Jurnal KomtekInfo

https://jkomtekinfo.org/ojs

2025 Vol. 12 No. 1 Hal: 22-6 e-ISSN: 2502-8758

Penerapan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan File Rekam Medis Pasien

Zulfiqar Tamin✉, Billy Hendrik

Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK", Padang, 25221, Indonesia

fiqartamin@gmail.com

Abstract

In the era of Industry 4.0, which describes the current trend of digital transformation and advancements in information systems, data and information security is of paramount importance for today's internet users. Data breaches involving patient medical records are among the most damaging incidents, necessitating enhanced security measures. This is the background for the development of this application. The problem analysis conducted by the researchers focuses on data file security. One effective method to enhance the security of your data or files is through encryption, specifically using the AES-128 cryptographic algorithm. Given the critical need for information security today, this research aims to implement cryptography using the AES-128 algorithm for encrypting and decrypting data in file formats. This study is implemented in a Python-based application, enabling users to protect sensitive data files. The data is encrypted, and only those with the application and the encryption key can decrypt or access the files. Several tests on this application have successfully encrypted and decrypted patient medical records in PDF format. The purpose of this application is to provide enhanced security for confidential file contents, ensuring that unauthorized parties cannot access them. The application was tested by encrypting and decrypting files in PDF format, with encryption and decryption times measured in seconds. The conclusion drawn from the AES-128 file encryption and decryption is that the larger the file size, the longer the encryption and decryption processes take.

Keywords: cryptography, advanced encryption standard, cyber security, file encryption, file decryption.

Abstrak

Era industri 4.0 yang menggambarkan tren yang berkembang saat ini tentang transformasi digital, dan kemajuan sistem informasi. Keamanan data dan informasi sangat penting bagi pengguna internet saat ini. Kasus pencurian data rekam medis pasien adalah salah satu kasus yang paling merusak, dan keamanan harus diperkuat karena hal ini dapat terjadi. Hal tersebut merupakan latar belakang dibuatnya aplikasi ini. Berdasarkan analisa masalah yang akan dilakukan oleh peneliti adalah terkait keamanan data file. Salah satu cara untuk meningkatkan keamanan data atau file adalah dengan menggunakan metode enkripsi dengan metode yang diusulkan yaitu kriptografi dengan algoritma *AES-128*. Saat ini keamanan informasi ini memerlukan perhatian khusus, sehingga penelitian ini akan menjadi implementasi kriptografi dari algoritma *AES-128* untuk enkripsi dan dekripsi data dalam format file. Penelitian ini di implementasikan dalam bentuk aplikasi berbasis berbasis *Python*. Memungkinkan pengguna untuk melindungi file data sensitif di mana data dienkripsi dan hanya data terenkripsi yang dapat didekripsi atau dibuka kembali orang yang memiliki aplikasi ini dan mengetahui kata kunci enkripsi nya. Beberapa hasil pengujian pada aplikasi ini berhasil melakukan enkripsi dan dekripsi file rekam medis pasien yang berformat pdf. Tujuan aplikasi ini di buat agar dapat memberikan keamanan lebih terhadap isi data file yang bersifat rahasia tanpa takut adanya pihak lain yang tidak bertanggung jawab. Uji coba aplikasi dilakukan dengan melakukan enkripsi dan dekripsi file dengan format *.pdf* dengan pengujian waktu enkripsi dan dekripsi menggunakan satuan detik. Kesimpulan dari enkripsi dan dekripsi file *AES-128* yaitu semakin besar file yang di enkripsi dan di dekripsi maka akan semakin lama proses.

Kata kunci: kriptografi, *advance encryption standard*, keamanan, enkripsi file, dekripsi file.

1. Pendahuluan

File adalah satu aset yang sangat penting sehingga perlu dilakukan berbagai teknik perlindungan untuk mengantisipasi adanya penggandaan serta penyebarluasan informasi yang sifatnya rahasia [1]. Kemajuan teknologi informasi, aktivitas digital semakin populer, termasuk pengeditan file. Berbagai perangkat lunak memungkinkan manipulasi *file* dengan tingkat realisme yang tinggi, mulai dari penyesuaian latar belakang hingga detail-detail tertentu. Hasil manipulasi yang cermat sering sulit dibedakan dari *file* asli [2].

Pemanfaat teknologi tentu sangat diperlukan, namun terdapat hal yang juga tidak bisa kita lupakan yaitu kemanan privasi dokumen karna pada dasarnya setiap dokumen mempunyai privasinya tersendiri [3]. Kriptografi memainkan peran penting dalam keamanan data menyediakan mekanisme penting untuk memastikan kerahasiaan data dan melindungi privasi pengguna di era digital [4]. Definisi singkat dari Kriptografi, dikatakan bahwa Kriptografi adalah algoritma matematika yang menggantikan kekerasan kerahasiaan perlindungan *long-length string* [4].

Advanced Encryption Standard (*AES*) adalah teknologi yang digunakan untuk melindungi informasi rahasia

Diterima: 24-12-2024 | Revisi: 15-01-2025 | Diterbitkan: 31-03-2025 | doi: 10.35134/komtekinfo.v12i1.592

dalam suatu aplikasi. *AES* sebagian besar diterapkan dalam perangkat lunak untuk mengenkripsi data sensitif dalam *system* [5]. Keamanan berbasis *AES* digunakan untuk sistem yang kompleks dalam manufaktur cerdas. Metode berbasis *Lightweight Advanced Encryption Standard* (*LAES*) digunakan untuk proses manajemen keamanan dalam sistem yang kompleks. *LAES* mengidentifikasi data sensitif dan menyediakan kunci enkripsi yang tepat untuk pemrosesan lebih lanjut. *LAES* mengurangi tingkat konsumsi waktu keseluruhan dalam enkripsi yang melindungi data dari serangan. Metode *LAES* menganalisis konten teks yang dilindungi untuk pengguna. Algoritma hibrida berbasis *AES* digunakan dalam sistem yang kompleks untuk tujuan keamanan [5]. Algoritma kriptografi *AES-128* memiliki kemampuan untuk beroperasi dengan blok *128-bit* atau 16 karakter [6]. Oleh karena itu, algoritma kriptografi *AES-128* sangat cocok untuk mengenkripsi teks pada file yang terdiri dari baris demi baris teks dengan panjang lebih dari 16 karakter [7].

