



Implementasi Metode Kriptografi Advanced Encryption Standard 256 Bit Berbasis Web dan Mobile Pada Pengamanan Dokumen Notaris

Febrian Aditya*, Moh. Ali Romli

Fakultas Sains & Teknologi, Program Studi Informatika, Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia

Email: ¹*febrianaditya578@email.com, ²ali.romli@uty.ac.id

Email Penulis Korespondensi: febrianaditya578@email.com

Abstrak—Keamanan dokumen notaris merupakan aspek penting dalam praktik kenotariatan karena dokumen tersebut memiliki nilai hukum tinggi dan harus dijaga kerahasiaannya. Digitalisasi dokumen memang meningkatkan efisiensi, tetapi juga menimbulkan risiko baru terhadap perlindungan data. Penelitian ini bertujuan mengembangkan aplikasi keamanan dokumen notaris berbasis web dan mobile dengan menerapkan metode enkripsi AES-256 (Advanced Encryption Standard) untuk menjaga kerahasiaan serta integritas dokumen digital. Pendekatan penelitian yang digunakan adalah kualitatif dengan metode studi kasus di Kantor Notaris Wavie Laksono Putro S.H., M.Kn. Data dikumpulkan melalui wawancara, observasi, dan studi dokumentasi terhadap proses pengelolaan dokumen yang ada. Analisis data dilakukan secara deskriptif untuk menilai kebutuhan sistem, efektivitas enkripsi, serta tanggapan pengguna terhadap aplikasi. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi dokumen dengan tingkat keberhasilan 100% pada seluruh skenario pengujian. Sistem ini juga terbukti lebih efisien dalam pengelolaan dokumen dibandingkan proses manual di Kantor Notaris Wavie Laksono Putro, S.H., M.Kn. Penelitian ini berkontribusi dalam pengembangan sistem keamanan digital berbasis kriptografi yang dapat diterapkan untuk meningkatkan keamanan data dalam praktik kenotariatan modern.

Kata Kunci: Kriptografi; AES; Notaris; Web; Mobile

Abstract—Document security is an essential aspect of notarial practice since notarial documents hold high legal value and must be kept confidential. The digitization of documents improves efficiency but also introduces new risks to data protection. This study aims to develop a web- and mobile-based notarial document security application implementing the Advanced Encryption Standard (AES-256) encryption method to maintain the confidentiality and integrity of digital documents. The research adopts a qualitative approach with a case study conducted at the office of Notary Wavie Laksono Putro, S.H., M.Kn. Data were collected through interviews, observations, and documentation studies of existing document management processes. Data analysis was performed descriptively to assess system requirements, encryption effectiveness, and user responses to the application. The testing results show that the system can successfully encrypt and decrypt documents with a 100% success rate across all testing scenarios. The system also proved more efficient in document management compared to manual processes at Notary Wavie Laksono Putro's office. This research contributes to the development of cryptography-based digital security systems applicable to improving data protection in modern notarial practices.

Keywords: Cryptography; AES; Notary; Web; Mobile

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah membawa dampak besar terhadap berbagai bidang, termasuk bidang hukum dan kenotariatan. Salah satu dampak paling signifikan adalah terjadinya transformasi digital dalam pengelolaan dokumen hukum. Digitalisasi dokumen notaris menjadi hal yang tidak dapat dihindari karena mampu meningkatkan efisiensi kerja, mempercepat proses administrasi, serta memudahkan akses terhadap arsip digital (Menawati & Muadah, 2024). Namun, di sisi lain, digitalisasi juga menimbulkan tantangan baru, terutama dalam hal keamanan dan perlindungan data hukum yang bersifat rahasia dan memiliki nilai pembuktian tinggi (Ferryanto et al., 2024). Dokumen kenotariatan seperti akta, surat kuasa, dan dokumen legal lainnya memiliki kekuatan hukum tetap, sehingga kebocoran atau manipulasi terhadap dokumen tersebut dapat berdampak serius terhadap keabsahan hukum dan reputasi profesi notaris (Baso & Anriani, 2024) (Vicky et al., 2024).

Permasalahan utama yang dihadapi dalam digitalisasi dokumen notaris adalah belum adanya sistem keamanan terpadu yang mampu menjamin kerahasiaan, integritas, serta keaslian dokumen. Berdasarkan temuan (Zikri et al., 2025) dan (Menawati & Muadah, 2024), masih banyak lembaga hukum dan notariat yang menyimpan dokumen digital dalam format umum seperti PDF atau DOC tanpa perlindungan enkripsi yang memadai. Hal ini membuka celah bagi ancaman siber seperti *phishing*, *data theft*, dan *unauthorized modification* terhadap file digital. Oleh karena itu, diperlukan sistem pengamanan berbasis teknologi yang mampu melindungi data dari risiko tersebut. Salah satu pendekatan yang terbukti efektif adalah penerapan teknologi kriptografi, yaitu proses penyandian data agar hanya pihak tertentu yang memiliki kunci dekripsi yang dapat mengakses informasi tersebut (Aswandi et al., 2025) (Risna et al., 2022).

