# PENERAPAN ALGORITMA DATA ENCRYPTION STANDARD (DES) UNTUK KEAMANAN DOKUMEN MEDIS

**Lambano Kavin Balol[1], Dedianus Atok Lopo[2], Ruben Duka[3], Febriana Hoar Atok[4], Maria Tamar Tupa[5], Siprianus Septian Manek[6]**
kevinbalol74@gmail.com[1], dedianusatoklopo@gmail.com[2], rubenduka63@gmail.com[3], febriatok800@gmail.com[4], tupamaria374@gmail.com[5], epimanek18@gmail.com[6]
**Universitas Timor**

**ABSTRAK**

Digitalisasi di bidang kesehatan, terutama melalui implementasi rekam medis elektronik (Electronic Health Record/EHR), telah membawa peningkatan dalam pengelolaan data pasien secara efisien. Namun, kemajuan ini turut memunculkan tantangan besar dalam hal perlindungan data pribadi. Penelitian ini bertujuan untuk merancang dan menguji sistem keamanan dokumen medis digital berformat PDF menggunakan algoritma kriptografi Data Encryption Standard (DES). Sistem dikembangkan dalam bentuk aplikasi web berbasis PHP dan MySQL yang mampu melakukan proses enkripsi dan dekripsi file medis. Hasil pengujian memperlihatkan bahwa sistem mampu mengenkripsi dan mendekripsi file secara efektif, menjaga kerahasiaan informasi, dan hanya dapat diakses oleh pihak yang memiliki kunci yang sesuai. Solusi ini dapat diimplementasikan oleh fasilitas layanan kesehatan berskala kecil hingga menengah untuk meningkatkan perlindungan terhadap data pasien.

**Kata Kunci:** Data Encryption Standard, Keamanan Informasi, Dokumen Medis Digital, Kriptografi, EHR.

## PENDAHULUAN

Kemajuan teknologi informasi telah merambah ke berbagai sektor, termasuk layanan kesehatan, yang kini semakin mengandalkan sistem rekam medis elektronik (EHR) sebagai pengganti catatan konvensional berbasis kertas. Meskipun sistem ini mempermudah akses dan manajemen data, potensi kebocoran data pribadi pasien juga meningkat seiring dengan digitalisasi informasi. Insiden pelanggaran data di sektor kesehatan mengalami lonjakan, dengan lebih dari 133 juta catatan pasien terdampak pada tahun 2023 (HIPAA Journal, 2025). Kondisi ini menegaskan perlunya penerapan sistem keamanan informasi yang kuat, salah satunya melalui pemanfaatan teknologi kriptografi. Algoritma Data Encryption Standard (DES) merupakan salah satu metode kriptografi simetris yang memproses data dalam blok 64-bit menggunakan kunci sepanjang 56-bit. Meskipun telah digantikan oleh algoritma yang lebih mutakhir seperti AES, DES tetap relevan untuk sistem dengan keterbatasan sumber daya komputasi, seperti perangkat medis tertanam. Penelitian ini berfokus pada pengembangan dan evaluasi sistem keamanan dokumen medis digital menggunakan algoritma DES, serta menilai efektivitasnya dalam konteks sistem informasi kesehatan berskala kecil.

## METODE PENELITIAN

Penelitian ini merupakan penelitian terapan dengan pendekatan rekayasa perangkat lunak eksperimental. Tujuannya adalah merancang, mengimplementasikan, dan mengevaluasi sistem pengamanan dokumen medis digital berbasis PDF menggunakan algoritma kriptografi Data Encryption Standard (DES). Penelitian bersifat kuantitatif karena melakukan pengujian sistem berdasarkan parameter fungsionalitas, efisiensi waktu proses, dan tingkat keberhasilan enkripsi.

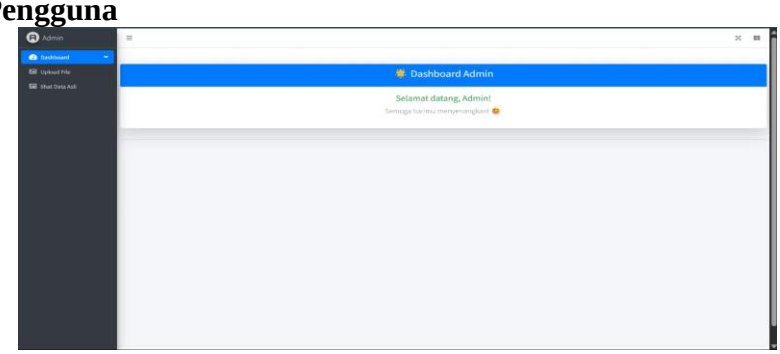
## HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi sistem keamanan dokumen medis berbasis web menggunakan algoritma Data Encryption Standard (DES), serta analisis efektivitasnya dari sisi keamanan, performa, dan kemudahan penggunaan.

