SENAFTI SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 Maret 2025 – Jakarta, Indonesia
Volume 4, Nomor 1, Maret 2025 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITMA AES-CBC DAN AES-GCM UNTUK PENGAMANAN DOKUMEN

Leonard Reinhard Roscott[1*], Subandi[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]1811502051@student.budiluhur.ac.id, [2]subandi@budiluhur.ac.id
(* : corresponding author)

Abstrak - Keamanan data menjadi prioritas utama bagi institusi yang mengelola informasi sensitif, seperti sebuah gereja yang menyimpan dokumen pribadi jemaat. Saat ini, sistem keamanan digital yang ada masih rentan terhadap kebocoran dan penyalahgunaan data. Untuk mengatasi masalah ini, penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan dokumen berbasis web. Sistem ini menggunakan kombinasi dua algoritma enkripsi simetris, yaitu AES-CBC (*Cipher Block Chaining*) dan AES-GCM (*Galois/Counter Mode*). Penggunaan kombinasi ini bertujuan untuk menciptakan perlindungan ganda melalui difusi blok data dan autentikasi integritas. Metodologi penelitian menggunakan model *Waterfall* yang mencakup analisis kebutuhan, perancangan, implementasi, dan pengujian. Sistem dikembangkan menggunakan platform *Node.js* dengan menerapkan proses enkripsi ganda (*AES-CBC* lalu *AES-GCM*) serta dilengkapi pengaturan hak akses pengguna. Hasil penelitian menunjukkan bahwa sistem yang dibangun berhasil melakukan enkripsi dan dekripsi secara akurat, menjaga kerahasiaan dan integritas dokumen. Implementasi sistem ini juga mempermudah pengelolaan data oleh pengurus dan jemaat. Pengujian dengan metode *black-box testing* membuktikan keberhasilan 100% tanpa adanya kegagalan dalam seluruh skenario uji. Penelitian ini menyimpulkan bahwa kombinasi AES-CBC dan AES-GCM efektif dalam menjaga keamanan data digital dan dapat menjadi referensi untuk pengembangan sistem serupa.

Kata Kunci: Keamanan data, AES-CBC, AES-GCM, Enkripsi, Node.js.

IMPLEMENTATION OF AES-CBC AND AES-GCM ALGORITHMS FOR SECURING CHURCH DOCUMENTS

Abstract- *Data security is a critical aspect of maintaining information confidentiality and integrity, particularly for institutions like a church that manages sensitive personal documents. The existing system lacks a sufficient digital security framework, making it vulnerable to data breaches and misuse. This research aims to design and implement a web-based digital document security system using a combination of two symmetric encryption algorithms: AES-CBC (Cipher Block Chaining) and AES-GCM (Galois/Counter Mode). This combination was chosen to leverage the strengths of both algorithms, namely AES-CBC's data block diffusion and AES-GCM's integrity authentication, to provide a multi-layered defense. The system was developed using the Waterfall methodology, which includes requirements analysis, design, implementation, and testing. Built on the Node.js platform, the system implements a dual encryption process (AES-CBC followed by AES-GCM) and is equipped with user access rights management. The results show that the system accurately performs encryption and decryption, effectively safeguarding document confidentiality and integrity. Its implementation also simplifies data management for administrators and members. Black-box testing confirmed a 100% success rate with no failures detected in the encryption or decryption processes across all test scenarios. This research proves that combining AES-CBC and AES-GCM is an effective solution for securing digital data in religious institutions and can serve as a reference for developing similar systems.*

Keywords*: Data security, AES-CBC, AES-GCM,encryption, Node.js.*

1. PENDAHULUAN

Keamanan data merupakan aspek krusial dalam menjaga kerahasiaan dan integritas informasi, terutama pada institusi yang memiliki banyak data sensitif. Gereja GPIB Gibeon Jakarta, yang menyimpan sekitar 400 kartu keluarga berisi informasi pribadi jemaat yang sensitif dan rahasia, menghadapi tantangan signifikan terkait

perlindungan data. Data ini mencakup nama lengkap, jenis kelamin, tempat tanggal lahir, alamat, nomor telepon, surat baptis, surat sidi, nikah gereja, catatan sipil, kartu keluarga, dan surat *atestasi* masuk. Tanpa mekanisme keamanan yang kuat, data ini rentan terhadap kebocoran dan manipulasi.

