**e-ISSN: 2987-1891**
Available online at http://pcinformatika.org/index.php/pcif/index
**Journal on Pustaka Cendekia Informatika**
**Volume 1 No. 2, Juli - September 2023, pp 133-141**

# Perancangan Aplikasi Keamanan data Rekam Medis menggunakan Algoritma AES (*Advanced Encryption Standard*)

**Hadi Wiyono[1]*, Al Bahrul Karim[2], Ilham Setyaka[3]**

[1,2,3] Teknik Informatika, Universitas Teknologi Yogyakarta, Jl. Siliwangi (Ringroad Utara), Jombor, Sleman, D.I. Yogyakarta, 55285, Indonesia
E-mail: hadiwiyono1945@gmail.com

* Corresponding Author https://doi.org/

**ARTICLE INFO**

**Article history**
*Received:23 September 2023*
*Revised: 29 September 2023*
*Accepted: 05 October 2023*

**Kata Kunci:**
Flutter, Keamanan Data, Rekam Medis, Enkripsi, Algoritma AES

**Keywords:**
Flutter, Data Security, Medical Records, Encryption, AES Algorithm

**ABSTRACT**

Aplikasi Keamanan Data Rekam Medis menggunakan Algoritma AES (*Advanced Encryption Standard*) dirancang untuk melindungi privasi dan kerahasiaan informasi medis pasien. Dalam sistem kesehatan modern, keamanan data rekam medis merupakan hal yang penting. Algoritma AES dipilih karena keamanannya yang tinggi dan penggunaannya yang luas dalam sistem keamanan informasi. Aplikasi ini memungkinkan pengguna, seperti dokter dan staf medis, untuk mengenkripsi dan dekripsi data rekam medis dengan kunci rahasia. Enkripsi dilakukan saat data disimpan atau ditransmisikan, sehingga hanya pihak yang memiliki kunci yang dapat mengakses informasi yang tersimpan. Selain itu, aplikasi ini memiliki fitur manajemen kunci yang aman untuk mencegah kebocoran informasi. Sistem keamanan yang kokoh akan diterapkan untuk melindung i kunci dan mencegah akses yang tidak sah. Dalam perancangan aplikasi ini, algoritma AES akan diimplementasikan dengan menggunakan pustaka kriptografi yang tersedia. Aplikasi akan dikembangkan menggunakan bahasa pemrograman Flutter dan diuji coba dengan contoh data rekam medis. Harapannya, aplikasi ini dapat memberikan tingkat keamanan yang tinggi, melindungi privasi pasien, dan memenuhi standar keamanan dalam lingkungan kesehatan. Dengan kontribusinya dalam meningkatkan keamanan data rekam medis, aplikasi ini diharapkan dapat menjaga privasi pasien dalam sistem kesehatan modern.

The Medical Record Data Security Application uses the AES (Advanced Encryption Standard) Algorithm designed to protect the privacy and confidentiality of patient medical information. In a modern health system, the security of medical record data is important. The AES algorithm was chosen because of its high security and extensive use in information security systems. This application allows users, such as doctors and medical staff, to encrypt and decrypt medical record data with a secret key. Encryption is performed when data is stored or transmitted, so that only those who have the key can access the stored information. In addition, this application has a secure key management feature to prevent information leakage. A robust security system will be put in place to protect the keys and prevent unauthorized access. In designing this application, the AES algorithm will be implemented using the available cryptographic libraries. The application will be developed using the Flutter programming language and tested with examples of medical record data. The hope is that this application can provide a high level of security, protect patient privacy, and meet safety standards in the healthcare environment. With its contribution to improving the security of medical record data, this application is expected to protect patient privacy in modern health systems.

