab itu, diperlukan sistem keamanan yang dapat melindungi berkas digital dari berbagai risiko yang ada. Salah satu cara yang mungkin dilakukan adalah dengan memanfaatkan metode kriptografi terutama, mengenkripsi berkas sebelum penyimpanannya (*Baso & Anriani L, 2024*). Proses enkripsi membuat

berkas yang disimpan tidak dapat dibaca tanpa kunci tertentu, sehingga memperkuat keamanan informasi (Irvai & Efranda, 2024).

2.2.1 Jenis-Jenis Dokumen Digital

Dokumen digital dapat diklasifikasikan berdasarkan jenis dan formatnya, yaitu sebagai berikut:

1. Dokumen Teks

Dokumen teks adalah jenis dokumen yang menyajikan informasi melalui tulisan dan dapat diubah maupun dibaca oleh pengguna. Contoh format dokumen teks antara lain *.txt*, *.doc*, dan *.pdf* yang banyak digunakan dalam penyimpanan data administrasi maupun akademik (Ayu Pramesthi Wardhani & Asriningtias, 2023).

2. Dokumen Gambar

Dokumen gambar merupakan dokumen dalam bentuk visual atau citra yang digunakan untuk menyimpan informasi berbasis grafis. Format yang umum digunakan antara lain *.jpg*, *.png*, dan *.bmp* (Naqiyah et al., 2025).

3. Dokumen Audio

Dokumen audio merupakan dokumen yang berisi rekaman suara yang biasanya digunakan untuk keperluan komunikasi maupun dokumentasi. Contoh formatnya adalah *.mp3* dan *.wav* (Surya et al., 2025).

4. Dokumen Video

Dokumen video merupakan dokumen dalam bentuk rekaman visual bergerak yang sering digunakan untuk dokumentasi multimedia. Format yang umum digunakan antara lain *.mp4* dan *.avi*.

2.2.2 Risiko Keamanan Dokumen Digital

Dokumen digital memiliki berbagai risiko keamanan yang perlu diperhatikan karena dapat mengancam kerahasiaan, keutuhan, dan ketersediaan data (Amanullah, 2025). Risiko-risiko tersebut dapat dipicu oleh berbagai faktor, baik dari dalam maupun luar sehingga diperlukan sistem pengamanan yang baik untuk meminimalkan dampaknya. Adapun beberapa risiko keamanan dokumen digital antara lain sebagai berikut:

1. Akses Tidak Sah

Akses tidak sah merupakan kondisi di mana dokumen digital dapat dibuka oleh individu yang tidak memiliki hak akses. Kondisi ini biasanya terjadi akibat lemahnya sistem autentikasi atau tidak adanya mekanisme pengamanan yang memadai (Binus University, 2024). Risiko ini dapat menyebabkan data rahasia terungkap kepada pihak yang tidak memiliki kewenangan.

2. Kebocoran Data

Kebocoran data terjadi ketika informasi penting tersebar tanpa sepengetahuan atau izin dari pemilik data. Hal ini dapat disebabkan oleh serangan siber, kesalahan pengguna, maupun kelemahan sistem. Dampak dari kebocoran data dapat merugikan individu maupun organisasi, terutama jika data yang bocor bersifat sensitive (Purba, 2025).

3. Manipulasi Data

Manipulasi data merupakan perubahan isi yang dilakukan tanpa persetujuan pihak yang memiliki kewenangan. Perubahan ini dapat menyebabkan informasi menjadi tidak akurat dan menyesatkan (Indriyawati *et al.*, 2021).

Untuk itu, keutuhan data perlu dipertahankan supaya tetap sesuai dengan kondisi aslinya.

4. Kehilangan Data

Kehilangan data merupakan kondisi di mana dokumen digital tidak dapat diakses atau hilang secara permanen. Hal ini dapat disebabkan oleh kerusakan sistem, kesalahan pengguna, maupun serangan seperti *malware*. Kehilangan data dapat mengakibatkan kerugian yang signifikan, terutama jika tidak terdapat sistem pencadangan (*backup*) (Putra et al., 2024).

2.3 Kriptografi

Kriptografi merupakan metode yang diterapkan untuk melindungi informasi dengan mengubah data ke dalam format yang tidak dapat dimengerti oleh orang-orang yang tidak memiliki izin (Aditya & Romli, 2025). Sasaran dari kriptografi adalah untuk menjaga kerahasiaan informasi, mencegah akses tanpa izin, serta memberikan perlindungan terhadap data dari berbagai potensi ancaman keamanan (Permana et al., 2025).

Dalam penerapannya, kriptografi memiliki peran penting dalam sistem keamanan informasi, khususnya dalam melindungi dokumen digital. Dengan menggunakan teknik kriptografi, data yang disimpan dalam sistem akan diproses ke dalam format terenkripsi sehingga hanya dapat dibaca dengan kunci tertentu (Ridho & Ali Romli, 2024).

2.3.1 Enkripsi

Enkripsi merupakan proses yang mengubah informasi asli menjadi data yang telah dienkripsi dengan menggunakan algoritma dan kunci spesifik (Irvai & Efranda, 2024). Tujuan dari enkripsi adalah untuk melindungi kerahasiaan

data agar informasi tersebut tidak dapat diakses oleh pihak yang tidak memiliki izin.

Dalam proses enkripsi, data yang semula dapat dibaca akan diubah menjadi bentuk acak yang sulit dipahami. Hasil dari proses ini disebut sebagai *ciphertext*, yang dapat diubah kembali ke bentuk aslinya menggunakan kunci yang tepat (Widodo & Purnomo, 2020).

$$C = E(P, K)$$

Keterangan:

$C = \text{Ciphertext}$

$P = \text{Plaintext}$

$K = \text{Key (kunci)}$



Gambar 2. 9 Proses Enkripsi dan Dekripsi

Sumber: Diolah oleh Penulis

Berdasarkan Gambar 2.2, proses kriptografi dimulai dari data asli (*plaintext*) yang akan melalui proses enkripsi dengan menggunakan suatu kunci (*key*), sehingga menghasilkan data yang telah tersandi (*ciphertext*). Selanjutnya, *ciphertext* tersebut dapat dipulihkan ke bentuk aslinya melalui proses dekripsi dengan kunci yang tepat (*Kaaffah et al., 2025*). Proses tersebut menjamin bahwa informasi hanya bisa dibaca oleh pihak yang memegang kunci, sehingga keamanan dan kerahasiaan informasi dapat terjaga.

2.3.2 Dekripsi

Dekripsi merupakan langkah yang berlawanan dengan enkripsi yaitu, mengubah kembali data yang telah terenskripsi (*ciphertext*) menjadi data

aslinya (*plaintext*) (Widodo & Purnomo, 2020). Langkah ini hanya dapat dilakukan jika pengguna memiliki kunci yang sama dengan yang digunakan pada saat proses enkripsi.

Dekripsi memungkinkan pengguna yang berwenang untuk mengakses kembali informasi yang telah diamankan, sehingga data tetap dapat digunakan tanpa mengurangi tingkat keamanannya (Amanullah, 2025).

$$P = D(C, K)$$

Keterangan:

$C = \text{Ciphertext}$

$P = \text{Plaintext}$

$K = \text{Key (kunci)}$

2.3.3 Jenis-Jenis Kriptografi

Kriptografi pada dasarnya terbagi ke dalam dua kategori utama, yaitu sebagai berikut:

1. Kriptografi Simetris

Kriptografi simetris adalah teknik kriptografi yang memakai kunci identik untuk proses enkripsi dan dekripsi (Widodo & Purnomo, 2020). Metode ini memiliki keunggulan dalam kecepatan proses, namun memiliki kelemahan dalam distribusi kunci. Salah satu algoritma yang termasuk dalam jenis ini adalah AES (NIST, 2023).

2. Kriptografi Asimetris

Kriptografi asimetris adalah teknik kriptografi yang menggunakan sepasang kunci berbeda, yaitu kunci publik (*public key*) dan kunci privat (*private key*) (Permana et al., 2025). Metode ini lebih aman dalam hal distribusi kunci,

namun memiliki proses yang lebih lambat dibandingkan kriptografi simetris.

2.4 Algoritma Advanced Encryption Standard (AES-256)

Algoritma *Advanced Encryption Standard* (AES) adalah jenis algoritma kriptografi simetris yang dimanfaatkan untuk melindungi data (Donald, 2023). AES ditentukan sebagai norma enkripsi oleh *National Institute of Standards and Technology* (NIST) dan diterapkan dalam berbagai sistem keamanan informasi karena tingkat keamanannya yang sangat baik serta efisiensinya dalam proses enkripsi dan dekripsi (NIST, 2023).

AES bekerja dengan memanfaatkan kunci yang sama dalam proses enkripsi maupun dekripsi. Algoritma ini memproses data dalam blok berukuran 128-bit dengan pilihan panjang kunci 128-bit, 192-bit, dan 256-bit (Ayu Pramesthi Wardhani & Asriningtias, 2024). Semakin panjang kunci yang diterapkan, semakin tinggi tingkat keamanan yang diperoleh.

2.4.1 AES-256

AES-256 merupakan salah satu varian algoritma AES dengan panjang kunci 256-bit. AES-256 memiliki tingkat keamanan yang sangat tinggi karena jumlah kemungkinan kombinasi kuncinya sangat banyak, sehingga lebih sulit dipecahkan melalui metode *brute force* (Surya et al., 2025).

Dalam AES-256, proses enkripsi dilakukan melalui 14 ronde (*round*) yang terdiri dari beberapa tahapan transformasi data. Setiap ronde bertujuan untuk meningkatkan kompleksitas hasil enkripsi sehingga data menjadi lebih aman (Putra et al., 2024).

2.4.2 Proses Kerja AES

Proses kerja algoritma *Advanced Encryption Standard* (AES) merupakan rangkaian transformasi yang dilakukan terhadap data untuk menghasilkan bentuk terenkripsi yang aman (Reddy Penubadi et al., 2023). Pada algoritma AES, data awal (*plaintext*) akan diubah menjadi bentuk matriks berukuran 4×4 *byte* yang disebut sebagai *state*. Selanjutnya, data tersebut akan diproses melalui beberapa tahapan transformasi secara berulang (*round*) hingga menghasilkan *ciphertext* (Indriyawati et al., 2021).

Pada AES-256, proses enkripsi dilakukan sebanyak 14 *round*. Setiap *round* bertujuan untuk meningkatkan tingkat kerumitan data sehingga sulit untuk dianalisis atau dipulihkan ke bentuk awal tanpa kunci yang tepat (Hayat Arka Putri et al., 2025). Sebelum memasuki *round* utama, terdapat proses awal yang disebut *initial round*, dan pada akhir proses terdapat *final round* yang sedikit berbeda dari *round* lainnya (Randy Fachrezi et al., 2026).

Adapun tahapan proses dalam algoritma AES adalah sebagai berikut:

1. *AddRoundKey*

Langkah ini menjadi proses awal dalam enkripsi, di mana *plaintext* dikombinasikan dengan kunci menggunakan operasi XOR. Tahapan ini bertujuan untuk menyisipkan elemen kunci ke dalam data sehingga data tidak lagi dalam bentuk aslinya sejak awal (NIST, 2023).

2. *SubBytes*

Pada tahap ini dilakukan penggantian setiap *byte* pada data melalui tabel substitusi yang dikenal sebagai S-Box. Tujuan dari tahap ini adalah

meningkatkan karakteristik *non-linear* pada data agar lebih sulit untuk dianalisis (*Permana et al., 2025*).

3. *ShiftRows*

Tahap ini merupakan proses penggeseran baris dalam matriks *state*. Masing-masing baris digeser dengan jumlah tertentu, sehingga susunan data mengalami perubahan. Proses ini bertujuan untuk menyebarkan pola data agar tidak mudah dikenali (*Randy Fachrezi et al., 2026*).

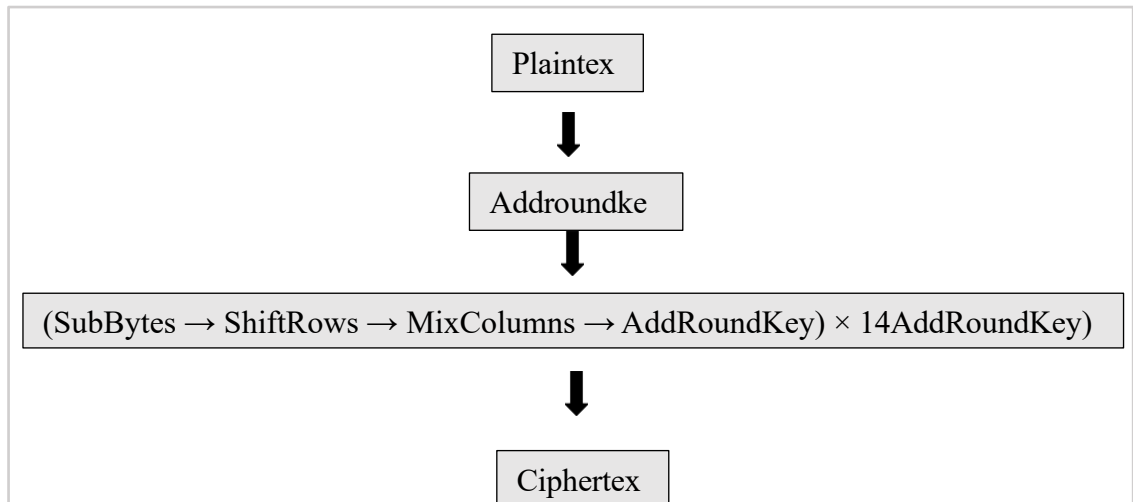
4. *MixColumns*

Pada tahap ini dilakukan operasi matematika pada setiap kolom dalam matriks *state*. Proses ini mencampurkan data antar kolom sehingga meningkatkan difusi, yaitu penyebaran perubahan data ke seluruh bagian.

5. *AddRoundKey*

Tahap ini kembali menggabungkan data dengan kunci menggunakan operasi XOR pada setiap *round*. Hal ini bertujuan untuk memastikan bahwa setiap tahap enkripsi bergantung pada kunci yang digunakan (*Kaaffah et al., 2025*).

Proses *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* akan diulang sebanyak 14 *round* pada AES-256. Namun, pada *round* terakhir (*final round*), proses *MixColumns* tidak dilakukan (*Donald, 2023*). Hal ini dilakukan untuk menghasilkan bentuk akhir *ciphertext* yang optimal. Proses tersebut dapat digambarkan secara sederhana seperti yang ditunjukkan pada Gambar 2.3.



Gambar 2. 14 Proses Enkripsi Algoritma AES-256

Sumber: Diolah oleh penulis

Berdasarkan Gambar 2.3, proses enkripsi AES dilakukan melalui beberapa tahapan yang berulang hingga menghasilkan *ciphertext* yang aman. Setiap tahapan transformasi yang dilakukan secara berulang tersebut meningkatkan kompleksitas data, sehingga algoritma AES mampu menghasilkan data terenkripsi dengan tingkat keamanan yang tinggi dan sulit untuk dipecahkan tanpa menggunakan kunci yang sesuai (Widodo & Purnomo, 2020).

2.4.3 Perbandingan Algoritma Kriptografi

Dalam pemilihan algoritma kriptografi, diperlukan pertimbangan terhadap tingkat keamanan, panjang kunci, serta efektivitas proses enkripsi dan dekripsi (Baso & Anriani L, 2024). Algoritma kriptografi yang sering diterapkan meliputi *Data Encryption Standard (DES)*, *Triple Data Encryption Standard (3DES)*, dan *Advanced Encryption Standard (AES)*.

DES merupakan algoritma kriptografi simetris dengan panjang kunci 56-bit. Meskipun pada masanya cukup populer, namun saat ini DES dianggap

kurang aman karena panjang kunci yang pendek sehingga rentan terhadap serangan *brute force*. Selanjutnya, 3DES dikembangkan sebagai peningkatan dari DES dengan menggunakan tiga kali proses enkripsi, sehingga memberikan tingkat keamanan yang lebih tinggi dibandingkan DES, namun prosesnya menjadi lebih lambat.

AES merupakan algoritma kriptografi yang dikembangkan dengan teknologi lebih baru dan memiliki keamanan yang lebih kuat dibandingkan DES dan 3DES (Ridho & Ali Romli, 2024). Algoritma ini tersedia dalam tiga pilihan panjang kunci, yaitu 128-bit, 192-bit, dan 256-bit. Dari ketiga pilihan tersebut, AES-256 menawarkan keamanan paling tinggi karena menggunakan ukuran kunci terbesar.