Dalam beberapa tahun terakhir, metode pengamanan data telah berkembang pesat. Algoritma enkripsi simetris seperti *Advanced Encryption Standard* (AES) telah menjadi standar industri. Dua mode operasi AES yang sering digunakan adalah AES-GCM (*Galois*/*Counter Mode*) dan AES-CBC (*Cipher Block Chaining*). AES-GCM dikenal karena kecepatan dan kemampuannya dalam enkripsi sekaligus autentikasi data, sementara AES-CBC populer karena keandalannya dalam keamanan data melalui difusi blok, meskipun memerlukan metode tambahan untuk autentikasi.

Penelitian di Indonesia mengenai enkripsi data menggunakan AES telah banyak dilakukan, namun belum banyak yang secara spesifik mengkaji penerapan algoritma AES-GCM dan AES-CBC dalam konteks keamanan data jemaat gereja. Penelitian sebelumnya lebih fokus pada pengamanan data di bidang perbankan, *e-commerce*, dan data medis. Oleh karena itu, penelitian ini bertujuan untuk mengusulkan dan mengimplementasikan kombinasi algoritma AES-GCM dan AES-CBC untuk mengamankan dokumen data jemaat pada Gereja GPIB Gibeon Jakarta, serta menganalisis efektivitasnya dalam menjaga kerahasiaan, integritas, dan keutuhan data.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi *waterfall* yang meliputi tahapan analisis kebutuhan, perancangan sistem, implementasi sistem, dan pengujian sistem.

2.1 Pengumpulan Data

Pengumpulan data dilakukan melalui tiga cara:

a. Wawancara
   Mengajukan pertanyaan kepada pengurus Gereja GPIB Gibeon Jakarta yang bertanggung jawab atas pengelolaan dokumen data jemaat.
b. Observasi
   Mengamati cara penyimpanan, keamanan, dan hak akses dokumen, serta implementasi algoritma AES-GCM dan AES-CBC pada dokumen.
c. Studi Pustaka
   Mencari referensi dari jurnal *online*, perpustakaan, dan *e-book* terkait kriptografi, algoritma AES, dan pengamanan data digital.
d. *Dataset* Simulasi
   Untuk menguji performa algoritma dalam skala yang lebih besar, kami menggunakan *dataset* simulasi yang terdiri dari dokumen dengan berbagai ukuran (kecil, sedang, dan besar). Data ini penting untuk mengevaluasi efisiensi algoritma dari segi kecepatan pemrosesan dan penggunaan sumber daya dalam kondisi beban kerja yang beragam.

2.2 Analisis Kebutuhan

Analisis kebutuhan berfokus pada identifikasi kebutuhan sistem untuk melindungi data jemaat, memudahkan akses dan penyimpanan, serta mencegah pencurian data.

2.3 Perancangan Sistem

Sistem dirancang sebagai platform berbasis web. Perancangan meliputi:

a. Arsitektur Sistem
   Menunjukkan skema proses kerja sistem.
b. Rancangan Basis Data
   Meliputi tabel *User*, Jemaat, Dokumen, dan Akses dengan spesifikasi *field* dan *key* masing-masing.
c. *Use Case Diagram*
   Menggambarkan interaksi antara aktor (Admin, Pengurus, Jemaat) dan sistem.
d. Rancangan Menu dan Layar
   Desain antarmuka pengguna untuk berbagai peran dan fungsi.