## PENDAHULUAN

Dalam era digital yang terus berkembang, sektor kesehatan juga mengalami transformasi yang signifikan. Penggunaan teknologi informasi dan rekam medis elektronik (*Electronic Medical Records/EMR*) telah menggantikan metode tradisional berbasis kertas dalam menyimpan, mengelola, dan mengakses informasi kesehatan pasien. Pergeseran ini memberikan banyak manfaat, seperti efisiensi, aksesibilitas yang lebih baik, pemrosesan data yang cepat, dan peningkatan kerjasama antarprofesional(Gunawan & Christianto, 2020)(Rizky & Tiorentap, 2020).

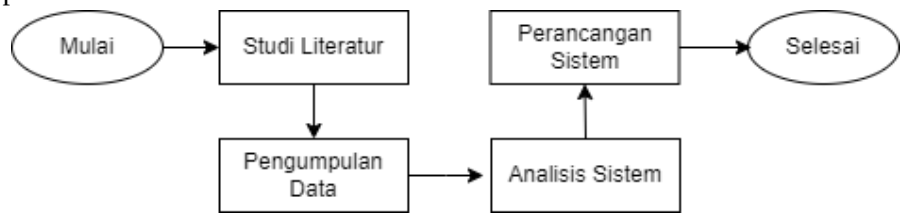
Namun, bersamaan dengan manfaat tersebut, tantangan baru dalam menjaga keamanan dan privasi data rekam medis juga muncul. Data rekam medis mengandung informasi pribadi dan sensitif yang harus dilindungi secara ketat untuk menjaga kerahasiaan pasien dan mematuhi regulasi privasi yang berlaku(Rizky Amanda Tiorentap, 2020). Jika data ini jatuh ke tangan yang salah atau diakses oleh pihak yang tidak berwenang, dapat terjadi pelanggaran privasi, penyalahgunaan informasi, atau bahkan pencurian identitas pasien.

Dalam upaya menjaga kerahasiaan dan integritas data rekam medis, enkripsi menjadi langkah penting. Enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca (*ciphertext*) kecuali dengan menggunakan kunci enkripsi yang sesuai(Khoirunnisa & Djuniadi, 2021). Dalam konteks ini, Algoritma Enkripsi Lanjutan (*Advanced Encryption Standard/AES*) muncul sebagai salah satu standar enkripsi yang paling kuat dan terpercaya yang digunakan secara luas di berbagai industri, termasuk sektor kesehatan.

Perancangan aplikasi keamanan data rekam medis menggunakan algoritma AES menjadi sangat relevan dan penting. Aplikasi ini akan memberikan sarana bagi penyedia layanan kesehatan untuk mengamankan data rekam medis pasien dengan mengenkripsi file-file tersebut sebelum penyimpanan atau pertukaran, serta mendekripsi file-file tersebut saat diperlukan. Dengan menggunakan AES, aplikasi ini akan memberikan tingkat perlindungan yang tinggi terhadap informasi medis yang sensitif, mencegah akses tanpa otorisasi, dan menjaga privasi pasien. Selain itu, aplikasi ini juga akan membantu institusi kesehatan mematuhi persyaratan keamanan dan privasi data yang diperlukan oleh undang-undang dan regulasi, sambil menjaga kualitas pelayanan kesehatan yang cepat, efisien, dan terpercaya(Prameshwari & Sastra, 2018).

## METODE

Penelitian ini menggunakan metodologi yang terdiri dari studi literatur, pengumpulan data, analisis sistem, dan perancangan sistem. Selain itu, juga dilakukan literatur review untuk menyajikan serangkaian penelitian yang relevan dengan topik atau tema penelitian yang diambil. Alur penelitian ini dapat dilihat pada Gambar 1.