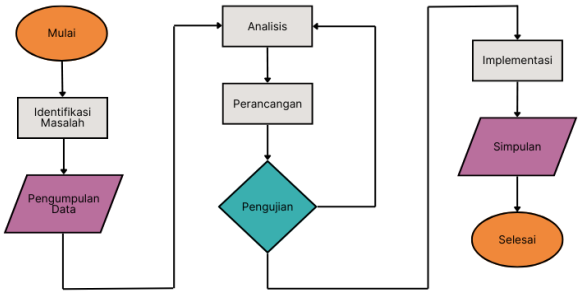
Rekam Medis adalah dokumen yang memuat data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang diberikan kepada pasien. Rekam Medis Elektronik bentuk rekam medis yang disusun menggunakan sistem elektronik yang berupa data ataupun file untuk pengelolaan rekam medis [8].

Keamanan data menjadi salah satu prioritas utama bagi banyak aplikasi dan sistem informasi [9]. Salah satu metode enkripsi yang paling diandalkan adalah *Advanced Encryption Standard* (*AES-128*), yang menawarkan keamanan tingkat tinggi dengan menggunakan kunci enkripsi sepanjang *128-bit*. Untuk memanfaatkan kekuatan *AES-128* dalam aplikasi, membuat aplikasi enkripsi dan dekripsi menggunakan bahasa pemrograman *Python* [10]. Menggunakan *library cryptography* yang tersedia, proses implementasi algoritma *AES-128* menjadi lebih sederhana dan efisien [11].

2. Metodologi Penelitian

Penelitian ini dilakukan dengan metode pembentukan kerangka kerja. Kerangka kerja merupakan tahapan-tahapan proses penelitan yang terurut berdasarkan langkah-langkah yang saling berkaitan. Langkah-langkah tersebut dimulai dengan proses Identifikasi Masalah, Pengumpulan Data, Analisa, Merancang Sistem, Pengujian Sistem, Implementasi, Kesimpulan. Perencanaan penelitian dapat dilihat pada Gambar 1.

Kerangka kerja penelitian ini secara sistematis memandu proses investigasi dari awal hingga akhir. Dimulai dari identifikasi masalah yang menjadi fokus kajian, penelitian ini kemudian berlanjut ke tahap pengumpulan data untuk memperoleh informasi yang relevan. Data yang diperoleh kemudian dianalisis secara mendalam untuk mengidentifikasi pola, tren, dan hubungan yang signifikan.



Gambar 1. Kerangka Penelitian

Hasil analisis ini menjadi dasar dalam merancang sistem atau solusi yang inovatif untuk mengatasi masalah yang telah diidentifikasi. Tahap pengujian sistem dilakukan untuk memastikan bahwa sistem yang dirancang berfungsi dengan baik dan efektif. Setelah melalui serangkaian pengujian, sistem kemudian diimplementasikan dalam konteks yang sebenarnya. Penelitian ini diakhiri dengan penarikan kesimpulan yang merangkum temuan-temuan penting dan implikasi dari penelitian ini. Berikut adalah penjelasan lebih lanjut mengenai kerangka penelitian ini.

2.1. Identifikasi Masalah

Meningkatnya kasus manipulasi data telah menjadi ancaman serius bagi individu dan organisasi. Dampak dari manipulasi data sangat luas, mulai dari kerugian finansial hingga kerusakan reputasi yang signifikan. Untuk mencegah terjadinya pelanggaran data yang semakin sering, pengawasan ketat terhadap praktik keamanan data di berbagai instansi mutlak diperlukan.

2.2. Pengumpulan Data

Peneliti melakukan pengumpulan data dari Instalasi Rekam Medis Rumah Sakit Universitas Andalas. Metode pengumpulan data yang digunakan meliputi wawancara, observasi, dan studi literatur. File *PDF* rekam medis yang diperoleh dari proses pengumpulan data tersebut kemudian digunakan sebagai data uji untuk algoritma kriptografi *AES-128*.

2.3. Analisis

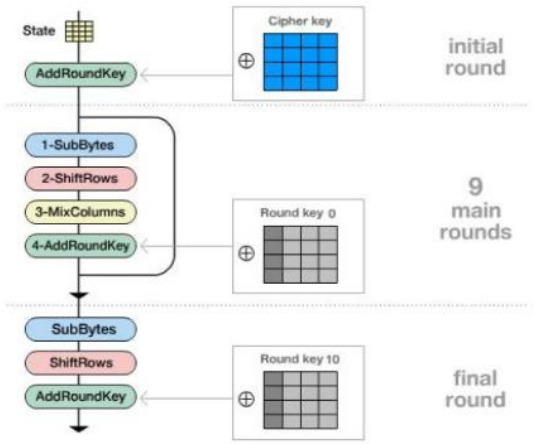
Pada tahap ini terlebih dahulu dilakukan analisis terhadap algoritma *Advanced Encryption Standard* (*AES-128*) sehingga dapat di implementasikan pada keamanan data rekam medis.

Advanced Encryption Standard (*AES*) adalah algoritma enkripsi simetris yang diperkenalkan oleh Institut Standar dan Teknologi Nasional AS pada tahun 2001. *AES* dirancang untuk menggantikan *DES* yang dianggap menggunakan kunci enkripsi terlalu kecil dan algoritmanya lambat. *AES* menggunakan *plaintext* dan kunci privat berukuran *128-bit*, yang digabungkan membentuk blok *128-bit* yang diwakili sebagai matriks persegi 4x4 [12].

Algoritma *AES* menggunakan metode substitusi-permutasi untuk melakukan enkripsi data. Proses enkripsi terdiri dari 10 putaran. Setiap putaran melibatkan empat tahapan utama, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Tahapan-tahapan ini akan mengubah struktur data secara signifikan. Putaran terakhir tidak termasuk tahapan *MixColumns*. Hasil akhir dari proses ini adalah *ciphertext* yang sulit dibaca tanpa kunci dekripsi yang sesuai [13, 14, 15]. Secara umum proses *AES-128* dapat dikategorikan menjadi 2 yaitu:

a. Enkripsi AES-128

Algoritma *AES* memulai proses enkripsi dengan menambahkan kunci awal pada *state*. *State* kemudian akan mengalami *round function* sebanyak *Nr* kali. *Round function* terdiri dari empat transformasi *non-linear* yang dirancang untuk meningkatkan keamanan. Pada putaran terakhir, transformasi linear (*MixColumns*) tidak dilakukan untuk menghasilkan *ciphertext* akhir [16, 17]. Ilustrasi proses awal enkripsi dengan menggunakan algoritma AES -128 dijelaskan pada Gambar 2.