Berikut merupakan perbandingan beberapa algoritma kriptografi:

Tabel 2.1 Perbandingan Algoritma Kriptografi

Algoritma	Tipe	Panjang Kunci	Tingkat Keamanan	Keterangan
DES	Simetris	56-bit	Rendah	Mudah dipecahkan dengan <i>brute force</i>
3DES	Simetris	168-bit	Sedang	Lebih aman dari DES, namun lambat
AES-128	Simetris	128-bit	Tinggi	Cepat dan cukup aman
AES-256	Simetris	256-bit	Sangat Tinggi	Digunakan pada sistem keamanan modern

Mengacu pada Tabel 2.1, terlihat bahwa algoritma AES, khususnya AES-256, memiliki tingkat keamanan lebih tinggi daripada algoritma lainnya. Keunggulan tersebut dipengaruhi oleh ukuran kunci yang lebih besar dan struktur algoritma yang lebih kompleks. Oleh karena itu, AES-256 dipilih

dalam penelitian ini sebagai metode untuk mengamankan dokumen digital (NIST, 2023).

2.4.4 Kelebihan AES-256

Algoritma *Advanced Encryption Standard (AES-256)* memiliki berbagai keunggulan yang menjadikannya sebagai salah satu pilihan algoritma kriptografi yang banyak diterapkan pada sistem keamanan informasi.

Keunggulan-keunggulan tersebut antara lain sebagai berikut:

1. Tingkat Keamanan yang Sangat Tinggi

AES-256 menggunakan panjang kunci sebesar 256-bit, sehingga memiliki jumlah kemungkinan kombinasi kunci yang sangat besar. Hal ini membuat algoritma ini sangat sulit untuk dipecahkan menggunakan metode *brute force* (Donald, 2023).

2. Tahan terhadap Berbagai Jenis Serangan

Struktur algoritma AES yang kompleks, dengan beberapa tahapan transformasi dalam setiap ronde, menjadikannya lebih kuat dalam menghadapi berbagai jenis serangan kriptografi, termasuk serangan diferensial maupun linear.

3. Efisiensi dalam Proses Enkripsi dan Dekripsi

Meskipun memiliki tingkat keamanan yang kuat, AES-256 tetap memiliki performa yang cukup baik dalam proses enkripsi dan dekripsi, sehingga dapat diterapkan pada berbagai sistem, termasuk sistem berbasis web (Widodo & Purnomo, 2020).

4. Standar Internasional

AES telah ditetapkan sebagai standar enkripsi oleh lembaga internasional, sehingga telah banyak digunakan dalam berbagai aplikasi keamanan data di seluruh dunia (Binus University, 2024) .

5. Fleksibel dalam Implementasi

AES-256 dapat diimplementasikan pada berbagai *platform*, baik itu aplikasi desktop, *mobile*, maupun web, sehingga memudahkan dalam pengembangan sistem keamanan yang terintegrasi.

Berdasarkan berbagai keunggulan tersebut, algoritma AES-256 dipilih dalam penelitian ini sebagai metode utama dalam mengamankan penyimpanan dokumen digital (Purba, 2025). Dengan tingkat keamanan yang tinggi serta efisiensi dalam implementasi, diharapkan sistem yang dibangun mampu memberikan perlindungan data yang optimal.

2.5 Sistem Berbasis Web

Sistem berbasis web merupakan suatu sistem informasi yang dapat dijalankan melalui koneksi internet menggunakan peramban (*browser*). Sistem ini memungkinkan pengguna mengoperasikan aplikasi secara langsung melalui perangkat tanpa melakukan proses pemasangan, sehingga penggunaannya menjadi lebih praktis dan mudah didistribusikan.

Perkembangan teknologi web telah memungkinkan berbagai layanan dapat diakses secara *online*, termasuk dalam pengelolaan dan penyimpanan dokumen digital. Sistem berbasis web menawarkan fleksibilitas dalam penggunaannya karena memungkinkan akses dari berbagai waktu dan lokasi selama tersedia koneksi internet. Kemudahan tersebut membuat sistem berbasis web

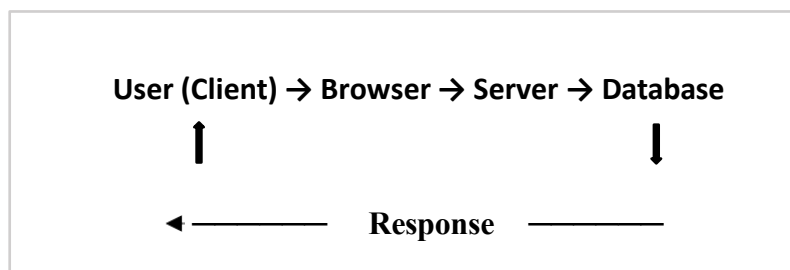
menjadi alternatif yang efektif untuk menunjang pengelolaan data sesuai dengan kebutuhan saat ini (Putra et al., 2024).

Dalam konteks keamanan, sistem berbasis web juga memiliki tantangan tersendiri, seperti ancaman akses tidak sah, pencurian data, serta serangan siber lainnya. Oleh karena itu, diperlukan penerapan mekanisme keamanan yang tepat, salah satunya dengan mengintegrasikan teknik kriptografi seperti algoritma AES-256 untuk melindungi informasi yang tersimpan pada sistem.

2.5.1 Arsitektur Sistem Berbasis Web

Sistem berbasis web umumnya menggunakan arsitektur *client-server*, di mana terdapat dua bagian utama yaitu *client* dan *server*. *Client* merupakan perangkat pengguna yang berfungsi untuk membuka dan menggunakan sistem melalui *browser*, sedangkan *server* merupakan tempat penyimpanan data dan pengolahan system (Reddy Penubadi et al., 2023).

Dalam arsitektur ini, pengguna (*client*) akan mengajukan permintaan (*request*) ke *server*, kemudian *server* akan memproses permintaan tersebut dan memberikan hasilnya kembali dalam bentuk *response*. Proses ini berlangsung secara terus-menerus selama sistem digunakan.



Gambar 2.22 Arsitektur Sistem Berbasis Web

Sumber: Diolah oleh Penulis

Berdasarkan Gambar 2.4, pengguna mengakses sistem melalui *browser* yang berperan sebagai *client*, kemudian permintaan dikirimkan ke *server* untuk diproses (*Surya et al., 2025*). Selanjutnya, *server* akan berinteraksi dengan database untuk mengelola data, kemudian hasilnya dikembalikan kepada pengguna dalam bentuk *response*.

2.5.2 Kelebihan Sistem Berbasis Web

Sistem berbasis web memiliki beberapa keunggulan yang menjadikannya banyak digunakan dalam pengembangan sistem informasi modern, antara lain sebagai berikut:

1. Aksesibilitas Tinggi

Sistem berbasis web memungkinkan akses dari berbagai tempat dan waktu selama tersedia koneksi internet. Hal ini memberikan kemudahan bagi pengguna dalam melakukan pengelolaan data tanpa terikat oleh batasan lokasi maupun waktu.

2. Tidak Memerlukan Instalasi

Pengguna tidak perlu menginstal aplikasi tambahan pada perangkat karena sistem dapat dijalankan langsung melalui browser. Hal ini mengurangi penggunaan ruang penyimpanan serta memudahkan distribusi sistem kepada pengguna.

3. Mudah dalam Pemeliharaan

Pemeliharaan dan pembaruan sistem dapat dilakukan secara terpusat melalui server, sehingga pengguna dapat langsung menggunakan versi terbaru tanpa harus memperbaruinya secara manual.

4. Fleksibel dan Skalabel

Sistem berbasis web dapat dikembangkan dan disesuaikan dengan kebutuhan pengguna. Selain itu, sistem juga dapat menangani peningkatan jumlah pengguna tanpa memerlukan perubahan besar pada sisi *client*.

5. Kemudahan Integrasi

Sistem berbasis web dapat dengan mudah diintegrasikan dengan berbagai layanan lain, seperti *database*, API, maupun sistem keamanan tambahan seperti kriptografi, sehingga mendukung pengembangan sistem yang lebih kompleks.

2.5.3 Keterkaitan dengan Penelitian

Dalam penelitian ini, sistem keamanan penyimpanan dokumen digital dibangun menggunakan *platform* berbasis web. Pemilihan sistem berbasis web didasarkan pada kemudahan akses yang diberikan kepada pengguna, sehingga dokumen dapat dikelola secara fleksibel tanpa terbatas oleh lokasi dan waktu (Ridho & Ali Romli, 2024).

Sistem yang dibangun memungkinkan pengguna untuk melakukan proses unggah (*upload*), penyimpanan, serta pengambilan dokumen secara *online*. Dalam proses tersebut, aspek keamanan menjadi aspek yang sangat penting untuk diperhatikan, mengingat dokumen yang disimpan dapat bersifat sensitif dan rahasia.

Untuk mengatasi permasalahan tersebut, sistem ini mengintegrasikan algoritma *Advanced Encryption Standard (AES-256)* sebagai metode utama dalam mengamankan dokumen digital (Kaaffah et al., 2025). Setiap dokumen yang diunggah akan dienkrpsi terlebih dahulu sebelum tersimpan pada server,

sehingga informasi yang tersimpan berada dalam bentuk *ciphertext*. Selanjutnya, ketika pengguna ingin mengakses kembali dokumen tersebut, sistem akan melakukan dekripsi dengan kunci yang tepat.

Selain itu, sistem ini juga dirancang untuk memastikan pengelolaan dokumen hanya dapat dilakukan oleh pengguna yang memiliki kewenangan (Ayu Pramesthi Wardhani & Asriningtias, 2024). Dengan demikian, sistem berbasis web yang dibangun tidak hanya memudahkan proses pengelolaan dokumen, tetapi juga memberikan perlindungan terhadap keamanan data melalui penerapan algoritma AES-256.

2.6 Flowchart

Flowchart adalah gambaran visual yang berfungsi untuk menjelaskan tahapan proses atau langkah kerja suatu sistem dengan cara sistematis melalui simbol-simbol tertentu. *Flowchart* berfungsi untuk mempermudah pemahaman terhadap proses yang berlangsung dalam sistem, mulai dari input, proses, hingga output yang dihasilkan (Rosa & Shalahuddin, 2018). Dalam pengembangan sistem informasi, *flowchart* dimanfaatkan sebagai sarana dalam menganalisis dan merancang sistem sehingga alur proses dapat disajikan secara jelas dan terstruktur. Dengan adanya *flowchart*, pengembang sistem dapat memahami urutan proses yang terjadi sehingga memudahkan dalam tahap implementasi program.

Flowchart juga membantu dalam mengidentifikasi proses, pengambilan keputusan, serta hubungan antar aktivitas dalam sistem. Selain itu, *flowchart* dapat digunakan sebagai dokumentasi sistem yang mempermudah proses pengembangan maupun pemeliharaan sistem di kemudian hari.

Dalam penelitian ini, *flowchart* dimanfaatkan untuk menjelaskan tahapan alur kerja sistem keamanan penyimpanan dokumen digital berbasis web yang menerapkan algoritma AES-256. *Flowchart* menggambarkan tahapan mulai dari proses login pengguna, unggah dokumen, proses enkripsi, penyimpanan data ke database, hingga proses dekripsi dokumen saat diakses kembali oleh pengguna.

2.6.1 Fungsi *Flowchart*

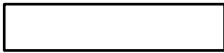
Flowchart memiliki beberapa fungsi penting dalam pengembangan sistem informasi, antara lain:

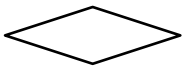
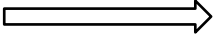
1. Mempermudah dalam memahami alur proses sistem.
2. Membantu proses analisis dan perancangan sistem secara terstruktur.
3. Menjelaskan urutan proses dan pengambilan keputusan dalam sistem.
4. Memudahkan pengembang dalam proses implementasi program.
5. Menjadi dokumentasi sistem yang dapat digunakan untuk pengembangan selanjutnya.

2.6.2 Simbol-Simbol *Flowchart*

Dalam penyusunan *flowchart*, terdapat berbagai simbol yang digunakan untuk merepresentasikan tahapan proses dalam sistem, yaitu sebagai berikut:

Tabel 2.2 Simbol *Flowchart*

No.	Simbol	Nama Simbol	Fungsi
1.		Terminal	Menunjukkan awal dan akhir proses
2.		Proses	Menunjukkan proses pengolahan data

No.	Simbol	Nama Simbol	Fungsi
3.		Keputusan (<i>Decision</i>)	Menunjukkan proses pengambilan keputusan
4.		Input/Output	Menunjukkan proses masukan atau keluaran data
5.		Garis Alur	Menunjukkan arah alur proses

Berdasarkan tabel simbol *flowchart* di atas, simbol-simbol tersebut digunakan untuk menggambarkan alur proses sistem keamanan penyimpanan dokumen digital berbasis web secara terstruktur dan mudah dipahami.

2.7 UML (Unified Modeling Language)

Unified Modeling Language (UML) merupakan bahasa pemodelan berbasis visual yang digunakan untuk merancang, memvisualisasikan, serta mendokumentasikan sistem perangkat lunak secara sistematis. UML berperan sebagai sarana pendukung dalam analisis dan perancangan sistem sehingga kebutuhan sistem dapat dipahami oleh pengembang dengan lebih mudah dan terstruktur (Rosa & Shalahuddin, 2018).

Dalam pengembangan sistem informasi, UML memiliki peran penting untuk memvisualisasikan proses, alur kerja, dan hubungan pengguna terhadap sistem. Penggunaan UML membantu memperjelas proses perancangan sistem, sehingga tahap implementasi dan pengembangan dapat dilakukan dengan lebih mudah.

UML mencakup berbagai diagram yang dapat dipilih berdasarkan kebutuhan dalam pengembangan sistem. Pada penelitian ini, diagram UML yang digunakan adalah *Use Case Diagram* dan *Activity Diagram* untuk menunjukkan

hubungan antara pengguna dengan sistem serta proses kegiatan yang berlangsung pada sistem keamanan penyimpanan dokumen digital berbasis web.

2.7.1 Fungsi UML

Unified Modeling Language (UML) memiliki beberapa fungsi dalam pengembangan sistem informasi, antara lain:

1. Mempermudah proses analisis dan perancangan sistem.
2. Menggambarkan alur kerja sistem secara visual.
3. Membantu pengembang memahami kebutuhan pengguna.
4. Menjadi dokumentasi sistem dalam proses pengembangan perangkat lunak.
5. Mempermudah komunikasi antara pengembang dan pengguna sistem.

2.7.2 Use Case Diagram

Use Case Diagram merupakan diagram UML yang berfungsi untuk menunjukkan interaksi antara aktor dan sistem. Diagram ini menampilkan berbagai fungsi utama dalam sistem beserta aktivitas yang dapat dilakukan oleh pengguna (Sukamto & Shalahuddin, 2018).

Dalam Use Case Diagram terdapat beberapa komponen utama, yaitu:

1. Aktor (Actor) merupakan pihak yang berperan dalam melakukan interaksi dengan sistem.
2. Use Case merupakan fitur atau layanan yang tersedia pada sistem.
3. Relationship merupakan bentuk keterkaitan antara aktor dan use case dalam sistem.

Dalam penelitian ini, Use Case Diagram berfungsi untuk menunjukkan hubungan pengguna dalam berinteraksi dengan sistem keamanan penyimpanan

dokumen digital berbasis web, seperti proses login, upload dokumen, enkripsi, dekripsi, dan penyimpanan data.

2.7.3 Activity Diagram

Activity Diagram merupakan diagram UML yang berfungsi untuk menunjukkan rangkaian aktivitas dalam sistem secara berurutan dari tahap awal sampai proses berakhir.

Diagram ini menampilkan rangkaian kegiatan, tahapan penentuan keputusan, serta keterkaitan antarproses dalam sistem. Activity Diagram digunakan untuk mempermudah dalam memahami proses bisnis maupun alur kerja sistem dengan susunan yang sistematis.

Dalam penelitian ini, Activity Diagram berfungsi untuk menjelaskan tahapan kerja dalam sistem keamanan dokumen digital mulai dari proses login pengguna, unggah dokumen, proses enkripsi AES-256, penyimpanan data, hingga proses dekripsi dokumen saat diakses kembali.