Gambar 1. Alur Penelitian

### *Studi Literatur*

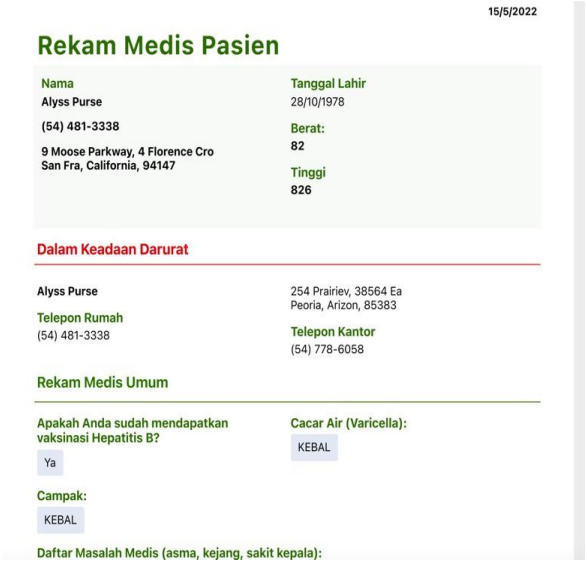
Pada tahap ini, dilakukan studi literatur yang mendalam mengenai topik penelitian, yaitu keamanan data rekam medis dan penggunaan algoritma AES. Studi literatur ini melibatkan pencarian dan analisis sumber-sumber informasi terkait seperti jurnal ilmiah, buku, artikel, dan publikasi terkait lainnya(Hermawan et al., 2021). Tujuannya adalah untuk memperoleh pemahaman yang komprehensif


ISSN 2987-1891 (online)

tentang konsep, teori, dan praktik terkini dalam keamanan data rekam medis serta implementasi algoritma AES.

***Pengumpulan Data***

Pada tahap ini, dilakukan pengumpulan beberapa data rekam medis yang terdiri dari informasi medis pasien. Data tersebut meliputi riwayat penyakit, hasil pemeriksaan laboratorium, diagnosis dokter, dan informasi terkait kondisi kesehatan pasien. Tujuan pengumpulan data ini adalah untuk memastikan bahwa data rekam medis yang relevan dan diperlukan tersedia untuk diproses dan dienkripsi dalam sistem(Studi et al., 2015). Contoh data dapat dilihat pada gambar 2.




Gambar 2. Data Rekam Medis Pasien

***Analisis Sistem***

Tahap ini dilakukan dengan melakukan identifikasi kebutuhan fungsional dan non-fungsional. Kebutuhan fungsional mengacu pada fitur dan fungsi yang harus ada dalam sistem, sedangkan kebutuhan non-fungsional berkaitan dengan analisa yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Berikut adalah hasil analisis kebutuhan fungsional dan non-fungsional sistem ini:

**Kebutuhan Fungsional**

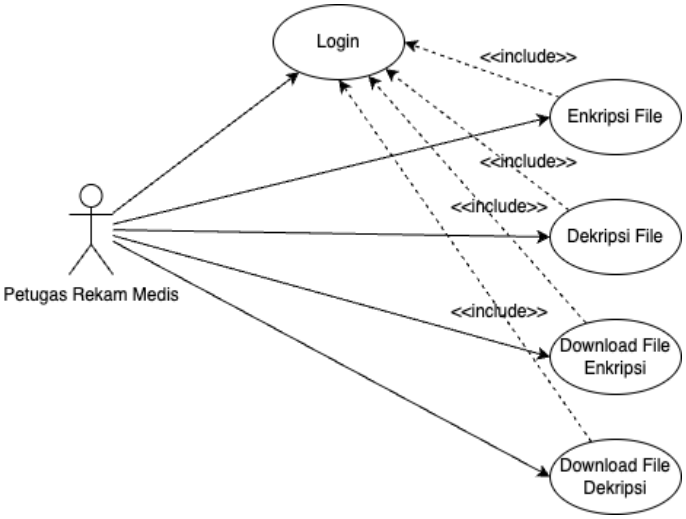
1. Enkripsi Data: Sistem harus mampu mengenkripsi data rekam medis menggunakan algoritma AES.
2. Dekripsi Data: Sistem harus dapat mendekripsi data yang telah dienkripsi menggunakan algoritma AES.
3. Penyimpanan Data: Sistem harus mampu menyimpan data rekam medis yang telah dienkripsi ke dalam database dengan keamanan yang terjamin.
4. Pengambilan Data: Sistem harus dapat mengambil data rekam medis yang telah dienkripsi dari database agar dapat dibuka dari penyimpanan internal.