2.4 Penerapan Algoritma AES

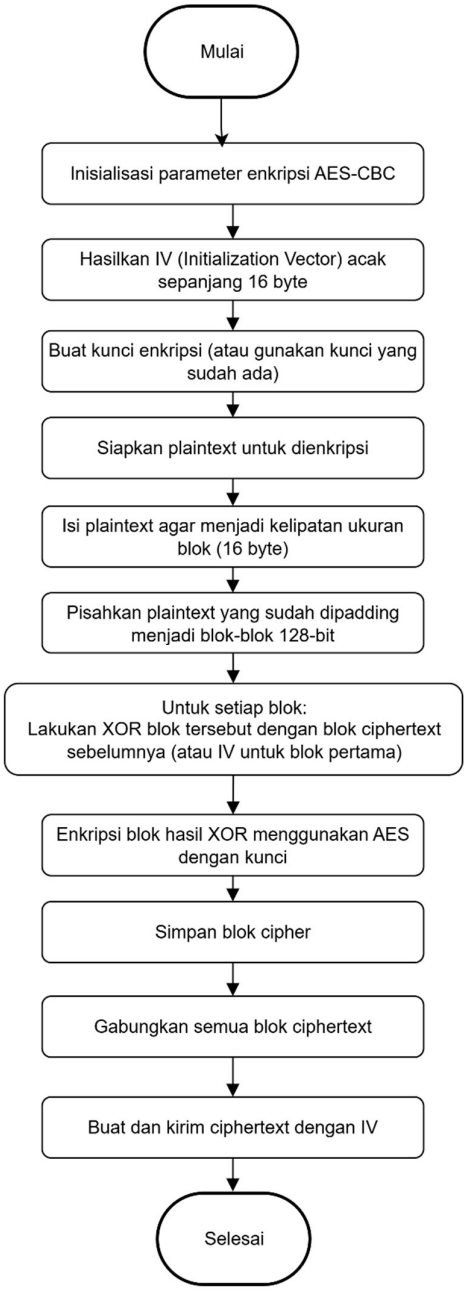
Penelitian ini mengimplementasikan algoritma AES dengan panjang kunci 256-bit dalam dua mode operasi: AES-CBC dan AES-GCM.

2.4.1 Proses Enkripsi Ganda

Dokumen data jemaat akan melalui proses enkripsi ganda:

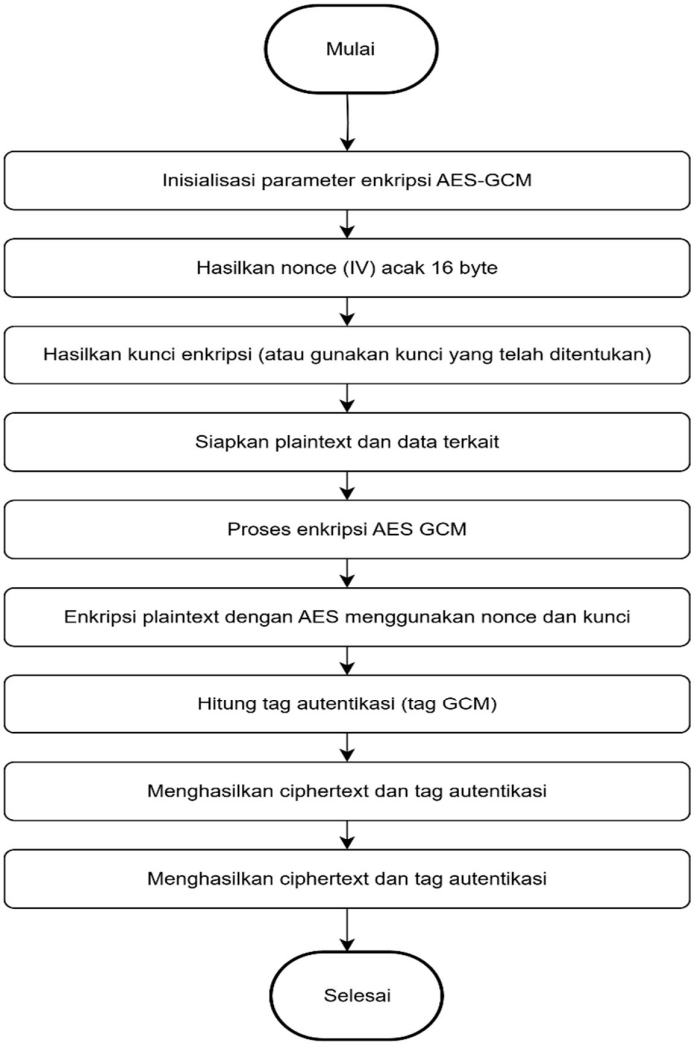
a. Enkripsi Pertama (AES-CBC 256-bit)

Data dienkripsi menggunakan AES-CBC dengan panjang kunci 256-bit. *Initialization Vector* (IV) 128-bit (16 *byte*) yang unik digunakan untuk setiap enkripsi. *Padding* diterapkan jika data tidak sesuai kelipatan 16 *byte*.



