



**IMPLEMENTASI ENKRIPSI AES-256 DENGAN MEKANISME
MASTER KEY PADA SERVER CLOUD BERBASIS
OWNCLOUD**

**TUGAS AKHIR
APLIKATIF**

**MUHAMAD ADRIAN
41522010071**

**UNIVERSITAS
MERCU BUANA**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026**



**IMPLEMENTASI ENKRIPSI AES-256 DENGAN MEKANISME
MASTER KEY PADA SERVER CLOUD BERBASIS
OWNCLOUD**

**TUGAS AKHIR
APLIKATIF**

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

**UNIVERSITAS
MERCU BUANA**
MUHAMAD ADRIAN
41522010071

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026**

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Muhamad Adrian
NIM : 41522010071
Program Studi : Fakultas Ilmu Komputer / Teknik Informatika

Menyatakan dengan sebenar-benarnya bahwa Tugas Akhir berjudul:

" Implementasi Enkripsi *AES-256* Dengan Mekanisme *Master Key* pada server Cloud Berbasis *OwnCloud* " adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Jakarta, 31 Juli 2026



Muhamad Adrian

PERNYATAAN SIMILARITY CHECK
/SIMILARITY CHECK STATEMENT

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh
/The undersigned, hereby declare that the scientific work written by

Nama /Name : Muhamad Adrian
NIM /Student ID Number : 41522010071
Program Studi /Study Program : Teknik Informatika

Dengan Judul Tugas Akhir

/The title:

“Implementasi Enkripsi AES-256 Dengan Mekanisme Master Key pada server Cloud Berbasis OwnCloud”

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:

/Similarity checks have been carried out with the Turnitin system on the date:

24 Juli 2026

dengan nilai persentase sebesar :

/with a percentage value of:

12%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

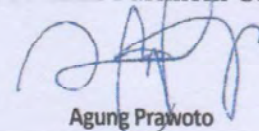
File hasil cek *similarity* turnitin:

/Turnitin similarity report file

https://drive.google.com/file/d/1XJ1Swoydu54_d3u3qP-oacqhvs9swUrU/view?usp=drive_link



Jakarta, 24 Juli 2026
Admin Turnitin Fasilkom UMB



Agung Prawoto, S.Kom., B.Sc
NIK : 322970503

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : MUHAMAD ADRIAN
NIM : 41522010071
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Tugas Akhir : Implementasi Enkripsi *AES-256* Dengan Mekanisme *Master Key* pada server Cloud Berbasis *OwnCloud*

Telah berhasil dipertahankan pada sidang tanggal 31 Juli 2026 dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh :
Pembimbing

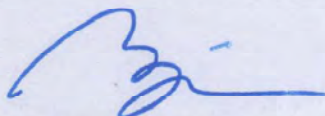
Dr. Andi Nugroho, S.T., M.Kom.

NIDN/NUPTK: 0305098303

Jakarta, 31 Juli 2026

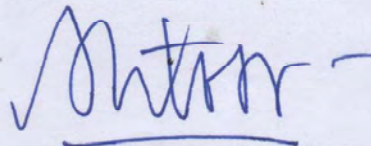
Mengetahui,

Dekan Fakultas Ilmu Komputer



Dr. Bambang Jokonowo, S.Si., MTI
NIDN/NUPTK: 0320037002

Ketua Program Studi
Teknik Informatika



Dr. Hadi Santoso, S.Kom., M.Kom
NIDN/NUPTK: 0225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Informatika pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Tugas Akhir ini, sangatlah sulit bagi saya untuk menyelesaikan Tugas Akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Dr. Andi Nugroho, ST, M.Kom. selaku dosen pembimbing Tugas Akhir yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan proposal penelitian ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensupport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 31 Juli 2026

Muhamad Adrian

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : MUHAMAD ADRIAN
NIM : 41522010071
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Laporan Skripsi : Implementasi Enkripsi AES-256 Dengan
Mekanisme Master Key pada server Cloud
Berbasis OwnCloud