**Kebutuhan Non Fungsional**

1. Laptop Macbook Air M1
2. *Smartphone* Oppo A54
3. Visual Studio Code
4. Android Studio

***Perancangan Sistem***

Dalam perancangan sistem ini, terdapat beberapa use case yang diidentifikasi untuk memahami kebutuhan pengguna dan memastikan bahwa sistem dapat memenuhi tujuan dan fungsi yang diharapkan(Hozeng, n.d.). Berikut adalah contoh use case yang terkait dengan perancangan sistem keamanan data rekam medis menggunakan algoritma AES yang dapat dilihat pada gambar 3.




Gambar 3. Use Case Diagram

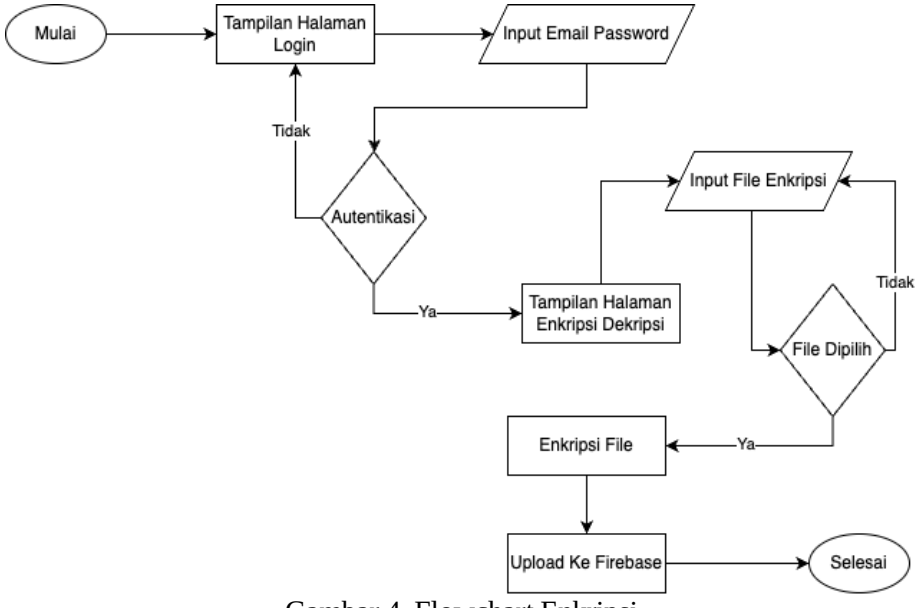
## HASIL DAN PEMBAHASAN

Dalam konteks yang telah dijelaskan sebelumnya, selanjutnya akan dibahas tentang penerapan algoritma kriptografi AES 128-bit untuk melakukan proses enkripsi dan dekripsi dokumen. Bagian ini akan menggambarkan implementasi melalui penggunaan flowchart, antarmuka sistem, serta menampilkan contoh hasil enkripsi dan dekripsi dokumen yang terdapat dalam aplikasi(Simangunsong et al., 2022).

Berikut ini adalah tampilan hasil dari program Perancangan Aplikasi Keamanan data Rekam Medis Menggunakan Algoritma AES.

***Flowchart Enkripsi File***

Flowchat ini menjelaskan tentang proses yang terjadi pada tahapan enkripsi file.

