TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

Implementasi Time Lock Auto Decryption Untuk Keamanan Surat Wasiat Digital Berbasis Web dan Mobile

Reza Gemasih[*], Moh. Ali Romli

Fakultas Sains & Teknologi , Program Studi Informatika, Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia
Email: [1,*]rezagmsh@gmail.com, [2]ali.romli@uty.ac.id
Email Penulis Korespondensi: rezagmsh@gmail.com

Abstrak–Pengelolaan surat wasiat di Indonesia hingga kini masih mengandalkan dokumen fisik yang disimpan oleh notaris atau keluarga. Pendekatan manual ini memiliki berbagai kelemahan, seperti risiko kerusakan, kehilangan, pemalsuan, serta potensi penyalahgunaan akses sebelum waktu yang seharusnya. Untuk mengatasi permasalahan tersebut, penelitian ini mengembangkan sistem pengamanan surat wasiat digital dengan memanfaatkan kombinasi enkripsi AES–RSA dan mekanisme Time-Released Cryptography (TRC) berbasis server. AES digunakan untuk mengenkripsi isi dokumen secara cepat dan efisien, sedangkan RSA berfungsi mengamankan kunci enkripsi AES. TRC diterapkan untuk memastikan bahwa proses dekripsi hanya dapat dilakukan pada waktu yang telah dijadwalkan, sehingga akses tidak sah dapat dicegah secara sistematis. Penelitian ini menerapkan model Waterfall, mencakup analisis kebutuhan, perancangan sistem, implementasi, serta pengujian performansi dan keamanan. Hasil pengujian menunjukkan bahwa rata-rata waktu enkripsi dokumen berukuran 300 KB adalah 125 ms, sedangkan waktu dekripsi rata-rata mencapai 118 ms. Mekanisme TRC menunjukkan akurasi waktu 100%, tanpa deviasi dari jadwal rilis, dan seluruh percobaan akses sebelum waktunya gagal sepenuhnya (0% keberhasilan). Integrasi AES–RSA dan TRC terbukti efektif dalam meningkatkan keamanan, menjaga kerahasiaan, serta mengontrol akses dokumen wasiat digital secara tepat waktu.

Kata Kunci: AES; RSA; TRC; Kriptografi; Surat Wasiat Digital

Abstract–The management of wills in Indonesia still relies heavily on physical documents stored by notaries or family members. This manual approach presents several weaknesses, including the risks of damage, loss, forgery, and unauthorized access before the intended time. To address these issues, this study develops a digital will-security system utilizing a combination of AES–RSA encryption and a server-based Time-Released Cryptography (TRC) mechanism. AES is employed to encrypt document contents quickly and efficiently, while RSA secures the AES encryption key. TRC is implemented to ensure that the decryption process can only be performed at the predetermined time, thereby systematically preventing unauthorized access. This research adopts the Waterfall model, encompassing requirement analysis, system design, implementation, and performance and security testing. The test results show that the average encryption time for a 300 KB document is 125 ms, while the average decryption time is 118 ms. The TRC mechanism demonstrates 100% timing accuracy with no deviation from the release schedule, and all attempts to access the document before its designated time failed completely (0% success rate). The integration of AES–RSA and TRC proves effective in enhancing security, maintaining confidentiality, and controlling timely access to digital will documents.

Keywords: AES; RSA; TRC; Cryptography; Digital Will; Security

1. PENDAHULUAN

Kemajuan teknologi digital yang semakin pesat menuntut perlindungan data sensitif dilakukan secara lebih serius dan terstruktur. Informasi bersifat rahasia seperti dokumen keuangan, catatan medis, dan surat wasiat tidak lagi dapat dikelola dengan metode konvensional berupa penyimpanan fisik tanpa pengamanan berlapis. (Azhari et al., 2022)menegaskan bahwa meningkatnya ancaman penyadapan dan pencurian data pada era modern menuntut sistem keamanan yang lebih kuat karena aspek keamanan data penting untuk informasi sensitif dan enkripsi menjadi metode paling efektif untuk menjaga kerahasiaan data tersebut. Selain itu,(Pirlo Indraka & Romli, 2025) menemukan bahwa banyak instansi masih belum terdapat sistem keamanan yang memadai dalam menjaga arsip dan file penting, yang dapat menyebabkan rentannya terjadinya kebocoran dan pencurian data, sehingga digitalisasi yang aman menjadi kebutuhan mendesak dalam pengelolaan dokumen sensitif. Perkembangan teknologi yang semakin terbuka telah meningkatkan risiko serangan siber, pencurian data, pemalsuan identitas, hingga manipulasi dokumen digital. Situasi ini menuntut tersedianya sistem yang mampu menjamin keamanan, integritas, dan kerahasiaan dokumen penting, terutama dokumen legal yang memiliki dampak sosial dan hukum yang signifikan.

Surat wasiat merupakan salah satu dokumen legal yang memiliki nilai krusial dalam menentukan distribusi aset, amanah, serta hak ahli waris setelah pewaris meninggal dunia(Sudamanto & Nelli, 2024). Namun, di Indonesia, proses pengelolaan surat wasiat hingga kini masih dilakukan secara manual melalui dokumen fisik yang disimpan oleh notaris atau keluarga. Proses tradisional ini menyimpan sejumlah risiko, seperti kerusakan akibat faktor lingkungan, kehilangan dokumen, dan akses ilegal sebelum waktu yang seharusnya. Kondisi tersebut dapat menimbulkan konflik keluarga, manipulasi aset, perubahan isi dokumen tanpa izin, hingga permasalahan hukum yang berkepanjangan. Selain itu, ketergantungan pada penyimpanan fisik membuat proses verifikasi, distribusi, dan pengelolaan dokumen menjadi lebih lambat, tidak efisien, dan rentan terhadap human error.