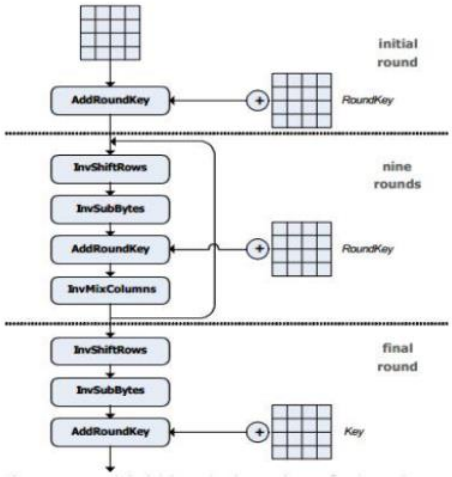


Gambar 2. *AES-128 Encryption* Process

Proses enkripsi *AES-128* melibatkan beberapa tahap berulang yang disebut putaran. Setiap putaran terdiri dari beberapa langkah yang mengubah data secara kompleks. Data asli (*plaintext*) dicampur dengan kunci rahasia menggunakan operasi *XOR*. Setelah itu, data akan melalui beberapa putaran yang melibatkan pergeseran baris, *substitusi byte*, pencampuran kolom, dan penambahan kunci rahasia lagi. Setiap putaran dirancang untuk semakin mengacak data sehingga sulit bagi pihak yang tidak berwenang untuk memahaminya. Pada putaran terakhir, beberapa langkah dihilangkan untuk menghasilkan data terenkripsi akhir.

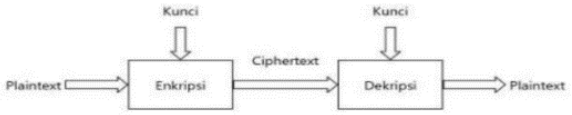
b. Dekripsi AES-128

Dekripsi merupakan proses kebalikan dari enkripsi, di mana data yang telah dienkripsi diubah kembali ke bentuk aslinya. Pada algoritma AES-128, proses dekripsi ini, yang juga disebut sebagai Inverse Cipher Rijndael, bekerja pada blok data sebesar 128 bit dengan menggunakan kunci 128 bit yang sama seperti saat proses enkripsi [18, 19]. Proses dekripsi ini diilustrasikan secara detail pada Gambar 3.



Gambar 3. *AES-128 Decryption* Process

Proses dekripsi AES-128 bekerja dimana *ciphertext* akan diubah kembali menjadi *plaintext* melalui langkah-langkah yang berlawanan dengan proses enkripsi. Dengan menggunakan kunci rahasia yang sama, setiap tahap dalam proses dekripsi akan membatalkan efek dari tahap yang sesuai dalam proses enkripsi, sehingga data asli dapat dipulihkan.

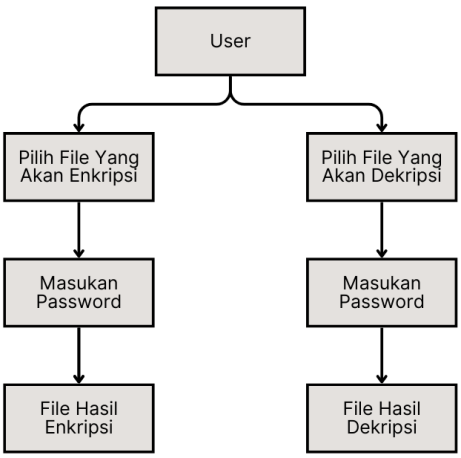


Gambar 4. *AES-128 Encryption and Decryption Scheme*

Gambar 4 memberikan gambaran yang jelas mengenai langkah-langkah yang terjadi pada proses enkripsi dan dekripsi menggunakan *AES-128*. Algoritma ini bekerja dengan cara mengubah data *plaintext* menjadi *ciphertext* melalui serangkaian transformasi matematis yang kompleks. Transformasi *InvMixColumns* merupakan salah satu tahapan penting dalam proses ini. Kekuatan *AES-128* terletak pada kombinasi antara kunci rahasia yang panjang, jumlah putaran yang banyak, dan desain algoritma yang sangat baik, seperti yang ditunjukkan dalam ilustrasi tersebut [20].

2.4. Perancangan

Pada tahap ini, penulis merancang dan mengembangkan sebuah aplikasi berbasis *Python* yang difungsikan sebagai alat untuk mengamankan data secara digital. Dengan memanfaatkan algoritma enkripsi yang kuat, yaitu *Advanced Encryption Standard* (*AES*) dengan panjang kunci 128 bit, aplikasi ini mampu mengubah data asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca secara langsung (*ciphertext*). Proses sebaliknya, yaitu mengubah *ciphertext* kembali menjadi *plaintext*, juga dapat dilakukan oleh aplikasi ini.



Gambar 5. *Activity Diagram*

Perencangan sistem dijelaskan melalui *activity diagram* yang terdapat pada Gambar 5, yang menggambarkan alur kerja secara keseluruhan. Proses pertama adalah enkripsi, dimulai dengan memilih lokasi file, kemudian memasukkan dan mengkonfirmasi kunci enkripsi. Setelah itu, proses enkripsi akan menghasilkan file terenkripsi beserta informasi waktu dan ukuran file. Proses kedua adalah dekripsi, di mana file yang sudah terenkripsi dimasukkan kembali dengan kunci yang sama untuk validasi. Output dari proses ini adalah file dokumen yang terdekripsi, lengkap dengan waktu dan ukuran file.

2.5. Pengujian

Pada tahap pengujian sistem, dilakukan serangkaian uji coba untuk memastikan bahwa sistem yang telah dikembangkan sesuai dengan hasil analisis dan berfungsi seperti yang diharapkan. Metode yang digunakan adalah *black box testing*, yang bertujuan untuk mengevaluasi aplikasi secara keseluruhan. Pendekatan ini memungkinkan pengujian fungsional serta identifikasi potensi *bug* dengan cara menilai respons aplikasi terhadap berbagai input dan memastikan bahwa output yang dihasilkan sesuai dengan harapan.

2.6. Implementasi

Pada tahap implementasi ini, penulis membangun sebuah aplikasi enkripsi dan dekripsi menggunakan bahasa pemrograman Python. Aplikasi ini dirancang untuk menjalankan algoritma *Advanced Encryption Standard* (*AES*) dengan kunci 128-bit. Aplikasi ini dibangun berdasarkan rancangan yang terdaat pada Gambar 5. Aplikasi ini pengguna dapat dengan mudah mengamankan data sensitif mereka menggunakan metode enkripsi yang kuat seperti *AES-128.* Aplikasi ini memberikan kemudahan bagi pengguna yang ingin melindungi data mereka dari akses yang tidak sah.

2.7. Simpulan

Pada tahap ini hasil penelitian dapat membuktikan bahwa algoritma *AES-128* sangat efektif dalam mengamankan data sensitif, seperti data pribadi dan finansial, pada aplikasi berbasis web yang telah dikembangkan. Melalui serangkaian pengujian yang ketat, dapat disimpulkan bahwa *AES-128* mampu memberikan perlindungan yang kuat dengan waktu enkripsi dan dekripsi yang cepat. *AES-128* dapat terbukti lebih efisien dan menawarkan tingkat keamanan yang lebih tinggi, sehingga menjadikannya pilihan yang sangat baik untuk mengamankan data dalam aplikasi modern.