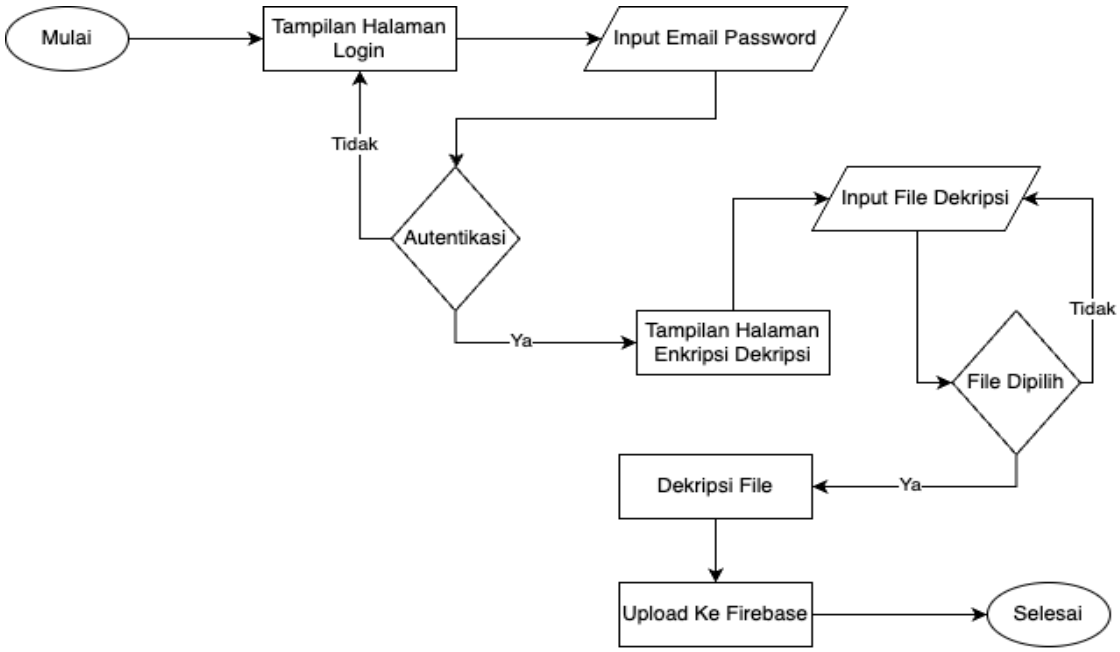



Gambar 4. Flowchart Enkripsi

Gambar 4 adalah sebuah flowchart yang menggambarkan proses enkripsi file dengan langkah awal yaitu melakukan login ke dalam aplikasi. Setelah berhasil login, file tersebut akan dienkripsi dan hasil enkripsi akan langsung diunggah ke database Firebase.

***Flowchart Dekripsi File***

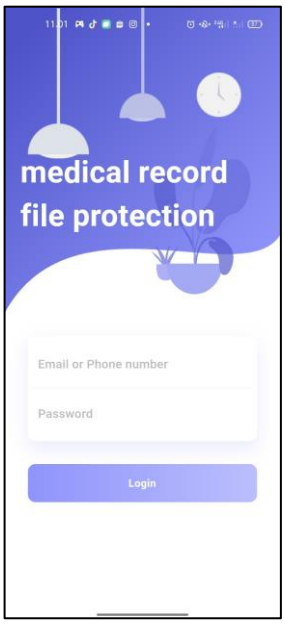

ISSN 2987-1891 (online)



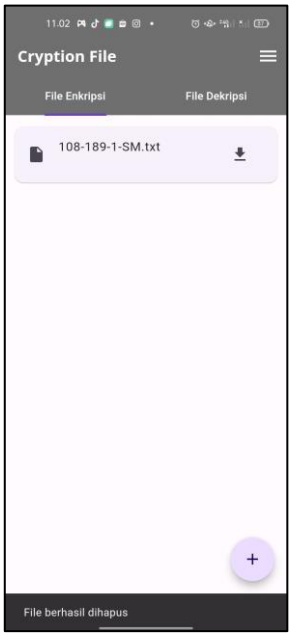

Gambar 5. Flowchart Dekripsi File

Gambar 5 adalah sebuah flowchart yang menggambarkan proses dekripsi file dengan langkah awal yaitu melakukan login ke dalam aplikasi. Setelah berhasil login, file tersebut akan didekripsi dan hasil dekripsi akan langsung diunggah ke database Firebase.