2.7.4 Simbol-Simbol UML

Dalam pembuatan diagram UML, terdapat beberapa simbol yang digunakan untuk menunjukkan proses, aktor, aktivitas, serta hubungan antar komponen dalam sistem. Simbol-simbol tersebut membantu dalam memvisualisasikan sistem agar lebih mudah dipahami dan dianalisis. Berbagai simbol UML yang digunakan pada penelitian ini ditampilkan dalam tabel berikut.

Tabel 2.3 Simbol UML

No.	Simbol	Nama Simbol	Fungsi
1.		Aktor	Menggambarkan pengguna yang berinteraksi dengan sistem
2.		Use Case	Menggambarkan fungsi atau layanan yang disediakan oleh sistem
3.		Association	Menggambarkan keterkaitan antara aktor dengan use case
4.		Activity	Menggambarkan aktivitas dalam sistem
5.		Decision	Menggambarkan percabangan keputusan
6.		Initial Node	Menggambarkan awal proses
7.		Final Node	Menggambarkan akhir proses

Berdasarkan tabel simbol UML di atas, simbol-simbol tersebut digunakan untuk menunjukkan hubungan pengguna terhadap sistem serta tahapan proses aktivitas keamanan penyimpanan dokumen digital berbasis web secara terstruktur dan mudah dipahami.

2.7.5 Keterkaitan UML dengan Penelitian

Dalam penelitian ini, UML dimanfaatkan sebagai media pemodelan untuk menggambarkan proses dan interaksi pada sistem keamanan penyimpanan dokumen digital berbasis web. Penggunaan UML membantu memperjelas gambaran sistem.

Use Case Diagram menunjukkan hubungan pengguna dengan fitur sistem, sedangkan Activity Diagram menggambarkan alur proses sistem.

Dengan demikian, perancangan sistem menjadi lebih terarah dan mudah dipahami.

2.8 Enkripsi dan Dekripsi Dokumen dalam Sistem

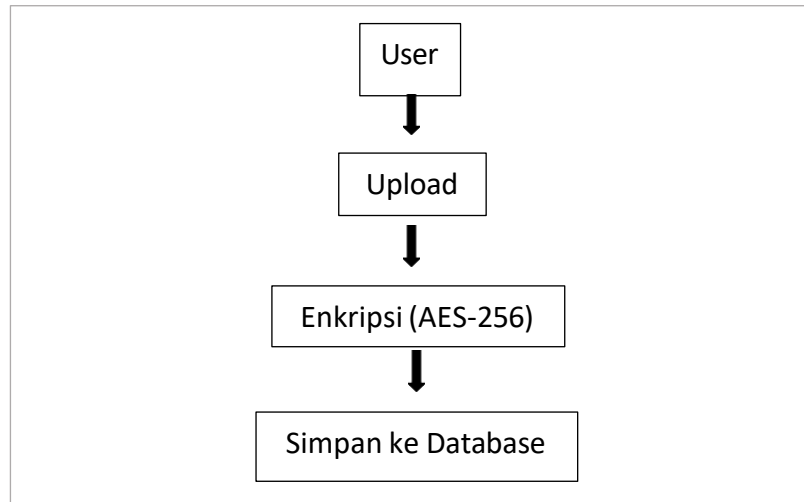
Enkripsi dan dekripsi dokumen dalam sistem merupakan proses utama yang digunakan untuk menjaga keamanan data yang disimpan. Dalam sistem yang dibangun, setiap dokumen digital yang diunggah pengguna akan diproses melalui enkripsi terlebih dahulu menggunakan algoritma *Advanced Encryption Standard* (AES-256) sebelum disimpan dalam sistem (Irvai & Efranda, 2024).

Proses ini dilakukan untuk mencegah akses tanpa izin, sehingga meskipun data diperoleh pihak lain, isi dokumen tidak dapat dibaca tanpa kunci yang tepat. Dengan demikian, keamanan data tetap terjaga terutama dalam sistem berbasis web yang rentan terhadap berbagai ancaman keamanan.

2.8.1 Proses Enkripsi Dokumen

Proses enkripsi dokumen dimulai ketika pengguna melakukan unggah (*upload*) dokumen ke dalam sistem. Dokumen yang diunggah akan dienkripsi dengan algoritma AES-256 dengan menggunakan kunci tertentu yang telah ditentukan oleh system (Ridho & Ali Romli, 2024).

Setelah melalui proses enkripsi, dokumen diubah menjadi *ciphertext* yang tidak dapat dibaca, kemudian disimpan pada database atau media penyimpanan di server. Dengan cara ini, data yang tersimpan tidak lagi dalam bentuk asli sehingga lebih aman dari risiko pencurian atau kebocoran data.



Gambar 2.23 Proses Enkripsi Dokumen

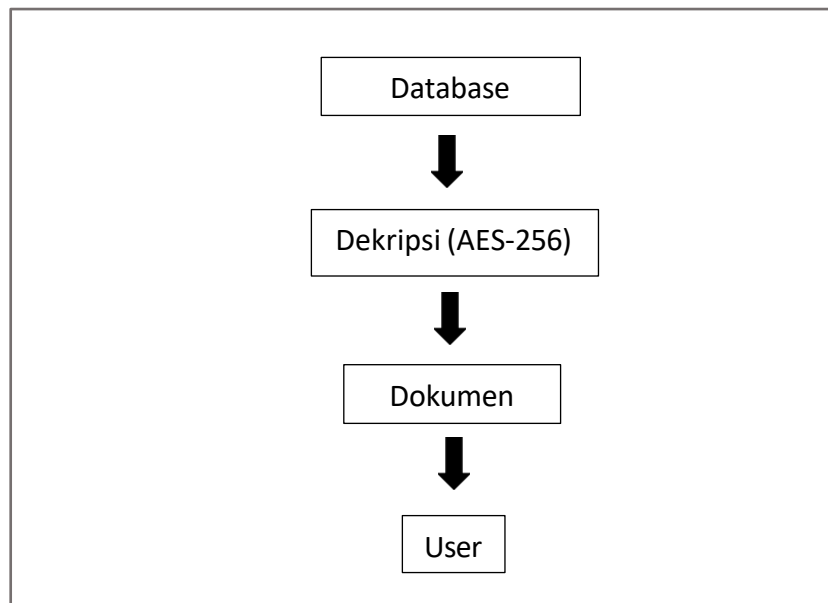
Sumber: Diolah oleh Penulis

Mengacu pada Gambar 2.5, dokumen yang diunggah pengguna akan dienkripsi terlebih dahulu sebelum tersimpan dalam database, sehingga data yang tersimpan berada dalam bentuk terenkripsi dan lebih aman.

2.8.2 Proses Dekripsi Dokumen

Proses dekripsi dokumen dilakukan saat pengguna hendak membuka kembali dokumen yang tersimpan. Sistem akan mengambil dokumen dalam bentuk *ciphertext* dari database, kemudian melakukan proses dekripsi menggunakan kunci yang sesuai (Surya et al., 2025).

Setelah proses dekripsi selesai, dokumen akan dikembalikan ke bentuk aslinya (*plaintext*) sehingga dapat dibaca atau digunakan oleh pengguna. Proses ini memastikan isi dokumen hanya dapat dilihat oleh pengguna yang memiliki hak akses.



Gambar 2.6 Proses Dekripsi Dokumen

Sumber: Diolah oleh Penulis

Berdasarkan Gambar 2.6, dokumen yang tersimpan dalam bentuk *ciphertext* akan melalui proses dekripsi sebelum ditampilkan kepada pengguna, sehingga hanya data yang telah diproses yang dapat diakses dalam bentuk aslinya (Permana et al., 2025).

2.9 Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai acuan untuk melihat perkembangan penelitian yang telah dilakukan sebelumnya serta sebagai dasar dalam mendukung penelitian yang dilakukan. Dengan adanya penelitian terdahulu, penulis dapat membandingkan metode yang digunakan serta mengidentifikasi kelebihan dan kekurangan dari penelitian sebelumnya.

Hasil kajian penelitian terdahulu menunjukkan bahwa sebagian besar penelitian telah berhasil mengimplementasikan algoritma AES-256 dalam

pengamanan dokumen digital. Namun, kajian tersebut masih menunjukkan adanya beberapa keterbatasan, di antaranya:

1. Sebagian penelitian hanya berfokus pada proses enkripsi tanpa membahas integrasi sistem secara menyeluruh berbasis web.
2. Belum banyak penelitian yang mengukur efektivitas sistem dari sisi keamanan secara sistematis.
3. Beberapa penelitian belum membahas pengelolaan kunci (key management) sebagai aspek penting dalam keamanan sistem.

Atas dasar tersebut, penelitian ini diarahkan pada pengembangan sistem keamanan dokumen digital berbasis web yang tidak hanya mengimplementasikan AES-256, tetapi juga mengintegrasikan proses enkripsi-dekripsi dalam sistem serta mengevaluasi tingkat keberhasilannya.

Tabel 2.4 Penelitian Terdahulu

No.	Peneliti	Tahun	Judul penelitian	Metode	Hasil	Research Gap
1.	Randy Fachrezi dkk	2026	Sistem Enkripsi Data Sensitif Berbasis Web	AES-256-CBC	Data terenkripsi dengan baik	Tidak membahas evaluasi performa sistem
2.	Naqiyah dkk	2025	Implementasi AES-256 Berbasis Web untuk Pengamanan Dokumen Digital	AES-256	Sistem aman	Tidak membahas evaluasi keamanan secara detail
3.	Kaaffah dkk	2025	Enkripsi Dokumen Digital dengan AES dan SHA-256	AES + SHA-256	Keamanan meningkat	Tidak fokus pada sistem penyimpanan dokumen

No.	Peneliti	Tahun	Judul penelitian	Metode	Hasil	Research Gap
4.	Irvai & Efranda	2024	Optimalisasi Enkripsi File Menggunakan Algoritma AES-256 Berbasis Web dengan Integrasi Kompresi Adaptif	AES-256	Efisien & aman	Fokus pada optimasi, bukan sistem keamanan menyeluruh
5.	Ridho & Romli	2024	Sistem Pengamanan Dokumen Menggunakan AES-256	AES-256	Dokumen lebih aman	Tidak berbasis web
6.	Dewi Anggraini	2024	Sistem Keamanan Data Berbasis Web	AES-256	Sistem berjalan dengan baik	Tidak membahas key management
7.	Putra dkk	2024	Tinjauan Implementasi AES-256 dalam Keamanan Data	AES-256	Analisis keamanan AES	Tidak ada implementasi sistem nyata
8.	Baso & Natalia	2023	Implementasi Kriptografi AES-256 untuk Keamanan File	AES-256	Data terlindungi	Tidak ada integrasi sistem
9.	Reddy Penubadi dkk	2023	Framework Keamanan Dokumen Digital	Encryption + Signature	Sistem komprehensif	Kompleks dan tidak spesifik ke AES-256
10.	Widodo & Purnomo	2020	Implementasi AES pada Enkripsi Dokumen Rahasia	AES-256	Data aman	Sistem sederhana dan tidak berbasis web

Hasil tinjauan pada tabel penelitian terdahulu menunjukkan bahwa algoritma AES-256 telah banyak diterapkan dalam pengamanan dokumen digital

karena tingkat keamanannya yang tinggi. Meskipun demikian, sejumlah penelitian masih menunjukkan beberapa keterbatasan, seperti belum adanya integrasi sistem berbasis web secara menyeluruh, kurangnya pembahasan mengenai pengelolaan kunci (key management), serta belum adanya evaluasi terhadap tingkat keamanan sistem yang dibangun. Dengan demikian, penelitian ini diarahkan untuk mengatasi keterbatasan tersebut dengan membangun sistem keamanan penyimpanan dokumen digital berbasis web yang terintegrasi serta melakukan evaluasi terhadap keamanan sistem.

2.10 Kerangka Pemikiran

Kerangka pemikiran merupakan gambaran alur penelitian yang menjelaskan hubungan antara permasalahan, solusi yang diusulkan, serta hasil yang diharapkan. Pada penelitian ini, permasalahan yang menjadi perhatian utama berkaitan dengan rendahnya tingkat keamanan dalam penyimpanan dokumen digital, sehingga berpotensi menimbulkan risiko seperti akses tidak sah, kebocoran data, dan manipulasi informasi (Reddy Penubadi et al., 2023).

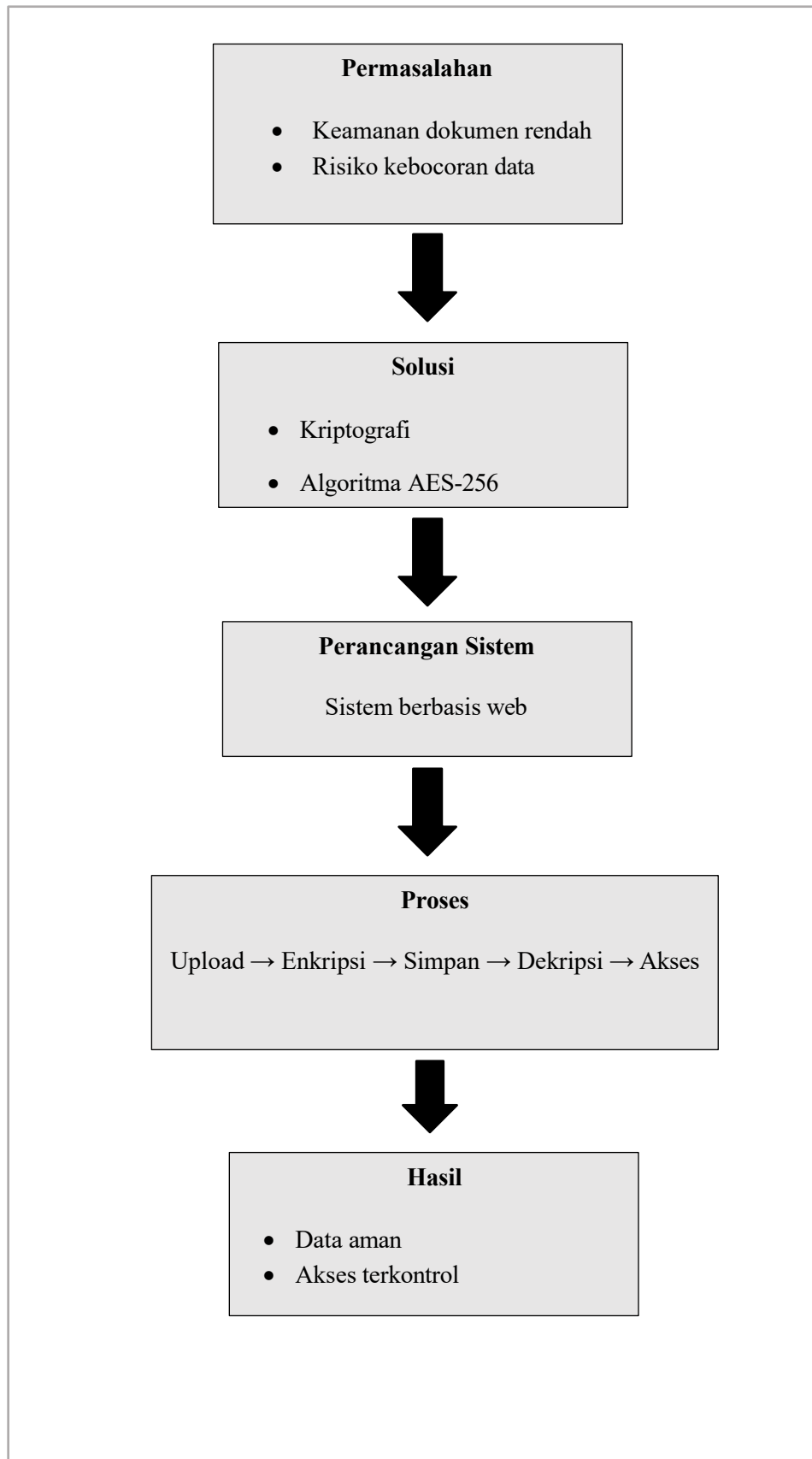
Sebagai solusi atas kondisi tersebut, dibutuhkan sistem keamanan yang dapat memberikan perlindungan terhadap dokumen digital secara efektif. Salah satu upaya yang dapat dilakukan yaitu dengan menerapkan teknik kriptografi, yaitu dengan mengimplementasikan algoritma *Advanced Encryption Standard (AES-256)* sebagai metode enkripsi data (Randy Fachrezi et al., 2026).