3. Hasil dan Pembahasan

Penelitian ini melakukan pengamanan data pada *file* penting Rekam Medis Rumah Sakit Universitas Andalas. Aplikasi yang dibangun digunakan dalam merahasikan data-data pasien yang bersifat penting. Setelah proses memasukan data pada sistem, sistem akan melakukan proses enkripsi menggunakan algoritma *AES-128 Bit* dan data akan tersimpan dalam bentuk terenkripsi sehingga terjamin kerahasiaannya. Untuk mengetahui isi data tersebut maka perlu dilakukan proses dekripsi data dengan menggunakan kunci.

3.1. Aplikasi *AES-128 Encryption Application*

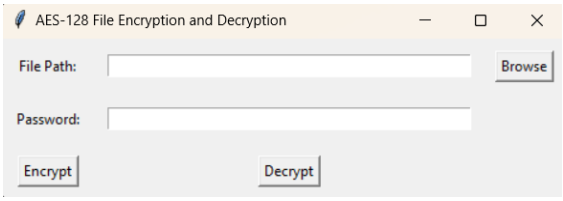
Aplikasi ini adalah *tools* kriptografi yang dirancang khusus untuk mengenkripsi dan mendekripsi file menggunakan algoritma *Advanced Encryption Standard* (*AES*) dengan ukuran kunci 128-bit (*AES-128*). Algoritma *AES-128* merupakan salah satu standar enkripsi yang paling aman dan banyak digunakan di seluruh dunia. Aplikasi ini bertujuan untuk melindungi data dari akses yang tidak sah. Dengan memanfaatkan kekuatan dan keamanan yang ditawarkan oleh *AES-128*, aplikasi ini memastikan bahwa data sensitif pengguna tetap terlindungi dari berbagai ancaman keamanan digital.

Aplikasi dibangun menggunakan bahasa pemrograman *Python*. *Python* dikenal akan kemudahan dan fleksibilitasnya. Hasil akhir dari pengembangan ini adalah sebuah program yang mampu melakukan enkripsi dan dekripsi data dengan aman menggunakan algoritma *AES-128*. Aplikasi ini juga memanfaatkan *library Tkinter* untuk menyediakan antarmuka pengguna grafis (*GUI*) yang intuitif dan ramah pengguna. Dengan antarmuka grafis ini, pengguna tidak perlu memahami detail teknis dari proses enkripsi dan dekripsi. Ini memungkinkan siapa saja, termasuk mereka yang tidak memiliki latar belakang teknis, untuk dengan mudah mengoperasikan aplikasi ini.

Pengguna aplikasi kriptografi ini dapat memilih file yang ingin mereka enkripsi atau dekripsi melalui antarmuka pengguna yang sederhana dan mudah digunakan. Setelah memilih file, pengguna cukup memasukkan password yang akan digunakan untuk

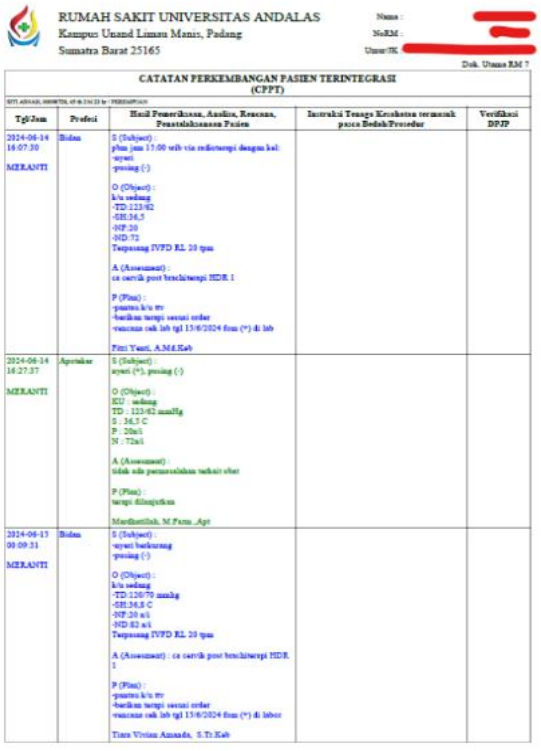
menghasilkan kunci enkripsi. Proses enkripsi akan mengenkripsi file yang dipilih dengan aman dan menyimpannya dalam format yang hanya bisa diakses kembali dengan menggunakan *password* yang benar. Demikian pula untuk mendekripsi file yang telah dienkripsi, pengguna hanya perlu memilih file tersebut dan memasukkan *password* yang sama untuk mengembalikan file ke format aslinya.

Fitur-fitur yang dimiliki aplikasi ini memberikan solusi yang efektif untuk melindungi data sensitif dari ancaman keamanan siber. Aplikasi ini memastikan bahwa informasi penting tetap aman dan hanya dapat diakses oleh mereka yang memiliki izin yang sesuai. Berikut adalah tampilan aplikasi kriptografi menggunakan algoritma *AES-128* yang terlihat pada Gambar 6.



Gambar 6. *AES-128 Encryption Application*

Data sampel yang digunakan dalam penelitian ini adalah data rekam medis pasien berekstensi *.pdf* sebanyak tujuh dokumen. Data rekam medis pasien ini akan dijadikan sampel untuk enkripsi menggunakan metode *AES-128* Bit. Contoh data rekam medis pasien sebelum dilakukan enkripsi dapat dilihat pada Gambar 7 dan Gambar 8.

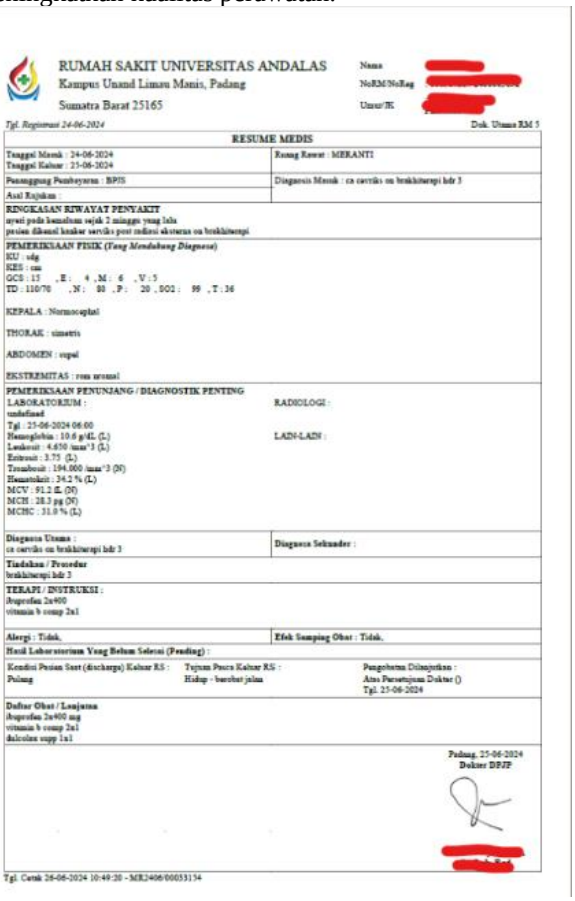

RUMAH SAKIT UNIVERSITAS ANDALAS
Kampus Unand Limau Manis, Padang
Sumatra Barat 25163