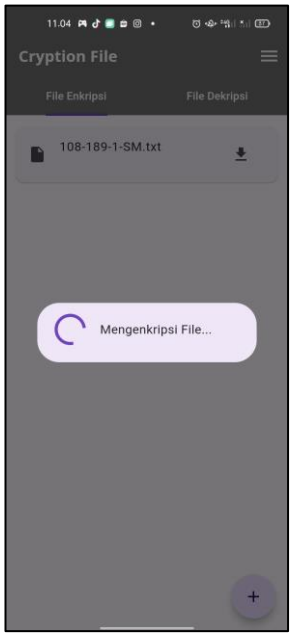
***Tampilan Sistem***



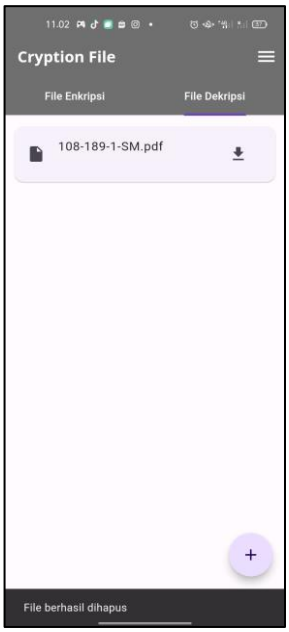

Gambar 6. Tampilan Menu Login




Gambar 7. Tampilan Menu Enkripsi



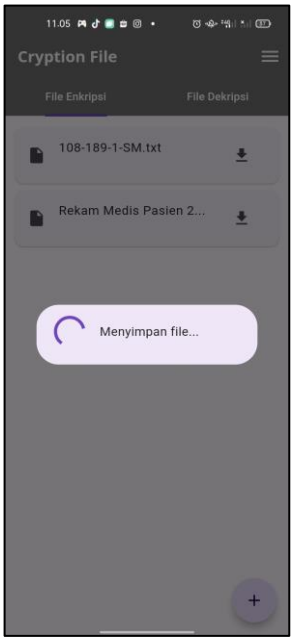

Gambar 8. Tampilan Enkripsi File



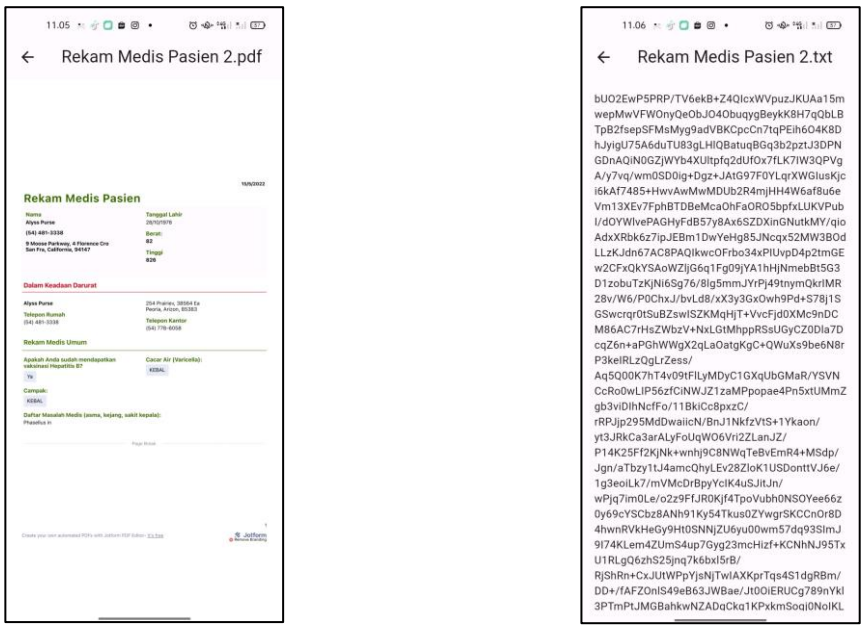

Gambar 9. Tampilan Menu Dekripsi


Gambar 10. Tampilan Dekripsi File


ISSN 2987-1891 (online)