Sistem yang dikembangkan pada penelitian ini menggunakan platform berbasis web, sehingga pengguna dapat dengan mudah mengakses dan mengelola dokumen secara online. Dalam sistem tersebut, setiap dokumen yang diunggah akan melalui proses enkripsi sebelum disimpan ke dalam database, sehingga data

tersimpan dalam bentuk *ciphertext* (Baso & Anriani L, 2024). Selanjutnya, dokumen hanya dapat diakses kembali melalui proses dekripsi dengan memanfaatkan kunci yang tepat.

Dengan penerapan sistem keamanan berbasis web yang terintegrasi dengan algoritma AES-256, diharapkan dapat meningkatkan keamanan penyimpanan dokumen digital serta meminimalkan risiko akses tidak sah dan kebocoran data (Donald, 2023).

Mengacu pada Gambar 2.7, kerangka pemikiran penelitian ini diawali dengan perumusan permasalahan mengenai keamanan dokumen digital, kemudian dilanjutkan dengan penerapan solusi menggunakan algoritma AES-256 dalam sistem berbasis web. Proses enkripsi dan dekripsi dilakukan untuk menjaga keamanan data, sehingga menghasilkan sistem yang mampu melindungi dokumen digital secara optimal.



Gambar 2.27 Kerangka Pemikiran

Sumber: Diolah oleh Penulis

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisis Permasalahan

Analisis permasalahan merupakan tahapan awal pada proses perancangan sistem yang dilakukan untuk mengetahui berbagai permasalahan yang muncul, serta menentukan solusi yang tepat untuk mengatasinya. Pada era digital saat ini, penggunaan dokumen dalam bentuk digital terus mengalami perkembangan karena dinilai lebih praktis, efisien, dan mudah dalam proses penyimpanan maupun distribusi.

Namun, kemudahan tersebut juga disertai dengan berbagai kendala yang berkaitan dengan keamanan dokumen digital. Salah satu permasalahan utama adalah rendahnya tingkat keamanan dalam proses penyimpanan dokumen, di mana banyak sistem yang masih menyimpan data dalam bentuk asli (*plaintext*) tanpa adanya mekanisme pengamanan yang memadai. Hal ini menyebabkan dokumen rentan terhadap berbagai ancaman, seperti akses tidak sah, kebocoran data, serta manipulasi isi dokumen.

Selain itu, sistem penyimpanan dokumen yang tidak dilengkapi dengan metode enkripsi memungkinkan pihak yang tidak berwenang untuk dengan mudah membaca isi dokumen apabila berhasil mengakses sistem. Permasalahan lainnya adalah kurangnya kontrol akses yang baik, sehingga tidak terdapat pembatasan yang jelas terhadap siapa saja yang dapat mengakses dokumen tersebut.

Apabila permasalahan ini tidak dikelola secara tepat, kondisi tersebut dapat menyebabkan berbagai dampak yang merugikan, seperti hilangnya

kerahasiaan informasi, penyalahgunaan data, serta berkurangnya kepercayaan pengguna terhadap sistem yang digunakan.

Berdasarkan permasalahan tersebut, dibutuhkan upaya yang dapat meningkatkan keamanan dalam penyimpanan dokumen digital. Salah satu solusi alternatif yang dapat dilakukan yaitu melalui penerapan teknik kriptografi, yaitu dengan menerapkan algoritma *Advanced Encryption Standard* (AES-256) untuk memberikan perlindungan terhadap data. Dengan menerapkan metode ini, dokumen yang disimpan akan diubah ke dalam bentuk terenkripsi (*ciphertext*), sehingga hanya dapat diakses kembali dengan melakukan dekripsi memakai kunci yang tepat

Selain itu, sistem yang dibangun dalam penelitian ini berbasis web, sehingga pengguna dapat lebih mudah mengakses dan mengelola dokumen secara fleksibel. Dengan adanya kombinasi antara sistem berbasis web dan algoritma AES-256, diharapkan mampu memberikan solusi yang efektif dalam meningkatkan keamanan penyimpanan dokumen digital.

3.2 Analisis Kebutuhan Sistem

Tahap analisis kebutuhan sistem dilakukan untuk menentukan berbagai kebutuhan yang diperlukan dalam pembangunan sistem. Tahap ini bertujuan untuk memastikan sistem yang dikembangkan dapat memenuhi kebutuhan pengguna sekaligus memberikan solusi terhadap permasalahan yang ditemukan sebelumnya.

Dalam penelitian ini, kebutuhan sistem dikelompokkan menjadi dua kategori, yakni kebutuhan fungsional dan non-fungsional. Kedua kategori tersebut digunakan sebagai landasan dalam perancangan hingga pengembangan sistem keamanan penyimpanan dokumen digital berbasis web.

3.2.1 Kebutuhan Fungsional

Kebutuhan fungsional mengacu pada berbagai fungsi atau fitur yang perlu tersedia agar sistem dapat berjalan sesuai dengan kebutuhan. Sistem yang dibangun harus mampu menyediakan layanan utama yang mendukung proses pengamanan dokumen digital. Adapun kebutuhan fungsional yang terdapat pada sistem ini meliputi sebagai berikut:

1. Sistem dapat melakukan proses *login* pengguna.
2. Sistem dapat mengunggah dokumen ke dalam sistem.
3. Sistem dapat melakukan proses enkripsi dokumen dengan menerapkan algoritma AES-256.
4. Sistem dapat menyimpan dokumen dalam bentuk terenkripsi (*ciphertext*).
5. Sistem dapat menyajikan daftar dokumen yang telah tersimpan.
6. Sistem dapat mendekripsi dokumen sehingga data kembali ke bentuk semula (*plaintext*).

3.2.2 Kebutuhan Non-Fungsional

Kebutuhan non-fungsional berkaitan dengan aspek kualitas yang harus dipenuhi oleh sistem. Meskipun tidak berhubungan langsung dengan fungsi utama, kebutuhan ini berperan dalam menunjang kinerja serta keamanan sistem secara menyeluruh. Adapun kebutuhan non-fungsional pada sistem ini meliputi sebagai berikut:

1. Keamanan

Sistem harus mampu menjaga keamanan data dengan menggunakan algoritma AES-256 agar tidak dapat diakses oleh pihak yang tidak memiliki kewenangan. Selain itu, data yang tersimpan pada database harus berada

dalam kondisi terenkripsi (*ciphertext*), sehingga apabila terjadi kebocoran data, isinya tetap terlindungi dan tidak dapat dibaca tanpa kunci yang tepat.

2. Aksesibilitas

Sistem berbasis web dapat diakses oleh pengguna dari berbagai tempat dan waktu selama tersedia koneksi internet. Kondisi ini memberikan keleluasaan bagi pengguna dalam melakukan pengelolaan dokumen tanpa terbatas oleh perangkat atau lokasi tertentu.

3. Kinerja Sistem

Sistem harus mampu memproses enkripsi dan dekripsi dokumen dengan waktu yang efisien. Kinerja yang baik diperlukan agar pengguna tidak mengalami keterlambatan yang signifikan saat melakukan unggah, penyimpanan, maupun pengambilan dokumen.

4. Kemudahan Penggunaan

Sistem dirancang dengan tampilan antarmuka yang sederhana sehingga mudah dipahami dan digunakan oleh pengguna. Desain sistem harus memperhatikan aspek *user-friendly* sehingga pengguna dapat menggunakan fitur yang tersedia tanpa memerlukan pelatihan khusus.

3.3 Algoritma Sistem

Algoritma sistem merupakan tahapan proses yang ditemukan berdasarkan hasil analisis.. Penelitian ini menerapkan algoritma *Advanced Encryption Standard (AES-256)* yang diintegrasikan ke dalam sistem berbasis web untuk mengamankan penyimpanan dokumen digital.

Dalam penelitian ini, algoritma AES-256 dipilih karena menawarkan tingkat keamanan yang kuat serta telah diakui sebagai standar internasional dalam

pengamanan data. AES-256 menggunakan ukuran kunci sebesar 256-bit yang memiliki ketahanan tinggi terhadap upaya pemecahan melalui serangan *brute force*. Selain itu, algoritma tersebut telah diterapkan pada berbagai sistem keamanan masa kini, seperti pada sistem perbankan, komunikasi digital, dan penyimpanan data sensitif. Dengan keunggulan tersebut, AES-256 dinilai mampu memberikan perlindungan yang efektif terhadap dokumen digital dari ancaman akses tidak sah maupun kebocoran data.

Perancangan algoritma tidak hanya diarahkan pada proses enkripsi dan dekripsi, tetapi turut melibatkan pengelolaan data beserta penerapan mekanisme keamanan secara keseluruhan. Setiap dokumen yang diunggah oleh pengguna tidak langsung disimpan sebagai bentuk asli (*plaintext*), tetapi terlebih dahulu diproses melalui tahap enkripsi sehingga berubah menjadi *ciphertext*. Dengan mekanisme tersebut, informasi yang tersimpan tetap terlindungi meskipun terdapat upaya akses dari pihak tanpa kewenangan.

3.3.1 Algoritma Enkripsi Dokumen

Enkripsi dokumen berlangsung setelah pengguna mengirimkan dokumen ke sistem. Selanjutnya, sistem menjalankan beberapa tahapan untuk mengonversi data asli menjadi bentuk terenkripsi.

Tahapan proses enkripsi dokumen adalah sebagai berikut:

1. Pengguna melakukan *login* ke dalam sistem untuk mendapatkan hak akses.
2. Pengguna mengunggah (*upload*) dokumen yang akan diamankan.
3. Sistem membaca *file* dokumen yang diunggah dan mengubahnya ke dalam bentuk data digital (*plaintext*).

4. Sistem menentukan kunci enkripsi (*key*) yang ditetapkan untuk keperluan enkripsi.
5. Data kemudian diolah dengan algoritma AES-256 melalui sejumlah tahap transformasi.
6. Hasil proses enkripsi berupa data terenkripsi (*ciphertext*).
7. Data hasil enkripsi selanjutnya ditempatkan pada database atau ruang penyimpanan di server.

Proses enkripsi ini bertujuan untuk memastikan bahwa dokumen yang tersimpan tidak dapat dibaca dalam bentuk aslinya sebelum dilakukan dekripsi.

3.3.2 Algoritma Dekripsi Dokumen

Dekripsi dilakukan saat pengguna hendak membuka kembali dokumen yang tersimpan. Tahapan ini berfungsi mengubah data terenkripsi menjadi bentuk semula.

Tahapan proses dekripsi dokumen adalah sebagai berikut:

1. Pengguna memilih dokumen yang ingin diakses dari sistem.
2. Sistem mengambil data dokumen dalam bentuk *ciphertext* dari database.
3. Sistem menggunakan kunci (*key*) yang sesuai dengan proses enkripsi.
4. Data diproses menggunakan algoritma AES-256 untuk proses dekripsi.
5. Data diubah dari bentuk *ciphertext* menjadi *plaintext*.
6. Dokumen ditampilkan kembali kepada pengguna dalam bentuk aslinya.

Mekanisme dekripsi tersebut membatasi pembacaan dokumen hanya kepada pengguna yang mempunyai hak akses.

3.3.3 Integrasi Algoritma dalam Sistem

Dalam sistem yang dibangun, algoritma AES-256 diintegrasikan secara langsung ke dalam alur kerja sistem berbasis web. Setiap proses unggah dokumen akan secara otomatis diikuti dengan tahap enkripsi terlebih dahulu sebelum data ditempatkan pada database. Sebaliknya, setiap proses pengambilan dokumen akan melalui proses dekripsi sebelum ditampilkan kepada pengguna.

Integrasi ini memungkinkan sistem untuk memberikan keamanan secara menyeluruh tanpa mengurangi kemudahan penggunaan. Selain itu, proses enkripsi dan dekripsi dilakukan secara transparan oleh sistem, sehingga pengguna tidak perlu melakukan proses tambahan secara manual.

3.3.4 Mekanisme Pengelolaan Kunci (*Key Management*)

Dalam penerapan algoritma AES-256, kunci (*key*) menjadi komponen penting yang memengaruhi keamanan sistem. Karena itu, pengaturan kunci perlu menjadi perhatian utama dalam penerapan sistem.

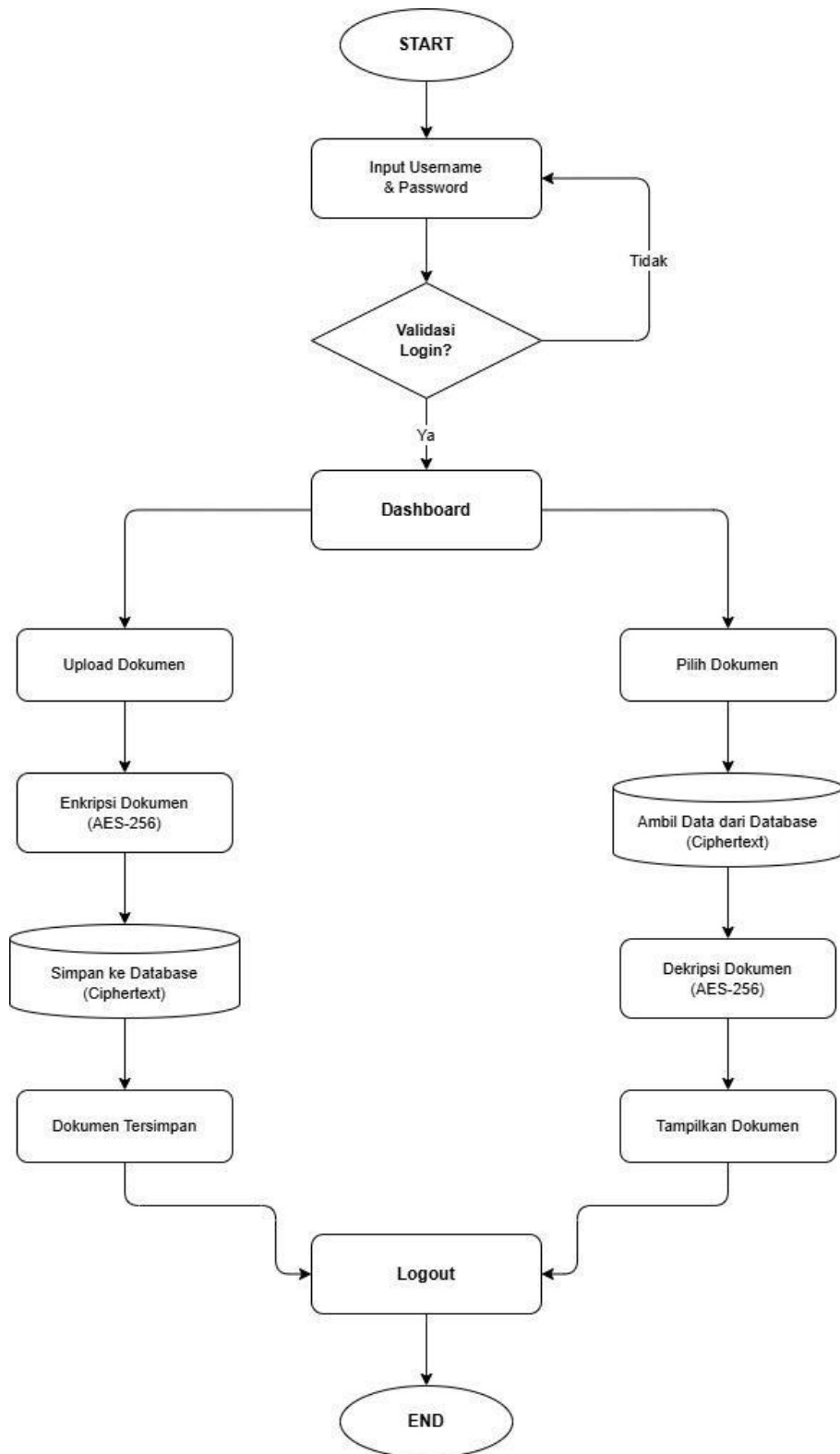
Pada sistem yang dibangun, kunci dimanfaatkan untuk menjalankan enkripsi maupun dekripsi. Kunci tersebut diamankan pada bagian server dan pemakaiannya dibatasi untuk kebutuhan pemrosesan data oleh sistem. Akses terhadap kunci dibatasi sehingga pihak tanpa kewenangan tidak dapat memanfaatkannya.

Pengaturan kunci secara tepat dilakukan untuk mengurangi risiko kebocoran informasi yang dapat menyebabkan data terenkripsi menjadi rentan. Dengan demikian, keamanan sistem turut ditentukan oleh tata kelola kunci, bukan hanya oleh algoritma yang diterapkan.