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 31 Juli 2026

Yang menyatakan ,



Muhamad Adrian

IMPLEMENTASI ENKRIPSI AES-256 DENGAN MEKANISME MASTER KEY PADA SERVER CLOUD BERBASIS OWNCLOUD

MUHAMAD ADRIAN

ABSTRAK

Kebutuhan akan penyimpanan data yang mandiri, aman, dan kolaboratif menjadi prioritas utama bagi organisasi yang mengelola informasi sensitif dalam jaringan lokal. Penelitian ini bertujuan mengimplementasikan sistem *private cloud storage* berbasis *ownCloud* yang mengintegrasikan enkripsi berlapis dan *collaborative editing* secara simultan menggunakan metode PPDIOO. Keamanan data diterapkan melalui dua mekanisme: *server-side encryption* berbasis *Master Key ownCloud* untuk melindungi data di sisi server, serta enkripsi kustom AES-256-CBC pada fitur *Download Encrypted* dan *Upload Encrypted* untuk melindungi data di sisi klien. Manajemen pengguna diterapkan menggunakan *Role Based Access Control (RBAC)* dengan 5 grup dan 20 akun, sedangkan *collaborative editing* disediakan melalui integrasi Collabora Online berbasis Docker pada server terpisah. Hasil pengujian menunjukkan seluruh fitur berjalan sesuai kebutuhan fungsional dengan rata-rata *response time* upload dan download normal sebesar 133–172 ms dan *error rate* 0,00%. Operasi enkripsi kustom membutuhkan waktu rata-rata 1,20–1,53 detik dengan penggunaan CPU tertinggi 52,75%, namun masih dalam batas kapasitas server. Sistem yang dikembangkan terbukti layak sebagai solusi penyimpanan berbasis cloud yang aman, fungsional, dan mendukung kolaborasi dokumen secara *real-time* untuk lingkungan multi-pengguna.

Kata Kunci: *Private cloud storage*, *ownCloud*, AES-256, RBAC, Collabora Online, PPDIOO

IMPLEMENTATION OF AES-256 ENCRYPTION WITH A MASTER KEY MECHANISM ON AN OWN CLOUD-BASED CLOUD SERVER

MUHAMAD ADRIAN

ABSTRACT

The need for independent, secure, and collaborative data storage has become a primary concern for organizations managing sensitive information within local networks. This study aims to implement a private cloud storage system based on ownCloud that simultaneously integrates layered encryption and collaborative editing using the PPDIOO method. Data security was implemented through two mechanisms: server-side encryption using ownCloud's Master Key to protect data at the server level, and a custom AES-256-CBC encryption scheme for the Download Encrypted and Upload Encrypted features to protect data at the client side. User management was implemented using Role Based Access Control (RBAC) with 5 groups and 20 accounts, while collaborative editing was provided through Collabora Online deployed via Docker on a separate server. Testing results confirmed that all features operated according to functional requirements, with average response times of 133–172 ms for normal upload and download operations and a 0.00% error rate. Custom encryption operations required an average of 1.20–1.53 seconds with a peak CPU usage of 52.75%, remaining within the server's capacity threshold. The developed system is proven suitable as a secure, functional, and real-time collaborative cloud storage solution for multi-user environments.

Kata Kunci: Private cloud storage, ownCloud, AES-256, RBAC, Collabora Online, PPDIOO

DAFTAR ISI

HALAMAN SAMPUL	0
HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN KARYA SENDIRI.....	ii
HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN	iii
HALAMAN PENGESAHAN.....	iv
KATA PENGANTAR	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB.....	vi
ABSTRAK	vii
ABSTRACT.....	viii
DAFTAR ISI	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	4
1.5 Batasan Penelitian	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Penelitian Terdahulu	6
2.2 Teori Pendukung.....	10
2.2.1 <i>Cloud computing</i>	10
2.2.2 <i>Private cloud storage</i>	11
2.2.3 Keamanan Informasi	12
2.2.4 <i>ownCloud</i>	13
2.2.4.1 Perbandingan <i>ownCloud</i> dengan <i>Nextcloud</i>	14
2.2.5 Advanced Encryption Standard (AES-256).....	15

2.2.6 Docker	16
2.2.7 Collabora Online	16
2.2.8 Metode PPDIOO	17
BAB III METODE PENELITIAN	19
3.1 Jenis Penelitian	19
3.2 Tahapan Penelitian.....	20
3.2.1 Prepare (Persiapan)	21
3.2.2 Plan (Perencanaan)	21
3.2.3 Design (Perancangan)	23
3.2.4 Implement (Implementasi).....	25
3.2.5 Operate (Operasional).....	26
3.2.6 Optimize (Optimasi)	27
BAB IV HASIL DAN PEMBAHASAN.....	29
4.1 Gambaran Umum Sistem	29
4.2 Implementasi <i>OwnCloud</i> Server	30
4.3 Implementasi AES 256 Encryption	38
4.3.1 Aktivasi Enkripsi <i>ownCloud</i>	38
4.3.2 Permasalahan Upload File Setelah Enkripsi Aktif.....	39
4.3.3 Konfigurasi OpenSSL Legacy Provider	40
4.3.4 Pengujian dan Verifikasi Enkripsi <i>Master Key</i>	41
4.4 Implementasi AES-256-CBC Kustom.....	42
4.4.1 Implementasi Fitur <i>Download Encrypted</i> dan <i>Upload Encrypted</i>	43
4.4.2 Implementasi Proses Enkripsi AES-256-CBC.....	44
4.4.3 Hasil File Terenkripsi.....	45
4.4.4 Implementasi Proses Dekripsi AES-256-CBC	46
4.4.5 Pengujian Restore File	47
4.4.6 Pengujian Enkripsi–Dekripsi Berbagai Jenis dan Ukuran Berkas.....	48
4.5 Implementasi Collabora Online.....	51
4.5.1 Instalasi Collabora Online menggunakan Docker	52
4.5.2 Integrasi Collabora Online dengan <i>ownCloud</i>	52
4.5.3 Hasil Integrasi dan Pengujian Collabora Online.....	53
4.6 Implementasi Manajemen <i>User</i> dan Hak Akses.....	54