Gambar 11. Tampilan Download File




(a) (b)

Gambar 12 Tampilan File. (a) Sebelum Enkripsi, (b) Sesudah Enkripsi

***Pengujian***

Uji coba terhadap sistem bertujuan untuk memastikan bahwa sistem sudah berada pada kondisi siap pakai. Instrument yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan metode blackbox testing yang dapat diliha pada Tabel 1 berikut.

Tabel 1 Hasil Pengujian

| ***Form* Uji** | **Data Masukan** | **Hasil Yang Diharapkan** | **Hasil Pengujian** |
|---|---|---|---|
| Login | Memasukkan *username* dan *password* dengan benar | Sistem akan menerima akses *login* kemudian langsung menampilkan halaman *home* | Valid |

| | | | |
|---|---|---|---|
| | masukkan username dan password yang salah | Sistem akan menolak akses login dan akan muncul pesan pemberitahuan | Valid |
| Enkripsi File | Pilih proses enkripsi, masukkan file kemudian masukkan *password* | Sistem akan mengenkripsi file yang terpilih kemudian mengupload file tersebut kedalam database | Valid |
| | Pilih proses enkripsi, masukkan file kemudian masukkan *password* dengan panjang yang tidak sesuai | Sistem akan menampilkan pesan bahwa *password* yang dimasukkan tidak sesuai | Valid |
| Dekripsi File | Pilih proses dekripsi, masukkan file kemudian masukkan *password* | Sistem akan mendekripsi file yang terpilih kemudian mengupload file tersebut kedalam database | Valid |
| | Pilih proses dekripsi, masukkan file kemudian masukkan *password* yang tidak sesuai | Sistem akan menampilkan pesan bahwa *password* yang dimasukkan tidak sesuai | Valid |
| *Download* File | Pilih file enkripsi/dekripsi kemudian tekan ikon *download* | Sistem akan membuka penyimpanan internal untuk memilih lokasi *download* | Valid |
| Menampilkan Hasil Enkripsi/Dekripsi File | Klik salah satu list file yang ada di halaman enkripsi/dekripsi | stem akan menampilkan isi dari file enkripsi/dekripsi | Valid |

Pada proses pengujian yang dilakukan, semua hasil dan skenario yang diuji berhasil dilewati dengan sempurna dan tidak ada satupun yang mengalami kegagalan atau masalah. Semua fitur dan fungsionalitas sistem bekerja dengan baik dan sesuai dengan harapan, menghasilkan output yang akurat dan konsisten. Proses pengujian yang komprehensif dan teliti memastikan bahwa sistem telah diuji secara menyeluruh dan memenuhi semua standar kualitas yang ditetapkan. Dengan demikian, dapat dikatakan bahwa pengujian ini telah memverifikasi kehandalan dan kualitas sistem yang dirancang.

## SIMPULAN

Sistem keamanan data rekam medis yang dirancang dengan menggunakan algoritma AES (Advanced Encryption Standard) telah menghasilkan hasil yang memuaskan dalam pengujian yang dilakukan. Seluruh fitur dan fungsionalitas sistem berjalan dengan baik dan tanpa ada kegagalan yang signifikan. Pengujian yang komprehensif dan teliti telah memastikan bahwa sistem ini dapat memenuhi kebutuhan keamanan data rekam medis dengan baik. Sistem ini mampu mengenkripsi dan mendekripsi data rekam medis dengan menggunakan algoritma AES, yang merupakan algoritma yang diakui dan teruji keamanannya. Pengelolaan kunci enkripsi juga telah diimplementasikan dengan baik, memastikan bahwa kunci enkripsi yang digunakan aman dan hanya dapat diakses oleh entitas yang berwenang.