Gambar 1. *Flowchart* Enkripsi AES-CBC

b. Enkripsi Kedua (AES-GCM 256-bit)
Hasil dari enkripsi AES-CBC kemudian dienkripsi ulang menggunakan AES-GCM dengan panjang kunci 256-bit. IV 128-bit (16 *byte*) yang unik juga digunakan, dan autentikasi tag dihasilkan untuk menjamin integritas. Dokumen hasil enkripsi ganda ini kemudian disimpan di server.

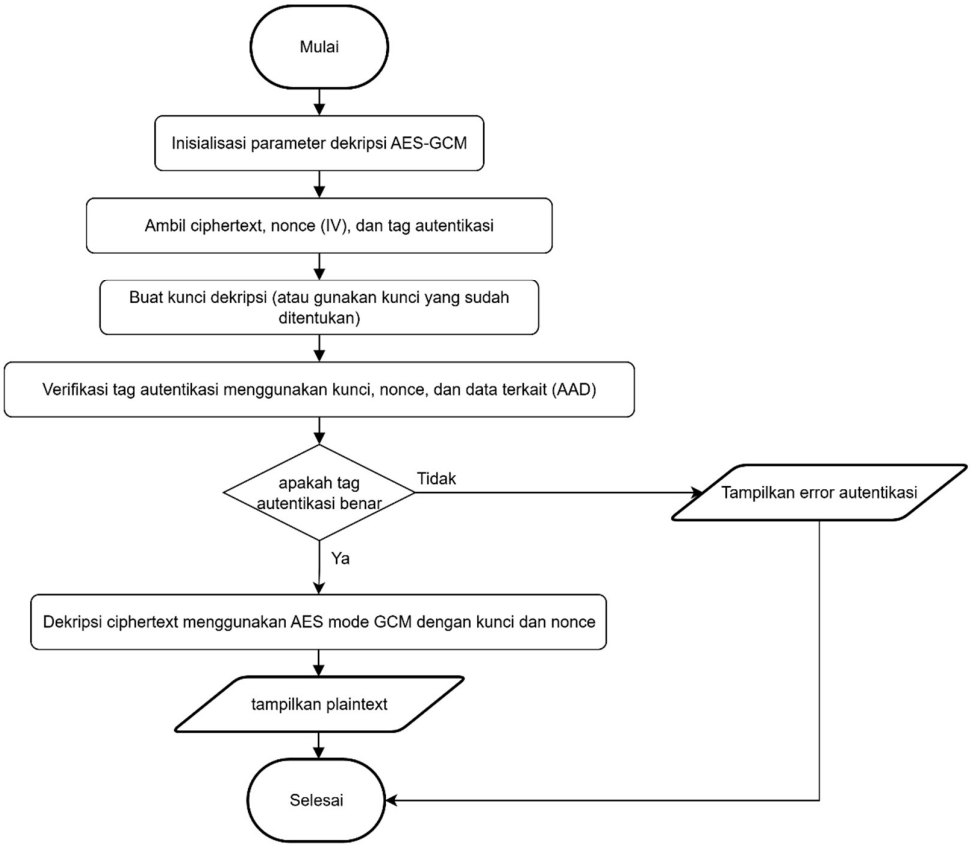


Gambar 2. *Flowchart* Enkripsi AES-GCM

2.4.2 Proses Dekripsi Ganda

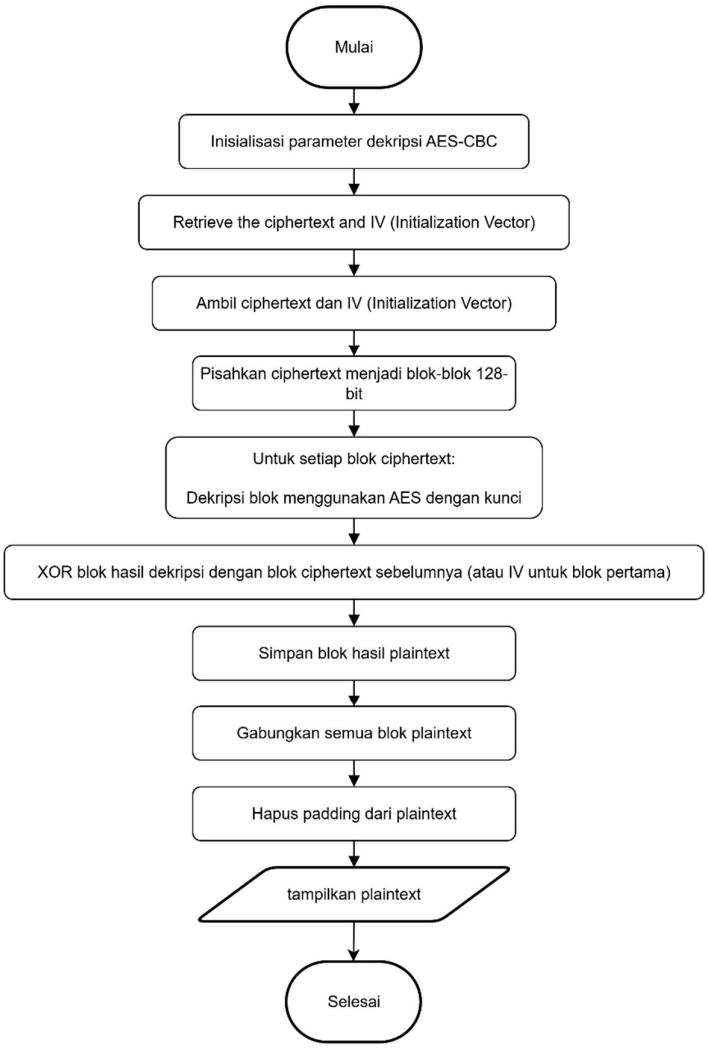
Proses dekripsi dilakukan secara berurutan terbalik:

a. Dekripsi Pertama (AES-GCM 256-bit)
Dokumen yang terenkripsi ganda didekripsi terlebih dahulu menggunakan AES-GCM, memverifikasi autentikasi tag.



Gambar 3. *Flowchart* Dekripsi AES-GCM

b. Dekripsi Kedua (AES-CBC 256-bit)
Hasil dekripsi dari AES-GCM kemudian didekripsi kembali menggunakan AES-CBC untuk mendapatkan dokumen asli. Padding yang sebelumnya ditambahkan akan dihapus. Setelah dekripsi selesai, dokumen dapat diakses dalam bentuk aslinya oleh pihak yang berwenang. Implementasi ini memanfaatkan *library* Crypto yang tersedia pada Node.js.



Gambar 4. *Flowchart* Dekripsi AES-CBC

2.5 Pengujian Sistem