3.3.5 *Flowchart* Sistem

Flowchart sistem menyajikan gambaran visual mengenai rangkaian kerja sistem secara sistematis, mulai dari proses input, pengolahan data, hingga menghasilkan *output*. *Flowchart* ini bertujuan untuk mempermudah dalam memahami proses yang terjadi dalam sistem, serta memberikan gambaran yang jelas mengenai tahapan-tahapan yang dilakukan.

Pada penelitian ini, *flowchart* sistem menjelaskan rangkaian pengamanan dokumen digital pada sistem berbasis web yang meliputi proses *login* pengguna, unggah dokumen, proses enkripsi menggunakan algoritma AES-256, penyimpanan data ke dalam database, sampai tahap dekripsi ketika pengguna kembali membuka dokumen.



Gambar 3.1 Flowchart Sistem
Sumber: Diolah oleh Penulis

Berdasarkan *flowchart* sistem di atas, proses dimulai ketika pengguna melakukan *input* username dan password untuk masuk menuju sistem. Selanjutnya sistem akan melakukan validasi *login*. Jika data *login* tidak valid, maka pengguna diarahkan kembali untuk memasukkan username dan password. Namun apabila autentikasi berhasil, sistem mengarahkan pengguna menuju halaman *dashboard*.

Dari halaman *dashboard*, pengguna dapat mengunggah dokumen. Dokumen yang diunggah kemudian akan diproses menggunakan algoritma AES-256 untuk mengenkripsi data sebelum ditempatkan pada *database* dalam bentuk *ciphertext*. Setelah proses penyimpanan selesai, dokumen akan tersimpan secara aman di *database*. Selain proses penyimpanan dokumen, pengguna juga dapat memilih dokumen yang telah tersimpan untuk diakses kembali.

Sistem akan mengambil data yang telah terenkripsi dari database lalu menjalankan tahap dekripsi menggunakan algoritma AES-256 sehingga dokumen dapat dikembalikan ke bentuk semula untuk selanjutnya ditampilkan kepada pengguna. Setelah seluruh aktivitas selesai, pengguna dapat keluar melalui fitur logout sehingga rangkaian proses sistem berakhir.

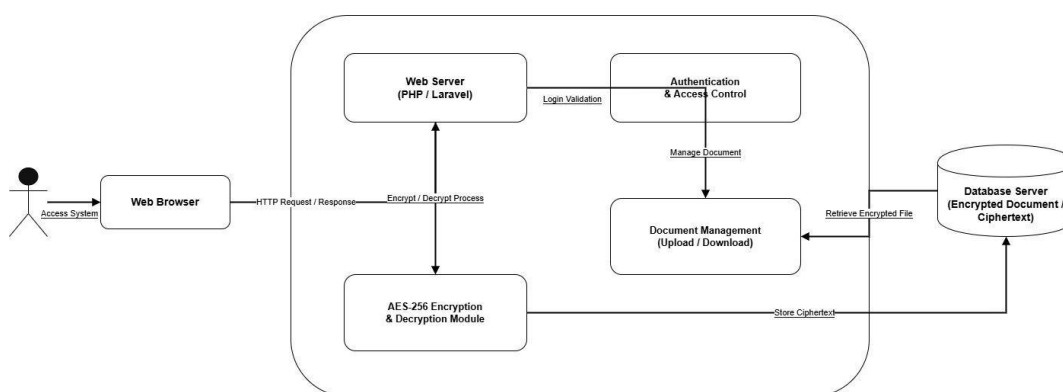
3.4 Pemodelan dan Perancangan Sistem

Pemodelan dan perancangan sistem dilakukan untuk menjelaskan rancangan pembangunan sistem sekaligus cara kerja sistem secara menyeluruh. Tahap ini diperlukan karena hasilnya digunakan sebagai pedoman pada tahap implementasi sistem.

Penelitian ini menggunakan *UML (Unified Modeling Language)* sebagai pendekatan dalam pemodelan sistem yang bertujuan untuk menunjukkan hubungan pengguna dengan sistem sekaligus menyajikan rangkaian proses yang berlangsung secara teratur. Dengan adanya pemodelan ini, diharapkan sistem yang dibangun dapat lebih terstruktur, mudah dipahami, serta memenuhi kebutuhan pengguna.

3.4.1 Arsitektur Sistem

Arsitektur sistem digunakan untuk menunjukkan keterkaitan antarkomponen dalam sistem keamanan penyimpanan dokumen digital berbasis web yang menerapkan algoritma AES-256. Komponen arsitektur tersebut meliputi pengguna, peramban web, server web, modul enkripsi dan dekripsi AES-256, serta server basis data.



Gambar 3.2 Arsitektur Sistem

Sumber: Diolah oleh Penulis

Sistem keamanan penyimpanan dokumen digital berbasis web tersebut tersusun atas sejumlah komponen utama, yaitu pengguna, peramban web, server web, autentikasi dan kontrol akses, modul enkripsi dan dekripsi AES-256, pengelolaan dokumen, serta server basis data.

Pengguna mengakses sistem melalui peramban web untuk melakukan proses masuk, mengunggah dokumen, maupun mengambil dokumen. Selanjutnya, peramban akan meneruskan permintaan ke server web untuk diproses oleh sistem.

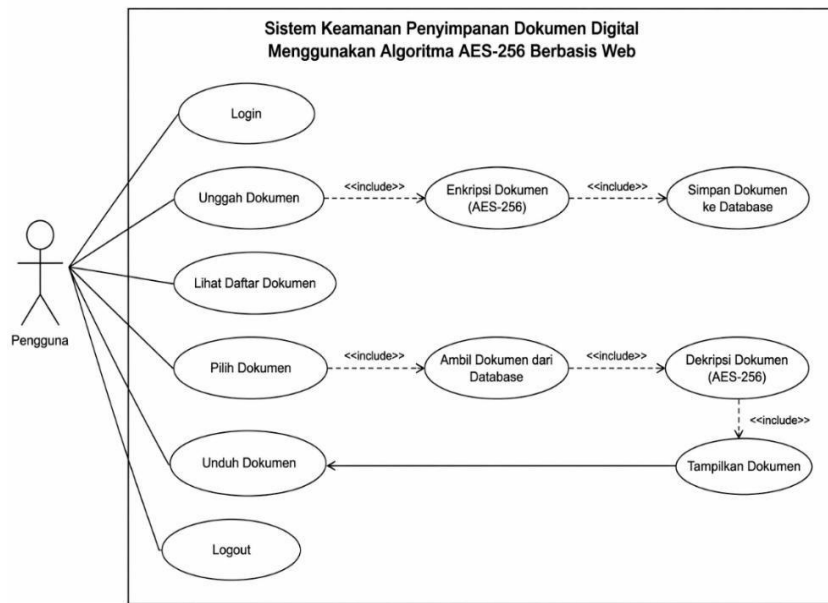
Server web berfungsi sebagai pusat pengolahan sistem yang menangani autentikasi pengguna, pengelolaan dokumen, serta tahapan enkripsi serta dekripsi dengan algoritma AES-256. Pada proses pengunggahan dokumen, sistem akan melakukan enkripsi terlebih dahulu sebelum dokumen disimpan ke dalam basis data dalam bentuk *ciphertext*. Hal ini bertujuan guna melindungi kerahasiaan informasi sehingga pihak tanpa kewenangan tidak dapat membacanya secara langsung.

Ketika pengguna ingin mengakses kembali dokumen, sistem akan mengambil data terenkripsi dari basis data, lalu memprosesnya melalui tahap proses dekripsi menggunakan algoritma AES-256 sehingga dokumen dapat dipulihkan menjadi bentuk semula (*plaintext*). Dengan arsitektur ini, sistem mampu memberikan keamanan terhadap dokumen digital melalui mekanisme enkripsi, autentikasi, dan kontrol akses secara terintegrasi.

3.4.2 Use Case Diagram

Use Case Diagram digunakan untuk menunjukkan keterkaitan antara aktor dan sistem yang dikembangkan. Diagram tersebut menyajikan fitur utama sistem beserta kewenangan pengguna dalam mengoperasikan setiap fungsi yang tersedia.

Sistem ini memiliki satu aktor utama yaitu pengguna yang melakukan interaksi secara langsung terhadap sistem. Pengguna memiliki akses untuk melakukan berbagai aktivitas seperti *login* ke dalam sistem, mengunggah dokumen, melakukan proses enkripsi secara otomatis menyimpan dokumen ke dalam database, serta mengakses kembali dokumen melalui proses dekripsi.



Gambar 3.3 Use Case Diagram

Sumber: Diolah oleh Penulis

Berdasarkan Gambar 3.2, sistem keamanan penyimpanan dokumen digital berbasis web memiliki satu aktor utama yaitu pengguna (*user*) yang berinteraksi langsung dengan sistem. Pengguna memiliki hak akses untuk melakukan berbagai aktivitas, dimulai dari proses *login* hingga *logout* dari sistem.

Setelah proses *login* berhasil, pengguna dapat memasukkan dokumen ke sistem. Pengunggahan dokumen secara otomatis menjalankan tahap enkripsi dengan AES-256 sebelum data ditempatkan pada database. Hal ini

bertujuan untuk memastikan bahwa dokumen tidak disimpan dalam bentuk asli (*plaintext*), melainkan dalam bentuk terenkripsi (*ciphertext*) sehingga lebih aman.

Pengguna juga dapat menampilkan daftar dokumen yang sudah tersimpan dalam sistem. Untuk mengakses dokumen, pengguna dapat memilih dokumen yang diinginkan, kemudian sistem akan mengambil data dari database dalam bentuk terenkripsi. Selanjutnya, sistem menjalankan dekripsi dengan AES-256 untuk memulihkan data menjadi bentuk semula sebelum ditampilkan kepada pengguna.

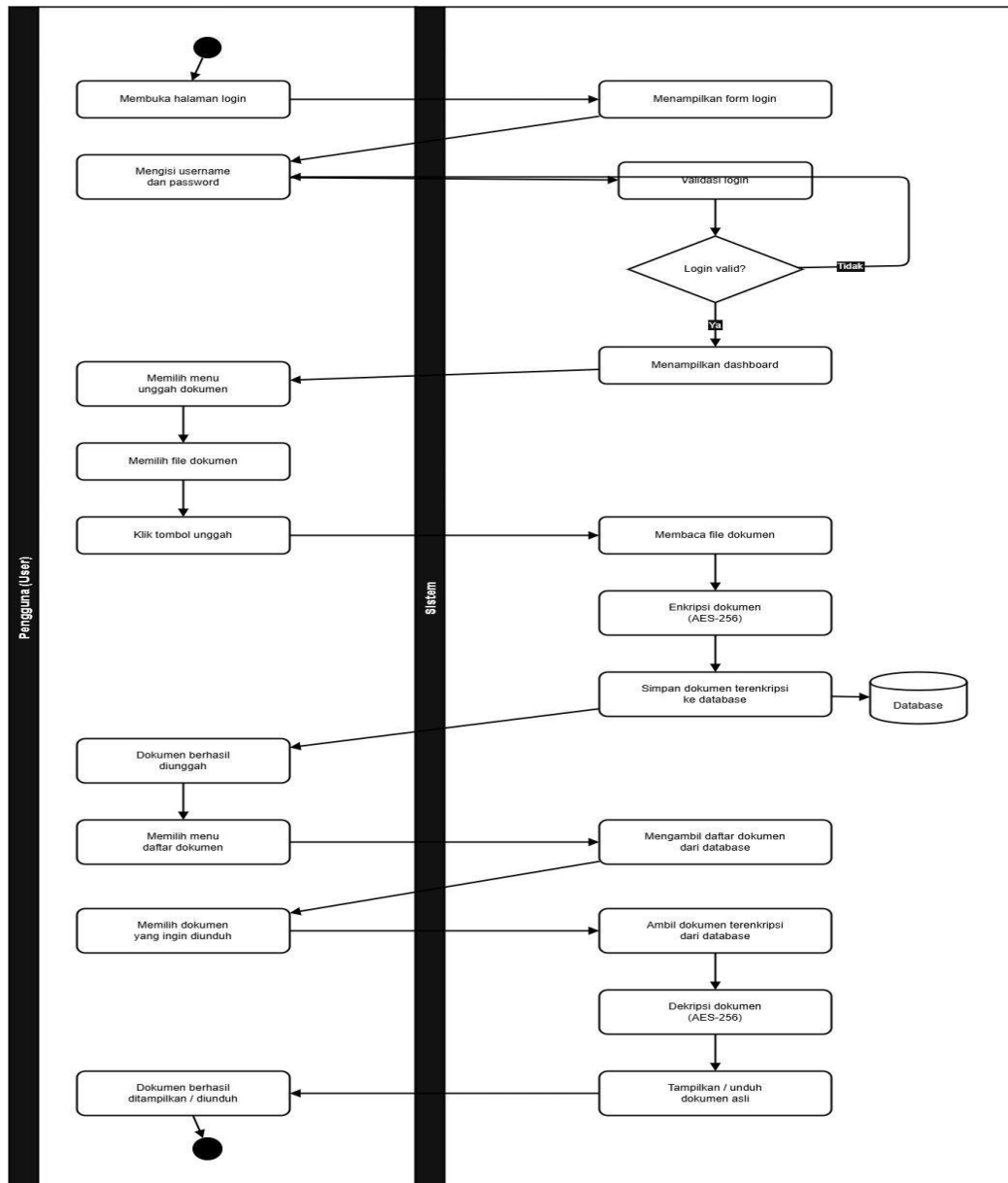
Diagram tersebut memperlihatkan hubungan *include* di antara beberapa *use case*, yang menunjukkan bahwa sejumlah proses menjadi bagian dari fungsi utama. Sebagai contoh, proses unggah dokumen mencakup proses enkripsi dan penyimpanan data, sedangkan proses pemilihan dokumen mencakup proses pengambilan data dan dekripsi sebelum dokumen ditampilkan.

Use Case Diagram membantu memperlihatkan ruang lingkup sistem beserta fungsi utama yang tersedia, sehingga memudahkan dalam proses pengembangan dan implementasi sistem.

3.4.3 Activity Diagram

Activity Diagram merupakan bagian dari dalam UML (*Unified Modeling Language*) yang digunakan untuk menyajikan rangkaian aktivitas atau proses sistem secara sistematis. Diagram ini memperlihatkan tahapan proses sejak dimulai sampai selesai, termasuk adanya percabangan keputusan yang mungkin terjadi selama sistem berjalan.

Dalam pengembangan sistem, *Activity Diagram* digunakan untuk memperjelas rangkaian kerja sistem, baik dari sisi pengguna maupun sistem itu sendiri. Melalui diagram tersebut, proses yang memiliki tahapan kompleks dapat disajikan dalam bentuk yang lebih sederhana sehingga memudahkan dalam memahami, merancang, dan mengimplementasikan sistem



Gambar 3.4 Activity Diagram
Sumber: Diolah oleh Penulis

Berdasarkan activity diagram di atas, rangkaian aktivitas diawali saat pengguna membuka halaman *login* lalu mengisi username dan password. Berikutnya, sistem menampilkan *form login* dan memeriksa validitas data yang dimasukkan pengguna. Jika informasi *login* tidak sesuai, pengguna diarahkan kembali ke tahap pengisian username dan password. Jika autentikasi berhasil, sistem kemudian membuka halaman dashboard.

Setelah masuk ke sistem, pengguna dapat memilih fitur dokumen dan memilih file dokumen yang akan diunggah. Sistem selanjutnya membaca berkas dan mengenkripsinya menggunakan algoritma AES-256 sebelum dokumen disimpan ke dalam database dalam bentuk terenkripsi (*ciphertext*). Setelah penyimpanan selesai, sistem memberikan pemberitahuan bahwa dokumen telah berhasil diunggah.

Selanjutnya pengguna dapat memilih menu daftar dokumen untuk melihat dokumen yang telah tersimpan pada database. Sistem akan mengambil daftar dokumen dari database kemudian pengguna memilih dokumen yang ingin diakses atau diunduh. Sistem selanjutnya mengambil dokumen terenkripsi dari database dan melakukan proses dekripsi menggunakan algoritma AES-256 sehingga dokumen dapat dikembalikan ke bentuk aslinya dan ditampilkan kepada pengguna. Setelah seluruh aktivitas selesai dilakukan, proses pada sistem berakhir.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Implementasi sistem merupakan proses merealisasikan rancangan dan hasil analisis pada Bab III menjadi aplikasi berbasis web. Pada tahap ini, keseluruhan rancangan diwujudkan dalam aplikasi untuk mengamankan penyimpanan dokumen digital yang menggunakan algoritma Advanced Encryption Standard (AES-256) sebagai mekanisme perlindungan dokumen dari akses tanpa izin.