Meskipun terdapat beberapa kekurangan seperti kebutuhan pemeliharaan sistem yang sederhana dan keterbatasan akses melalui versi seluler saja, secara keseluruhan sistem ini dapat dianggap sebagai solusi yang handal dan efektif dalam menjaga keamanan data rekam medis. Perancangan dan pengujian sistem ini telah memastikan bahwa kebutuhan fungsional dan non-fungsional terpenuhi dengan baik. Secara keseluruhan, perancangan sistem keamanan data rekam medis ini telah memberikan solusi yang efektif dalam menjaga kerahasiaan dan keamanan informasi sensitif. Dengan implementasi yang tepat


ISSN 2987-1891 (online)

dan pemeliharaan yang teratur, sistem ini dapat menjadi alat yang berharga dalam menjaga privasi dan keamanan data rekam medis.

Berdasarkan hasil perancangan dan pengujian sistem ini, terdapat beberapa saran yang dapat diberikan untuk meningkatkan kinerja dan fungsionalitas sistem. Pertama, mengingat keterbatasan sistem saat ini hanya tersedia dalam versi seluler, disarankan untuk mengembangkan juga versi website agar pengguna dapat mengakses sistem dari berbagai platform, termasuk perangkat komputer. Kedua, untuk mengantisipasi kemungkinan kehilangan data atau kesalahan enkripsi, disarankan untuk mempertimbangkan pengembangan fitur pemulihan data yang memungkinkan pengguna untuk mengembalikan data ke keadaan semula dengan menggunakan metode tertentu, seperti penggunaan kunci pemulihan atau cadangan data terenkripsi.

## UCAPAN TERIMA KASIH

Peneliti menyampaikan ucapan terima kasih kepada pihak yang sudah berkontribusi dalam pelaksanaan penelitian dan penyusunan artikel ini.

## REFERENSI

Hermawan, A., Iman, E., & Ujianto, H. (2021). *Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA*. *5*(2). https://doi.org/10.30743/infotekjar.v5i2.3585

Hozeng, S. (n.d.). Perancangan Aplikasi Enkripsi Menggunakan Algoritma AES Berbasis Android Encryption Application Design Using Android-Based AES Algorithm. In *Prosiding Seminar Nasional Komunikasi dan Informatika #3 Tahun* (Vol. 2019).

Khoirunnisa, O. G., & Djuniadi, D. (2021). Implementasi Algoritma AES untuk Keamanan Data Rekam Medis. *PETIR*, *15*(1), 21–27. https://doi.org/10.33322/petir.v15i1.1333

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Rizky Amanda Tiorentap, D. (2020). *Prosiding 4 SENWODIPA*.

Rizky, D., & Tiorentap, A. (2020). Manfaat Penerapan Rekam Medis Elektronik Di Negara Berkembang: Systematic Literature Review. In *Health Information Management Journal ISSN* (Vol. 8, Issue 2).

Simangunsong, H., Agung Raharja, M., & Raya Kampus Unud, J. (2022). Penerapan Algoritma Advanced Encryption Standard (AES-128) Dengan Mode ECB Dalam Pengamanan File. In *Jurnal Nasional Teknologi Informasi dan Aplikasinya* (Vol. 1, Issue 1).

Studi, P., Sarjana, P., Administrasi, K., Sakit, R., Administrasi, D., Kebijakan, D., Fakultas, K., & Masyarakat, K. (2015). *Analisis Sistem Penyelenggaraan Rekam Medis di Instalasi Rekam Medis RS "X" Tangerang Periode April-Mei 2015 Analysis of Medical Record Implementation System in Installation Medical Record "X" Hospital Tangerang period from April to May 2015 Novita Nuraini*.