. Pengujian dilakukan menggunakan metode *Black-box* testing untuk memastikan fungsionalitas sistem sesuai dengan tujuan. Pengujian meliputi fungsi *login*, manajemen *user*, pemberian akses, tambah/*update*/unduh dokumen jemaat, serta fungsi enkripsi dan dekripsi dokumen. Untuk pengujian, digunakan data *dummy*/sintetik yang merepresentasikan berbagai jenis dan ukuran dokumen

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

a. Perangkat Keras
   Prosesor Intel(R) *Core*(TM) i5-4310U CPU @ 2.00GHz, RAM 8GB, SSD 120GB
b. Perangkat Lunak
   Visual Studio Code, *MySQL* Server 8, Node.js, Google *Chrome*, Firefox.

3.2 Implementasi Sistem

Sistem berbasis web berhasil diimplementasikan dengan fitur-fitur utama yang mendukung pengelolaan dokumen data jemaat secara aman. Proses enkripsi ganda (AES-CBC kemudian AES-GCM) diterapkan pada

setiap dokumen yang diunggah. Sebaliknya, proses dekripsi dilakukan secara berurutan terbalik (AES-GCM kemudian AES-CBC) saat dokumen diunduh.

3.3 Analisis Kuantitatif Enkripsi dan Deskripsi

Untuk mengevaluasi efektivitas dan efisiensi kombinasi AES-CBC dan AES-GCM, dilakukan analisis kuantitatif terhadap waktu proses enkripsi dan dekripsi pada data *dummy* dengan berbagai ukuran. Tabel 1 menunjukkan hasil pengujian waktu proses dan perubahan ukuran *file*.