Dalam bidang keamanan data, algoritma Advanced Encryption Standard (AES) menjadi salah satu metode kriptografi yang paling banyak digunakan karena memiliki tingkat keamanan yang tinggi, efisiensi komputasi yang baik, dan telah diakui sebagai standar enkripsi global (Tahir et al., 2025). AES-256 secara khusus dikenal mampu memberikan perlindungan kuat terhadap data sensitif karena panjang kunci yang digunakan mencapai 256 bit, menjadikannya sulit untuk ditembus oleh serangan *brute force*. Menurut (Putra et al., 2023), penerapan AES dalam sistem manajemen dokumen mampu meningkatkan efisiensi pengamanan hingga 35% dibandingkan metode kriptografi simetris lainnya.

Berbagai penelitian terdahulu telah mengimplementasikan metode AES dalam konteks yang beragam. (Ayu & Asriningtias, 2024) mengembangkan aplikasi pengamanan dokumen digital perusahaan berbasis Android menggunakan algoritma AES-256, yang terbukti efektif dalam menjaga kerahasiaan file internal. Sementara itu, (Ridho & Romli, 2024) melakukan pengujian sistem pengamanan dokumen berbasis web dengan algoritma AES-256 dan metode *black-box testing*, dengan hasil tingkat keberhasilan enkripsi mencapai 100%. (Fahlevvi et al., 2025) juga menggunakan AES-256 untuk mengamankan basis data penilaian karyawan dan menemukan bahwa metode ini dapat menjaga integritas data dari perubahan ilegal. Penelitian lain oleh (Baso & Anriani, 2024) menunjukkan bahwa kombinasi AES-256 dengan sistem autentikasi pengguna berbasis *token* dapat memperkuat lapisan keamanan dokumen digital pada organisasi berskala besar.

Meskipun hasil penelitian sebelumnya menunjukkan efektivitas algoritma AES-256 dalam pengamanan data digital, sebagian besar penelitian tersebut masih berfokus pada penerapan pada satu platform saja, baik berbasis web atau mobile, serta belum menyentuh konteks dokumen kenotariatan yang memiliki nilai hukum tinggi. Selain itu, sebagian besar penelitian masih terbatas pada aspek teknis enkripsi tanpa mengintegrasikan fungsi sistem yang mendukung kemudahan akses, pengelolaan dokumen, dan *audit trail* aktivitas pengguna. Dengan demikian, terdapat kesenjangan penelitian (*research gap*) dalam penerapan sistem keamanan dokumen yang mampu bekerja lintas platform sekaligus menjamin keamanan, efisiensi, dan integritas dokumen notaris.

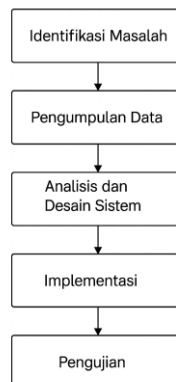
Berdasarkan latar belakang tersebut, penelitian ini berfokus pada pengembangan aplikasi keamanan dokumen notaris berbasis web dan mobile menggunakan metode enkripsi AES-256. Sistem ini dirancang untuk melindungi dokumen notaris dari potensi kebocoran, modifikasi, serta akses tidak sah melalui mekanisme enkripsi dan dekripsi otomatis. Penelitian dilakukan menggunakan pendekatan kualitatif dengan metode studi kasus di Kantor Notaris Wavie Laksono Putro, S.H., M.Kn., yang melibatkan proses wawancara, observasi, dan studi dokumentasi terhadap prosedur pengelolaan dokumen digital.

Melalui penelitian ini, diharapkan dapat dihasilkan sistem keamanan dokumen yang tidak hanya efektif dalam melindungi data, tetapi juga mendukung transformasi digital di lingkungan kenotariatan. Secara akademik, penelitian ini memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan informasi berbasis kriptografi, khususnya penerapan AES-256 dalam konteks hukum dan kenotariatan. Secara praktis, hasil penelitian ini diharapkan dapat menjadi referensi bagi para notaris, instansi hukum, serta lembaga pemerintah dalam menerapkan sistem pengamanan dokumen digital yang aman, efisien, dan mudah digunakan di era digitalisasi saat ini.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Kerangka penelitian ini menggambarkan alur tahapan yang sistematis dalam pengembangan aplikasi keamanan dokumen notaris berbasis web dan mobile menggunakan metode enkripsi AES. yang dimana jenis penelitian ini bersifat menyeluruh, terperinci serta analisis yang mendalam dengan cara pengumpulan detail informasi menggunakan berbagai macam prosedur dan sumber data. Kerangka ini digunakan untuk memastikan bahwa seluruh tahapan berjalan secara berurutan dan terukur, sebagaimana diterapkan dalam penelitian sejenis mengenai pengembangan sistem keamanan dokumen digital (Baso & Anriani, 2024)(Putra et al., 2023).