CATATAN PERKEMBANGAN PASIEN TERINTEGRASI
(CPPT)

Tgl/Jam	Profesi	Hasil Pemeriksaan, Analisa, Rencana, Penatalaksanaan Pasien	Instruksi Tenaga Kesehatan termasuk pasca Bedah/Prosedur	Verifikasi DPJP
2024-06-14 16:07:30 MERANTI	Bidan	S (Subject) : pkm jam 17:00 wib via rediterapi dengan kel: -nyeri -pusing (-) O (Object) : k/u sedang -TD:123/82 -SH:36,5 -NF:20 -ND:72 Terpasang IVFD RL 20 tpm A (Assessment) : ca cervik post brachiterapi HDR 1 P (Plan) : -pantau k/u tv -berikan terapi sesuai order -rencana cek lab tgl 15/6/2024 ibm (*) di lab Fitri Yanti, A.Md.Keb		
2024-06-14 16:27:37 MERANTI	Apotaker	S (Subject) : nyeri (*), pusing (-) O (Object) : KU : sedang TD : 123/82 mmHg S : 36,7 C P : 20x/i N : 72x/i A (Assessment) : tidak ada permasalahan terkait obat P (Plan) : terapi dilanjutkan Marlinettiah, M.Farm .,Apt		
2024-06-15 00:09:21 MERANTI	Bidan	S (Subject) : -nyeri berkurang -pusing (-) O (Object) : k/u sedang -TD:120/70 mmHg -SH:36,8 C -NF:20 x/i -ND:82 x/i Terpasang IVFD RL 20 tpm A (Assessment) : ca cervik post brachiterapi HDR 1 P (Plan) : -pantau k/u tv -berikan terapi sesuai order -rencana cek lab tgl 15/6/2024 ibm (*) di labor Tiara Vivian Amanda, S.Tr.Keb		

Gambar 7. Catatan Perkembangan Pasien Terintegrasi

Catatan Perkembangan Pasien Terintegrasi merupakan dokumentasi yang mencakup semua informasi terkait kondisi kesehatan, perawatan, dan kemajuan pasien secara menyeluruh. Dokumentasi ini biasanya mencakup riwayat medis, hasil pemeriksaan, diagnosis, rencana perawatan, serta catatan tentang respons pasien terhadap terapi dan intervensi. Dengan sistem terintegrasi, data ini dapat diakses oleh berbagai tim medis, memastikan komunikasi yang lebih baik dan koordinasi dalam perawatan pasien. Tujuannya adalah untuk memberikan gambaran lengkap mengenai status pasien, mendukung pengambilan keputusan klinis, dan meningkatkan kualitas perawatan.


RUMAH SAKIT UNIVERSITAS ANDALAS
Kampus Unand Limau Manis, Padang
Sumatra Barat 25163

RESUME MEDIS

Tanggal Masuk : 24-06-2024
Tanggal Keluar : 25-06-2024
Ruang Rawat : MERANTI
Penanggung Pembayaran : BPJS
Diagnosis Masuk : ca cervikx on brakhiterapi hdr 3
Asal Rujukan :

RINGKASAN RIWAYAT PENYAKIT
ayuni pada kunjungan sejak 2 minggu yang lalu
pasien dikenal kanker cervikx post radiasi eksterna on brakhiterapi

PEMERIKSAAN FISIK (*Yang Mendukung Diagnosa*)
KU : sdg
KES : cm
GCS : 15 ,E : 4 ,M : 6 ,V : 5
TD : 110/70 ,N : 80 ,P : 20 ,SO2 : 99 ,T : 36
KEPALA : Normocephal
THORAK : simetris
ABDOMEN : cupul
EKSTREMITAS : reas normal

PEMERIKSAAN PENUNJANG / DIAGNOSTIK PENTING
LABORATORIUM :
undefined
Tgl : 25-06-2024 06:00
Hemoglobin : 10.6 g/dL (L)
Leukosit : 4.650 /mm^3 (L)
Eritrosit : 3.75 (L)
Trombosit : 194.000 /mm^3 (N)
Hematokrit : 34.2 % (L)
MCV : 91.2 fL (N)
MCH : 28.3 pg (N)
MCHC : 31.0 % (L)
RADIOLOGI :
LAIN-LAIN :

Diagnosa Utama :
ca cervikx on brakhiterapi hdr 3
Diagnosa Sekunder :

Tindakan / Prosedur
brakhiterapi hdr 3

TERAPI / INSTRUKSI :
ibuprofen 2x400
vitamin b comp 2x1

Alergi : Tidak.
Efek Samping Obat : Tidak.

Hasil Laboratorium Yang Belum Selesai (Pending) :

Kondisi Pesan Saat (discharge) Keluar RS : Pulang
Tujuan Pasca Keluar RS : Hidup - berobat jalan
Pengobatan Dilanjutkan : Atas Persetujuan Dokter ()
Tgl. 25-06-2024

Daftar Obat / Lanjutan
ibuprofen 2x400 mg
vitamin b comp 2x1
dalcolax supp 1x1

Padang, 25-06-2024
Dokter DPJP

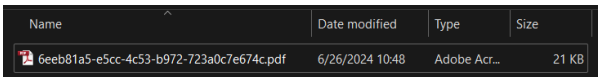
Gambar 8. Resume Medis

Resume medis merupakan catatan kesehatan komprehensif yang sangat penting dalam sistem pelayanan kesehatan. Dokumen ini berisi riwayat kesehatan lengkap pasien, mulai dari diagnosis hingga perawatan yang telah diberikan, sehingga menjadi referensi berharga bagi tenaga medis dalam memberikan pelayanan yang optimal. Sebagai alat komunikasi yang efektif, resume medis memfasilitasi pertukaran informasi antara tenaga medis yang berbeda. Dengan adanya resume medis, dokter, perawat, dan tenaga kesehatan lainnya dapat mengakses informasi pasien secara cepat dan akurat, sehingga dapat memberikan perawatan yang kontinu dan terintegrasi. Resume medis juga berfungsi sebagai dasar dalam pengambilan keputusan klinis, perencanaan perawatan, dan evaluasi hasil pengobatan. Informasi yang

terkandung dalam resume medis membantu tenaga medis dalam menentukan diagnosis yang tepat, merencanakan perawatan yang sesuai, serta mengevaluasi efektivitas pengobatan yang telah diberikan.