Tabel 1. Hasil Pengujian Waktu Proses dan Ukuran File

Ukuran file asli	Waktu Enkripsi	Ukuran File Terenkripsi	Waktu Deskripsi
100 KB	15	100.05 KB	12
500 KB	70	500.25 KB	60
1 MB	140	1.0005 MB	120
3 MB	420	3.0015 MB	360

Dari Tabel 1, terlihat bahwa waktu enkripsi dan dekripsi meningkat seiring dengan bertambahnya ukuran *file*, namun masih dalam rentang yang dapat diterima untuk aplikasi web. Peningkatan ukuran *file* terenkripsi sangat minimal (sekitar 0.05% dari ukuran asli), yang disebabkan oleh penambahan IV dan autentikasi tag oleh AES-GCM serta *padding* oleh AES-CBC. Hal ini menunjukkan bahwa kombinasi algoritma tidak secara signifikan menambah beban penyimpanan.

3.4 Analisa Keamanan dan Fungsionalitas

Pengujian *black-box* menunjukkan bahwa semua fungsionalitas sistem berjalan dengan baik. Proses enkripsi ganda berhasil mengubah data asli menjadi *ciphertext* yang tidak dapat dibaca atau diakses tanpa proses dekripsi yang benar. Ketika file terenkripsi dibuka dengan aplikasi standar, hasilnya adalah data yang rusak atau tidak dikenali, membuktikan keberhasilan enkripsi. Sebaliknya, proses dekripsi berhasil mengembalikan *file* ke bentuk aslinya, memastikan akses yang sah.

Kombinasi AES-CBC dan AES-GCM memberikan perlindungan berlapis:

a. AES-CBC
   Menjamin kerahasiaan dan menyamarkan pola data asli melalui mekanisme *chaining*, di mana setiap blok *ciphertext* bergantung pada blok sebelumnya. Ini efektif melawan serangan yang mencoba menemukan pola dalam data terenkripsi.
b. AES-GCM
   Selain kerahasiaan, AES-GCM juga menyediakan autentikasi dan integritas data. Ini berarti sistem dapat mendeteksi jika ada upaya modifikasi pada *ciphertext* atau jika *ciphertext* berasal dari sumber yang tidak sah. Fitur ini sangat penting untuk data sensitif seperti dokumen jemaat, karena tidak hanya mencegah pengungkapan informasi tetapi juga memastikan keasliannya.

4. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem pengamanan dokumen jemaat Gereja GPIB Gibeon Jakarta menggunakan algoritma AES-GCM dan AES-CBC, dapat disimpulkan beberapa hal sebagai berikut.

a. Penerapan algoritma AES-GCM dan AES-CBC berhasil meningkatkan keamanan dokumen jemaat. Dokumen yang telah dienkripsi dengan kedua algoritma tidak dapat dibaca tanpa proses dekripsi yang tepat, sehingga mampu menjaga kerahasiaan dan integritas data jemaat dari pihak yang tidak berwenang.
b. Proses enkripsi ganda (*double encryption*), yaitu menggunakan kombinasi AES-CBC dan AES-GCM, memberikan lapisan keamanan tambahan. AES-CBC digunakan untuk mengenkripsi isi dokumen berdasarkan blok data dengan pengaruh dari blok sebelumnya, sedangkan AES-GCM berfungsi untuk memberikan autentikasi tambahan terhadap dokumen yang telah dienkripsi.
c. Efektivitas pengamanan terbukti melalui uji coba yang dilakukan dalam pengujian sistem. Seluruh fitur sistem — mulai dari unggah dokumen, pemberian hak akses, hingga proses enkripsi dan dekripsi — telah berjalan sesuai dengan fungsionalitas yang dirancang.
d. Penggunaan metode *black-box testing* menunjukkan bahwa sistem berjalan dengan baik dari sisi pengguna. Semua fungsi utama dapat diakses dengan benar oleh masing-masing peran (admin, pengurus, jemaat), serta sistem dapat menangani validasi, penyimpanan, dan distribusi dokumen dengan aman.

e. Sistem berbasis web yang dirancang memberikan antarmuka yang mudah digunakan bagi semua kategori pengguna, serta memfasilitasi pengelolaan dokumen digital yang aman dan terstruktur.

DAFTAR PUSTAKA

[1] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," Jurnal Ilmiah FIFO, vol. 12, no. 1, p. 12, 2020. doi: 10.22441/fifo.2020.v12i1.002.