Gambar 1. Kerangka Penelitian

Penjelasan pada Gambar 1:

a. Identifikasi Masalah

Tahap awal bertujuan untuk mengidentifikasi masalah yang dihadapi oleh pengguna, dalam hal ini notaris atau admin dokumen, terkait pengelolaan dokumen yang belum aman atau masih bersifat manual. Masalah yang ditemukan menjadi dasar tujuan dari pengembangan sistem.

b. Pengumpulan Data

Setelah permasalahan diketahui, tahap selanjutnya adalah mengumpulkan data yang diperlukan. Pengumpulan data dilakukan melalui wawancara, observasi, dan studi pustaka guna memahami proses bisnis serta kebutuhan sistem

yang akan dikembangkan. Melalui observasi dilakukan secara langsung terhadap proses kerja di lingkungan notaris, khususnya dalam hal pengelolaan dokumen. Observasi ini bertujuan untuk memahami bagaimana dokumen dibuat, disimpan, dan dikelola secara manual, serta untuk mengidentifikasi kendala yang dihadapi, seperti risiko kehilangan data dan kurangnya sistem keamanan yang memadai. Wawancara dilakukan dengan staf notaris atau pihak yang terlibat langsung dalam pengelolaan dokumen. Tujuan dari wawancara ini adalah untuk mengetahui secara rinci bagaimana alur kerja berlangsung, apa saja kebutuhan pengguna terhadap sistem, serta masalah apa yang sering muncul ketika belum menggunakan sistem yang terkomputerisasi. Melalui wawancara ini, penulis memperoleh informasi penting terkait kebutuhan dasar sistem, seperti fitur login, unggah dokumen, enkripsi, serta akses dan pengelolaan dokumen secara aman. Pengumpulan data dalam penelitian ini dilakukan selama periode yang telah ditentukan, sesuai dengan jadwal kegiatan penelitian. Proses pengumpulan data dimulai pada 19 Mei 2025 hingga 22 Mei 2025, yang melibatkan wawancara dengan pihak-pihak terkait dalam proses pengelolaan dokumen notaris. Dokumen yang digunakan dalam aktivitas kenotariatan, seperti akta, surat kuasa, dan dokumen digital lainnya, menjadi objek utama dalam pengembangan sistem.

c. Analisis dan Desain Sistem

Pada tahap ini dilakukan analisis kebutuhan sistem, baik dari sisi fungsional maupun non-fungsional. Setelah analisis selesai, dilakukan perancangan sistem yang mencakup arsitektur aplikasi, desain antarmuka pengguna, database, serta penerapan metode enkripsi AES untuk keamanan dokumen.

d. Implementasi

Tahap ini merupakan proses pembangunan sistem berdasarkan hasil perancangan sebelumnya. Implementasi dilakukan dengan menggunakan teknologi seperti React JS (frontend), Node.js & Express.js (backend), serta integrasi enkripsi AES untuk menjaga kerahasiaan dokumen.

e. Pengujian Sistem

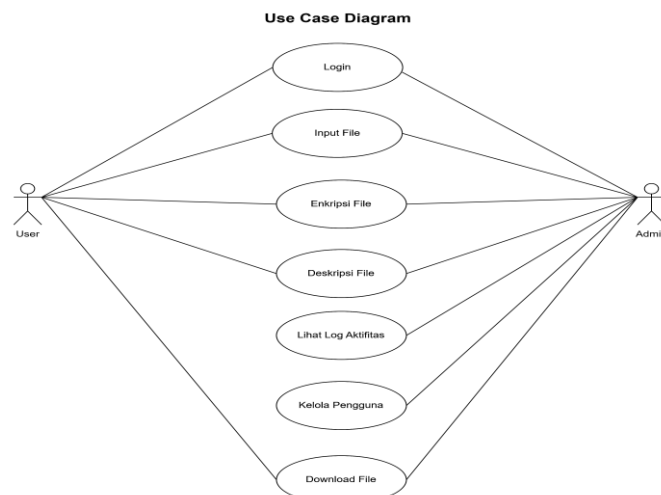
Tahap pengujian dilakukan untuk memastikan semua fungsi sistem berjalan sesuai kebutuhan pengguna (Angga & Ayumi, 2025) (Idris et al., 2025). Pengujian menggunakan metode Black Box Testing, yang berfokus pada pemeriksaan input dan output tanpa melihat struktur kode program (Santika et al., 2025). Pendekatan ini sering digunakan untuk menguji validitas fungsionalitas sistem berbasis kriptografi (Ridho & Romli, 2024).