3.2. Enkripsi File

Sebagai bagian dari evaluasi sistem keamanan, kami telah menguji coba algoritma enkripsi pada sebuah file rekam medis pasien dengan format *PDF*. File dengan nama "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" ini berisi data lengkap mengenai perkembangan kondisi kesehatan seorang pasien, termasuk hasil pemeriksaan, diagnosis, dan rencana perawatan. Pemilihan file *PDF* sebagai data uji didasarkan pada prevalensi penggunaan format ini dalam penyimpanan rekam medis elektronik. Hasil pengujian ini dapat memberikan gambaran yang lebih akurat mengenai efektivitas sistem enkripsi dalam melindungi data sensitif pasien dalam lingkungan medis yang sebenarnya. Melalui proses enkripsi peneliti bertujuan untuk mengubah data yang dapat dibaca menjadi bentuk yang tidak dapat dipahami tanpa kunci dekripsi yang sesuai. Informasi pribadi pasien yang sangat sensitif ini dapat terlindungi dari akses oleh pihak yang tidak berwenang, sehingga menjaga kerahasiaan dan keamanan data pasien. Hasil pengujian ini diharapkan dapat memberikan bukti empiris mengenai kemampuan sistem enkripsi dalam mengamankan data rekam medis pasien. Data yang diperoleh dari pengujian ini akan menjadi dasar dalam menilai keandalan dan efektivitas sistem enkripsi yang telah dikembangkan.



Gambar 9. File Sebelum Proses Enkripsi

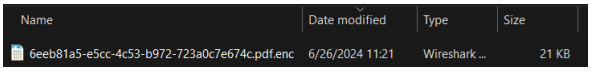
File rekam medis dengan nama "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" memiliki format *Portable Document Format* (*PDF*) dengan ukuran 21 *kilobyte*. Berdasarkan data yang tercatat, file ini terakhir kali mengalami perubahan pada tanggal 26 Juni 2024. Informasi mengenai ukuran dan tanggal modifikasi file ini memberikan petunjuk mengenai riwayat dan karakteristik dari dokumen rekam medis tersebut.

Gambar 10. Proses Enkripsi File

Proses enkripsi pada file rekam medis pasien "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" telah berhasil dilakukan menggunakan Aplikasi *AES-128* dengan kata sandi "*enkrip123@*". Seperti yang terlihat pada Gambar 10, sistem berhasil mengenkripsi file *PDF* tersebut dan menghasilkan file output baru dengan ekstensi *.enc*. Proses enkripsi ini berlangsung dengan cepat, hanya membutuhkan waktu 0,59 detik seperti yang ditunjukkan pada Gambar 11.

Gambar 11. Notifikasi Proses Enkripsi Sukses

Proses enkripsi yang dilakukan pada file "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" telah mengubah format file asli menjadi format baru yang ditandai dengan ekstensi *.enc*. Perubahan format ini mengindikasikan bahwa data di dalam file telah dienkripsi dan diubah menjadi kode yang tidak dapat dibaca secara langsung oleh aplikasi umum. Tujuan utama dari proses enkripsi ini adalah untuk melindungi kerahasiaan data dengan mengubah struktur data menjadi bentuk yang hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang sesuai.



Gambar 11. File setelah proses enkripsi

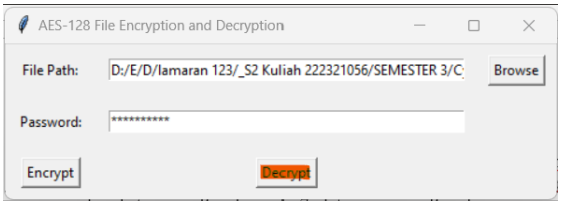
File hasil enkripsi dengan nama "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf.enc*" tidak dapat dibaca secara langsung menggunakan perangkat lunak pembaca PDF konvensional. Ketika file ini dibuka menggunakan aplikasi *notepad*, tampilan yang dihasilkan adalah kumpulan karakter yang tidak bermakna seperti yang terlihat pada Gambar 12. Hal ini menunjukkan bahwa proses enkripsi telah berhasil mengubah struktur data file sehingga menjadi tidak dapat dikenali oleh aplikasi yang tidak memiliki kemampuan untuk mendekripsi data tersebut.

Gambar 12. Tampilan isi file setelah enkripsi

Algoritma enkripsi *AES-128* telah mengubah struktur data dalam file "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" secara signifikan. Proses ini telah menghasilkan sebuah file terenkripsi yang tidak dapat dibaca oleh aplikasi umum seperti pemroses teks. File yang telah dienkripsi ini kini berada dalam format yang aman dan terlindungi, sehingga hanya dapat diakses oleh individu yang memiliki kunci dekripsi yang sesuai dan aplikasi *AES-128 Encryption* yang telah dikembangkan.

3.3. Dekripsi File

Setelah proses enkripsi selesai dilakukan peneliti kemudian melakukan proses kebalikannya, yaitu dekripsi. Dengan cara memilih file yang telah dienkripsi berformat *.enc*, peneliti memasukkan kata sandi yang sama persis seperti yang digunakan saat proses enkripsi. Proses ini memungkinkan file yang sebelumnya telah terenkripsi menjadi dapat dibaca kembali seperti semula, seperti terlihat dalam Gambar 13.



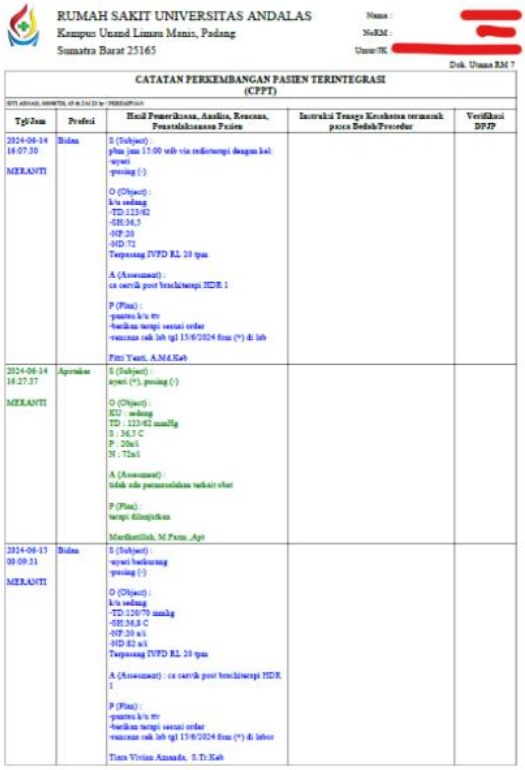
Gambar 13. Proses Dekripsi File

Proses dekripsi berhasil memulihkan file *PDF* dengan nama "*6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf*" dalam waktu 0,16 detik. Hasil dekripsi ini menunjukkan bahwa algoritma yang digunakan efektif dalam mengembalikan data ke bentuk aslinya. Kecepatan proses dekripsi yang sangat singkat mengindikasikan efisiensi algoritma dalam menjalankan tugasnya. Visualisasi hasil dekripsi dapat dilihat secara detail pada Gambar 14.