Sistem yang dibangun memiliki beberapa fungsi utama, yaitu autentikasi pengguna, pengunggahan dokumen, proses enkripsi dokumen menggunakan algoritma AES-256, penyimpanan dokumen dalam bentuk terenkripsi (*ciphertext*), proses dekripsi dokumen, serta pengunduhan dokumen. Dengan mekanisme tersebut, dokumen yang berada dalam penyimpanan sistem tidak disimpan sebagai bentuk asli (*plaintext*), sehingga pembukaan kembali isi dokumen hanya dapat dilakukan oleh pengguna yang mempunyai hak akses serta kunci yang tepat.

Sistem dikembangkan dengan framework Laravel menggunakan bahasa pemrograman PHP, sementara pengelolaan basis data menggunakan MySQL. Proses enkripsi dan dekripsi memanfaatkan pustaka OpenSSL yang mendukung implementasi algoritma AES-256. Pada subbab berikutnya akan dijelaskan implementasi setiap komponen sistem, meliputi lingkungan implementasi, basis data, antarmuka pengguna, implementasi algoritma AES-256, serta hasil pengujian sistem.

4.1.1 Lingkungan Implementasi

Pengembangan dan pengujian aplikasi dilakukan dengan dukungan perangkat lunak serta perangkat keras yang sesuai. Aplikasi yang dikembangkan merupakan sistem berbasis web dengan memanfaatkan framework Laravel dan bahasa pemrograman PHP. Basis data yang digunakan adalah SQLite yang berfungsi sebagai tempat penyimpanan data aplikasi. Seluruh proses enkripsi dan dekripsi dokumen memanfaatkan pustaka OpenSSL menggunakan algoritma Advanced Encryption Standard (AES-256-CBC).

Rincian lingkungan implementasi yang digunakan ditampilkan pada tabel berikut.

Tabel 4.1 Detail Environment

Komponen	Keterangan
Sistem Operasi	Windows 11
Framework	Laravel 12
Bahasa Pemrograman	PHP
Basis Data	SQLite
Library Kriptografi	OpenSSL (AES-256-CBC)
Text Editor	Visual Studio Code

4.1.2 Basis Data

Basis data berperan sebagai tempat penyimpanan berbagai informasi yang diperlukan sistem. Penelitian ini menggunakan SQLite sebagai basis data yang terhubung dengan *framework* Laravel. Struktur basis data disusun untuk menunjang autentikasi pengguna dan penyimpanan metadata dokumen yang telah dienkrpsi menggunakan algoritma AES-256.

Sistem menggunakan dua tabel utama pada basis datanya, yaitu `users` dan `documents`. Tabel `users` berfungsi menyimpan data akun pengguna yang memperoleh hak akses ke sistem, sementara tabel `documents` menyimpan data dokumen yang diunggah, berikut metadata dari hasil enkripsinya.

1. Tabel Users

Tabel `users` berfungsi mencatat data pengguna yang mempunyai akses ke sistem. Informasi yang dicatat mencakup identitas pengguna, email, *hashed password*, serta waktu pembuatan dan perubahan data.

column_name	data_type	is_nullable	column_default	foreign_key
id	INTEGER	NO	NULL	EMPTY
name	varchar	NO	NULL	EMPTY
email	varchar	NO	NULL	EMPTY
email_verified_at	datetime	YES	NULL	EMPTY
password	varchar	NO	NULL	EMPTY
remember_token	varchar	YES	NULL	EMPTY
created_at	datetime	YES	NULL	EMPTY
updated_at	datetime	YES	NULL	EMPTY

Gambar 4.1 Struktur Tabel Users

Sumber: Diolah oleh Penulis

2. Tabel Documents

Tabel `documents` menjadi tabel utama untuk mencatat informasi dokumen digital setelah diproses menggunakan algoritma AES-256. Tabel ini tidak menyimpan isi dokumen secara langsung di dalam basis data, melainkan hanya menyimpan metadata dokumen.

File terenkripsi disimpan pada media penyimpanan (*storage*) aplikasi, sedangkan basis data menyimpan lokasi file beserta informasi pendukung lainnya. Kolom `user_id` digunakan untuk menghubungkan dokumen dengan

pengguna yang mengunggahnya. Kolom `encrypted_path` menyimpan lokasi file hasil enkripsi pada direktori penyimpanan aplikasi.

Selanjutnya, kolom `iv` (*Initialization Vector*) digunakan dalam tahapan enkripsi maupun dekripsi AES-256-CBC sebagai bagian dari perlindungan data. Nilai IV berbeda untuk setiap dokumen dan disimpan dalam format Base64, sehingga dapat disimpan pada basis data karena nilai tersebut tidak berfungsi sebagai kunci enkripsi.

column_name	data_type	is_nullable	column_default	foreign_key
id	INTEGER	NO	NULL	EMPTY
user_id	INTEGER	NO	NULL	users(id)
original_name	varchar	NO	NULL	EMPTY
encrypted_path	varchar	NO	NULL	EMPTY
file_type	varchar	NO	NULL	EMPTY
file_size	INTEGER	NO	NULL	EMPTY
iv	varchar	NO	NULL	EMPTY
created_at	datetime	YES	NULL	EMPTY
updated_at	datetime	YES	NULL	EMPTY

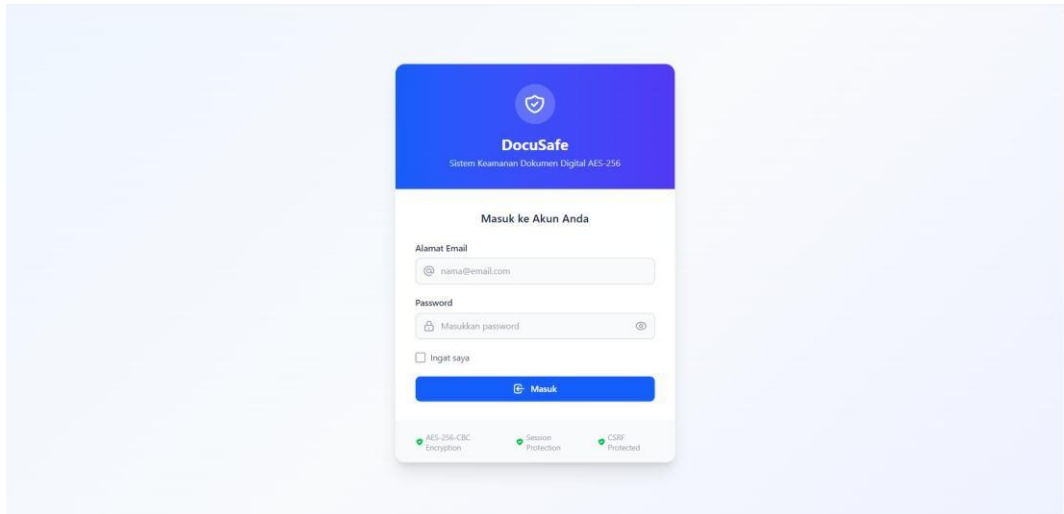
Gambar 4.2 Struktur Tabel Documents

Sumber: Diolah oleh Penulis

4.1.3 Implementasi Antarmuka Sistem

Tahap ini merupakan realisasi rancangan antarmuka dari Bab III menjadi tampilan aplikasi yang dapat dioperasikan pengguna. Perancangan antarmuka memperhatikan aspek kemudahan penggunaan agar setiap fitur dapat dioperasikan pengguna secara sederhana. Antarmuka sistem mencakup tiga halaman utama, yaitu login, dashboard, dan upload dokumen.

1. Halaman Login



Gambar 4.3 Tampilan Halaman Login

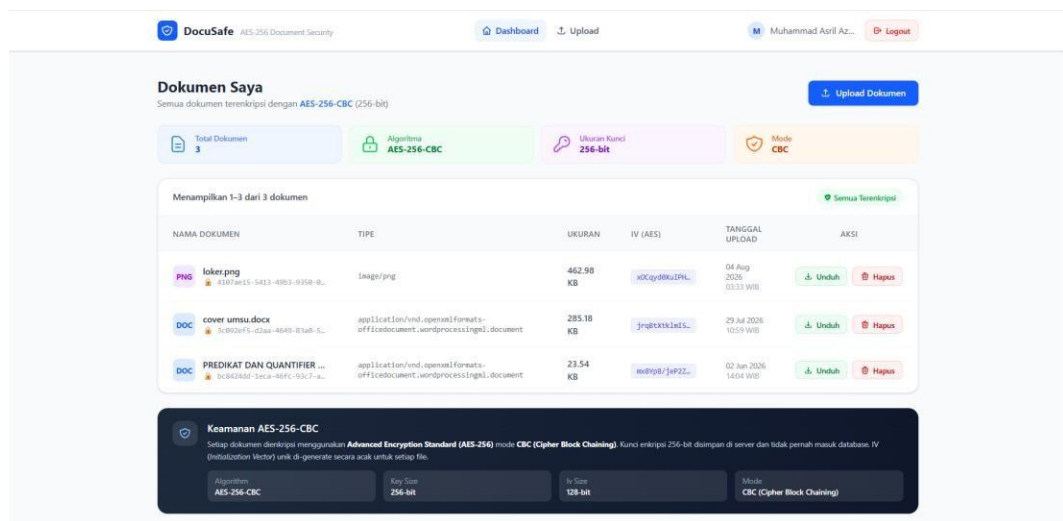
Sumber: Diolah oleh Penulis

Halaman login menjadi bagian autentikasi yang digunakan pengguna sebagai akses awal menuju aplikasi DocuSafe. Pengguna perlu mengisikan email dan kata sandi yang sebelumnya telah terdaftar. Data tersebut kemudian diperiksa oleh sistem guna memastikan kewenangan pengguna dalam mengakses aplikasi.

Halaman login dilengkapi dengan fitur *toggle visibility* pada kolom kata sandi untuk membantu pengguna dalam memastikan kebenaran data yang diinputkan. Selain itu, sistem menerapkan mekanisme keamanan berupa *Session Protection* untuk menjaga keamanan sesi pengguna setelah berhasil melakukan autentikasi serta *Cross-Site Request Forgery (CSRF) Protection* untuk mencegah serangan yang memanfaatkan permintaan palsu selama proses login.

Ketika autentikasi berhasil, sistem mengarahkan pengguna menuju dashboard untuk menggunakan fitur yang tersedia. Jika email atau kata sandi tidak cocok, sistem memberikan pemberitahuan kesalahan dan pengguna dapat mencoba login kembali menggunakan data yang sesuai.

2. Halaman Dashboard



Gambar 4.4 Tampilan Halaman Dashboard

Sumber: Diolah oleh Penulis

Dashboard menjadi halaman awal yang muncul setelah pengguna berhasil melewati proses autentikasi. Halaman tersebut menjadi pusat pengelolaan dokumen sekaligus menyediakan informasi sistem dan akses menuju berbagai fitur utama.

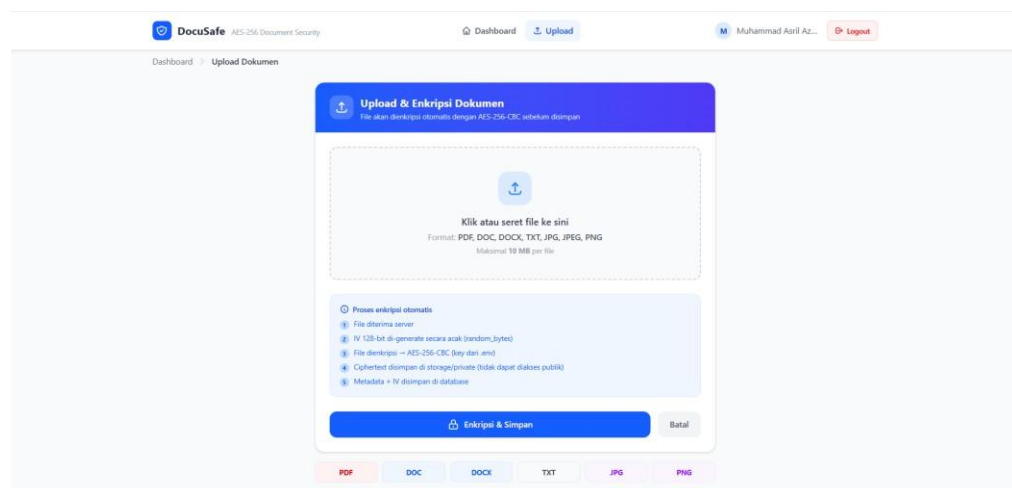
Pada halaman Dashboard ditampilkan ringkasan informasi mengenai jumlah dokumen yang tersimpan dan konfigurasi algoritma kriptografi yang digunakan, meliputi algoritma AES-256-CBC, ukuran kunci 256-bit, dan mode operasi *Cipher Block Chaining* (CBC). Informasi tersebut membantu pengguna mengetahui mekanisme keamanan yang digunakan oleh sistem.

Dashboard tidak hanya menyajikan informasi sistem, tetapi juga menampilkan dokumen yang sebelumnya telah diunggah. Setiap dokumen disertai informasi berupa nama dokumen, jenis file, ukuran file, nilai *Initialization Vector (IV)*, serta waktu pengunggahan.

Melalui halaman Dashboard, pengguna dapat melakukan berbagai tindakan terhadap dokumen, seperti mengunggah dokumen baru, mengunduh dokumen melalui proses dekripsi, maupun menghapus dokumen yang tidak lagi diperlukan. Dengan adanya fitur tersebut, pengguna dapat mengelola dokumen yang tersimpan dalam sistem secara lebih mudah dan terstruktur.

Melalui dashboard, pengelolaan seluruh dokumen terenkripsi dapat dilakukan dalam satu halaman secara terpusat sehingga memudahkan pengguna dalam mengelola dokumen sekaligus memperoleh informasi mengenai status keamanan dokumen yang tersimpan di dalam sistem.

3. Halaman Upload



Gambar 4.5 Tampilan Halaman Upload

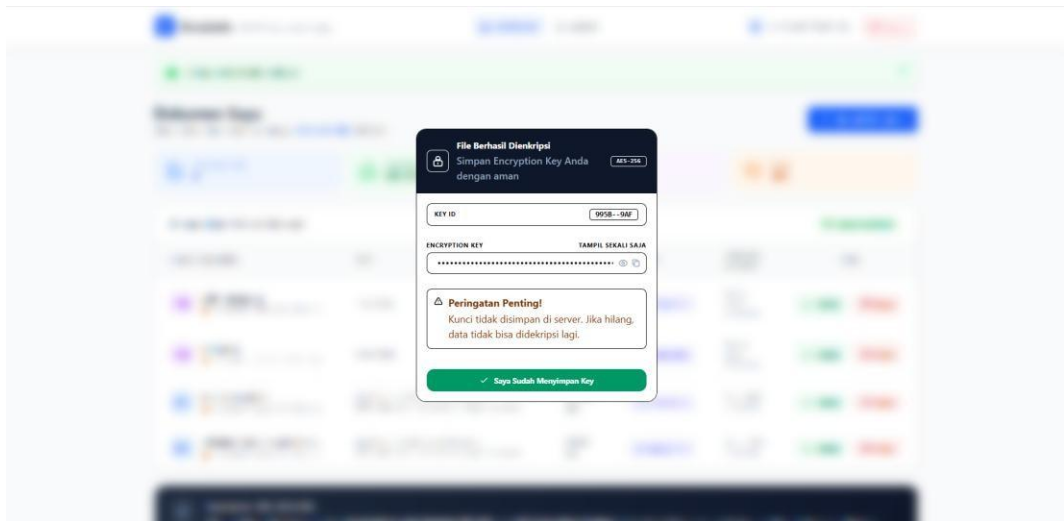
Sumber: Diolah oleh Penulis

Halaman Upload Dokumen menyediakan tampilan bagi pengguna untuk memasukkan dokumen digital yang akan diproteksi dengan AES-256-CBC. Melalui halaman ini, pengguna dapat memilih dokumen dari media penyimpanan perangkat untuk diproses oleh sistem sebelum disimpan dalam bentuk terenkripsi. Sistem mendukung beberapa format dokumen, seperti PDF, DOC, DOCX, TXT, JPG, JPEG, dan PNG, dengan batas ukuran berkas maksimal 10 MB.