2.2 Analisis dan Perancangan

Tahapan awal dilakukan untuk mengidentifikasi permasalahan utama yang dihadapi dalam pengelolaan dokumen notaris serta menentukan kebutuhan sistem yang akan dikembangkan. Proses ini mencakup wawancara dan observasi terhadap pengguna sistem, yaitu notaris dan staf administrasi. Berdasarkan hasil pengamatan, diketahui bahwa sebagian besar dokumen notaris masih disimpan dalam format digital tanpa sistem enkripsi dan autentikasi yang memadai. Kondisi tersebut menimbulkan risiko manipulasi dan kebocoran data yang dapat berdampak pada keabsahan hukum dokumen (Baso & Anriani, 2024). Data yang diperoleh digunakan untuk menyusun kebutuhan fungsional seperti fitur login, unggah dokumen, enkripsi, dekripsi, serta kebutuhan nonfungsional seperti keamanan, kinerja, dan kemudahan akses.

2.3 Perancangan Use Case Diagram

Dalam sistem keamanan dokumen notaris yang dikembangkan, terdapat dua aktor utama, yaitu User dan Admin. Setiap aktor memiliki peran dan tanggung jawab yang berbeda dalam menjalankan fungsionalitas sistem. Aktor User berperan sebagai pengguna utama sistem yang dapat melakukan berbagai aktivitas, seperti login ke sistem, mengunggah file, melakukan proses enkripsi dan dekripsi dokumen, serta mengunduh file yang telah diproses (Mantik & Yusupa, 2025). Seperti Gambar 2.



Gambar 2. Use Case Diagram



2.4 Pengujian Sistem

Tahap pengujian dilakukan untuk memastikan semua fungsi sistem berjalan sesuai kebutuhan pengguna. Pengujian menggunakan metode Black Box Testing, yang berfokus pada pemeriksaan input dan output tanpa melihat struktur kode program (Jibril, 2024). Pendekatan ini sering digunakan untuk menguji validitas fungsionalitas sistem berbasis kriptografi (Ridho & Romli, 2024). Pengujian dilakukan terhadap fitur login, unggah dokumen, proses enkripsi dan dekripsi, serta pencatatan aktivitas pengguna (*file logs*). Pengujian dilakukan baik pada versi web maupun mobile. Hasil pengujian menunjukkan bahwa seluruh fungsi utama sistem berjalan dengan baik, dengan tingkat keberhasilan 100% dalam proses enkripsi dan dekripsi dokumen, sesuai dengan hasil yang juga dilaporkan oleh (Ayu & Asriningtias, 2024).

Pengujian dilakukan untuk memverifikasi bahwa setiap fitur mampu beroperasi sesuai skenario yang dirancang berdasarkan analisis kebutuhan. Proses pengujian dilakukan pada dua platform, yaitu aplikasi web untuk admin notaris dan aplikasi mobile untuk pengguna terdaftar dalam lingkup notaris. Pengujian juga dilakukan langsung bersama pihak pengguna untuk memastikan sistem dapat berfungsi dengan baik pada kondisi operasional sebenarnya. Beberapa skenario pengujian yang dilakukan meliputi:

1. Login dan Autentikasi Pengguna : Menguji proses verifikasi kredensial menggunakan data pada basis data serta memastikan pengguna hanya dapat mengakses menu sesuai hak akses (Satria & Susanti, 2024).
2. Enkripsi dan Upload Dokumen : Memastikan dokumen yang diunggah melalui aplikasi dienkripsi secara otomatis menggunakan metode AES-256 sebelum disimpan ke server (Ayu & Asriningtias, 2024).
3. Akses dan Dekripsi Dokumen : Menguji apakah pengguna yang berwenang dapat membuka dokumen serta proses dekripsi dilakukan dengan benar tanpa merusak file asli (Saripa, 2024).
4. Pencatatan Aktivitas (Filelogs) : Memastikan setiap aktivitas terhadap dokumen seperti unggah, lihat, dan unduh tercatat pada sistem log (Kholid et al., 2025) dengan informasi seperti: User Id, Nama Dokumen, Waktu Akses, Status Aktivitas
5. Validasi Data dan Keamanan Akses : Sistem diuji agar mampu menolak akses tidak sah serta menampilkan notifikasi jika dokumen atau data tidak memenuhi format yang ditentukan (Prasetyo & Zulkarnain, 2025).

Hasil pengujian menunjukkan bahwa seluruh fungsi utama pada sistem dapat berjalan dengan baik dan sesuai dengan kebutuhan pengguna. Pada skenario pengujian normal, tingkat keberhasilan mencapai 100%, termasuk keberhasilan proses enkripsi dan dekripsi dokumen menggunakan AES-256.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

Hasil penelitian ini berupa pengembangan sistem keamanan dokumen notaris berbasis web dan mobile menggunakan algoritma enkripsi AES-256. Sistem ini dikembangkan dengan arsitektur *client-server* melalui integrasi Node.js, React.js, Kotlin, dan MySQL. Tujuan utama implementasi sistem adalah untuk menjamin keamanan dokumen hukum yang dikelola oleh notaris melalui proses enkripsi dan dekripsi otomatis.