4.6.1 Implementasi Group <i>User</i> pada <i>OwnCloud</i>	55
4.6.2 Implementasi <i>User</i> dan Role Hierarchy.....	56
4.6.3 Implementasi Hak Akses Dokumen.....	58
4.6.4 Pengujian Hak Akses Pengguna	60
4.7 Evaluasi Keseluruhan Sistem	63
4.7.1 Analisis Pemilihan Arsitektur Dua <i>Virtual machine</i>	64
4.7.2 Pengujian Fungsionalitas Sistem	65
4.7.3 Pengujian Keamanan Enkripsi.....	67
4.7.3.1 Pengujian Keamanan Mekanisme <i>Master Key</i>	70
4.7.4 Pengujian Performa Upload dan Download menggunakan JMeter.....	75
4.7.4.1 Pengujian Upload dan Download Normal menggunakan JMeter	75
4.7.4.2 Pengujian <i>Upload Encrypted</i> dan <i>Download Encrypted</i> menggunakan Browser DevTools	79
4.7.5 Pengujian Beban Server menggunakan Netdata.....	82
4.7.6 Pengujian <i>Collaborative editing</i>	86
4.7.7 Pengujian Integritas Data Menggunakan SHA-256	88
BAB V KESIMPULAN DAN SARAN	91
5.1 Kesimpulan.....	91
5.2 Saran.....	92
DAFTAR PUSTAKA.....	94
LAMPIRAN.....	99

DAFTAR TABEL

Tabel 2. 1 Ringkasan Penelitian Terdahulu.....	6
Tabel 3. 1 Spesifikasi Perangkat Host.....	22
Tabel 3. 2 Spesifikasi Virtual machine ownCloud Server.....	22
Tabel 3. 3 Spesifikasi Virtual machine Collabora Server.....	23
Tabel 3. 4 Pembagian IP Address Tiap Lokasi.....	25
Tabel 3. 5 Rencana Skenario Pengujian Sistem	26
Tabel 3. 6 Kriteria Keberhasilan Sistem	27
Tabel 4. 1 Spesifikasi VM ownCloud server.....	30
Tabel 4. 2 Spesifikasi VM collabora server	30
Tabel 4. 3 Tabel pengujian enkripsi - Dekripsi.....	49
Tabel 4. 4 Distribusi User Sistem.....	55
Tabel 4. 5 Matriks Hak Akses Sistem	58
Tabel 4. 6 Hasil Pengujian Hak Akses	60
Tabel 4. 7 Perbandingan Implementasi Satu VM dan Dua VM.....	65
Tabel 4. 8 Hasil Pengujian Fungsionalitas Sistem	66
Tabel 4. 9 Konfigurasi Pengujian JMeter via WebDAV	76
Tabel 4. 10 Skenario Pengujian menggunakan JMeter.....	76
Tabel 4. 11 Hasil Pengujian Performa Upload dan Download menggunakan Jmeter	77
Tabel 4. 12 Skenario Pengujian Upload Encrypted dan Download Encrypted.....	79
Tabel 4. 13 Hasil Pengujian Upload Encrypted dan Download Encrypted menggunakan Browser DevTools	80
Tabel 4. 14 Konfigurasi Pemantauan Beban Server menggunakan Netdata.....	83
Tabel 4. 15 Skenario Pengujian Beban Server	83
Tabel 4. 16 Hasil Pemantauan Beban Server menggunakan Netdata	84
Tabel 4. 17 Hasil Pengujian Collaborative editing.....	87
Tabel 4. 18 Hasil Pengujian Integritas Data Menggunakan SHA-256.....	88