[2] A. M. Almorabea and M. A. Aslam, "Symmetric Key Encryption Using AES-GCM and External Key Derivation for Smart Phones," Int. J. Comput. Sci. Mob. Comput., vol. 3, no. 6, pp. 264–270, 2015. [Online]. Available: https://www.academia.edu/79442444/Symmetric_Key_Encryption_Using_AES_GCM_and_External_Key_Derivation_for_Smart_Phones

[3] A. Amrulloh and E. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," Jurnal CoreIT, vol. 5, no. 2, pp. 71–77, 2019. [Online]. Available: https://ejournal.uin-suska.ac.id/index.php/coreit/article/view/8674

[4] I. Djohan and A. Siswanto, "Analisis Kriptografi AES Terhadap File Gambar," Jurnal Teknologi Informasi dan Ilmu Komputer, 2022.

[5] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), vol. 4, pp. 78–86, 2020. doi: 10.30865/komik.v4i1.2590.

[6] R. N. Ihsan et al., "Web Server: Fungsi dan Mekanisme Dasar," Jurnal Teknologi Informasi dan Komputer, 2020.

[7] N. Jamaluddin et al., "Penerapan AES-GCM Dalam Keamanan Data Digital Berbasis Web," Jurnal Ilmiah Teknologi dan Komputer, 2020.

[8] F. Noviyanti and P. Mira, "Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris pada Keamanan File," Jurnal Rekayasa dan Keamanan Siber, 2022.

[9] R. Prayudha et al., "Analisis Transformasi SubBytes dan ShiftRows pada AES," Jurnal Informatika dan Sistem Informasi, 2019.

[10] P. A. Rizky, S. Soim, and S. Sholihin, "Implementasi Algoritma Kriptografi AES CBC Untuk Keamanan Komunikasi Data Pada Hardware," Jurnal RESISTOR (Rekayasa Sistem Komputer), vol. 7, no. 2, pp. 71–78, 2024. doi: 10.31598/jurnalresistor.v7i2.1650.

[11] H. S. Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode RC4 Dan AES-256 Untuk Mengamankan File Dokumen Pada PT Varnion Technology Semesta," in Proc. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), Jakarta, Indonesia, Sep. 2022, pp. 149–158. [Online]. Available: https://senafti.budiluhur.ac.id/senafti/article/view/138

[12] A. D. Saputra and M. Syafrullah, "Algoritme AES-256 Untuk Keamanan Basis Data Penilaian Pegawai Pada PT. Buana Jaya Korindo," in Proc. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), Sep. 2022, pp. 295–301. [Online]. Available: http://senafti.budiluhur.ac.id/index.php/senafti/article/view/237

[13] Y. Yusrizal, Pengantar Kriptografi dan Keamanan Data. Bandung: Informatika, 2019.

[14] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," JRKT (Jurnal Rekayasa Komputasi Terapan), vol. 1, no. 2, pp. 108–114, 2021. doi: 10.30998/jrkt.v1i02.4096.

[15] W. Gondowarsito, "Multi-Format Data Encryption and Decryption with AES Cipher Block Chaining in Python," Crossroad Research Journal, vol. 2, no. 2, pp. 56–65, 2025. doi: 10.61402/crj.v2i2.348.

[16] W. Patriaji, "Analisa Keamanan Kombinasi Algoritma AES dengan GCM (Galois/Counter Mode) Pada Data Gambar Kanker Kulit," Doctoral dissertation, Univ. Muhammadiyah Malang, 2025. [Online]. Available: https://eprints.umm.ac.id/id/eprint/17425/

[17] P. N. Latip, "Implementasi Algoritma Kriptografi AES dalam Pengamanan File Teks," Jurnal Riset Sistem Informasi, vol. 2, no. 3, pp. 1–4, 2025. doi: 10.69714/k6pr0s45.

[18] W. Prabowo and N. Anwar, "Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC," IKRA-ITH Informatika: Jurnal Komputer dan Informatika, vol. 9, no. 1, pp. 178–186, 2025. [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/4775

[19] F. Shofyan and R. T. Shita, "Implementasi Web Service Restful API dengan Autentikasi Personal Access Tokens dan Algoritma AES 256," Jurnal Ticom: Technology of Information and Communication, vol. 12, no. 3, pp. 108–114, 2024. doi: 10.70309/ticom.v12i3.130.