Gambar 14. Notifikasi Proses Dekripsi Sukses

Proses dekripsi telah berhasil mengembalikan data terenkripsi ke bentuk aslinya yang dapat dibaca oleh komputer. File yang semula dalam keadaan terenkripsi kini telah berhasil diubah menjadi format *Portable Document Format* (*PDF*). Hal ini menunjukkan bahwa algoritma dekripsi yang digunakan mampu memulihkan struktur dan konten file dengan akurat. Hasil dekripsi yang berupa file *PDF* dengan ekstensi *.pdf* mengindikasikan bahwa proses konversi dari data terenkripsi ke format yang dapat dibaca manusia telah berjalan dengan sukses.

Selain berhasil memulihkan format file, proses dekripsi juga telah memastikan bahwa isi dari file *PDF* yang dihasilkan identik dengan file asli sebelum dienkripsi. Setiap karakter, gambar, dan elemen lain dalam dokumen telah berhasil dipulihkan tanpa adanya kerusakan atau perubahan data. Keberhasilan dalam menjaga integritas data selama proses dekripsi ini membuktikan kehandalan algoritma yang digunakan. Hasil yang akurat ini menunjukkan bahwa sistem keamanan yang diterapkan mampu melindungi kerahasiaan dan integritas data secara efektif.


RUMAH SAKIT UNIVERSITAS ANDALAS
Kampus Unand Limau Manis, Padang
Sumatra Barat 25165

CATATAN PERKEMBANGAN PASIEN TERINTEGRASI
(CPPT)

Tgl/Jam	Profesi	Hasil Pemeriksaan, Analisa, Rencana, Penatalaksanaan Pasien	Instruksi Tenaga Kesehatan termasuk paca Bedah/Prosedur	Verifikasi DPJP
2024-06-14 16:07:30 MERANTI	Bidan	S (Subject) : plan jam 17:00 wib via rediterapi dengan kel: -nyeri -pusing (-) O (Object) : k/u sedang -TD:123/82 -SH:36,5 -NP:20 -ND:72 Terpasang IVFD KL 20 tpm A (Assessment) : ce cervik post brachiterapi HDR 1 P (Plan) : -pasien k/u rr -berikan terapi sesuai order -rencana cek lab tgl 15/6/2024 fosa (*) di lab Fitri Yanti, A.Md.Keb		
2024-06-14 16:27:37 MERANTI	Apotaker	S (Subject) : nyeri (*), pusing (-) O (Object) : KU : sedang TD : 123/82 mmHg S : 36,5 C P : 20x/i N : 72x/i A (Assessment) : tidak ada permasalahan terkait obat P (Plan) : terapi dilanjutkan Marthottilah, M Farm ,Apt		
2024-06-15 08:09:31 MERANTI	Bidan	S (Subject) : -nyeri berkurang -pusing (-) O (Object) : k/u sedang -TD:126/79 mmHg -SH:36,8 C -NP:20 x/i -ND:82 x/i Terpasang IVFD KL 20 tpm A (Assessment) : ce cervik post brachiterapi HDR 1 P (Plan) : -pasien k/u rr -berikan terapi sesuai order -rencana cek lab tgl 15/6/2024 fosa (*) di labor Tiara Vivian Amanda, S.Tr.Keb		

Gambar 15. Tampilan File setelah dilakukan Dekripsi

Gambar 15 menunjukan bahwa file *"6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf"* dapat dibuka secara normal menggunakan *pdf reader*. Hal ini menandakan proses enkripsi dan dekripsi menggunakan aplikasi *AES-128 Encryption Application* yang telah peneliti bangun berhasil menjalankan fungsi nya dengan menerapkan metode kriptografi menggunakan algoritma *AES-128*.

3.4. Proses Enkripsi dan Dekripsi *AES-128*

Pengujian kinerja dilakukan terhadap tujuh file PDF rekam medis yang memiliki ukuran dan jenis yang bervariasi. Data lengkap mengenai file uji dapat dilihat pada Tabel 1. Waktu yang diperlukan untuk menyelesaikan proses enkripsi dan dekripsi pada setiap file akan dicatat untuk analisis lebih lanjut.

Tabel 1. *File Testing Upload* Enkripsi dan Dekripsi

Nama *File*	Ukuran	Ekstensi
6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf	21 kb	.pdf
b734ffb3-0faf-4a19-812a-75fa63e69fde.pdf	11 kb	.pdf
ea0d4af7-b3f3-43c8-a09a-1a87f037b814.pdf	10 kb	.pdf
6483ae92-b7a5-4a6c-9806-0105723c0c70.pdf	20 kb	.pdf
e04373f3-d037-46f8-8698-49dfef93b48f.pdf	11 kb	.pdf
feff9caa-8210-49ef-99d5-aab9e9b5b15c.pdf	121 kb	.pdf
e588bc20-8da3-4dde-b115-971f95109fe2.pdf	11 kb	.pdf

Efisiensi algoritma enkripsi dan dekripsi sangat penting untuk diukur. Dalam penelitian ini waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dicatat dalam satuan detik dan disajikan dalam bentuk tabel. Tabel 2 memberikan gambaran jelas mengenai kinerja algoritma yang digunakan.

Tabel 2. Perbandingan Uji Waktu Enkripsi dan Dekripsi

Nama *File*	Wakt Enkripsi	Waktu Deskripsi
6eeb81a5-e5cc-4c53-b972-723a0c7e674c.pdf	0.40	0.41
b734ffb3-0faf-4a19-812a-75fa63e69fde.pdf	0.23	0.21
ea0d4af7-b3f3-43c8-a09a-1a87f037b814.pdf	0.21	0.22
6483ae92-b7a5-4a6c-9806-0105723c0c70.pdf	0.40	0.44
e04373f3-d037-46f8-8698-49dfef93b48f.pdf	0.20	0.23
feff9caa-8210-49ef-99d5-aab9e9b5b15c.pdf	0.52	0.49
e588bc20-8da3-4dde-b115-971f95109fe2.pdf	0.22	0.22

Hasil pengujian waktu yang diperlukan untuk proses enkripsi dan dekripsi pada file. Setiap baris pada tabel merepresentasikan satu file yang diuji, dengan kolom waktu enkripsi dan dekripsi menunjukkan durasi masing-masing proses dalam satuan detik. Data pada tabel ini dapat digunakan untuk membandingkan efisiensi algoritma enkripsi yang digunakan.

