OPTIMALISASI KEAMANAN DATA MENGGUNAKAN HYBRID ENKRIPSI AES 256-BIT DAN ECC PADA RASPBERRY PI GENERASI 5 BERBASIS API

AFIDZ ACHMAD
NOVENDI

55423110003

PROGRAM STUDI TEKNIK ELEKTRO
MAGISTER TEKNIK ELEKTRO
UNIVERSITAS MERCU BUANA
JAKARTA 2025

SURAT KETERANGAN HASIL *SIMILARITY*

Menerangkan bahwa Karya Ilmiah/Laporan Tugas Akhir/Skripsi pada BAB I, BAB II, BAB III, BAB IV dan BAB V atas nama:

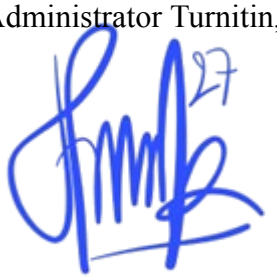
Nama	**:**	**Afidz Achmad Novendi**
NIM	**:**	**55423110003**
Program Studi	**:**	**Magister Teknik Elektro**
Judul Tugas Akhir / Tesis / Praktek Keinsinyuran	**:**	**OPTIMALISASI KEAMANAN DATA MENGGUNAKAN HYBRID ENKRIPSI AES 256-BIT DAN ECC PADA RASPBERRY PI GENERASI 5 BERBASIS API**

Telah dilakukan pengecekan *Similarity* menggunakan aplikasi/sistem *Turnitin* pada **Kamis, 7 Agustus 2025** dengan hasil presentase sebesar **19 %** dan dinyatakan memenuhi standar sesuai dengan ketentuan yang berlaku di Fakultas Teknik Universitas Mercu Buana.

Demikian surat keterangan ini dibuat dan digunakan sebagaimana mestinya.

Jakarta, 7 Agustus 2025

Administrator Turnitin,



Itmam Haidi Syarif

HALAMAN PENGESAHAN

Laporan Skripsi / Tesis ini diajukan oleh :

Nama	:	Afidz Achmad Novendi
NIM	:	55423110003
Program Studi	:	Magister Teknik Elektro
Judul Skripsi / Tesis	:	OPTIMALISASI KEAMANAN DATA MENGGUNAKAN HYBRID ENKRIPSI AES 256-BIT DAN ECC PADA RASPBERRY PI GENERASI 5 BERBASIS API

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Strata S2 pada Program Studi Magister Teknik Elektro, Fakultas Teknik Universitas Mercu Buana.

Disahkan Oleh :

Pembimbing	:	Fadli Sirait, S.Si, M.T, Ph.D	( )
NIDN	:	0320057603	
Ketua Penguji	:	Yudhi Gunardi, S.T., M.T., Ph.D	( )
NIDN	:	0330086902	
Anggota Penguji	:	Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., I.P.U., Asean-Eng., APEC-Eng	( )
NIDN	:	0312118206	

Jakarta, 4 Agustus 2025

Mengetahui,

Dekan	Ketua Program Studi
Fakultas Teknik	Magister Teknik Elektro
Dr. Zulfa Fitri Ikatrinasari, MT	Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., I.P.U., Asean-Eng., APEC-Eng

HALAMAN PERNYATAAN KARYA SENDIRI

Yang bertanda tangan di bawah ini :

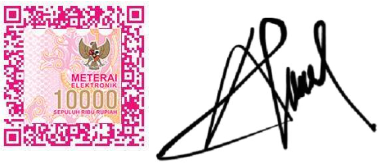
Nama Lengkap	: Afidz Achmad Novendi
NIM	: 55423110003
Tempat/Tanggal Lahir	: Semarang, 3 November 1995
Program Studi	: Magister Teknik Elektro

Dengan ini menyatakan bahwa karya dengan judul "OPTIMALISASI KEAMANAN DATA MENGGUNAKAN HYBRID ENKRIPSI AES 256-BIT DAN ECC PADA RASPBERRY PI 5 BERBASIS API" adalah hasil karya sendiri dan belum pernah dipublikasikan serta belum pernah diikutsertakan dalam perlombaan di tingkat Regional, Nasional atau Internasional sebelumnya serta tidak mengandung unsur plagiat di dalamnya.

Demikianlah pernyataan ini dibuat dalam keadaan sadar dan tanpa ada unsur paksaan dari siapapun. Jika di kemudian hari ditemukan ketidakbenaran informasi, maka saya bersedia mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 24 Juli 2025

Yang menyatakan,



Afidz Achmad Novendi

KATA PENGANTAR

Puji syukur Alhamdulillah, penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga pada akhirnya penulis dapat menyelesaikan penulisan laporan tesis ini dengan baik. Laporan tesis ini penulis sajikan dalam bentuk buku yang sederhana. Adapun judul penulisan dari tesis ini adalah **:**

"OPTIMALISASI KEAMANAN DATA MENGGUNAKAN HYBRID ENKRIPSI AES 256-BIT DAN ECC PADA RASPBERRY PI 5 BERBASIS API"

Tujuan penulisan laporan tesis ini dibuat sebagai salah satu syarat kelulusan Program Strata Dua (S2) Magister Teknik Elektro Universitas Mercu Buana. Penulis menyadari bahwa tanpa bimbingan dan dorongan beberapa pihak, maka penulisan laporan tesis ini tidak akan lancar. Oleh karena itu pada kesempatan ini, ijinkanlah penulis menyampaikan ucapan terima kasih kepada :