Setelah pengguna memilih dokumen dan menjalankan proses unggah, sistem secara otomatis melakukan proses enkripsi pada sisi server. Tahapan yang dilakukan meliputi pembacaan isi dokumen, pembuatan Initialization Vector (IV) dengan nilai acak menggunakan fungsi `random_bytes()`, enkripsi dokumen dengan AES-256-CBC yang dijalankan melalui library OpenSSL, penyimpanan dokumen hasil enkripsi (*ciphertext*) ke media penyimpanan aplikasi, serta penyimpanan metadata dokumen dan nilai IV ke dalam basis data.

Melalui halaman ini, pengguna tidak perlu mengenkripsi dokumen secara manual karena seluruh proses telah ditangani otomatis oleh sistem. Dengan demikian, dokumen yang tersimpan pada media penyimpanan aplikasi berada dalam kondisi terenkripsi sehingga kerahasiaan data dapat terjaga sebelum nantinya dilakukan proses dekripsi oleh pengguna yang memiliki kunci enkripsi.

4. Modal Box Private Key



Gambar 4.6 Tampilan Modal Box Private Key

Sumber: Diolah oleh Penulis

Modal Box Private Key muncul secara otomatis setelah sistem berhasil mengenkripsi dokumen. Tampilan ini memberikan *encryption key* kepada pengguna yang nantinya diperlukan untuk melakukan dekripsi dokumen.

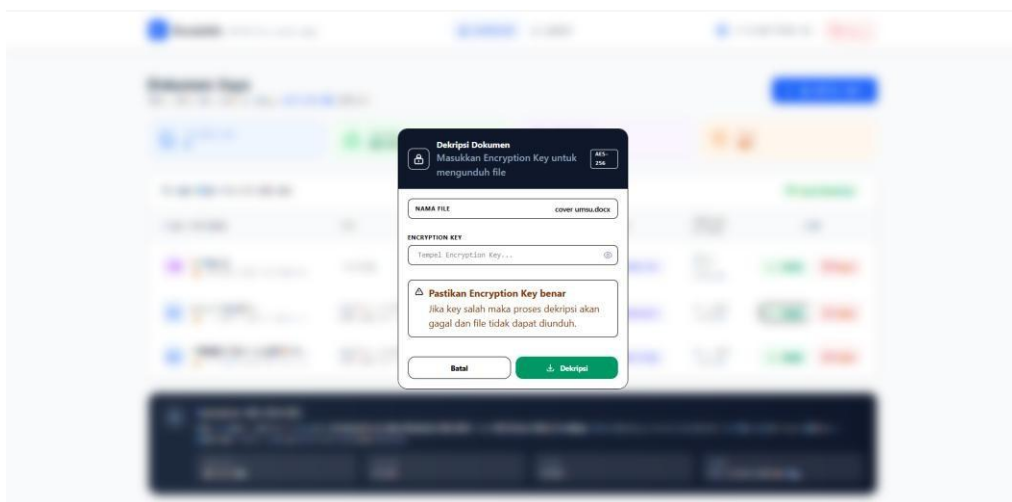
Setiap proses enkripsi menghasilkan kunci unik yang hanya diperlihatkan kepada pengguna satu kali. Karena itu, pengguna harus menyimpan kunci tersebut dengan aman karena sistem tidak menyediakan salinan kunci pada basis data ataupun penyimpanan aplikasi. Jika kunci hilang atau salah, sistem tidak dapat menjalankan dekripsi sehingga dokumen tidak dapat dipulihkan.

Tampilan ini menyediakan fitur untuk melihat dan menyalin kunci enkripsi agar lebih mudah disimpan pengguna sebelum modal ditutup. Setelah pengguna mengonfirmasi bahwa kunci telah disimpan, proses enkripsi

dinyatakan selesai dan pengguna dapat kembali ke halaman utama untuk melanjutkan pengelolaan dokumen.

Mekanisme tersebut menerapkan prinsip kerahasiaan (*confidentiality*) dalam kriptografi karena dekripsi hanya dapat dilakukan oleh pengguna yang mempunyai kunci enkripsi yang tepat terhadap dokumen yang telah diamankan menggunakan algoritma AES-256-CBC.

5. Modal Box Dekripsi Dokumen



Gambar 4.7 Tampilan Modal Box Input Private Key Dekripsi

Sumber: Diolah oleh Penulis

Modal Box Dekripsi Dokumen muncul ketika pengguna memilih dokumen terenkripsi untuk diunduh. Tampilan tersebut menjadi tahap pemeriksaan keamanan sebelum sistem menjalankan dekripsi dan memulihkan dokumen ke bentuk aslinya (*plaintext*).

Pada modal ini, sistem menampilkan informasi berupa nama dokumen yang akan didekripsi serta menyediakan kolom untuk memasukkan *Encryption Key* yang dimiliki pengguna. Selain itu, tersedia fitur *toggle visibility* yang

membantu pengguna memastikan kebenaran kunci yang dimasukkan sebelum proses dekripsi dijalankan.

Setelah *Encryption Key* dimasukkan, sistem memeriksa kesesuaiannya dengan dokumen yang dipilih. Apabila kunci yang dimasukkan benar, sistem akan melakukan proses dekripsi menggunakan algoritma AES-256-CBC, kemudian mengunduh dokumen dalam bentuk aslinya. Sebaliknya, jika kunci yang diberikan salah, dekripsi tidak dapat dilanjutkan sehingga dokumen tidak dapat dibuka. Penerapan mekanisme tersebut membatasi akses dokumen terenkripsi kepada pengguna yang mempunyai *Encryption Key* yang sesuai.

4.2 Implementasi Algoritma AES-256

Penerapan algoritma Advanced Encryption Standard (AES-256) ditujukan untuk melindungi kerahasiaan dokumen digital yang dimasukkan pengguna. Sistem menerapkan AES-256 dengan mode operasi *Cipher Block Chaining* (CBC) dengan memanfaatkan pustaka OpenSSL pada framework Laravel. Pada mode ini, setiap dokumen yang masuk akan diproses menggunakan *secret key* dan Initialization Vector (IV) yang dibuat secara acak pada setiap proses enkripsi.

Penerapan AES-256 pada sistem mencakup tiga tahapan utama, yaitu proses enkripsi dokumen, proses dekripsi dokumen, serta pengelolaan kunci enkripsi. Ketiga tahapan tersebut saling berhubungan satu sama lain untuk menjaga keamanan penyimpanan serta membatasi akses dokumen kepada pengguna yang berwenang.

4.2.1 Proses Enkripsi

Enkripsi dijalankan setelah dokumen berhasil diterima oleh sistem. Setelah dokumen diterima oleh aplikasi, sistem membaca isi file kemudian membuat Initialization Vector (IV) secara acak yang digunakan sebagai parameter tambahan pada algoritma AES-256-CBC. Selanjutnya, dokumen dienkripsi menggunakan kunci rahasia (*secret key*) yang telah dikonfigurasi pada aplikasi.

Enkripsi menghasilkan *ciphertext* yang tidak dapat dipahami secara langsung oleh pengguna. Dokumen yang telah dienkripsi selanjutnya ditempatkan pada *storage* aplikasi, sedangkan metadata seperti nama dokumen, ukuran file, tipe file, lokasi penyimpanan, serta nilai IV disimpan ke dalam basis data.

4.2.2 Proses Dekripsi

Dekripsi dijalankan saat pengguna hendak membuka dokumen yang sebelumnya telah dienkripsi. Sistem mengambil dokumen terenkripsi beserta nilai *Initialization Vector (IV)* yang tersimpan pada basis data. Selanjutnya, sistem memanfaatkan kunci rahasia yang digunakan pada saat enkripsi untuk mengembalikan dokumen ke bentuk aslinya.

Apabila kunci yang digunakan sesuai, maka sistem berhasil menghasilkan kembali dokumen dalam bentuk *plaintext* sehingga dapat diunduh dan dibuka oleh pengguna. Sebaliknya, apabila kunci yang digunakan tidak sesuai atau data dokumen mengalami perubahan, maka proses dekripsi akan gagal dan dokumen tidak dapat dibaca.

4.2.3 Pengelolaan Kunci

Key management menjadi salah satu komponen penting dalam penerapan AES-256 karena keamanan sistem turut ditentukan oleh terjaganya kerahasiaan kunci. Pada sistem yang dibangun, kunci enkripsi tidak disimpan pada basis data, melainkan dikelola melalui konfigurasi aplikasi Laravel sehingga tidak dapat diakses secara langsung oleh pengguna.

Sistem juga membuat Initialization Vector (IV) yang berbeda pada masing-masing dokumen. Nilai IV disimpan pada basis data bersama metadata dokumen karena IV bukan merupakan kunci rahasia dan diperlukan kembali pada proses dekripsi. Perbedaan IV pada setiap proses enkripsi diterapkan sebagai upaya meningkatkan keamanan dengan mencegah dihasilkannya *ciphertext* yang sama meskipun dokumen yang dienkripsi memiliki isi yang identik.

Melalui mekanisme tersebut, perlindungan sistem tidak semata-mata ditentukan oleh AES-256, tetapi turut dipengaruhi oleh pengaturan kunci serta penerapan IV secara tepat. Penerapan tersebut sejalan dengan prinsip kerahasiaan data (*confidentiality*) karena dokumen hanya dapat dikembalikan ke bentuk aslinya apabila proses dekripsi menggunakan kunci yang sesuai.

4.3 Pengujian Sistem

Pengujian sistem dilakukan pada tahap akhir pengembangan untuk memeriksa kesesuaian fungsi yang telah diterapkan dengan kebutuhan sistem. Pengujian penelitian mencakup sejumlah fungsi utama pada aplikasi, meliputi proses login, unggah dokumen, enkripsi dokumen, dan dekripsi dokumen. Hasil

pengujian menjadi dasar untuk menilai kesesuaian kerja setiap fungsi dengan rancangan yang telah ditetapkan.

4.3.1 Metode Pengujian

Metode pengujian yang digunakan pada penelitian ini adalah *Black Box Testing*. *Black Box Testing* menguji perangkat lunak berdasarkan *input* dan *output* yang dihasilkan tanpa meninjau struktur internal maupun kode program. Metode tersebut digunakan untuk memeriksa apakah setiap fitur aplikasi telah memenuhi fungsi yang direncanakan.

Setiap fitur utama diuji menggunakan beberapa kondisi masukan, baik berupa data yang sesuai maupun yang tidak sesuai. Hasil keluaran sistem kemudian dicocokkan dengan keluaran yang telah ditentukan sebelumnya. Jika hasil aktual sesuai dengan hasil yang ditargetkan, fitur dinyatakan Berhasil dan dianggap telah berjalan sebagaimana mestinya.

Fitur yang menjadi objek pengujian dalam penelitian ini mencakup:

1. Pengujian proses *login*.
2. Pengujian proses unggah dokumen.
3. Pengujian proses enkripsi dokumen menggunakan algoritma AES-256-CBC.
4. Pengujian proses dekripsi dokumen menggunakan *Encryption Key* yang dimasukkan oleh pengguna.
5. Pengujian proses penghapusan dokumen.

Hasil setiap pengujian ditampilkan pada subbab berikut melalui tabel *Black Box* yang berisi skenario, *input*, hasil yang diharapkan, hasil aktual, dan status pengujian.

4.3.2 Pengujian Login

Tabel 4.2 Pengujian Login

No.	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	Melakukan <i>login</i> dengan email serta password yang benar	Email dan password valid	Sistem memverifikasi pengguna lalu membuka halaman dashboard	Sistem berhasil menampilkan halaman dashboard	Berhasil
2.	Mencoba <i>login</i> menggunakan password yang tidak tepat	Email valid, password salah	Sistem memberikan notifikasi kesalahan dan pengguna tetap berada pada halaman login	Sistem menampilkan pesan kesalahan	Berhasil
3.	Melakukan <i>login</i> menggunakan email yang belum terdaftar	Email tidak terdaftar	Sistem menampilkan pesan kesalahan	Sistem menampilkan pesan kesalahan	Berhasil
4.	Mencoba <i>login</i> tanpa memasukkan email serta password	Kolom email dan password kosong	Sistem memberikan validasi bahwa kolom harus dilengkapi	Sistem menampilkan validasi	Berhasil

4.3.3 Pengujian Upload

Tabel 4. 3 Pengujian Upload

No .	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	Menguji pengunggahan dokumen pada format yang diperbolehkan	File PDF/DOC/DOCX/TXT/JPG/JPEG/PNG	Dokumen berhasil diunggah	Dokumen berhasil diunggah	Berhasil

No .	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
2.	Mengunggah dokumen melebihi batas ukuran	File > 10 MB	Sistem menolak proses upload dan menampilkan pesan kesalahan	Sistem memberikan pemberitahuan kesalahan	Berhasil
3.	Mengunggah file dengan format yang tidak didukung	File EXE	Sistem menolak file	Sistem menolak file	Berhasil
4.	Tidak memilih file	Tidak ada file	Sistem meminta pengguna memilih file	Sistem menampilkan validasi	Berhasil

4.3.4 Pengujian Enkripsi

Tabel 4.4 Pengujian Enkripsi

No.	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	Menjalankan enkripsi setelah proses unggah berhasil	File valid	Dokumen berhasil diproses dengan AES-256-CBC hingga menjadi terenkripsi	Dokumen berhasil dienkripsi	Berhasil
2.	Menampilkan Encryption Key	Proses enkripsi berhasil	Sistem menampilkan Encryption Key kepada pengguna	Sistem berhasil menampilkan Encryption Key	Berhasil
3.	Menyimpan dokumen terenkripsi	Proses enkripsi berhasil	Ciphertext disimpan pada media penyimpanan aplikasi	Sistem berhasil menyimpan dokumen dalam kondisi terenkripsi	Berhasil

No.	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
4.	Menyimpan metadata dokumen	Proses enkripsi berhasil	Metadata dan IV tersimpan pada basis data	Data metadata berhasil dicatat dalam basis data	Berhasil

4.3.5 Pengujian Dekripsi

Tabel 4.5 Pengujian Dekripsi

No.	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	Melakukan dekripsi dengan Encryption Key yang sesuai	Encryption Key valid	Dokumen berhasil dipulihkan lalu diunduh	Dokumen berhasil didekripsi dan diunduh	Berhasil
2.	Dekripsi menggunakan Encryption Key yang salah	Encryption Key tidak valid	Sistem menolak proses dekripsi dan menampilkan pesan kesalahan	Sistem memberikan notifikasi bahwa terjadi kesalahan	Berhasil
3.	Dekripsi tanpa mengisi Encryption Key	Kolom Encryption Key kosong	Sistem meminta pengguna mengisi Encryption Key	Sistem menampilkan validasi	Berhasil
4.	Dekripsi dokumen yang telah terenkripsi	Encryption Key valid	Isi dokumen yang diunduh sama dengan dokumen asli	Dokumen berhasil dikembalikan dan sesuai dengan berkas awal	Berhasil

4.3.6 Pengujian Penghapusan Dokumen

Tabel 4.6 Pengujian Penghapusan Dokumen

No.	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	Menjalankan penghapusan pada dokumen yang telah dipilih	Pengguna memilih tombol Hapus pada dokumen yang akan dihapus	Sistem menghilangkan dokumen dari daftar, database, serta ruang penyimpanannya	Dokumen berhasil dihapus dari sistem	Berhasil
2.	Membatalkan proses penghapusan	Pengguna memilih Batal pada dialog konfirmasi	Dokumen tetap tersimpan dan tidak terjadi penghapusan	Dokumen tetap tersedia pada sistem	Berhasil

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan tahapan perancangan, penerapan, dan pengujian yang telah dilaksanakan, maka dapat diperoleh beberapa kesimpulan sebagai berikut.

1. Penelitian ini menghasilkan aplikasi berbasis web untuk pengamanan dokumen digital yang dikembangkan menggunakan framework Laravel dan AES-256-CBC. Sistem yang dibangun mampu mengelola dokumen melalui fitur login, unggah dokumen, enkripsi, dekripsi, pengunduhan, dan penghapusan dokumen.
2. Implementasi algoritma AES-256-CBC berhasil diterapkan untuk mengamankan dokumen digital. Dokumen yang diunggah oleh pengguna secara otomatis dienkripsi sebelum disimpan ke media penyimpanan aplikasi, sehingga dokumen tidak tersimpan dalam bentuk asli (*plaintext*). Penggunaan Initialization Vector (IV) yang berbeda pada setiap proses enkripsi turut memberikan perlindungan tambahan terhadap data yang tersimpan.
3. Mekanisme pengelolaan *Encryption Key* berhasil diterapkan dengan menampilkan kunci enkripsi hanya satu kali setelah proses enkripsi selesai. Sistem tidak menyimpan kunci tersebut, sehingga proses dekripsi hanya dapat dilakukan oleh pengguna yang mempunyai *Encryption Key* yang tepat dan memperoleh kembali dokumen dalam bentuk aslinya.