4. Kesimpulan

Dari hasil aplikasi enkripsi dan dekripsi file rekam medis, dapat disimpulkan bahwa aplikasi ini diharapkan dapat digunakan untuk mengamankan file-file penting yang bersifat rahasia. Implementasi metode *Advanced Encryption Standard* (*AES-128*) dengan menggunakan bahasa *Python* telah berhasil dilakukan dalam pembuatan aplikasi enkripsi dan dekripsi file. Penelitian ini menunjukkan keberhasilan dalam mengenkripsi dan mendekripsi file rekam medis dengan format *.pdf*, yang menegaskan efektivitas metode *AES-128* dalam menjaga keamanan data.

Ucapan Terimakasih

Penulis mengucapkan terima kasih yang tulus kepada semua yang terlibat yang mendukung penelitian ini. Ucapan terima kasih khusus disampaikan kepada Dr. Billy Hendrik atas bimbingannya pada mata kuliah *Cyber Security*. Kami juga menghargai bantuan staf teknis dan dukungan yang tak tergoyahkan dari keluarga dan teman-teman kami. Kontribusi Anda sangat penting bagi keberhasilan penelitian ini.

Daftar Rujukan

[1] H. Linda, S. Sitorus, and U. Ristian, "Penerapan Algoritma Advanced Encryption Standard (Aes)-128 Bit Pada Keamanan Database Aplikasi Kepelangganan (Studi," *Komput. dan Apl.*, vol. 11, no. 01, pp. 128–136, 2023.

[2] M. H. K. Arta, I. G. B. Kusuma, M. R. R. Askar, I. B. G. K. Dyatmika, D. Riani, and L. H. Siahaan, "Analisis Citra Digital Dengan Tools Image Forensic Berupa Fotoforensic, Jpegsnoop, Ghiro, Dan Forensically," pp. 1–16, 2019.

[3] M. Alenezi, M. Nadeem, and R. Asif, "SQL injection attacks countermeasures assessments," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 2, pp. 1121–1131, 2020, doi: 10.11591/ijeecs.v21.i2.pp1121-1131.

[4] S. B. Far and A. I. Rad, "When cryptography stops data science: Strategies for resolving the conflicts between data scientists and cryptographers," *Data Sci. Manag.*, 2024, doi: 10.1016/j.dsm.2024.03.001.

[5] X. Huo and X. Wang, "Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system," *Results Eng.*, vol. 20, no. November, p. 101589, 2023, doi: 10.1016/j.rineng.2023.101589.

[6] S. P. Ananda and S. Lukman, "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital," *J. Ilm. Komputasi*, vol. 21, no. 3, pp. 333–344, 2022, doi: 10.32409/jikstik.21.3.2973.

[7] K. J. Nadia, A. T. Toko, and K. Jati, "Penerapan Algoritme Advanced Encryption Standard (Aes-128) Untuk Mengamankan File Dokumen Di Toko Implementation of the Advanced Encryption Standard (Aes-128) Algorithm for Document File Security," vol. 2, no. September, pp. 103–112, 2023.

[8] Menteri Kesehatan RI, *Peraturan Menteri Kesehatan Republik Indonesia No 24 Tahun 2022 Tentang Rekam Medis*, No 24 2023. Menteri Kesehatan RI, 2022. [Online]. Available: https://yankes.kemkes.go.id/unduhan/fileunduhan_1662611251_882318.pdf

[9] J. E. Wahyu Perkasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," *J. Ilm. Teknol. Inf. Asia*, vol. 14, no. 2, pp. 75–84, 2020.

[10] L. A. Muhamad, F. Mahardika, and S. Deris, "Implementation of aes and sha-3 cryptography algorithms in securing user sensitive data on the artesian water bill payment transaction website," vol. 1, no. 1, pp. 41–54, 2024.

[11] T. M. Mudo, Ferdiansyah, and I. Susanti, "Penerapan Kriptografi Menggunakan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan Data Pengiriman Customer Agen JNE Andara," *Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 2, no. 2, pp. 214–224, 2023, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index%7C

[12] N. Putu, A. Astriyani, D. Rimbawa, and B. Raharjo, "Studi Perbandingan AES 128 dan 256 untuk Pengamanan Sistem Informasi Manajemen Rumah Sakit Dr. Mintoharjo," *J. Educ.*, vol. 06, no. 02, pp. 13293–13300, 2024.

[13] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File,"

KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer), vol. 02, no. 01, pp. 31–42, 2020, doi: 10.54367/kakifikom.v2i1.666.

[14] A. Aprizald, M. A. Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *JEKIN - J. Tek. Inform.*, vol. 2, no. 2, pp. 85–95, 2023, doi: 10.58794/jekin.v2i2.225.

[15] H. Wijaya, "Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection," *J. Akad.*, vol. 17, no. 1, pp. 8–13, 2020, [Online]. Available: https://www.ejournal.lppmunidayan.ac.id/index.php/akd

[16] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[17] R. Firdaus and R. R. Santika, "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," *Semin. Nas. Mhs. Fak. Teknol. Inf. Univ. Budi Luhur*, no. September, pp. 111–120, 2022.

[18] R. M. T. Pasaribu, R. Dewi, and I. Parlina, "Implementasi Kombinasi Algoritma Rinjdael dengan Caesar Cipher pada Pengamanan Dokumen Digital," *Hello World J. Ilmu Komput.*, vol. 1, no. 1, pp. 36–52, 2022, doi: 10.56211/helloworld.v1i1.11.

[19] M. Fahri H Damanik, Indra Gunawan, Zulaini Masruro Nasution, Sumarno, and Ika Okta Kirana, "Pemanfaatan Algoritma Aes Untuk Keamanann Data Karyawan Pt. Telkom Indonesia Pematangsiantar," *STORAGE J. Ilm. Tek. dan Ilmu Komput.*, vol. 1, no. 1, pp. 32–37, 2022, doi: 10.55123/storage.v1i1.157.

[20] Melenia Bayu Aryanto, Muhlis Tahir, Silvia Irma Devita, Zuda Nuril Mustofa, Qurrotun Ainiyah, and Shelviatus Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 89–104, 2023, doi: 10.55606/juisik.v3i1.434.