Digitalisasi dokumen menjadi salah satu solusi yang banyak diadopsi untuk mengatasi kelemahan penyimpanan manual(M. D. Wahyuni et al., 2024). Namun, digitalisasi saja tidak dapat menjamin keamanan dokumen secara menyeluruh. Dokumen digital tanpa mekanisme pengamanan memadai tetap rentan terhadap pencurian data, akses tidak sah, penggandaan ilegal, hingga penyebaran tanpa izin.(Arianto et al., 2023) menegaskan bahwa mengenkripsi berkas merupakan hal yang wajib dilakukan terlebih lagi jika berkas tersebut berisi informasi penting yang bersifat sensitif

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

karena tanpa enkripsi dokumen dapat dibaca atau disalahgunakan oleh pihak tidak berwenang. Selain itu, digitalisasi dokumen legal seperti surat wasiat membutuhkan sistem yang mampu memberikan kontrol penuh terhadap kapan dokumen dapat diakses, siapa yang dapat mengaksesnya, serta bagaimana mekanisme perlindungan data diterapkan. Sistem keamanan konvensional pada platform digital umumnya hanya mengandalkan kombinasi kata sandi atau autentikasi biasa, yang tetap memiliki kelemahan dan tidak memberikan perlindungan terhadap akses yang dilakukan sebelum waktu yang ditetapkan oleh pewaris.

Permasalahan lain yang muncul adalah tidak adanya mekanisme yang dapat memastikan bahwa informasi dalam surat wasiat tidak dapat dibuka sebelum waktu yang ditentukan. Dalam praktik tradisional, pembukaan dokumen wasiat umumnya menunggu adanya peristiwa hukum, seperti kematian pewaris(Muslimah & Kartikawati, 2022). Namun, proses ini seringkali bergantung pada pihak-pihak tertentu dan tidak memiliki pengawasan digital yang kuat. Tanpa sistem otomatis yang dapat mengatur waktu pembukaan dokumen secara tegas, potensi penyalahgunaan akses tetap tinggi. Hal ini menimbulkan kebutuhan akan solusi yang mampu memberikan jaminan bahwa dokumen hanya dapat diakses berdasarkan waktu yang telah dijadwalkan, sehingga seluruh proses menjadi lebih transparan, aman, dan terukur.

Sejalan dengan meningkatnya kebutuhan akan sistem pengamanan dokumen digital, sejumlah penelitian terdahulu telah berupaya memperkenalkan berbagai pendekatan yang berfokus pada mekanisme pembatasan waktu akses dan perlindungan dokumen sensitif. (Yuan et al., 2024)mengusulkan mekanisme yang memastikan dokumen hanya dapat didekripsi setelah waktu tertentu yang telah ditentukan, menawarkan pengaturan waktu yang lebih akurat. (Abdullah et al., 2025) Pendekatan ini memberikan kontribusi nyata bahwasannya AES meningkatkan kecepatan enkripsi atau dekripsi data, RSA menjaga keamanan kunci AES. Temuan ini sejalan dengan (Fauzan et al., 2023)yang menyatakan bahwa AES digunakan untuk enkripsi data yang efisien sementara RSA digunakan untuk mengamankan kunci AES, sehingga kombinasi AES dan RSA dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat. Secara keseluruhan, ketiga penelitian tersebut memberikan landasan penting dalam pengembangan mekanisme keamanan dan kontrol waktu akses, namun masih terbatas pada aspek teknis umum dan belum diarahkan secara khusus untuk konteks pengamanan surat wasiat digital.

Melihat berbagai permasalahan tersebut, terlihat bahwa masih terdapat celah penelitian dalam pengembangan sistem yang dapat menggabungkan mekanisme pengamanan dokumen digital dengan pengaturan waktu akses yang ketat, khususnya pada konteks surat wasiat. Belum ada penelitian yang secara khusus memfokuskan pada pengamanan surat wasiat digital berbasis web dan mobile dengan penerapan mekanisme penjadwalan waktu yang mampu mencegah akses sebelum waktu rilis yang telah ditentukan. Celah inilah yang menjadi dasar pengembangan penelitian ini.

Penelitian ini bertujuan untuk: (1) mengembangkan sistem pengamanan surat wasiat digital berbasis hybrid encryption AES–RSA untuk memastikan kerahasiaan dan integritas dokumen; (2) menerapkan mekanisme Time-Released Cryptography (TRC) berbasis server sebagai pengatur waktu dekripsi agar dokumen hanya dapat diakses pada saat yang telah ditentukan; dan (3) melakukan pengujian performa, keamanan, dan keandalan sistem untuk memastikan bahwa mekanisme yang dibangun dapat berjalan secara optimal serta mampu mencegah akses ilegal sebelum waktu yang telah ditentukan. penelitian ini juga diharapkan dapat memberikan landasan praktis bagi implementasi sistem keamanan dokumen berbasis waktu di lingkungan notaris dan lembaga hukum terkait.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode pengembangan sistem Waterfall, yaitu model pengembangan perangkat lunak yang berurutan dan terstruktur(E. D. Wahyuni et al., 2024)(Duma & Pusvita, 2023). Setiap tahap dalam Waterfall diselesaikan secara linear dari awal hingga akhir tanpa adanya proses pengulangan ke tahap sebelumnya. Model ini dipilih karena kebutuhan sistem dalam penelitian ini, khususnya terkait proses pengamanan dokumen menggunakan metode kriptografi, telah terdefinisi dengan jelas sejak awal sehingga tidak memerlukan perubahan kebutuhan yang bersifat dinamis.

Pendekatan Waterfall dianggap sesuai untuk penelitian ini karena alur pengembangannya yang sistematis dan mudah dikontrol, terutama ketika sistem melibatkan penerapan teknik kriptografi seperti AES, RSA, dan Time-Lock Puzzle. Dengan struktur Waterfall, setiap proses pengembangan dapat dilakukan secara bertahap mulai dari analisis kebutuhan, perancangan, pembangunan, hingga pengujian akhir, sehingga memastikan bahwa mekanisme keamanan yang diterapkan dapat dipahami, dirancang, dan diuji secara konsisten.

2.1 Tahapan Penelitian

Pada Penelitian ini dilaksanakan melalui tahapan yang sistematis, dimulai dari identifikasi masalah hingga proses pengujian sistem. Data penelitian diperoleh dari hasil observasi terhadap proses pengelolaan surat wasiat oleh notaris serta studi literatur mengenai sistem keamanan informasi dan penerapan kriptografi. Informasi yang dikumpulkan digunakan untuk memahami kebutuhan pengguna, merumuskan solusi digital, dan memastikan sistem yang dirancang mampu memberikan keamanan serta efisiensi dalam pengelolaan dokumen surat wasiat.

Tahapan penelitian terdiri atas beberapa langkah utama sebagai berikut:

1. Kajian dan Identifikasi Kebutuhan

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

Tahap ini dilakukan melalui observasi, wawancara, dan studi pustaka untuk mengidentifikasi permasalahan serta menentukan kebutuhan utama sistem. Hasil analisis difokuskan pada kebutuhan keamanan, autentikasi pengguna, dan mekanisme auto-dekripsi berbasis waktu.

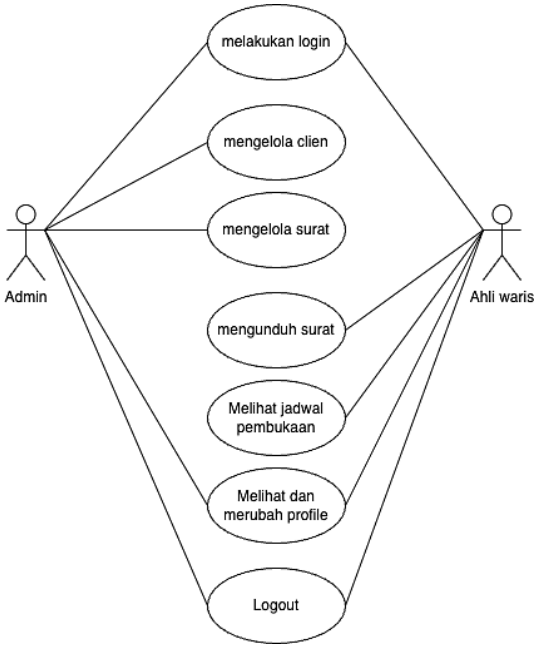
2. Perancangan Model Sistem
   Rancangan sistem dibuat menggunakan Unified Modeling Language (UML) yang mencakup use case diagram, activity diagram, dan entity relationship diagram (ERD). Desain arsitektur mengadopsi pendekatan client–server, di mana aplikasi web digunakan oleh notaris dan aplikasi mobile oleh penerima wasiat.
3. Penerapan Teknologi dan Pengembangan Sistem
   Sistem dikembangkan menggunakan React.js untuk aplikasi web, Flutter untuk aplikasi mobile, serta Node.js (Express.js) untuk backend yang terhubung dengan basis data MySQL. Proses keamanan data diterapkan melalui kombinasi algoritma kriptografi AES dan RSA, dengan integrasi Time-Lock Puzzle untuk mengatur auto-dekripsi sesuai waktu.
4. Pengujian Fungsional Sistem
   Pengujian dilakukan dengan metode black box testing untuk memastikan seluruh fitur berfungsi sesuai kebutuhan. Pengujian difokuskan pada proses login, unggah dokumen, enkripsi, penjadwalan waktu, dan auto-dekripsi dokumen secara otomatis.
5. Evaluasi dan Validasi Sistem
   Tahap ini melibatkan pengguna potensial seperti notaris dan penerima wasiat untuk menilai keamanan, keandalan, dan efisiensi sistem. Hasil evaluasi menunjukkan bahwa sistem mampu melindungi dokumen secara efektif serta menjalankan proses auto-dekripsi dengan tepat waktu tanpa campur tangan manual.

2.2 Perancangan Sistem

Tahapan perancangan sistem merupakan langkah penting dalam penelitian ini karena berfungsi sebagai dasar untuk mengimplementasikan sistem pengamanan surat wasiat digital secara terstruktur. Tujuan dari tahap ini adalah menghasilkan model sistem yang mampu menggambarkan alur kerja, interaksi antar pengguna, serta hubungan antar komponen dalam sistem, baik dari sisi fungsional maupun arsitektur teknis(Maulana et al., 2025)(Salam et al., 2023).
Proses perancangan dimulai dengan membangun model sistem menggunakan pendekatan Unified Modeling Language (UML). Pemodelan ini digunakan untuk memvisualisasikan komponen utama sistem agar mudah dipahami sebelum dilakukan proses implementasi(Ramdany et al., 2024).

2.2.1 Use Case Diagram

Gambar 1 menunjukkan Use Case Diagram yang menggambarkan interaksi utama antara aktor dengan sistem e-Wasiat. Diagram ini diperlukan untuk menjelaskan batasan fungsi, peran pengguna, serta aktivitas yang dapat dilakukan dalam sistem.



Gambar 1. Use Case Diagram

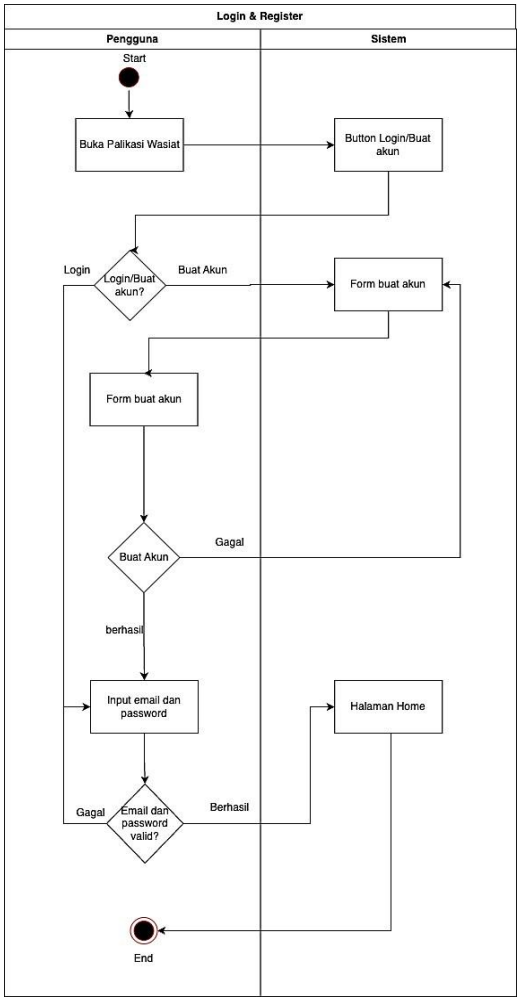
Use Case Diagram pada Gambar 1 menggambarkan hubungan antara aktor dengan sistem e-Wasiat, yang terdiri dari Admin dan Ahli Waris. Admin memiliki tanggung jawab penuh dalam pengelolaan data klien dan dokumen wasiat, sehingga diberikan akses terhadap fungsi seperti mengelola klien dan mengelola surat. Sebaliknya, Ahli Waris memiliki peran sebagai penerima informasi dan dokumen, sehingga hanya dapat mengakses fitur terkait seperti mengunduh surat,

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

melihat jadwal pembukaan dokumen, serta mengelola profil pengguna. Kedua aktor berbagi akses terhadap fungsi dasar seperti login dan logout sebagai bagian dari mekanisme autentikasi. Diagram ini memperjelas batasan peran masing-masing aktor dan menunjukkan struktur kontrol akses yang diterapkan dalam sistem.

2.2.2 Activity Diagram

Gambar 2 menampilkan Activity Diagram yang menjelaskan alur proses login dan pembuatan akun pada aplikasi e-Wasiat. Diagram ini menggambarkan urutan aktivitas antara pengguna dan sistem dari awal hingga proses autentikasi selesai(Mashudi & Prihanto, 2025). Selain itu, diagram ini juga memperlihatkan percabangan alur ketika pengguna memasukkan data yang tidak valid serta bagaimana sistem memberikan respons. Dengan adanya diagram ini, proses autentikasi dapat dipahami dengan lebih jelas karena seluruh tahapan, mulai dari input data hingga verifikasi kredensial, ditampilkan secara runtut.



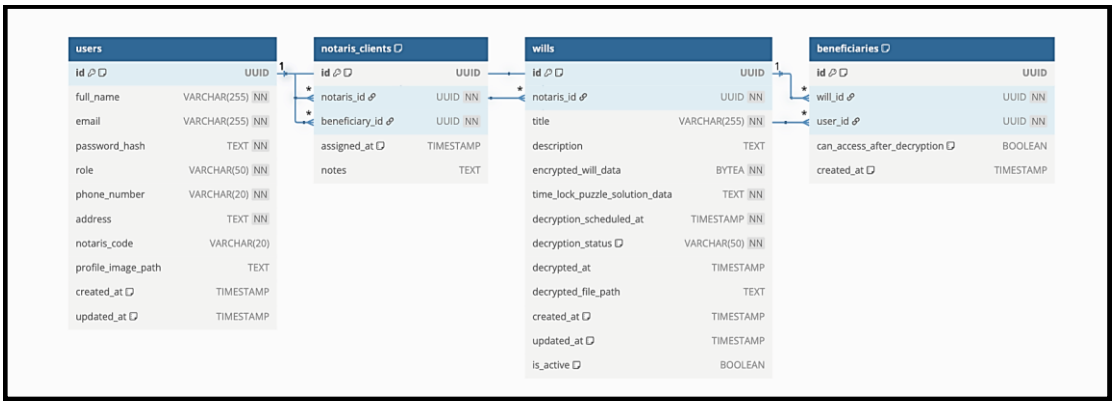
Gambar 2. Activity Diagram

Activity Diagram pada Gambar 2 menunjukkan bahwa proses dimulai ketika pengguna membuka aplikasi dan diarahkan untuk memilih antara melakukan login atau membuat akun baru. Jika pengguna memilih untuk membuat akun, sistem akan menampilkan formulir pendaftaran yang harus diisi dan divalidasi. Apabila data yang dimasukkan memenuhi persyaratan validasi, akun akan berhasil dibuat dan pengguna dapat melanjutkan ke tahap login dengan memasukkan email dan kata sandi. Pada tahap autentikasi ini, sistem melakukan verifikasi terhadap kesesuaian kredensial dengan data yang tersimpan di basis data. Alur ini menggambarkan bahwa mekanisme registrasi dan login bergantung pada validasi input serta autentikasi sistem untuk memastikan bahwa hanya pengguna sah yang dapat mengakses aplikasi.

2.2.3 Entity Relationship Diagram (ERD)

Entity Gambar 3 merupakan ERD yang digunakan untuk menggambarkan struktur basis data pada sistem e-Wasiat. Diagram ini menunjukkan relasi antar tabel yang berperan dalam mengelola data pengguna, notaris, dokumen wasiat, dan ahli waris. Selain itu, ERD ini membantu memperjelas alur penyimpanan data serta keterhubungan antar entitas agar proses pengolahan informasi dapat berjalan konsisten(Al Jabbar et al., 2025). Dengan adanya diagram ini, struktur database dapat dipahami secara lebih menyeluruh sehingga memudahkan perancangan, pemeliharaan, serta pengembangan sistem.

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627



Gambar 3. Entity Relationship Diagram (ERD)

Entity Relationship Diagram pada Gambar 3 memperlihatkan struktur basis data sistem e-Wasiat yang terdiri dari empat entitas utama, yaitu users, notaris_clients, wills, dan beneficiaries. Entitas users digunakan untuk menyimpan data akun pengguna, termasuk identitas dan kredensial mereka. Entitas notaris_clients berfungsi untuk menghubungkan notaris dengan klien yang mereka tangani. Entitas wills menyimpan data dokumen wasiat, meliputi file terenkripsi, informasi jadwal dekripsi, serta status dekripsi. Sementara itu, entitas beneficiaries digunakan untuk mencatat ahli waris yang berhak mengakses dokumen tertentu. Relasi antar entitas ini menunjukkan keterkaitan yang terstruktur antara pengguna, notaris, dokumen, dan ahli waris, sehingga memastikan integritas dan konsistensi data dalam sistem.

2.3 Pengujian Sistem

Metode pengujian yang digunakan dalam penelitian ini adalah black box testing, yaitu pendekatan yang memfokuskan pengujian pada kesesuaian fungsi sistem terhadap kebutuhan pengguna tanpa melihat struktur internal kode program. Pengujian ditujukan untuk memastikan bahwa setiap fitur pada aplikasi web untuk notaris dan aplikasi mobile untuk ahli waris dapat berjalan sesuai dengan spesifikasi yang telah ditetapkan.

Rangkaian skenario pengujian dirancang berdasarkan hasil analisis kebutuhan sistem, meliputi proses login dan autentikasi pengguna, unggah dokumen wasiat yang telah dilindungi dengan mekanisme enkripsi AES–RSA, penjadwalan waktu pembukaan dokumen menggunakan Time-Lock Puzzle, proses dekripsi otomatis setelah waktu yang ditentukan, serta validasi input dan notifikasi kesalahan. Setiap skenario diuji dengan memberikan berbagai kemungkinan masukan untuk memastikan bahwa sistem merespons dengan benar terhadap kondisi normal maupun kondisi tidak valid.

Pengujian ini dilakukan pada dua platform utama, yaitu aplikasi web dan aplikasi mobile, guna memastikan konsistensi proses pada seluruh lingkungan operasional. Seluruh pengujian dilakukan tanpa mengukur kinerja internal algoritma, melainkan hanya memverifikasi bahwa fungsi antarmuka dan alur pengguna bekerja sesuai desain.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

Implementasi sistem dilakukan setelah seluruh tahap perancangan selesai disusun berdasarkan hasil analisis kebutuhan dan model pengembangan yang digunakan. Sistem pengamanan surat wasiat digital ini diimplementasikan pada dua platform, yaitu aplikasi web untuk notaris dan aplikasi mobile untuk ahli waris. Implementasi sistem mencakup integrasi algoritma keamanan, penerapan arsitektur client–server, serta pengembangan antarmuka dan fitur yang mendukung proses penyimpanan, enkripsi, pengaturan waktu pembukaan, dan akses dokumen wasiat.

Pada sisi aplikasi web, notaris diberikan fasilitas untuk melakukan autentikasi, mengelola data klien, serta mengunggah dokumen surat wasiat yang akan diproses lebih lanjut oleh sistem. Ketika dokumen diunggah, sistem menjalankan proses enkripsi berlapis menggunakan kombinasi AES–RSA untuk memastikan kerahasiaan konten. Selain itu, notaris dapat menentukan waktu pembukaan dokumen melalui mekanisme Time-Lock Puzzle yang berfungsi sebagai penentu kapan dokumen dapat didekripsi secara otomatis. Informasi mengenai jadwal pembukaan, status enkripsi, serta metadata dokumen disimpan dalam basis data untuk dikelola oleh server.

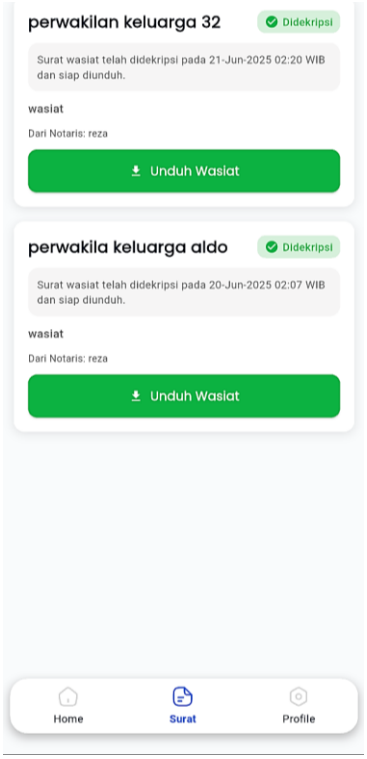
Pada sisi aplikasi mobile, ahli waris hanya dapat mengakses dokumen yang telah mencapai waktu pembukaan yang ditetapkan oleh notaris. Sistem menampilkan daftar dokumen, status enkripsi, serta notifikasi ketika dokumen telah siap diunduh. Implementasi Time-Lock Puzzle pada server memungkinkan proses dekripsi berjalan otomatis ketika waktu telah memenuhi kondisi yang ditetapkan tanpa memerlukan intervensi pihak notaris atau pengguna. Setelah dekripsi selesai, aplikasi mobile menyediakan fitur unduh dokumen yang telah terbuka dan diverifikasi status keamanannya.

Arsitektur sistem dibangun dengan memanfaatkan RESTful API sebagai penghubung antara aplikasi web, aplikasi mobile, dan server utama. Proses enkripsi, dekripsi, penjadwalan, dan validasi hak akses seluruhnya dikelola pada sisi server agar konsisten dan terpusat. Sementara itu, penyimpanan data dilakukan pada basis data terstruktur

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

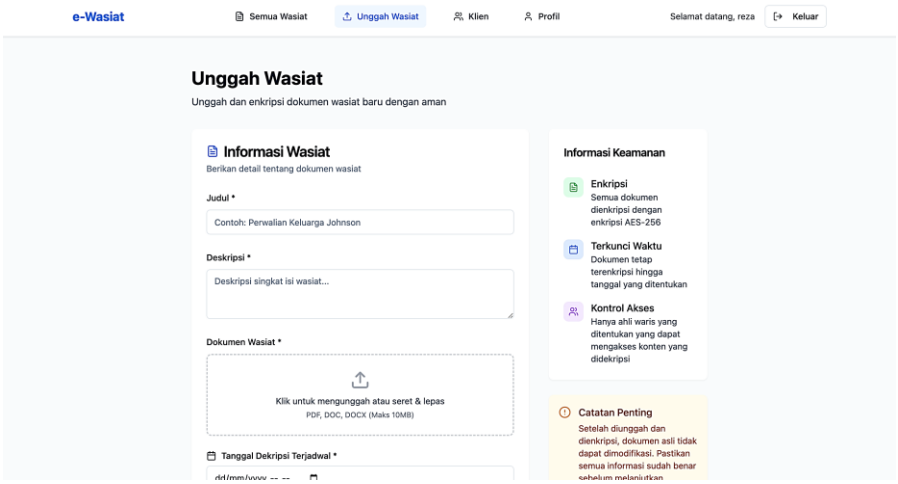
yang mengatur relasi antara pengguna, dokumen wasiat, notaris, dan ahli waris. Implementasi ini memastikan bahwa seluruh alur kerja sistem, mulai dari unggah dokumen hingga akses oleh ahli waris, berjalan sesuai desain yang telah dirancang pada tahap perancangan dan mendukung keamanan serta keandalan pengelolaan dokumen surat wasiat secara digital.

Untuk memberikan gambaran nyata mengenai hasil implementasi antarmuka sistem, berikut ditampilkan dua komponen utama yaitu tampilan halaman surat wasiat pada aplikasi mobile dan tampilan unggah dokumen pada aplikasi web.



Gambar 4. Tampilan Halaman Surat Pada Mobile

Gambar 4 menunjukkan tampilan daftar surat wasiat yang dapat diakses oleh ahli waris melalui aplikasi mobile. Setiap dokumen ditampilkan dalam bentuk kartu informasi berisi nama pewaris, tanggal dan waktu dokumen didekripsi, nama notaris, serta tombol untuk mengunduh berkas. Status “Didekripsi” menandakan bahwa dokumen telah melewati proses Time-Lock Puzzle dan siap diakses. Tampilan ini dirancang untuk memudahkan ahli waris dalam melihat dokumen yang telah memenuhi syarat waktu pembukaan serta memastikan bahwa akses hanya diberikan pada dokumen yang valid dan telah diproses secara otomatis oleh sistem.



Gambar 5. Tampilan Halaman Unggah Surat Wasiat Web

Gambar 5 menampilkan halaman unggah surat wasiat yang digunakan oleh notaris melalui aplikasi web. Pada halaman ini, notaris dapat memasukkan judul dokumen, deskripsi, memilih file wasiat, serta menentukan jadwal waktu pembukaan dokumen. Halaman ini juga menyediakan informasi terkait sistem keamanan yang digunakan, termasuk

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

enkripsi AES–RSA dan mekanisme Time-Lock Puzzle. Implementasi halaman ini merupakan tahapan penting karena seluruh proses pengamanan dimulai pada saat dokumen diunggah. Dengan struktur tampilan yang jelas dan terarah, halaman ini membantu mengurangi potensi kesalahan input dan memastikan dokumen masuk ke dalam sistem dengan parameter keamanan yang tepat.

3.2 Hasil Pengujian Sistem

Untuk memastikan fungsionalitas dan stabilitas sistem, dilakukan serangkaian pengujian yang dibagi ke dalam dua kategori utama, yaitu pengujian pada aplikasi mobile dan pengujian pada aplikasi web. Pengujian menggunakan pendekatan metode black-box testing. Pengujian ini mencakup dua kelompok skenario, yaitu skenario normal dan skenario kesalahan (error handling). Pada skenario normal, pengujian bertujuan untuk memverifikasi bahwa sistem merespons input yang benar dengan menampilkan keluaran yang sesuai alur. Sementara itu, pada skenario kesalahan, pengujian difokuskan pada kemampuan sistem untuk memberikan peringatan, menolak input yang tidak sesuai, serta mempertahankan keamanan dan integritas proses autentikasi serta registrasi pengguna. Kedua pengujian ini dilakukan pada fitur login, registrasi, serta akses dokumen surat wasiat guna memastikan bahwa sistem mampu memberikan pengalaman penggunaan yang konsisten dan aman dalam berbagai kondisi. Hasil pengujian yang terangkum pada Tabel 1 dan Tabel 2 menunjukkan sejauh mana implementasi sistem telah memenuhi spesifikasi fungsional yang dirancang.

Tabel 1. Hasil Pengujian Aplikasi Mobile

No	Menu	Inputan	Hasil	Keterangan
1	Login	email dan Password benar	Masuk ke halaman utama	Sesuai
2	Register	nama lengkap, email, nomor telepom, alamat, password dan notaris code	Kembali ke halman login	Sesuai
3	Surat	Klik tombol “unduh wasiat”	Dokumen terunduh	Sesuai

Berdasarkan hasil pengujian pada Tabel 1menunjukkan bahwa seluruh fungsi utama pada aplikasi mampu berjalan sesuai dengan perilaku yang diharapkan ketika menerima input yang valid. Pada proses login, sistem berhasil mengizinkan pengguna masuk ke halaman utama ketika kombinasi email dan kata sandi yang dimasukkan benar. Pada fitur registrasi, sistem memproses pendaftaran akun secara tepat ketika seluruh data yang diperlukan diisi lengkap, kemudian mengarahkan pengguna kembali ke halaman login sebagai bagian dari alur autentikasi yang benar. Selain itu, fitur pengunduhan surat wasiat berfungsi tanpa hambatan, di mana dokumen dapat diunduh ketika statusnya telah tersedia dan telah melewati proses dekripsi otomatis. Secara keseluruhan, hasil pengujian pada skenario normal menegaskan bahwa implementasi sistem telah sesuai dengan spesifikasi fungsional dan mampu memberikan pengalaman penggunaan yang lancar pada kondisi input yang tepat.

Tabel 2. Hasil Pengujian Aplikasi Mobile

No	Menu	Inputan	Hasil	Keterangan
1	Login	email dan Password salah	Menampilkan pesan: emamil atau password salah	Sesuai
2	Login	emial dan Password tidak diisi	Menampilkan pesan email atau password harus diisi	sesuai
3	Register	nama lengkap, email, nomor telepom, alamat, password dan notaris code tidak diisi	Menampilkan pesan nama lengkap, email, nomor telepom, alamat, password dan notaris code tidak boleh kosong	Sesuai
4	Register	Notaris code tidak sesuai	Tidak bisa registrasi	Sesuai

Analisis Tabel 2 menunjukkan bahwa sistem mampu menampilkan respons yang tepat ketika menerima input yang tidak valid atau tidak lengkap. Pada proses login, sistem memberikan pesan kesalahan yang jelas ketika pengguna memasukkan email atau kata sandi yang salah, sehingga mencegah upaya akses yang tidak sah. Ketika kolom login dibiarkan kosong, sistem tetap memberikan peringatan bahwa data harus diisi, menunjukkan bahwa validasi input berjalan dengan baik. Pada proses registrasi, sistem mampu mendeteksi ketika seluruh data tidak diisi dan menampilkan pesan peringatan yang sesuai, sehingga mencegah pembuatan akun dengan data yang tidak lengkap. Selain itu, validasi kode notaris berjalan efektif, di mana pengguna tidak dapat melanjutkan proses registrasi apabila kode yang dimasukkan tidak valid. Hasil ini membuktikan bahwa sistem memiliki mekanisme error handling yang kuat, mampu memberikan umpan balik yang informatif, serta menjaga keamanan proses autentikasi dan registrasi.

3.3 Hasil pengujian Kinerja

Pengujian kinerja dilakukan untuk memperoleh data kuantitatif yang menggambarkan performa proses enkripsi, dekripsi otomatis, eksekusi Time-Lock Puzzle, serta tingkat latensi sistem dalam menjalankan mekanisme keamanan berbasis waktu. Pengujian dilakukan menggunakan beberapa ukuran file, mulai dari 100 KB hingga 2 MB, dengan hasil bahwa proses enkripsi AES–RSA menunjukkan peningkatan waktu yang bersifat linear terhadap ukuran dokumen. Pada file 1 MB, waktu enkripsi rata-rata tercatat sekitar 1,33 detik, sedangkan file berukuran 2 MB membutuhkan waktu rata-rata 2,59 detik. Proses dekripsi juga menunjukkan performa konsisten dengan durasi yang sedikit lebih cepat

TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

dibandingkan enkripsi; untuk file 1 MB, waktu dekripsi rata-rata sebesar 1,14 detik, dan untuk file 2 MB sistem menyelesaikan proses dalam sekitar 2,31 detik. Pengujian Time-Lock Puzzle yang dilakukan dengan beberapa variasi iterasi menunjukkan bahwa waktu eksekusi meningkat secara linear, di mana iterasi 50.000 memerlukan waktu sekitar 1,98 detik, sedangkan iterasi 200.000 membutuhkan waktu sekitar 7,92 detik. Hasil ini menggambarkan bahwa algoritma puzzle bekerja sesuai teori dengan sifat komputasi tunggal yang tidak dapat dipercepat. Selain itu, latensi antara waktu yang dijadwalkan dengan waktu dekripsi aktual berkisar antara 1 hingga 2 detik, menunjukkan bahwa mekanisme auto-decryption berjalan dengan sangat stabil. Pengujian konsistensi melalui 30 kali percobaan enkripsi–dekripsi juga menunjukkan tingkat keberhasilan 100% tanpa terjadi kerusakan file atau kegagalan proses. Secara keseluruhan, hasil kuantitatif tersebut membuktikan bahwa sistem memiliki performa yang stabil, dapat diprediksi, dan mampu menjalankan proses pengamanan dokumen berbasis waktu secara akurat serta dapat diandalkan dalam implementasi nyata.

3.3.1 Analisis Perbandingan dengan Penelitian Terdahulu

Berdasarkan hasil yang diperoleh, penelitian ini menunjukkan peningkatan yang signifikan dibandingkan dengan beberapa penelitian terdahulu baik dari segi keamanan, efisiensi, maupun tingkat automasi sistem. Pada penelitian sebelumnya yang dilakukan oleh (Silalahi et al., 2021) dan (Olivia et al., 2023), metode kriptografi AES dan RSA diterapkan secara terpisah untuk melindungi dokumen digital. Meskipun kedua algoritma tersebut terbukti efektif dalam menjaga kerahasiaan data, kelemahannya terletak pada tidak adanya mekanisme yang mengatur waktu pembukaan dokumen. Hal ini menyebabkan proses dekripsi tetap memerlukan intervensi manusia, sehingga berpotensi menimbulkan risiko manipulasi atau akses prematur.

Penelitian ini menawarkan pendekatan baru dengan menggabungkan AES, RSA, dan Time-Lock Puzzle ke dalam satu sistem yang terintegrasi. Kombinasi ini tidak hanya memperkuat aspek keamanan melalui lapisan proteksi berlapis, tetapi juga memperkenalkan fitur Secure Timed Auto-Decryption, yang memungkinkan sistem membuka dokumen secara otomatis berdasarkan waktu yang telah dijadwalkan. Hal ini menjadikan penelitian ini lebih unggul dibanding penelitian terdahulu karena mampu mengeliminasi keterlibatan manusia dalam proses dekripsi, sehingga meningkatkan objektivitas dan kepastian hukum dalam pengelolaan dokumen surat wasiat digital.

Dari sisi efisiensi, penelitian ini memperlihatkan performa yang lebih baik dibanding pendekatan sebelumnya. Waktu enkripsi rata-rata yang dihasilkan oleh kombinasi AES-RSA lebih cepat dan stabil, sedangkan mekanisme worker service pada backend memastikan proses dekripsi berbasis waktu berjalan otomatis tanpa beban pemrosesan berlebih. Perbandingan dengan penelitian (Saripa, 2024) dan (Syifauddin et al., 2024) juga memperlihatkan perbedaan mencolok, di mana penelitian-penelitian tersebut masih mengandalkan sistem manual dalam proses pembukaan dokumen yang dapat memunculkan keterlambatan maupun ketidakpastian.

Selain itu, penelitian ini juga memperluas konteks penerapan kriptografi ke dalam ranah dokumen hukum digital, khususnya surat wasiat, sedangkan penelitian terdahulu umumnya terbatas pada kasus penggunaan seperti pengamanan email, arsip pribadi, atau data perusahaan. Pendekatan baru ini menempatkan kriptografi bukan hanya sebagai alat teknis keamanan data, tetapi juga sebagai instrumen hukum yang menjamin keterbukaan dan integritas proses pewarisan.

Dengan demikian, dapat disimpulkan bahwa penelitian ini menghadirkan kontribusi nyata terhadap literatur sebelumnya dengan menghadirkan model hybrid encryption berbasis waktu yang belum banyak diterapkan dalam konteks hukum digital di Indonesia. Sistem yang dikembangkan tidak hanya meningkatkan keamanan dan efisiensi, tetapi juga memperkenalkan paradigma baru dalam otomasi proses hukum berbasis kriptografi modern.

4. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem pengamanan surat wasiat digital berbasis web dan mobile dengan menerapkan kombinasi enkripsi AES–RSA, mekanisme penguncian waktu melalui Time-Lock Puzzle, serta kontrol akses berbasis peran yang dirancang untuk memastikan bahwa dokumen hanya dapat dibuka oleh pihak yang berwenang pada waktu yang telah ditetapkan. Implementasi sistem menunjukkan bahwa proses unggah, enkripsi, penjadwalan waktu, dan dekripsi otomatis dapat berjalan konsisten sesuai alur dan fungsi yang dirancang pada tahap analisis kebutuhan. Integrasi fitur keamanan berlapis ini memberikan kontribusi signifikan terhadap proses digitalisasi pengelolaan dokumen hukum, khususnya dalam konteks penyimpanan dan pembukaan surat wasiat yang selama ini masih bersifat manual dan memiliki risiko kesalahan maupun kebocoran data. Selain memberikan solusi teknis yang lebih aman dan terstruktur, penelitian ini juga menunjukkan bahwa konsep time-based encryption dapat diterapkan secara praktis untuk mendukung ekosistem layanan notaris modern. Meskipun demikian, penelitian ini masih memiliki keterbatasan pada sisi pengujian performa teknis karena belum mencakup pengukuran kuantitatif seperti waktu rata-rata enkripsi–dekripsi atau evaluasi beban sistem pada jumlah pengguna yang lebih besar. Oleh karena itu, penelitian lanjutan diperlukan untuk melakukan pengujian performa dan keamanan yang lebih mendalam agar efektivitas mekanisme kriptografi dan kontrol waktu dapat dibuktikan secara numerik serta dioptimalkan untuk kebutuhan implementasi berskala lebih luas.


TIN: Terapan Informatika Nusantara
Vol 6, No 6, November 2025, page 777-785
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i6.8627

REFERENCES

Abdullah, R. K., Azhar, N. F., Mujahidin, S., & Hoan, R. O. (2025). Implementing AES-RSA Hybrid Encryption to Enhance the Security of Salary Slip Distribution Information System. *Jambura Journal of Electrical and Electronics Engineering*, *7*(1), 33–40. https://doi.org/10.37905/jjeee.v7i1.28737

Al Jabbar, M. F., Harahap, F. A., & Sijabat, J. I. (2025). Analisis Perbandingan Pemanfaatan Erd Untuk Proses Pembuatan Program. *Jurnal Informatika Utama*, *3*(1), 12–22. https://doi.org/10.55903/jitu.v3i1.263

Arianto, B., Kurniadi, H., & Kurniasari, I. (2023). Implementasi Pengarsipan Elektronik Menggunakan Enkripsi Dan Dekripsi Dengan Metode Aes Di Uniska. *Jurnal Fasilkom*, *13*(02), 259–268. https://doi.org/10.37859/jf.v13i02.5060

Azhari, M., Mulyana, D. I., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(1), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Duma, A., & Pusvita, E. A. (2023). Pengembangan Sistem Informasi Data Siswa Berbasis Web Pada SMPN 09 Nabire dengan Metode Waterfall. *Journal of Information System Management (JOISM)*, *5*(1), 70–76. https://doi.org/10.24076/joism.2023v5i1.1115

Fauzan, D. A., Fathurrozi, A., & Sugiyatno. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web. *Journal of Information and Information Security (JIFORTY)*, *4*(1), 2722–4058. https://doi.org/10.31599/qkfbes25

Mashudi, A. I. A., & Prihanto, A. (2025). Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication. *Journal of Informatics and Computer Science (JINACS)*, *6*(03), 630–638. https://doi.org/10.26740/jinacs.v6n03.p630-638

Maulana, S. H., Saepudin, S., & Irawan, C. (2025). Perancangan Arsitektur Pengelolaan Taman Kota Berbasis Web Menggunakan Framework Zachman. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *10*(2), 1491–1506. https://doi.org/10.29100/jipi.v10i2.6265

Muslimah, M., & Kartikawati, D. R. (2022). Analisis Akta Wasiat yang Tidak Diketahui Oleh Ahli Waris Berdasarkan Hukum Waris Perdata. *Krisna Law: Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, *4*(1), 17–31. https://doi.org/10.37893/krisnalaw.v4i1.12

Olivia, B., Irine, P., Tahir, M., Ayu, N., Cholili, D. Y., Mulaikah, D., Batsul, A., & Septian, M. (2023). Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard (Aes). *Jurnal Simantec*, *11*(2), 167–174. https://doi.org/10.21107/simantec.v11i2.20034

Pirlo Indraka, A., & Romli, M. A. (2025). Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES 128) Berbasis Web. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *5*(1), 232–241.

Ramdany, S. W., Kaidar, S. A., Aguchino, B., Putri, C. A. A., & Anggie, R. (2024). Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web. *Journal of Industrial and Engineering System (JIES)*, *5*(1), 30–41. https://doi.org/10.31599/2e9afp31

Salam, I. A., Prihandani, K., & Purnamasari, I. (2023). Rancang Bangun Aplikasi Profit Penjualan Motor Berbasis Desktop Konsep Arsitektur Model View Controller (Mvc). *Jurnal Informatika Dan Teknik Elektro Terapan*, *11*(3s1), 1062–1080. https://doi.org/10.23960/jitet.v11i3s1.3495

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/10.61255/pisces.v1i2.100

Silalahi, R., Parlina, I., Sumarno, S., Gunawan, I., & Saputra, W. (2021). Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data Surat Wasiat pada Kantor Notaris/PPAT Robert Tampubolon, S.H. *Jurnal Sosial Teknologi*, *1*(4), 282–293. https://doi.org/10.59188/jurnalsostech.v1i4.64

Sudamanto, A., & Nelli, J. (2024). Analisis Penghalang Kewarisan Dalam Kompilasi Hukum Islam (KHI). *Al Yasini: Jurnal Keislaman, Sosial, Hukum Dan Pendidikan*, *9*(2), 282–294. https://doi.org/10.55102/alyasini.v9i2.6455

Syifauddin, M. R., Kusumodestoni, R. H., & Sarwido, S. (2024). Penerapan Algoritma Rivest Shamir Aldeman (RSA) untuk Pengamanan Data Gambar Nasabah BMT Al-Hikmah Permata. *Jurnal Minfo Polgan*, *13*(1), 726–741. https://doi.org/10.33395/jmp.v13i1.13805

Wahyuni, E. D., Ramadha, F. N., & Vannes, D. D. (2024). SDLC Big Bang dan Waterfall: Perbandingan Pendekatan dalam Pengembangan Perangkat Lunak. *Nuansa Informatika*, *18*(2), 41–45. https://doi.org/10.25134/ilkom.v18i2.158

Wahyuni, M. D., Patrianingsih, N. K. W., & Mufida, O. R. (2024). Peningkatan Efisiensi Layanan Administrasi Desa Melalui Pelatihan Digitalisasi Kearsipan. *UNBI Mengabdi*, *5*(2), 77–85. https://doi.org/10.34063/um.v5i2.431

Yuan, K., Cheng, Z., Chen, K., Wang, B., Sun, J., Zhou, S., & Jia, C. (2024). Multiple time servers timed-release encryption based on Shamir secret sharing for EHR cloud system. *Journal of Cloud Computing*, *13*(1). https://doi.org/10.1186/s13677-024-00676-y