4. Hasil pengujian dengan metode Black Box Testing menunjukkan bahwa seluruh fungsi utama sistem, yaitu proses login, unggah dokumen, enkripsi, dekripsi, pengunduhan, dan penghapusan dokumen, telah beroperasi sesuai dengan kebutuhan fungsional yang ditetapkan. Pengujian memperlihatkan bahwa keluaran sistem telah sesuai dengan skenario yang digunakan dalam pengujian.

5.2 Saran

Hasil penelitian ini juga memberikan beberapa rekomendasi yang dapat dipertimbangkan untuk pengembangan pada penelitian berikutnya, yaitu:

1. Pengembangan sistem selanjutnya dapat menambahkan mekanisme autentikasi yang lebih aman, seperti autentikasi dua tahap (*Two-Factor Authentication/2FA*), guna memperkuat perlindungan pada akses pengguna.
2. Pengembangan selanjutnya dapat menerapkan algoritma kriptografi hibrida, yaitu mengombinasikan algoritma simetris seperti AES dengan algoritma asimetris, sehingga proses distribusi dan pengelolaan kunci menjadi lebih aman.
3. Sistem dapat dikembangkan agar mendukung penyimpanan dokumen pada layanan *cloud storage* sehingga memudahkan proses pengelolaan dan pencadangan dokumen secara terpusat.
4. Penelitian selanjutnya dapat melakukan pengujian terhadap performa sistem, seperti durasi enkripsi dan dekripsi pada dokumen dengan ukuran yang beragam, sehingga dapat diketahui efisiensi implementasi algoritma AES-256-CBC pada aplikasi.

5. Sistem dapat dikembangkan dengan menambahkan fitur manajemen dokumen yang lebih lengkap, seperti pengelompokan dokumen berdasarkan kategori, pencarian dokumen, serta riwayat aktivitas pengguna (*activity log*) untuk meningkatkan kemudahan penggunaan dan keamanan sistem.

DAFTAR PUSTAKA

- Aditya, F., & Romli, M. A. (2025). Implementasi Metode Kriptografi Advanced Encryption Standard 256 Bit Berbasis Web dan Mobile Pada Pengamanan Dokumen Notaris. *Jurnal Terapan Informatika Nusantara*, 6(6), 707–714. <https://doi.org/10.47065/tin.v6i6.8637>
- Amanullah, S. (2025). *Implementasi Keamanan Data Berbasis Web Menggunakan Kombinasi Algoritma Secure Hash Algorithm 256 Dan Advanced Encryption Standard Cipher Block Chaining 256 Dengan Manajemen Database Firestore Pada Akun Website*.
- Ayu Pramesthi Wardhani, T. D., & Asriningtias, Y. (2023). Implementasi Algoritma AES-256 Dalam Perancangan Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android. *Journal of Information Technology and Computer Science (INTECOMS)*, 6(2), 1–5.
- Ayu Pramesthi Wardhani, T. D., & Asriningtias, Y. (2024). Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android Menggunakan Algoritma AES-256. *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, 12(1), 143–154. <https://doi.org/10.26418/justin.v12i1.71449>
- Baso, F., & Anriani L, N. (2024). Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File. *Journal: Information Technology Education Journal*, 3(3), 84–87.
- Binus University. (2024, September 14). *Bagaimana menyimpan data dengan aman di cloud?* Binus. <https://binus.ac.id/bekasi/2024/08/bagaimana-menyimpan-data-dengan-aman-di-cloud/>
- Donald. (2023). *Advanced Encryption Standard (AES)*. <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- Hayat Arka Putri, Z., Arye Yustraini, Y., Ariansyah, R., Choirun Nisa, N., Dyar Wahyuni, E., & Brastama Putra, A. (2025). Pengamanan Data Akademik Berbasis Web dengan Enkripsi AES-256 (Studi Kasus pada Pendataan Digital SMA XYZ). *Jurnal Nasional Teknologi Informasi Dan Aplikasinya*, 3(3), 2025.

- Indriyawati, H., Winarti, T., & Vydia, V. (2021). Web-Based Document Certification System With Advanced Encryption Standard Digital Signature. *Indonesian Journal of Electrical Engineering and Computer Science*, 22(1), 516–521. <https://doi.org/10.11591/ijeecs.v22.i1.pp516-521>
- Irvai, M., & Efranda, N. (2024). Optimalisasi Enkripsi File Menggunakan Algoritma Aes-256 Berbasis Web Dengan Integrasi Kompresi Adaptif. *Jurnal Ilmiah Betrik*, 15(3), 1–9.
- Kaaffah, F. M., Nugroho, N., Nurnaningsih, D., & Harriansyah. (2025). Sistem Enkripsi Dokumen Digital Melalui Kombinasi AES-128 dan Hashing SHA-256 Berbasis Salt. *Jurnal Ilmiah FIFO*, 17(1), 78–90. <https://doi.org/10.22441/fifo.2025.v17i1.009>
- Naqiyah, A., Hayati, L. N., & Faradibah, A. (2025). Implementasi Algoritma AES-256 Berbasis Web untuk Pengamanan Dokumen Digital di CV. Karya Eksklusif Nusantara. *Jurnal Ilmiah Informatika Komputer*, 30(3), 275–286. <https://doi.org/10.35760/ik.2025.v30i3.60>
- NIST. (2023). *Advanced Encryption Standard (AES)*. <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- Permana, A. A., Maulindar, J., & Hartanti, D. (2025). Implementasi Sistem Kriptografi Algoritma AES (256-bit) Berbasis Web API untuk Mengamankan Data Pribadi di CV. Elang Cahaya Sukses Surakarta. *Jurnal Teknik Informatika*, 4(2), 1.
- Purba, A. (2025, December 9). *RSA, AES, dan SHA-256 Pilar Keamanan Data di Dunia Digital 2020–2025*. Telkom University. <https://bse-sby.telkomuniversity.ac.id/rsa-aes-dan-sha-256-pilar-keamanan-data-di-dunia-digital-2020-2025/>
- Putra, J. S., Ardianto, R., & Purwono. (2024). Tinjauan Terhadap Implementasi Advanced Encryption Standard 256 Dalam Keamanan Data. *Journal Computer Science And Information Technology* |, 5(2), 335–355.
- Randy Fachrezi, M., Oldi Amsyah, dwiky, Syahputra, A., & Rusydi, I. (2026). Perancangan dan Implementasi Sistem Enkripsi Data Sensitif Menggunakan AES-

- 256-CBC pada Aplikasi Berbasis Web Sederhana. *Jurnal Ilmu Komputer Dan Teknik Informatika*, 2(1), 55–62. <https://doi.org/10.64803/juikti.v2i1.100>
- Reddy Penubadi, H., Shah, P., Sekhar, R., Alrasheedy, M. N., Niu, Y., Dheyaa Radhi, A., Tharwat, M., Fadhil Tawfeq, J., Muwafaq Gheni, H., & Shawkat Abdulbaqi, A. (2023). Sustainable Electronic Document Security: A Comprehensive Framework Integrating Encryption, Digital Signature And Watermarking Algorithms. *Original Research*, 5(2), 391–404. <https://doi.org/10.37868/hsd.v4i1.359>
- Ridho, A., & Ali Romli, M. (2024). Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256). *Jurnal Informatika Teknologi Dan Sains (JINTEKS)*, 6(4), 1.
- Surya, J., Louis, A., Rini, F., Mulyati, S., & Elzas. (2025). Cryptographic Framework For Cloud-Based Document Storage Using AES-256 and SHA-256 Hybrid Systems. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, 11(2), 535–549. <https://doi.org/10.33480/jitk.v11i2.7132>
- Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY. *Jurnal Teknik Informatika (Jutif)*, 1(2), 69–77. <https://doi.org/10.20884/1.jutif.2020.1.2.21>

LAMPIRAN

1. Berita Acara



Berita Acara Pembimbingan Skripsi

Nama Mahasiswa : Muhammad Asril Azmi
 NPM : 2209010100
 Program Studi : Sistem Informasi
 Judul Penelitian : RANCANG BANGUN SISTEM KEAMANAN PENYIMPANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB
 Nama Dosen Pembimbing : Rizaldy Khair, S.Kom., M.Kom

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
29-7-2026	1. Perbaikan pada latar belakang 2. Perbaikan pada rumusan masalah & tujuan penelitian 3. Perbaiki tabel penelitian terdahulu dan menambahkan research gap	
3-8-2026	Revisi Bab 2 -Menambahkan teori tentang flowchart dan UMM/Use Case Revisi Bab 3 -Menambahkan arsitektur sistem dan gambar arsitektur sistem	
4-8-2026	Revisi -Perbaiki nomor halaman	
5-8-2026	Revisi Bab 2 -Menambahkan Tabel UML seperti tabel pada flowchart dan menjelaskan keterangan icon pada bab 2 Revisi Bab 3 -Perbaiki gambar flowchart	
5-8-2026	Rapihkan daftar pustaka	
7-8-2026	Revisi pada exhibition -Menambahkan tampilan output pada saat file di enkripsi	
13-8-2026	Revisi -Perbaiki semua tabel di bab 2,3,4	
14-8-2026	ACC SIDANG	



UMSU

Unggul | Cerdas | Terpercaya

Bila diperlukan untuk keperluan dokumentasi
nama dan tanggalnya

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

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

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

<https://fktis.umsu.ac.id>

fktis@umsu.ac.id

[fktisumsu](#)

[umsu](#)

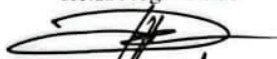
[umsu](#)

[umsu](#)

Medan, ...

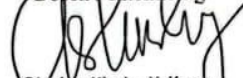
Diketahui oleh :

Ketua Program Studi


(Makhsudulca)

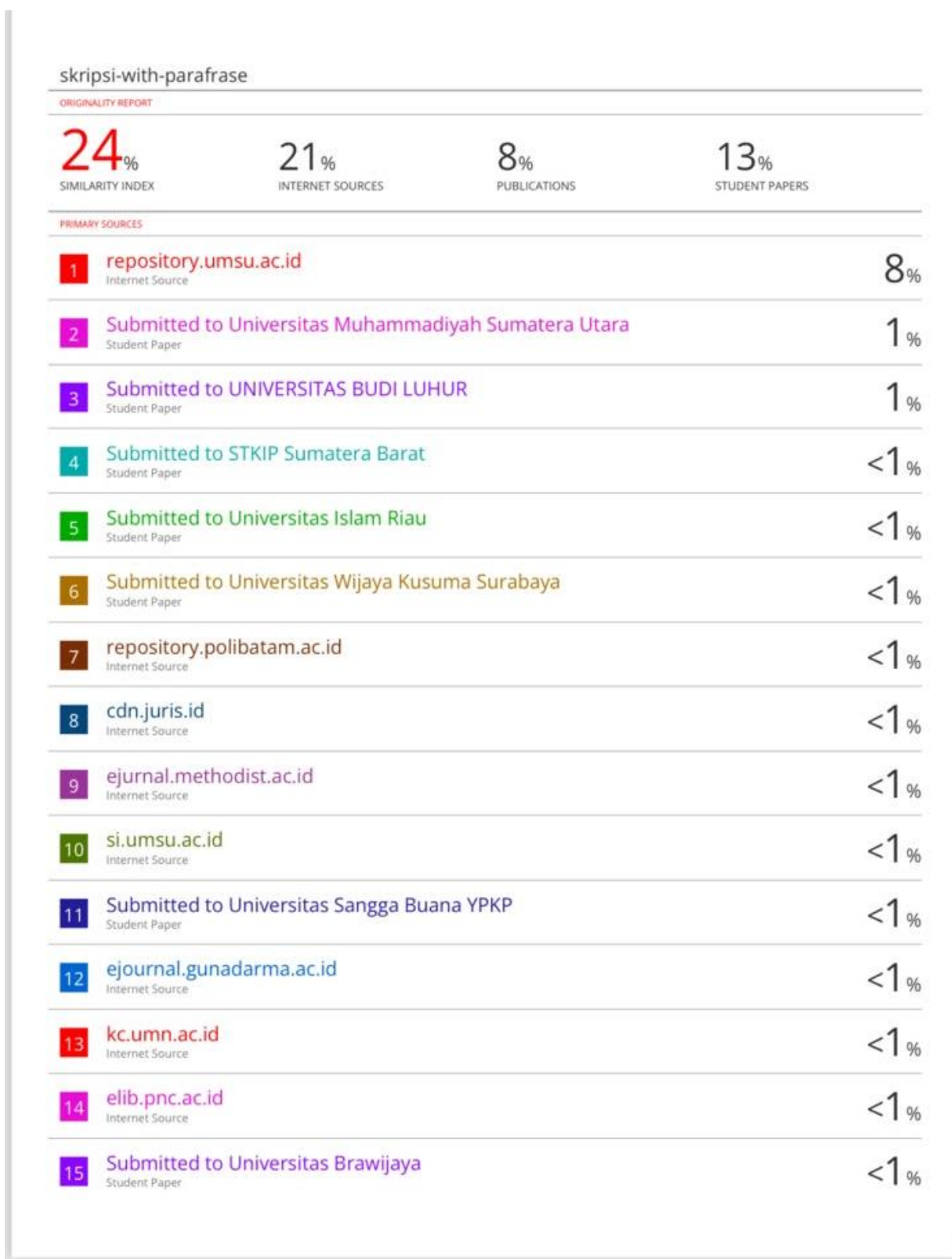
Disetujui oleh :

Dosen Pembimbing


Bizalzy Khair, M.Kom



2. Turnitin



3. Formulir Perbaikan Sidang



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
 UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BSN-PT/Ja-Ppy/PT/BB/2024
 Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
 Email: info@umsu.ac.id Website: umsu.ac.id Instagram: @umsuamedan Facebook: umsumedan Twitter: umsumedan YouTube: umsumedan

FORMULIR PERBAIKAN UJIAN SKRIPSI

Pada hari ini, Kamis 27 Agustus 2026 telah dilaksanakan Ujian Skripsi bagi mahasiswa Fakultas Ilmu Komputer Dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Sbb:

Nama Mahasiswa : Muhammad Asril Azmi
 NPM : 2209010100
 Program Studi : Sistem Informasi
 Judul Proposal : Rancang Bangun Sistem Keamanan Penyimpanan Dokumen Digital Menggunakan Algoritma Aes-256 Berbasis Web

Materi/Point yang Diperbaiki :

		Paraf
Rizaldy Khair, M.Kom	ok, lanjutkan publikasi	
Martiano, S.Kom., M.Kom.	OK	
Fatma Sari Hutagalung, S.Kom., M.Kom	ok	

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

4. LoA Jurnal



Indonesian Journal of Multidisciplinary Scientific Studies

E-ISSN: 2988-7046

Sekretariat: STAI Raudhatul Akmal, Jln. Nusa Indah Gg. Melati No. 66, Batang Kuis, 20372

<https://ojs.staira.ac.id/index.php/IJOMSS/index>

Deli Serdang, 22 September 2026

No : 015/IJOMSS/LoA/IX/2026
Lamp : -
Hal : Surat Penerimaan Naskah Jurnal

Kepada Yth.
Para Penulis
di Tempat

Letter of Accepted (LOA)

Terima kasih telah mengirimkan naskah anda ke **Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS)** dengan data sebagai berikut:

Penulis	Judul
1. MUHAMMAD ASRIL AZMI	<i>SISTEM KEAMANAN PENYIMPANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB</i>
2. RIZALDY KHAIR	

Berdasarkan hasil review akhir yang telah kami lakukan, dengan ini dinyatakan bahwa Paper tersebut **Telah dinyatakan DITERIMA** untuk dipublikasi pada **Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS)**.

Demikian surat penerimaan ini kami sampaikan. Atas perhatian dan kerja sama yang baik, kami ucapkan terima kasih.

Hormat Kami,



Dr. Muhammad Azhari, M.Pd
Editor in Chief

INDEX COPERNICUS
INTERNATIONAL

GARUDA
AKSI RUDRA DIGITAL

Google
Scholar

BASE