DAFTAR GAMBAR

Gambar 2. 1 Cloud Service Models [19]	11
Gambar 2. 2 CIA Triad Diagram [24]	12
Gambar 2. 3 OwnCloud Architechture	13
Gambar 2. 4 AES Encryption Process[26]	15
Gambar 2. 5 Arsitektur dan Komponen Utama Docker [29]	16
Gambar 2. 6 PPDIOO Life Cycle Program [30]	17
Gambar 3. 1 Kerangka Pemikiran Penelitian (Research Framework)	20
Gambar 3. 2 Topologi Jaringan	24
Gambar 4. 1 Hasil setting virtual machine OwnCloud	31
Gambar 4. 2 Proses Instalasi Ubuntu	32
Gambar 4. 3 Proses instalasi apache2	33
Gambar 4. 4 Proses Instalasi MariaDb	33
Gambar 4. 5 Proses Instalasi PHP	34
Gambar 4. 6 Proses Instalasi OwnCloud	35
Gambar 4. 7 Proses Konfigurasi database ownCloud	35
Gambar 4. 8 Proses Konfigurasi Apache Virtual Host	36
Gambar 4. 9 Mengkoneksikan database mariadb ke ownCloud	37
Gambar 4. 10 Tampilan awal ownCloud	37
Gambar 4. 11 Proses pengaktifan enkripsi ownCloud	39
Gambar 4. 12 Permasalahan upload file di ownCloud	40
Gambar 4. 13 Proses aktivafi legacy provider openssl	41
Gambar 4. 14 Tampilan file yang terenripsi	42
Gambar 4. 15 Tampilan modifikasi interface ownCloud	44
Gambar 4. 16 Proses implementasi encryption	45
Gambar 4. 17 Tampilan file yang berhasil di enkripsi	46
Gambar 4. 18 Proses implementasi decryption	47
Gambar 4. 19 Hasil file yang telah terdekripsi	48
Gambar 4. 20 Hasil Percobaan Akses Langsung Berkas Terenkripsi pada Direktori Storage Server	50

Gambar 4. 21 Tampilan Berkas Hasil Restorasi/Dekripsi yang Kembali Utuh pada Interface ownCloud.....	50
Gambar 4. 22 Hasil seting virtual machine server Collabora Online	51
Gambar 4. 23 Proses installasi collabora	52
Gambar 4. 24 Proses integrasi collabora ke ownCloud	53
Gambar 4. 25 Tampilan file yang dibuka dengan collabora online	54
Gambar 4. 26 Tampilan Daftar Group User pada ownCloud.....	56
Gambar 4. 27 Implementasi Akun User pada ownCloud.....	57
Gambar 4. 28 Konfigurasi Group Admin For pada User admin dan Dosen1	58
Gambar 4. 29 Konfigurasi Sharing Permission Folder pada ownCloud.....	59
Gambar 4. 30 Tampilan Hak Akses Read only pada User Guest.....	60
Gambar 4. 31 Pengujian Upload File pada Folder Shared oleh User Guest	61
Gambar 4. 32 Pengujian Collaborative editing Multi-user	62
Gambar 4. 33 Pengujian Permission denied pada Folder Admin.....	62
Gambar 4. 34 Hasil Pengujian pada Direktori Encryption Key Menggunakan User Non-Admin	63
Gambar 4. 35 Hasil Percobaan Akses Langsung File pada Direktori Storage Server	68
Gambar 4. 36 Hasil Percobaan Membuka File .encrypted menggunakan LibreOffice.....	69
Gambar 4. 37 Hasil Upload Encrypted yang tidak valid	70
Gambar 4. 38 Proses mengubah password di file upload_chiper.PHP	71
Gambar 4. 39 Gagal memproses dekripsi file.....	71
Gambar 4. 40 Sistem menolak request disable enkripsi	72
Gambar 4. 41 Lokasi direktori Master Key	73
Gambar 4. 42 Hasil Pemeriksaan Hak Akses Master Key	73
Gambar 4. 43 Hasil Backup Master Key	74
Gambar 4. 44 Hasil Simulasi Restore Master Key	74
Gambar 4. 45 Tampilan Laporan Summary Report JMeter Hasil Pengujian Performa.....	78
Gambar 4. 46 Tampilan Browser DevTools saat Pengujian Upload Encrypted ...	81

Gambar 4. 47 Tampilan Browser DevTools saat Pengujian Download Encrypted	82
Gambar 4. 48 Tampilan Dashboard Netdata Pemantauan Beban Server pada Kondisi Upload Encrypted.....	86
Gambar 4. 49 Pengujian Sinkronisasi Real-time pada Dua Sesi Collaborative editing.....	87
Gambar 4. 50 Hasil Perhitungan Nilai SHA-256.....	89



DAFTAR LAMPIRAN

Lampiran 1 Kartu Asistensi.....	99
Lampiran 2 Curriculum Vitae	100
Lampiran 3 Surat Pernyataan & Pengalihan HAKI	101
Lampiran 4 Script Instalasi	103