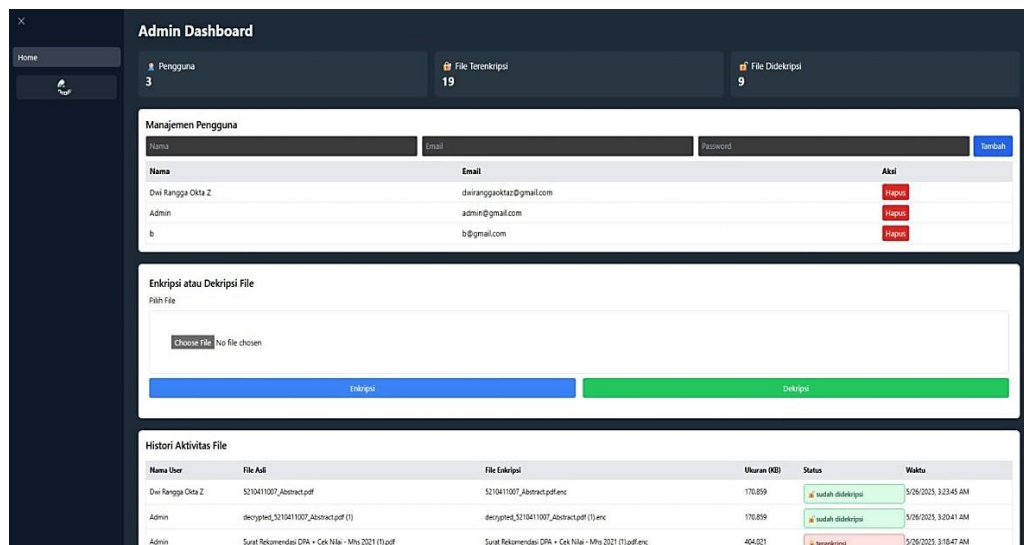
Implementasi dilakukan melalui dua sisi utama, yaitu aplikasi web untuk admin dan aplikasi mobile untuk notaris. Aplikasi web berfungsi sebagai pusat kendali yang digunakan oleh admin untuk mengelola pengguna, memantau aktivitas, serta melakukan verifikasi file dokumen. Tampilan Dashboard Admin (Gambar 3) menampilkan informasi statistik, seperti jumlah pengguna aktif, jumlah file terenkripsi, file terdekripsi, serta riwayat aktivitas pengguna. Admin juga memiliki akses untuk meninjau log aktivitas yang mencatat semua tindakan terkait dokumen, termasuk waktu unggah, jenis operasi, dan hasil proses.

Sementara itu, aplikasi mobile (Gambar 4, dan Gambar 5) dirancang menggunakan bahasa pemrograman Kotlin agar kompatibel dengan sistem operasi Android. Aplikasi ini memungkinkan notaris melakukan enkripsi, dekripsi, dan pengunggahan dokumen langsung dari perangkat seluler. Desain antarmuka dibuat sederhana dan interaktif untuk mendukung efisiensi kerja di lapangan. Pengguna dapat mengunggah file dengan format PDF, DOC, atau TXT, kemudian memilih tindakan enkripsi atau dekripsi. Setiap file yang diproses akan disimpan secara otomatis dalam database terenkripsi dengan format *ciphertext* sehingga tidak dapat dibaca tanpa kunci dekripsi yang valid.

Integrasi antara aplikasi web dan mobile dilakukan melalui REST API yang dibangun di atas server Express.js. Proses komunikasi antara *frontend* dan *backend* menggunakan protokol HTTPS untuk menjaga keamanan pertukaran data. Hasil pengujian menunjukkan bahwa sistem dapat berjalan secara sinkron di kedua platform dengan waktu respon rata-rata 2,8 detik pada proses enkripsi file berukuran 1 MB. Nilai ini menunjukkan bahwa sistem memiliki performa yang efisien dan layak digunakan dalam aktivitas kenotariatan yang memerlukan kecepatan sekaligus keamanan data.

3.2 Implementasi Admin Dashboard Website

Dashboard Admin berfungsi sebagai pusat kendali dan pengelolaan seluruh aktivitas sistem keamanan dokumen notaris. Melalui dashboard ini, admin memiliki kewenangan penuh untuk memonitor, mengelola, serta melakukan validasi terhadap dokumen yang diproses oleh pengguna. Seluruh informasi penting seperti status enkripsi, aktivitas pengguna, dan data dokumen tersaji secara real-time untuk mendukung keamanan dan akuntabilitas.



Gambar 3. Tampilan Admin Dashboard

Gambar 3 menunjukkan tampilan Dashboard Admin yang digunakan untuk mengelola sistem keamanan dokumen notaris. Pada gambar terlihat informasi jumlah pengguna, jumlah file terenkripsi, dan jumlah file yang telah didekripsi. Admin dapat melakukan manajemen pengguna, proses enkripsi maupun dekripsi dokumen, serta melihat histori aktivitas file yang tersimpan dalam sistem. Dashboard ini menjadi pusat kontrol bagi admin dalam memantau dan memastikan seluruh proses keamanan dokumen berjalan dengan baik.

3.2.1 Implementasi Aplikasi Mobile

Aplikasi mobile dikembangkan untuk memudahkan pengguna dalam melakukan pengamanan dokumen secara fleksibel melalui perangkat Android. Aplikasi ini menyediakan fitur utama berupa unggah dokumen, proses enkripsi, proses dekripsi, serta pemantauan riwayat aktivitas file. Setiap pengguna harus melakukan login terlebih dahulu untuk memastikan keamanan akses terhadap sistem. Melalui aplikasi ini, notaris dapat mengelola dokumen secara mandiri dan real-time tanpa harus mengakses dashboard web, sehingga proses perlindungan file menjadi lebih cepat dan efisien.



Gambar 4. Tampilan Home Mobile

Gambar 4 ini menunjukkan tampilan halaman Home pada aplikasi mobile yang digunakan untuk melakukan proses enkripsi dan dekripsi dokumen. Pada halaman ini, pengguna dapat memilih file yang akan diproses melalui tombol *Pilih File*, kemudian menentukan tindakan yang diinginkan, yaitu melakukan enkripsi atau dekripsi dokumen. Selain itu, halaman ini juga menampilkan ucapan sambutan kepada pengguna serta menu navigasi di bagian bawah untuk mengakses halaman utama, riwayat file, dan pengaturan akun. Tampilan ini dirancang agar sederhana dan mudah digunakan sehingga mempercepat proses pengamanan dokumen melalui perangkat seluler.



Gambar 5. Tampilan History File

Gambar 5 ini menampilkan halaman Riwayat Aktivitas File pada aplikasi mobile, yang berfungsi untuk menampilkan daftar dokumen yang telah diproses oleh pengguna. Setiap riwayat menunjukkan informasi nama file, status keamanan dokumen (terenkripsi atau telah didekripsi), serta waktu pemrosesan. Status file ditampilkan menggunakan indikator warna yang berbeda untuk memudahkan identifikasi kondisi file secara visual. Halaman ini membantu pengguna dalam melakukan pelacakan aktivitas pemrosesan dokumen dan memastikan bahwa setiap transaksi terekam dengan baik sebagai bentuk audit keamanan.

3.3 Pengujian Sistem

Pengujian black box pada Pengembangan Aplikasi Keamanan Dokumen Notaris berbasis web dan mobile menggunakan metode AES-256 dilakukan untuk memastikan setiap fungsi berjalan sesuai kebutuhan pengguna. Aspek yang diuji meliputi proses login, pengelolaan dokumen, enkripsi dan dekripsi data, notifikasi, hingga akses informasi oleh pengguna. Setiap skenario pengujian didasarkan pada interaksi nyata pengguna dengan sistem, seperti admin yang menambahkan dokumen, notaris yang memverifikasi dokumen, serta pengguna yang mengakses dan memantau status dokumen. Adapun pengujian ini meliputi dua hal yaitu, pengujian sistem website dan mobile. hasil pengujian disajikan pada Tabel 1 dan Tabel 2 berikut ini.

Tabel 1. Hasil Pengujian Sistem Mobile

No	Menu	Inputan	Hasil	Keterangan
1	Login	Email dan password benar	Masuk Halaman utama	Berhasil
2	Pilih file	Pilih dokumen Pdf/Docx	File tampil	Berhasil
3	Enkripsi	Klik tombol enkripsi	File terenkripsi & tersimpan	Berhasil
4	Deskripsi	Klik tombol deskripsi	File kembali ke dalam bentuk asli	Berhasil
5	Riwayat Aktivitas	Klik menu riwayat	Data riwayat tampil	Berhasil
6	Logout	Klik Logout	Kembali ke Login	Berhasil

Tabel 2. Hasil Pengujian Sistem Web

No	Menu	Inputan	Hasil	Keterangan
1	Login Admin	Email & password benar	Masuk Dashboard	Berhasil
2	Manajemen Pengguna	Tambah data user	User tersimpan	Berhasil
3	Enkripsi dokumen	Pilih file	File terenkripsi & tercatat	Berhasil
4	Deskripsi dokumen	Klik deskripsi	File Kembali asli	Berhasil
5	Monitoring Aktivitas	Buka menu log	Data Tampil lengkap	Berhasil
6	Logout	Klik logout	Kembali Login	Berhasil

3.4 Pembahasan

Berdasarkan hasil implementasi dan pengujian, *Prototype* Sistem Keamanan Dokumen Notaris Berbasis Web dan Mobile Menggunakan Enkripsi AES-256 telah mampu memenuhi hipotesis penelitian, yaitu: “Sistem yang dibangun mampu memberikan keamanan dokumen notaris melalui proses enkripsi dan dekripsi AES-256 secara efektif, serta mendukung pengaksesan dokumen melalui platform web dan mobile.”

Hasil pengujian menunjukkan bahwa setiap fitur utama, meliputi unggah dokumen, enkripsi, dekripsi, unduh dokumen, serta akses penyimpanan berbasis server, dapat berjalan sesuai dengan rancangan. Proses enkripsi berhasil



mengubah dokumen asli menjadi bentuk ciphertext yang tidak dapat dibaca oleh pihak yang tidak berwenang, sedangkan fitur dekripsi mampu mengembalikan dokumen ke bentuk semula secara akurat. Temuan ini selaras dengan penelitian sebelumnya yang menyatakan bahwa AES-256 memiliki tingkat keamanan tinggi dan kinerja proses yang efisien dalam pengamanan data digital (Putra et al., 2023). Sistem juga menunjukkan kemampuan yang baik dalam integrasi basis data untuk menyimpan informasi dokumen terenkripsi secara terstruktur dan aman. Dengan demikian, *prototype* yang dikembangkan telah memberikan bukti bahwa kombinasi AES-256 dengan arsitektur sistem multiplatform dapat menjadi solusi yang relevan dalam meningkatkan keamanan dokumen notaris di era digital.

Secara keseluruhan, hasil penelitian ini menguatkan asumsi awal penelitian bahwa penerapan metode kriptografi modern mampu meminimalkan risiko kebocoran dokumen, serta meningkatkan keamanan transaksi data, sesuai dengan kajian literatur yang dirujuk pada bagian pendahuluan (Aswandi et al., 2025)(Risna et al., 2022).

4. KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa sistem keamanan dokumen notaris berbasis web dan mobile menggunakan algoritma AES-256 berhasil dikembangkan dan diimplementasikan guna meningkatkan perlindungan kerahasiaan dokumen legal yang dikelola oleh Notaris Wavie Laksono Putro, S.H., M.Kn. Sistem mampu melakukan proses enkripsi dan dekripsi dokumen secara optimal pada kedua platform, sehingga hanya pengguna yang memiliki otorisasi yang dapat mengakses data yang disimpan. Pengujian menggunakan metode *black box testing* menunjukkan bahwa seluruh fungsi berjalan sesuai spesifikasi, termasuk unggah dokumen, enkripsi, penyimpanan aman ke database, dekripsi, dan pengunduhan kembali dalam bentuk aslinya. Hal ini membuktikan bahwa sistem mampu menjawab permasalahan utama dalam penelitian, yaitu potensi risiko kebocoran, penyalahgunaan, dan hilangnya dokumen yang sebelumnya dikelola secara manual. Meskipun demikian, penelitian ini masih memiliki keterbatasan, seperti belum diterapkannya mekanisme keamanan tambahan berupa *digital signature*, manajemen kunci enkripsi secara terdistribusi, serta belum adanya integrasi dengan sistem arsip kenotariatan nasional. Oleh karena itu, pada penelitian selanjutnya disarankan untuk mengembangkan sistem dengan penambahan fitur autentikasi berlapis, pencatatan aktivitas pengguna yang lebih detail, serta optimalisasi performa untuk file berukuran besar. Dengan hasil dan evaluasi yang telah diperoleh, sistem ini dinilai layak digunakan dan dapat menjadi solusi efektif dalam mendukung proses digitalisasi keamanan dokumen notaris di Indonesia.

REFERENCES

- Angga, T. D., & Ayumi, V. (2025). Pengembangan Model Sistem Informasi Penerimaan Peserta Didik Baru di SMK Kebangsaan Menggunakan Metode Waterfal. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, 7(1), 48–55. <https://doi.org/https://doi.org/10.51401/jinteks.v7i1.5121>
- Aswandi, A. S., Sutoyo, M. N., & Pradipta, A. (2025). Analisis Performa dan Keamanan Implementasi Kriptografi Aes Untuk Penyandian Dokumen Berbasis Web. *Jurnal Mnemonic*, 8(1), 24–32. <https://doi.org/https://doi.org/10.36040/mnemonic.v8i1.12053>
- Ayu, T. D., & Asriningtias, Y. (2024). Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android Menggunakan Algoritma AES-256. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, 12(1), 143–154. <https://doi.org/https://doi.org/10.26418/justin.v12i1.71449>
- Baso, F., & Anriani, N. (2024). Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File. *Information Technology Education Journal*, 3(3), 84–87. <https://doi.org/https://doi.org/10.59562/intec.v3i3.5525>
- Fahlevvi, M. R., Putra, D. S. A., & Ariandi, W. (2025). Algoritma AES128-CBC (Advanced Encryption Standard) Untuk Enkripsi Dan Dekripsi Berkas Dokumen PT. Adiarta Muzizat. *Journal of Innovation And Future Technology (IFTECH)*, 7(1), 166–176. <https://doi.org/https://doi.org/10.47080/iftech.v7i1.3929>
- Ferryanto, J., Tan, W., & Sudirman, L. (2024). Potensi dan Tantangan Hukum Digitalisasi Layanan Kenotariatan: Analisis Komparatif Indonesia dan Amerika Serikat. *Jurnal Mediasas: Media Ilmu Syari'ah Dan Ahwal Al-Syakhshiyyah*, 7(2), 306–326. <https://doi.org/https://doi.org/10.58824/mediasas.v7i2.135>
- Idris, J. F., Prastyo, Y. D., Hardiansyah, R., Noventona, A. M. F., Haikal, F., Gusdevi, H., & Naseer, M. (2025). Pengujian Fungsional dan Struktural Aplikasi Pengajuan Cuti dengan Metode Black Box dan White Box. *Naratif: Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, 7(1), 84–102. <https://doi.org/https://doi.org/10.53580/naratif.v7i1.315>
- Jibril, M. (2024). Pengujian Sistem Informasi E-Modul Pada Smpn 1 Tempuling Menggunakan Black Box Testing. *Jurnal Perangkat Lunak*, 6(2), 327–332. <https://doi.org/https://doi.org/10.32520/jupel.v6i2.3326>
- Kholid, F., Anwar, M. M., Adiansyah, D., & Haryono, W. (2025). Perancangan Sistem Manajemen Dokumen Laporan Perusahaan Berbasis Web pada PT Inti Teknologi Indonesia. *Jurnal Komputer Antartika*, 3(2), 61–70. <https://doi.org/https://doi.org/10.70052/jka.v3i2.853>
- Mantik, J. T., & Yusupa, A. (2025). Pengembangan Sistem Manajemen File Terpusat Berbasis Web di Jaringan Lokal. *Applied Information Technology and Computer Science (AICOMS)*, 4(1), 33–42. <https://doi.org/https://doi.org/10.58466/aicoms.v4i1.1793>
- Menawati, E., & Muadah, S. (2024). Urgensi Penyimpngan Protokol Notaris Secara Elektronik Menuju Era Cyber Notaris. *Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced*, 2(4), 652–660.



- <https://doi.org/https://doi.org/10.61579/future.v2i4.232>
- Prasetyo, A., & Zulkarnain, A. (2025). Perancangan Sistem Absensi Berbasis Web yang Aman dengan Validasi Lokasi Menggunakan QR Code dan Pengendalian Akses Berbasis IP. *INSERT: Information System and Emerging Technology Journal*, 6(1), 72–82. <https://doi.org/https://doi.org/10.23887/insert.v6i1.94824>
- Putra, W., Fahlevi, M. R., & Hidayat, A. T. (2023). Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Dokumen. *Jurnal Ilmu Komputer, Teknologi Dan Informasi*, 1(2), 76–83. <https://doi.org/https://doi.org/10.62866/jurikti.v1i2.55>
- Ridho, A., & Romli, M. A. (2024). Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256). *Jurnal Informatika Teknologi Dan Sains (JINTEKS)*, 6(4), 1044–1052. <https://doi.org/https://doi.org/10.51401/jinteks.v6i4.4887>
- Risna, R., Amaliah, Y., & Yunita, S. (2022). Implementasi kriptografi pada pengamanan data pembayaran piutang pelanggan menggunakan Vigenere Cipher. *Sebatik*, 26(2), 525–534. <https://doi.org/https://doi.org/10.46984/sebatik.v26i2.2061>
- Santika, R., Febrianti, S., Hakeki, S., Supriyanto, Y., Abdullah, Z. F., & Atmaja, S. A. (2025). Analisis Kinerja Fungsional pada Aplikasi Mobile JKN Melalui Pengujian Black Box Testing. *Journal on Pustaka Cendekia Informatika*, 3(1), 59–68. <https://doi.org/https://doi.org/10.70292/pctif.v3i1.47>
- Saripa, S. (2024). Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi. *Progressive Information, Security, Computer, and Embedded System*, 2(1), 35–45. <https://doi.org/https://doi.org/10.61255/pisces.v1i2.100>
- Satria, R. Y., & Susanti, A. R. (2024). Implementasi Sistem Pengelolaan Data Verifikasi Calon Penerima Honorarium PTK PAUD Berbasis Web dengan Laravel. *Karimah Tauhid*, 3(10), 11118–11144. <https://doi.org/https://doi.org/10.30997/karimahtauhid.v3i10.15265>
- Tahir, M., Saputri, M. S., Aini, Q., & Hermawan, T. W. (2025). Penggunaan Algoritma AES (Advanced Encryption Standard) Pada Veracrypt Untuk Mengamankan Data Pada Perangkat Penyimpanan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(4), 6912–6918. <https://doi.org/https://doi.org/10.36040/jati.v9i4.14318>
- Vicky, V., Samosir, T., & Harlina, I. (2024). Akibat Hukum Bagi Notaris Yang Tidak Saksama Dalam Pembuatan Akta Kuasa Menjual (Studi Kasus Putusan No 20pk/Pid/2020). *Jurnal Hukum Sasana*, 10(2), 48–59. <https://doi.org/https://doi.org/10.31599/sasana.v10i2.2737>
- Zikri, M. A., Gazali, M. I., & Nugraha, R. D. (2025). Tantangan Dan Peluang Profesi Notaris Diera Digital. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 3(2), 2040–2046. <https://doi.org/https://doi.org/10.62976/ijijel.v3i2.1205>