1. Rektor Universitas Mercu Buana Bapak Prof. Dr. Andi Adriansyah, M.Eng.
2. Dekan Fakultas Teknik Universitas Mercu Buana Ibu Dr. Zulfa Fitri Ikatrinasari, MT
3. Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana Bapak Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., I.P.M., Asean-Eng., APEC-Eng
4. Bapak Fadli Sirait, S.Si, MT, Ph.D, selaku Dosen Pembimbing Tesis.
5. Staff / karyawan / dosen di lingkungan Universitas Mercu Buana.
6. Orang tua, keluarga dan teman-teman yang telah memberikan dukungan moral maupun spiritual.

Serta semua pihak yang terlalu banyak untuk disebut satu persatu sehingga terwujudnya penulisan ini. Penulis menyadari bahwa penulisan laporan tesis ini masih jauh dari sempurna, untuk itu penulis mohon kritik dan saran yang bersifat membangun demi kesempurnaan penulisan dimasa yang akan datang.

Akhir kata semoga laporan tesis ini dapat berguna bagi penulis khususnya dan bagi para pembaca yang berminat pada umumnya.

Jakarta, 24 Juli 2025

Afidz Achmad Noven

Abstrak

Di era digital modern, keamanan data menjadi prioritas utama seiring dengan meningkatnya intensitas serangan siber yang menargetkan berbagai jenis informasi, baik bersifat pribadi maupun organisasi. Penelitian ini bertujuan untuk meningkatkan keamanan data melalui pengembangan sistem enkripsi hybrid yang menggabungkan algoritma Advanced Encryption Standard (AES) 256-bit dalam mode Cipher Block Chaining (CBC) dan Elliptic Curve Cryptography (ECC). Dalam sistem ini, AES digunakan untuk mengenkripsi data utama karena kecepatan, efisiensi serta kehandalannya, sementara ECC berperan dalam mengenkripsi kunci AES sebelum didistribusikan guna memperkuat keamanan pada proses pertukaran kunci. Prototipe sistem dikembangkan pada perangkat Raspberry Pi generasi 5, yang dikenal sebagai perangkat berdaya rendah namun populer dalam pengembangan aplikasi Internet of Things (IoT). Sistem diimplementasikan dalam bentuk layanan berbasis Application Programming Interface (API) menggunakan framework Lumen dan diuji menggunakan file data berformat PDF dengan berbagai ukuran untuk mengevaluasi performa, integritas data, serta ketahanan terhadap serangan. Pengujian dilakukan termasuk simulasi serangan Man-in-the-Middle (MITM) menggunakan metode sniffing. Hasil penelitian menunjukkan bahwa Raspberry Pi 5 mampu menjalankan algoritma hybrid ini secara efisien. Proses enkripsi dan dekripsi berjalan otomatis melalui API tanpa intervensi manual, dan pertukaran kunci berhasil diamankan dari serangan MITM. Sistem juga menunjukkan performa yang stabil dan efisien untuk ukuran data hingga 160 KB, dengan waktu pemrosesan yang baik. Dengan pendekatan ini, sistem enkripsi hybrid tidak hanywa memperkuat keamanan distribusi kunci, tetapi juga dapat diimplementasikan secara praktis tanpa perlu modifikasi besar pada infrastruktur yang ada. Hal ini menjadikannya relevan untuk berbagai aplikasi berbasis IoT maupun sistem tertanam lainnya.

Kata kunci: AES-256-CBC, Elliptic Curve Cryptography, Raspberry Pi 5, enkripsi hybrid, API, IoT, Man-in-the-Middle

Abstract

In the modern digital era, data security has become a top priority due to the increasing frequency of cyberattacks targeting various types of information, whether personal or organisational. This study aims to enhance data security by developing a hybrid encryption system that combines the Advanced Encryption Standard (AES) 256-bit algorithm in Cipher Block Chaining (CBC) mode with Elliptic Curve Cryptography (ECC). In this system, AES is employed to encrypt the primary data due to its speed, efficiency, and reliability, while ECC is used to encrypt the AES key before distribution, thereby strengthening the security of the key exchange process. The system prototype was developed on a Raspberry Pi 5, a low-power device widely used in the development of Internet of Things (IoT) applications. The system was implemented as a service-based Application Programming Interface (API) using the Lumen framework and tested with PDF files of varying sizes to evaluate performance, data integrity, and resilience against attacks. Testing included a simulation of a Man-in-the-Middle (MITM) attack using data sniffing techniques. The results demonstrate that the Raspberry Pi 5 can efficiently execute the hybrid encryption algorithm. The encryption and decryption processes run automatically via the API without manual intervention, and the key exchange is successfully protected against MITM attacks. The system also exhibited stable and efficient performance for data sizes up to 160 KB, with processing times remaining within acceptable operational limits. This hybrid encryption approach not only strengthens key distribution security but also allows for practical implementation without major modifications to existing infrastructure, making it highly relevant for various IoT-based or embedded system applications.

Keywords: AES-256-CBC, Elliptic Curve Cryptography, Raspberry Pi 5, hybrid encryption, API, IoT, Man-in-the-Middle

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL