Jurnal Sains Informatika Terapan (JSIT)

E-ISSN: 2828-1659, Volume: 5, Issue: 1, Month: February, Year: 2026
Page: 76 - 84, Available online at: https://rcf-indonesia.org/home/

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 (RIJNDAEL) UNTUK KEAMANAN INFORMASI DOKUMEN RAHASIA PT. PLN (PERSERO) UP2B SISTEM MINAHASA

Merlin Aprilia Liow[1)], Gladly Caren Rorimpandey[2)*], Alfiansyah Hasibuan[3)]

[1,2,3] Program Studi Teknik Informatika, Universitas Negeri Manado
Corresponding Author: [2]gladlycrorimpandey@unima.ac.id

Article Info

Article history:

Received: Des 12, 2025
Revised: Des 19, 2025
Accepted: Des 22, 2025
Published: Feb 01, 2026

Keywords:

Document
AES-128
Encryption
Decryption
Security

ABSTRACT

The rapid advancement of digital technologies in the electricity sector has increased the demand for stronger information security systems, particularly in managing confidential documents that support operational decision-making. PT PLN (Persero) UP2B Sistem Minahasa serves as a critical unit responsible for regulating and monitoring electrical load distribution in North Sulawesi, making the protection of internal documents essential to maintaining operational integrity and confidentiality. However, the current document management process still relies on conventional methods and lacks the support of modern encryption technologies, leaving sensitive data vulnerable to unauthorized access, information leakage, and misuse. These risks became more evident following several data breach incidents reported in 2022 and 2023. This research focuses on developing a digital document security system utilizing the Advanced Encryption Standard (AES-128) algorithm to protect files in PDF, DOCX, XLS, and TXT formats. The research stages include requirement analysis, system design, implementation using PHP, MySQL, and OpenSSL, and performance testing for the encryption and decryption processes. The results indicate that AES-128 efficiently encrypts documents and produces files that cannot be accessed without a valid key, while the decryption process successfully restores the original content with an accuracy level of up to 90%. Overall, the implementation of this system significantly improves document security within UP2B Sistem Minahasa and can serve as a reference for strengthening information security policies across PLN units.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah cara institusi mengelola data dan dokumen, termasuk di sektor ketenagalistrikan [1]. Proses mengubah sistem manual atau analog menjadi sistem digital adalah digitalisasi [2]. Digitalisasi memberikan kemudahan dalam penyimpanan dan distribusi informasi, tetapi juga menghadirkan risiko baru berupa ancaman kebocoran, peretasan, dan penyalahgunaan data sensitif [3]. PT PLN (Persero), khususnya UP2B Sistem Minahasa, sangat bergantung pada dokumen digital seperti laporan beban harian, strategi pengendalian daya, evaluasiperforma sistem, serta dokumen kepegawaian rahasia yang mendukung pengambilan keputusan operasional. Meskipun digunakan oleh sekitar 40 pegawai dari berbagai divisi, perlindungan dokumen masih terbatas pada penggunaan kata sandi tanpa penerapan enkripsi menyeluruh. Kondisi ini meningkatkan potensi terjadinya kebocoran data, seperti dua insiden besar yang melibatkan jutaan data pelanggan PLN pada tahun 2022 dan 2023 [4,5]. Hal ini menunjukkan pentingnya perlindungan data pribadi sesuai ketentuan UU No. 27 Tahun 2022, karena kebocoran dapat berdampak pada manipulasi informasi, kerusakan sistem, hingga menurunnya kepercayaan publik [6].

Penerapan algoritma kriptografi seperti Advanced Encryption Standard (AES-128) dinilai sebagai solusi efektif karena menawarkan keamanan tinggi, kecepatan proses, dan efisiensi komputasi dibandingkan algoritma lama seperti DES atau 3DES yang telah dianggap rentan [7]. Oleh sebab itu, penelitian ini mengembangkan sistem enkripsi–dekripsi dokumen digital untuk format PDF, DOC,

XLS, dan TXT dengan memanfaatkan algoritma AES-128 (Rijndael) sebagai mekanisme utama perlindungan data.

2. METODOLOGI PENELITIAN

2.1. Metode Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan dengan memanfaatkan beragam metode untuk memperoleh informasi yang akurat, relevan, dan dapat dipertanggungjawabkan terkait sistem keamanan data di PT PLN (Persero) UP2B Sistem Minahasa. Pengumpulan data dilakukan melalui pengguna atau pemangku kepentingan untuk merumuskan kebutuhan sistem serta informasi yang diperlukan [9].

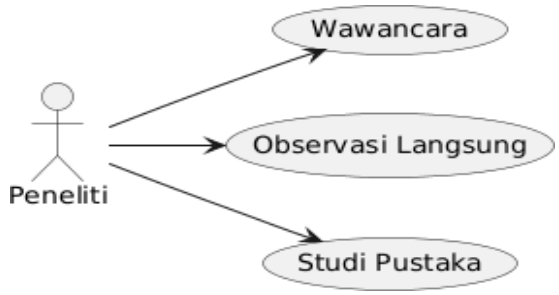

Figure 1. Metode Pengumpulan Data

2.1.1. Wawancara

Wawancara dilakukan untuk mengetahui kebutuhan pengguna terhadap sistem aplikasi, termasuk fitur yang diperlukan dan masalah yang ditemui selama penggunaan [15]. Wawancara dilakukan secara terstruktur dengan pihak-pihak terkait, yaitu Divisi Pengelola Data dan IT serta Divisi Keuangan dan Umum. Tujuan dari wawancara ini antara lain: memahami prosedur operasional standar (SOP) yang berlaku dalam pengelolaan data di UP2B Sistem Minahasa, mengidentifikasi kebijakan dan praktik keamanan data yang diterapkan, serta mengetahui permasalahan dan tantangan yang dihadapi dalam menjaga keamanan data.

2.1.2. Observasi Langsung (Direct Observation)

Observasi adalah teknik pengumpulan data yang melibatkan pengamatan langsung terhadap objek atau fenomena, dengan tujuan merekam kejadian, perilaku, atau situasi secara sistematis untuk mendapatkan data yang akurat [16]. Observasi dilakukan untuk mendapatkan pemahaman langsung mengenai beberapa hal, yaitu alur pengelolaan data, cara pencadangan (backup) data beserta langkah-langkah pengamanan fisik pada server, dan penerapan teknologi enkripsi pada server atau basis data apabila sudah diterapkan**.**

2.1.3. Studi Pustaka (Literature Study)

Studi pustaka adalah metode pengumpulan data yang dilakukan dengan cara menelaah dan menganalisis berbagai sumber tertulis, seperti buku, artikel jurnal, prosiding, dan publikasi ilmiah lainnya, yang relevan dengan topik penelitian guna memperoleh landasan teori, konsep, serta temuan terdahulu sebagai dasar dalam penyusunan penelitian [14]. Tujuan dari studi pustaka ini adalah untuk memperkuat landasan teori dalam pengembangan sistem pengamanan data dan untuk membandingkan praktik yang diterapkan di PLN UP2B Sistem Minahasa dengan praktik terbaik (best practices) secara global.

2.2. Tahapan Penelitian

Tahapan penelitian adalah serangkaian langkah yang disusun secara sistematis untuk membimbing peneliti dalam melaksanakan penelitian [14]. Tujuan utamanya adalah memastikan bahwa proses penelitian berlangsung terarah, hasil yang diperoleh valid, dan selaras dengan sasaran yang telah ditentukan. Dengan adanya tahapan ini, peneliti dapat menjalankan penelitian secara efisien dan mencapai tujuan penelitian secara optimal sesuai dengan tujuan yang telah ditentukan.

Berikut adalah tahapan penelitian yang dilakukan :

Tahapan penelitian merupakan langkah-langkah sistematis yang membimbing peneliti agar proses penelitian berjalan terarah, hasilnya valid, dan tujuan penelitian tercapai secara optimal. Berikut adalah tahapan penelitian yang dilakukan :

Figure 2. Tahapan Penelitian

2.1.1. Identifikasi Masalah

Tahapan pertama adalah identifikasi masalah, di mana peneliti menelaah kelemahan sistem pengelolaan dokumen digital di PT PLN (Persero) UP2B Sistem Minahasa, yang masih mengandalkan perlindungan konvensional tanpa enkripsi.

2.1.2. Studi Literatur

Selanjutnya, dilakukan studi literatur untuk memperkuat dasar teori, meninjau konsep keamanan informasi, kriptografi, dan penelitian terdahulu terkait penerapan AES-128.

2.1.3. Pengumpulan Data

Tahap pengumpulan data dilakukan melalui wawancara dengan pihak terkait, observasi lapangan, dan pengambilan dokumen operasional sebagai sampel untuk implementasi enkripsi.

2.1.4. Analisis Sistem yang Ada

Setelah data diperoleh, peneliti melakukan analisis sistem yang ada untuk memahami alur kerja, kelemahan, dan risiko yang dihadapi, sebagai dasar

2.1.5. Perancangan Sitem yang di usulkan

Perancangan sistem baru berbasis AES-128.

2.1.6. Implementasi

Sistem kemudian diimplementasikan menggunakan PHP, MySQL, dan OpenSSL, serta diuji pada berbagai jenis file dokumen (PDF, DOC, XLS, TXT).

2.1.7. Pengujian Sistem

Tahap pengujian sistem menilai fungsi enkripsi dan dekripsi, serta performa sistem dari sisi kecepatan, efisiensi, dan keamanan.

2.1.8. Evaluasi Hasil Penelitian

Hasil pengujian dibandingkan dengan sistem lama dalam tahap evaluasi, untuk mengetahui peningkatan keamanan dokumen rahasia.

2.1.9. Kesimpulan

Kesimpulan disusun sebagai ringkasan temuan utama dan rekomendasi pengembangan lebih lanjut agar sistem dapat diadaptasi di unit lain atau sektor serupa.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Kinerja Sistem Saat Ini dan Usulan Optimalisasi Sistem.

Sistem penyimpanan dokumen rahasia di Kantor PLN UP2B Sistem Minahasa saat ini masih memiliki keterbatasan. Dokumen hanya disimpan di komputer lokal tanpa mekanisme keamanan tambahan, dan belum tersedia fasilitas untuk penyimpanan atau pengolahan data secara online. Hal ini menimbulkan risiko serius terhadap kerahasiaan dokumen, termasuk kemungkinan kehilangan atau kebocoran data yang dapat disalahgunakan pihak tidak berwenang. Untuk mengatasi kelemahan tersebut, dibutuhkan sistem pengamanan digital yang lebih andal. Sistem yang diusulkan berupa website untuk enkripsi dan dekripsi dokumen, yang mampu mengubah file dokumen rahasia menjadi bentuk terenkripsi sehingga tidak dapat dipahami isinya. Sistem ini akan memanfaatkan database web hosting untuk penyimpanan online, dengan akses terbatas hanya kepada admin pengelola data. Dokumen akan dienkripsi menggunakan algoritma AES 128 Bit (Rijndael), memastikan bahwa data rahasia tetap terlindungi baik saat disimpan maupun saat diakses. Rancangan penelitian ini menekankan pembangunan sistem yang dapat mengenkripsi dokumen rahasia secara aman, sekaligus memberikan kemudahan dalam pengelolaan dan akses online.

3.1.1. Kondisi Awal

Pada tahap ini, data yang disiapkan terdiri dari dokumen rahasia yang diperoleh dari PLN UP2B Sistem Minahasa. File yang digunakan meliputi format *.docx, *.pdf, dan *.xls, masing-masing berisi informasi strategis dan sensitif milik PLN UP2B Sistem Minahasa.

3.1.2. Usulan Model

Tahapan implementasi enkripsi dokumen rahasia akan menggunakan algoritma AES 128 Bit (Rijndael). Model yang diusulkan meliputi beberapa langkah berikut:

a. Tahap Pertama

File diunggah ke sistem dengan format yang didukung (*.pdf, *.docx, *.xls, .txt) dan ukuran maksimal 5 MB.

b. Tahap Kedua

Pengguna memasukkan kunci simetris dengan panjang maksimal 16 karakter, yang akan digunakan untuk proses enkripsi file.

c. Tahap Ketiga

File yang diunggah dipecah menjadi blok string 16 karakter, kemudian di-XOR-kan dengan kunci simetris. Proses ini dalam algoritma AES dikenal sebagai AddRoundKey.

d. Tahap Keempat

Dilakukan proses SubBytes, yaitu substitusi hasil state sebelumnya menggunakan tabel S-Box, untuk mengacak data sesuai aturan algoritma AES 128 Bit.

e. Tahap Kelima

Dilakukan Shift-Row, di mana setiap baris pada array state digeser secara wrapping untuk meningkatkan keacakan data.

f. Tahap Keenam

Proses Mix-Column dilakukan dengan mengalikan array state hasil Shift-Row dengan matriks bilangan polinomial, untuk memperkuat difusi data.

g. Tahap Ketujuh

Dilakukan kembali AddRoundKey, di mana array state hasil Mix-Column di-XOR-kan dengan kunci simetris yang sama seperti tahap awal.

h. Tahap Kedelapan

Proses dari tahap ketiga hingga ketujuh diulang sebanyak 9 putaran. Putaran terakhir hanya melibatkan tahap AddRoundKey, Shift-Row, dan SubBytes, tanpa melalui Mix-Column, sesuai aturan AES-128.

i. Kondisi Akhir

Hasil akhir dari proses ini adalah file terenkripsi dengan ekstensi .rda, berisi karakter acak yang sulit dipahami. Dengan sistem ini, risiko penyalahgunaan dokumen bocor menjadi rendah, karena file hanya dapat dikembalikan ke bentuk semula melalui dekripsi menggunakan kunci simetris yang telah dimasukkan pada awal proses enkripsi.

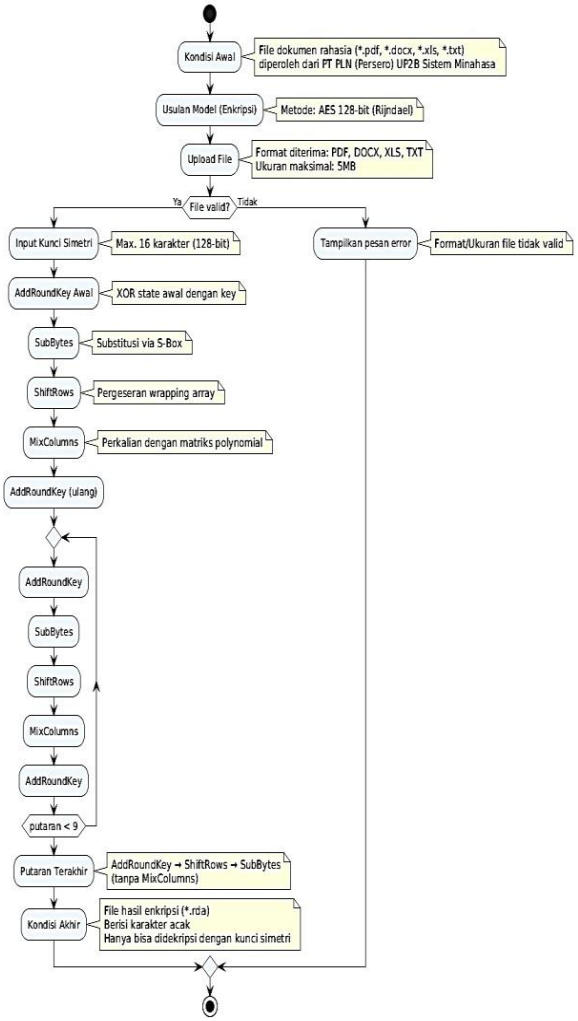

Figure 3. Flowchard Sistem yang di usulkan

3.2. Analisis Kebutuhan Sistem

3.2.1 Analisis Fungsional

Analisis fungsional adalah proses sistematis untuk mengidentifikasi, mendeskripsikan, dan mengatur fungsi-fungsi yang harus dilakukan oleh suatu sistem agar tujuan dan kebutuhan pemangku kepentingan dapat terpenuhi [13]. Kebutuhan fungsional pada sistem yang akan dikembangkan meliputi:

a. Analisis Kebutuhan Input

1) Input File Dokumen Rahasia

Sistem menerima file dokumen rahasia sebagai bahan untuk proses enkripsi dan dekripsi. File ini berisi data pegawai serta data operasional.

2) Input Kunci Simetris untuk Enkripsi

Sistem memerlukan kata kunci simetris dengan panjang maksimal 16 karakter, yang digunakan untuk proses enkripsi dan dekripsi dokumen.

b. Analisis Kebutuhan Proses

1) Proses Preprocessing

Tahap pengolahan awal file dokumen rahasia sebelum dilakukan enkripsi.

2) Proses Enkripsi

Tahap konversi dokumen dari bentuk asli (plaintext) menjadi bentuk terenkripsi (ciphertext), sehingga isi dokumen tidak dapat dipahami tanpa kunci yang sesuai.

3) Proses Dekripsi

Proses kebalikan dari enkripsi, yakni mengembalikan dokumen dari ciphertext menjadi plaintext menggunakan kunci simetris agar dokumen dapat diakses kembali.

c. Analisis Kebutuhan Output

1) Hasil Enkripsi

File hasil enkripsi dengan format .rda, berisi ciphertext yang tidak dapat dibaca secara langsung.

2) Hasil Dekripsi

File hasil dekripsi yang dikembalikan ke format asli sesuai file yang diunggah sebelumnya.

3.2.2. Analisis Non Fungsional

Kebutuhan non-fungsional mencakup spesifikasi perangkat keras dan perangkat lunak yang diperlukan agar sistem berjalan stabil, efisien, dan andal. Kebutuhan tersebut meliputi:

a. Perangkat Keras (Hardware)

Laptop yang digunakan dalam pengembangan sistem memiliki spesifikasi:

ASUS VivoBook X415EA Intel Core i5-1135G7 RAM 4GB SSD 256GB

b. Perangkat Lunak (Software)

Visual Studio Code digunakan sebagai editor untuk menulis dan mengelola kode program berbasis PHP. XAMPP digunakan sebagai server lokal untuk pengembangan dan pengujian aplikasi sebelum dipublikasikan.

3.3. Desain Sistem

Desain sistem dilakukan untuk menghasilkan rancangan teknis yang menjadi dasar implementasi sistem secara efektif [10]

3.3.1 Flowchard Sistem

Flowchart sistem digunakan untuk menggambarkan alur proses dan keputusan dalam suatu sistem secara sistematis [12]

Proses enkripsi diawali dengan pengunggahan file dokumen rahasia sebagai input, kemudian dilanjutkan dengan memasukkan kunci simetris.

Tahap pertama dalam enkripsi adalah AddRoundKey, di mana dilakukan operasi XOR antara state dan kunci, kemudian hasilnya dikonversi ke dalam bentuk bilangan heksadesimal. Selanjutnya, sistem memasuki tahap SubBytes, yaitu substitusi setiap byte menggunakan tabel S-Box untuk meningkatkan keamanan data.

Tahap berikutnya adalah ShiftRows, di mana setiap baris pada array state digeser menggunakan metode wrapping sehingga posisi byte berubah secara teratur. Setelah itu, dilakukan tahap MixColumns, yang berfungsi untuk mengacak data di setiap kolom array state sehingga difusi data lebih kuat.

Setelah tahap MixColumns, proses kembali ke AddRoundKey dan seluruh tahapan diulang sesuai jumlah putaran yang ditentukan. Pada final round, tahapan MixColumns tidak dilakukan, sehingga dihasilkan file dokumen rahasia dalam bentuk terenkripsi.

Proses dekripsi mengikuti langkah-langkah yang sama dengan enkripsi, tetapi dilakukan secara terbalik, dimulai dari tahap akhir menuju awal, sehingga dokumen terenkripsi dapat dikembalikan ke bentuk aslinya.. Flowchart algortima sistem yang dibangun dapat dilihat pada Figure 4. dan Figure 5.

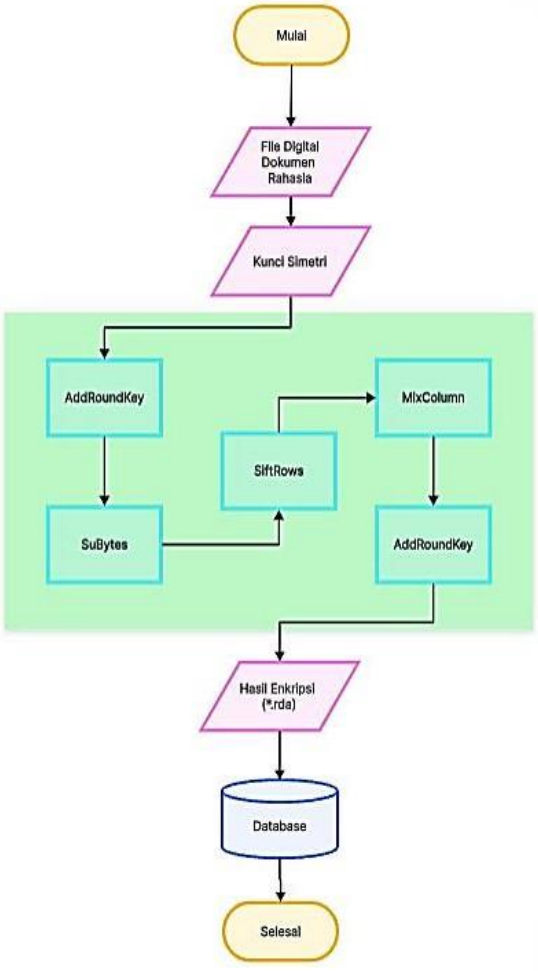

Figure 4. Proses Enkripsi

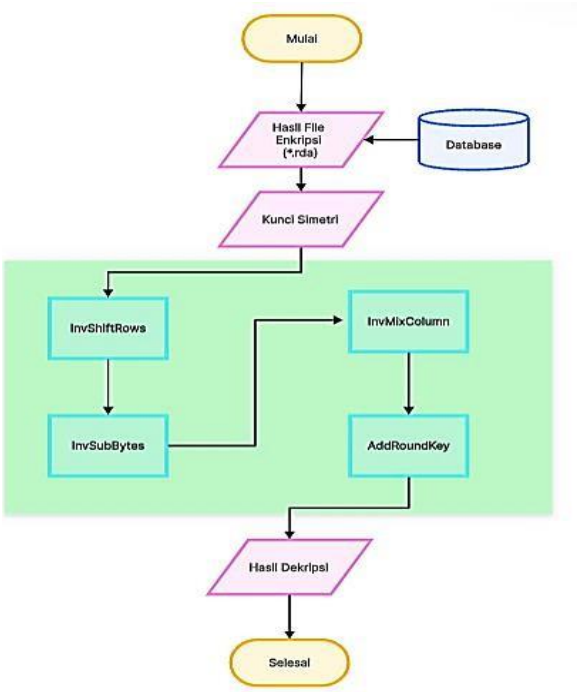

Figure 5. Proses Dekripsi

3.3.2 Use Case Diagram

Use Case Diagram merupakan bagian dari Unified Modeling Language (UML) yang digunakan untuk menggambarkan interaksi antara aktor dan sistem, serta menunjukkan fungsi-fungsi utama yang disediakan sistem dari sudut pandang pengguna tanpa menampilkan detail proses internal sistem [11]. Use Case Diagram bertujuan untuk menggambarkan fungsi utama sistem dari sudut pandang pengguna, dalam hal ini hanya aktor Admin. Admin memiliki beberapa kemampuan utama, yaitu login untuk mengakses sistem, mengunggah file sebagai dokumen sumber, melakukan enkripsi file menggunakan algoritma AES-128 dengan kunci 16 karakter, mendekripsi file untuk mengembalikan file terenkripsi menjadi file asli, melihat daftar file yang pernah diunggah atau dienkripsi, mengunduh file hasil enkripsi atau dekripsi, serta logout untuk keluar dari sistem.

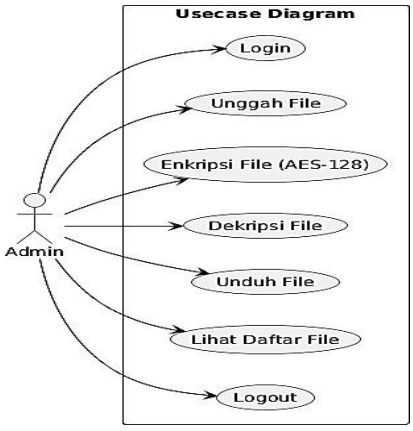

Figure 6. Use Case Diagram

Pada sistem ini, beberapa proses utama dijalankan oleh aktor Admin. Pertama, use case Login dilakukan ketika Admin membuka halaman login untuk memasukkan username dan password yang telah dimiliki. Sistem kemudian memvalidasi kredensial tersebut, dan apabila valid, Admin diarahkan ke halaman utama sehingga sesi login berhasil dilakukan. Selanjutnya, terdapat use case Unggah Dokumen, yang dilakukan setelah Admin berhasil login. Proses ini dimulai ketika Admin memilih menu unggah dokumen, kemudian memilih file dengan format *.docx, *.pdf, atau *.xls. Sistem akan menyimpan file tersebut ke basis data atau server, dan menampilkan pesan bahwa unggahan berhasil, sehingga dokumen tersimpan dalam sistem.

Untuk mengakses data, Admin dapat melakukan use case Lihat Daftar Dokumen. Ketika menu “Daftar Dokumen” dipilih, sistem mengambil seluruh data dokumen dari basis data dan menampilkannya di layar sehingga Admin dapat melihat daftar lengkap dokumen yang tersedia.

Proses berikutnya adalah use case Enkripsi File, yang bertujuan mengenkripsi dokumen menggunakan algoritma AES-128. Setelah Admin memilih dokumen dan menekan tombol “Enkripsi”, sistem mengambil dokumen tersebut, memprosesnya dengan algoritma AES-128, kemudian menyimpan hasil enkripsinya dalam bentuk ciphertext. Sistem juga menampilkan notifikasi bahwa proses enkripsi telah berhasil.

Selanjutnya, use case Dekripsi File dilakukan ketika Admin ingin mengembalikan dokumen terenkripsi ke bentuk aslinya. Admin memilih dokumen terenkripsi dan menekan tombol “Dekripsi”, lalu sistem mengambil ciphertext dan memprosesnya melalui dekripsi AES-128. Dokumen hasil dekripsi kemudian ditampilkan atau disimpan kembali sehingga file asli dapat digunakan kembali.

Selain itu, terdapat use case Hapus Dokumen, yang dilakukan ketika Admin ingin menghapus dokumen yang sudah tidak diperlukan. Setelah Admin memilih dokumen dan menekan tombol “Hapus”, sistem meminta konfirmasi terlebih dahulu. Jika Admin mengonfirmasi, sistem akan menghapus dokumen dari basis data atau server sehingga dokumen tersebut tidak lagi tersedia.

Terakhir, use case Logout dilakukan saat Admin ingin keluar dari sistem. Dengan memilih tombol “Logout”, sistem akan menutup sesi login dan mengarahkan Admin kembali ke halaman login, memastikan bahwa sesi berakhir dengan aman.

3.3.3 Activity Diagram

Proses dimulai ketika Admin melakukan login. Jika login berhasil, Admin dapat mengunggah file. Sistem kemudian memvalidasi file, misalnya berdasarkan jenis dan ukuran (≤ 5 MB). Jika valid, Admin memasukkan kunci enkripsi, dan file diproses melalui 10 ronde AES-128 yang terdiri dari AddRoundKey, SubBytes, ShiftRows, dan MixColumns. File kemudian digabungkan menjadi ciphertext dan disimpan di database sebagai file *.rda. Jika terjadi kegagalan, misalnya login salah atau file tidak valid, sistem menampilkan pesan error.

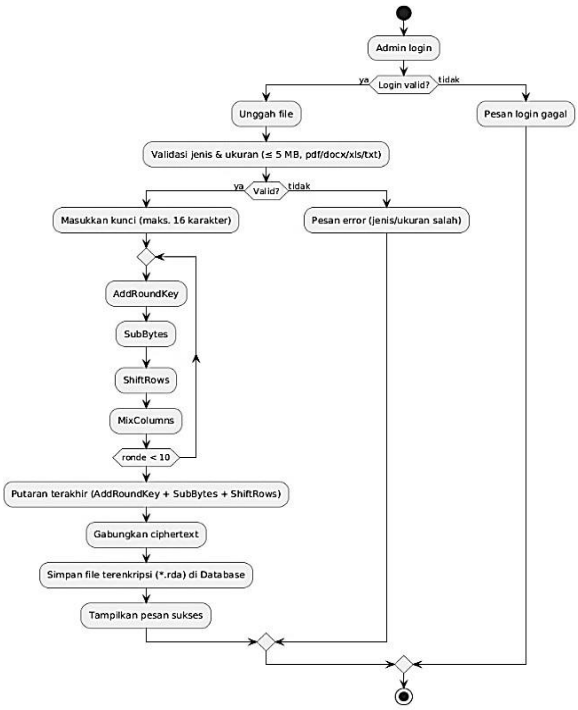

Figure 7. Activity Diagram

3.3.4 Sequence Diagram

Sequence Diagram memperlihatkan interaksi antar komponen sistem secara kronologis.

Figure 8. Sequence Diagram

Figure 8. Menjelaskan Admin berinteraksi dengan antarmuka web (UI), yang kemudian mengirimkan file beserta kunci ke Pengendali Sistem. Pengendali Sistem memvalidasi file dan mengirimkannya ke Layanan AES untuk diproses.
Layanan AES menjalankan algoritma enkripsi dan mengembalikan hasil ciphertext. Ciphertext beserta metadata disimpan di Database, lalu sistem memberikan respon balik ke UI untuk menampilkan pesan sukses atau error. Sequence diagram membantu memahami bagaimana alur komunikasi antar objek (Admin, UI, Controller, Layanan AES, Database) berlangsung secara runtut.

3.3.5 Tabel Relasi

Terdapat 2 tabel pada database sistem enkripsi dan dekripsi, yaitu tabel user dan tabe file. Fungsi tabel user adalah menyimpan data dari user yang dapat mengakses sistem. Sedangkan, tabel file menyimpan File Dokumen Rahasia yang telah dienkripsi. Relasi tabel dapat dilihat pada Figure 9.

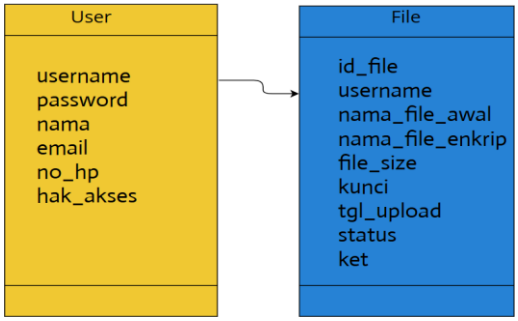

Figure 9. Tabel Relasi

3.4. Hasil

Pada tahap hasil ini, peneliti membahas output dari Implementasi Algoritma Enkripsi AES 128 Bit Pada Dokumen Rahasia Di PT PLN (Persero) UP2B Sistem Minahasa yang telah di bangun. Output dari proses sistem ini berupa hasil enkripsi terhadap dokumen rahasia. Berikut ini merupakan tampilan antarmuka (interface) dari program yang telah dibuat.

3.4.1. Halaman Login

Figure 10. Halaman Login

Figure 10. merupakan halaman login yaitu tampilan awal saat admin ingin masuk ke sistem. Pada halaman ini, admin harus memasukkan username dan password yang benar agar bisa mengakses menu utama sistem.

3.4.2. Halaman Dashboard

Figure 11. Halaman Dashboard

Figure 11. merupakan halaman dashboard yaitu tampilan utama sistem setelah admin berhasil login. Pada halaman ini, admin dapat melihat informasi dan menu utama yang tersedia di dalam sistem.

3.4.3. Halaman Enkripsi

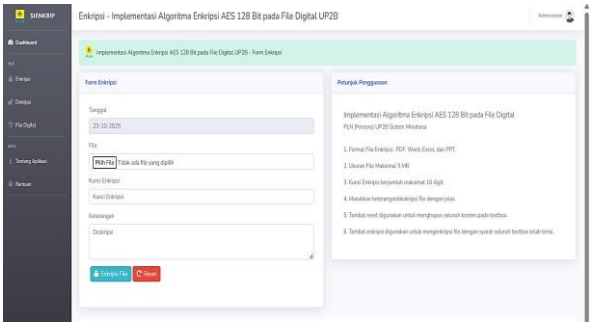

Figure 12. Halaman Dashboard

Figure 12. merupakan halaman enkripsi yaitu bagian sistem yang digunakan Algoritma AES 128 Bit. Pada halaman ini, admin dapat memilih file yang ingin dienkripsi agar isinya tidak dapat dibaca oleh pihak yang tidak memiliki kunci.

3.4.4. Halaman Proses Enkripsi

Halaman ini merupakan tampilan jika user menekan button “enkripsi file” pada halaman enkripsi. Tampilan yang ditampilkan adalah proses dari enkripsi mulai dari AddroundKey, SubBytes, ShiftRow, sampai dengan Mix Column yang berjumlah 10 kali putaran. Halaman Proses enkripsi dapat dilihat pada Figure. 13, 14, 15, 16,17.

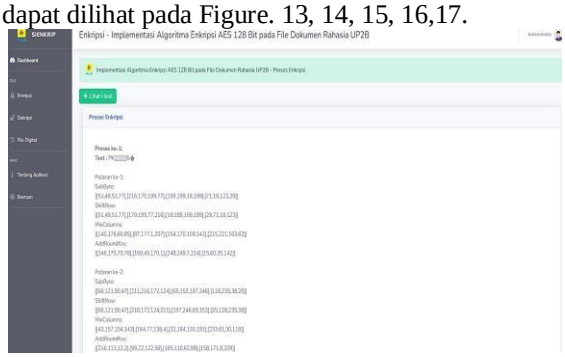

Figure 13. Proses Enkripsi (Putaran 1-2)

Figure 14. Proses Enkripsi (Putaran 3-4)

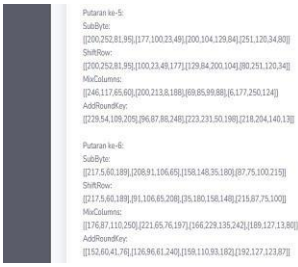

Figure 15. Proses Enkripsi (Putaran 5-6)

Figure 16. Proses Enkripsi (Putaran 7-8)

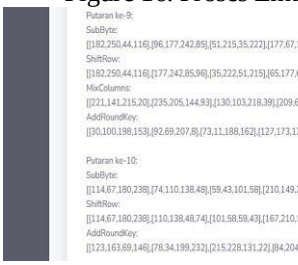

Figure 17. Proses Enkripsi (Putaran 9-10)

3.4.5. Halaman Dekripsi 1

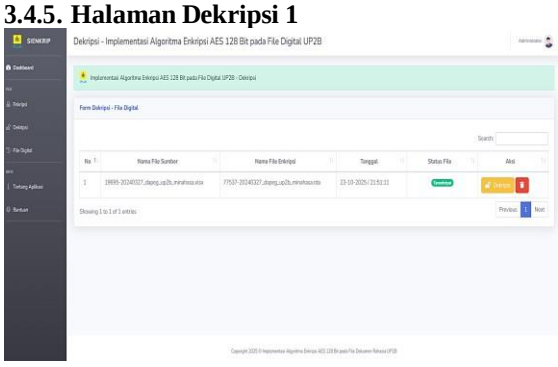

Figure 18. Halaman Dekripsi 1

Figure 18. merupakan halaman dekripsi 1 yaitu halaman yang digunakan untuk mendekripsi file dokumen rahasia yang telah dienkripsi. Halaman ini merupakan halaman daftar dari file yang telah dienkripsi. Jika user menekan button Dekripsi maka akan masuk ke halaman selanjutnya yaitu Dekripsi 2. Pada halaman ini user juga dapat menghapus file

3.4.6. Halaman Dekripsi 2

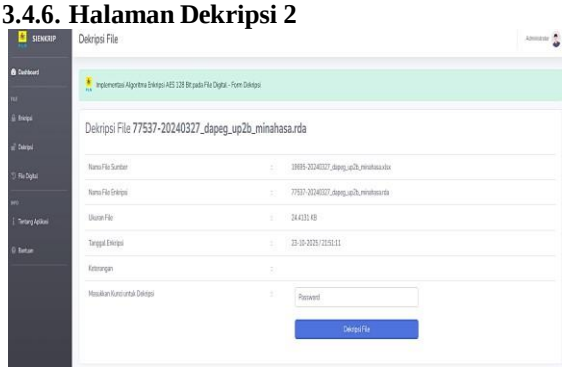

Figure 19. Halaman Dekripsi 2

Figure 19. merupakan Halaman Dekripsi 2 yaitu halaman yang digunakan untuk mendekripsi file dokumen rahasia yang telah dienkripsi. User wajib memasukkan kunci simetri yang dimasukkan pada saat proses enkripsi diawal.

3.4.7. Hasil Enkripsi

Figure 20. Hasil Enkripsi

Figure 20. merupakan Hasil dari enkripsi menggunakan Algoritma AES 128 bit berbentuk file dengan ekstensi *.rda, dimana file ini dapat dibuka menggunakan notepad. Hasil dari enkripsi ini menggunakan fitur randomize karakter agar file yang telah dienkripsi menjadi semakin aman.

3.4.8. Hasil Dekripsi

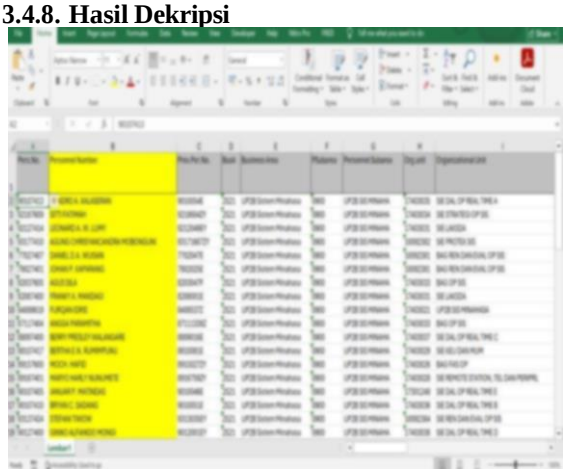

Figure 21. Hasil Enkripsi

Figure 21. merupakan Hasil dari dekripsi menggunakan Algoritma AES 128 bit berbentuk file dengan ekstensi sesuai dengan bentuk awal, jika file yang dienkripsi berbentuk excel maka hasil dari dekripsi akan berbentuk file excel. Persentase akurasi kemiripan antara file asli dengan file yang telah didekripsi mencapai 90%, karena terdapat beberapa ukuran dan jenis font yang berubah.

4. KESIMPULAN

Penerapan algoritma kriptografi AES-128 (Rijndael) berperan signifikan dalam meningkatkan keamanan dokumen rahasia pada PT PLN (Persero) UP2B Sistem Minahasa. Sistem yang dirancang mampu menjalankan proses enkripsi dan dekripsi terhadap berbagai format file seperti PDF, DOCX, XLS, dan TXT dengan kinerja yang optimal.

Dengan adanya sistem ini, dokumen penting dapat terlindungi dari pihak yang tidak memiliki izin akses, sebab data yang telah dienkripsi hanya dapat dibuka menggunakan kunci simetri yang valid. Hasil pengujian menunjukkan bahwa algoritma AES-128 memiliki kecepatan serta efisiensi tinggi, sehingga cocok diterapkan pada lingkungan kerja PLN yang menuntut keamanan data dan performa sistem secara bersamaan.

Penerapan sistem berbasis web turut membantu membatasi akses hanya bagi pengguna yang memiliki hak otorisasi, sehingga keamanan informasi internal lebih terjamin. Secara keseluruhan, sistem yang dikembangkan ini menjadi solusi efektif untuk menjaga kerahasiaan, integritas, dan keandalan dokumen digital, serta memperkuat upaya PLN dalam meningkatkan keamanan informasi di lingkungannya.

REFERENSI

[1] Christiani Makarawung, F. E., & Rorimpandey, G. C. (2025). Optimalisasi Pelaporan Kerusakan Inventaris di PT PLN Nusantara Power Unit Pembangkitan Minahasa melalui Digitalisasi Proses Pelaporan Berbasis Web Menggunakan Metode Prototype. Jurnal Komputer, Informasi dan Teknologi, 5(1), 9. https://doi.org/10.53697/jkomitek.v5i1.2800

[2] Tinambunan, M. H., Wahyuni, S., Yasir, A., & lainnya. (2024). Implementasi Metode Agile dalam Pengembangan Aplikasi Absensi Berbasis QRCode pada SMP Negeri 7 Percut Sei Tuan. Jurnal Dharmawangsa – DJTechno. https://jurnal.dharmawangsa.ac.id/index.php/djtechno/article/view/4812/pdf

[3] Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. International Journal of Information Management, 74, 102719. [3] Y. Lecun, Y. Bengio, and G. Hinton, “Deep learning,” Nature. 2015, doi: 10.1038/nature14539.

[4] Pranita, E. D. (2022, Agustus 19). Data 17 juta pelanggan PLN diduga bocor dan dijual di forum online. Kompas Tekno. https://tekno.kompas.com/read/2022/08/19/15284937/data-17-juta-pelanggan-pln-diduga-bocor-dan-dijual-di-forum-online

[5] Febrian, H. (2023, Oktober 21). Data 44 juta pelanggan PLN diduga bocor, ini penjelasannya.CNNIndonesia.https://www.cnnindonesia.com/teknologi/20231021164754-185-1012114/data-44-juta-pelanggan-pln-diduga-bocor-ini-penjelasannya

[6] Rorimpandey, G. C., Kalalo, T., & Pratasik, M. (2023). Pembuatan aplikasi Website Helpdesk IT Bank Prisma Dana. Journal of Informatics, Business, Education and Innovation Technology (JIBEIT), 1(2). PLN Annual Report. (2023). PT PLN (Persero) Annual Report 2023. https://web.pln.co.id/statics/uploads/2023-annual-report.pdfhttps://jibeit.teknikinformatika.org/index.php/jibeit/article/view/23

[7] NIST. (2023). Announcing the Advanced Encryption Standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd.pdf

[8] PLN Annual Report. (2023). PT PLN (Persero) Annual Report 2023. https://web.pln.co.id/statics/uploads/2023-annual-report.pdf

[9] Runtu, R. R., Maramis, G. D. P., & Hasibuan, A. (2025). Implementasi algoritma rule-based classification pada aplikasi arsip web menggunakan metode RAD dan evaluasi ISO/IEC 25010. Jurnal Minfo Polgan, 14(2). https://doi.org/10.33395/jmp.v14i2.15505

[10] Pressman, R. S., & Maxim, B. R. (2020). Software engineering: A practitioner’s approach (9th ed.). McGraw-Hill Education.

[11] Sitompul, H., Matondang, Z., Daryanto, E., & Syahputra, F. (2024). Use case diagram design for information system services to students at the Faculty of Engineering Universitas Negeri Medan. Proceedings of the International Conference on Innovation in Education, Science, and Culture. https://doi.org/10.4108/eai.24-10-2023.2342345

[12] Kendall, K. E., & Kendall, J. E. (2020). Systems analysis and design (10th ed.). Pearson Education.

[13] Technia. (2025). What is functional analysis? https://www.technia.com/en/functional-analysis/

[14] Sugiyono. (2021). Metode penelitian kuantitatif, kualitatif, dan R&D. Alfabeta.

[15] Rahmawati, D. (2021). Analisis kebutuhan pengguna sistem informasi melalui wawancara. Jurnal Teknologi Informasi, 5(1), 12–21.

[16] Neuman, W. L. (2020). Social research methods: Qualitative and quantitative approaches (8th ed.). Pearson.