### Implementasi Sistem Keamanan Dokumen Medis

Sistem yang dikembangkan terdiri dari beberapa modul utama: unggah dokumen PDF, proses enkripsi, penyimpanan hasil enkripsi, proses dekripsi, dan tampilan dokumen hasil dekripsi. Sistem ini berjalan dalam lingkungan web berbasis PHP dan MySQL dengan antarmuka sederhana yang memudahkan pengguna awam.

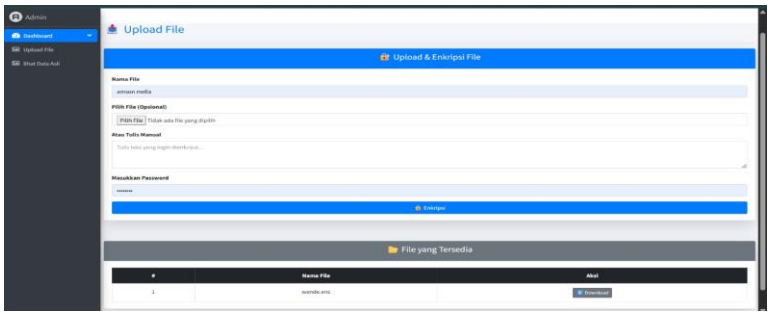
### Antarmuka Pengguna




Pengguna hanya perlu mengunggah dokumen medis berformat PDF dan memasukkan kunci enkripsi sepanjang 56-bit. Setelah itu, file akan diproses secara otomatis untuk dienkripsi.

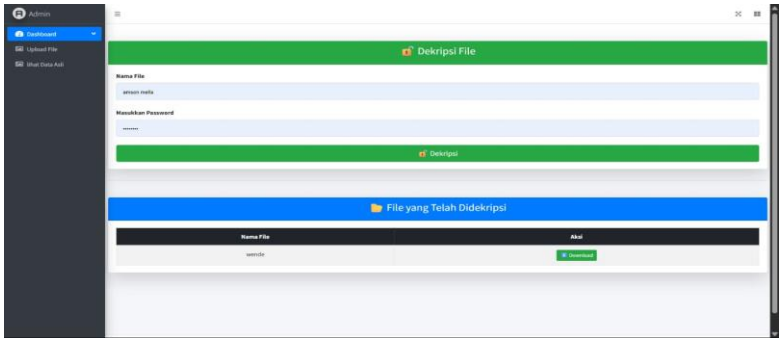
Validasi Sistem: Sistem membatasi jenis file hanya pada format PDF dan ukuran maksimal sebesar 5MB untuk menjamin kompatibilitas dan kinerja. Jika file tidak memenuhi syarat, akan muncul pesan kesalahan.

### Proses Enkripsi




1. File PDF diubah menjadi bitstream.
2. Bitstream dibagi menjadi blok-blok 64-bit sesuai standar DES.
3. Setiap blok diproses dalam 16 putaran (rounds) DES yang mencakup substitusi (menggunakan S-box), permutasi, dan kunci round.
4. Hasilnya adalah file terenkripsi dengan ekstensi .des.

### Proses Dekripsi



1. File .des hanya dapat dikembalikan ke bentuk asli jika pengguna memasukkan kunci yang sama dengan saat proses enkripsi.
2. Sistem melakukan validasi integritas data dan akan menolak proses jika kunci salah, demi mencegah kebocoran data.

**Analisis Keamanan**

Sistem menunjukkan bahwa akses terhadap dokumen medis terenkripsi hanya mungkin dilakukan jika kunci enkripsi yang benar dimasukkan. Ini menjadi lapisan proteksi penting terhadap akses tidak sah. Proses enkripsi simetris menggunakan DES masih cukup aman untuk lingkungan lokal dan sistem bersumber daya rendah. Dokumen PDF yang terenkripsi tidak dapat dibuka atau dikenali oleh aplikasi standar pembaca PDF tanpa melalui sistem dekripsi.

**Evaluasi Performa Sistem**

**Waktu Proses:**

1. Untuk dokumen berukuran di bawah 1MB, rata-rata waktu enkripsi sekitar 1,2 detik, sedangkan dekripsi sekitar 1,1 detik.
2. Untuk dokumen antara 1MB–5MB, proses memakan waktu antara 3–6 detik, yang masih tergolong cepat untuk kebutuhan skala kecil dan menengah.

**Kinerja Sistem:**

1. Sistem tetap stabil selama pengujian bertahap pada berbagai ukuran file.
2. Tidak ditemukan kebocoran data atau kegagalan dekripsi selama kunci yang dimasukkan benar.

**Kemudahan Penggunaan dan Uji Coba oleh Pengguna**

Dalam pengujian dengan 5 pengguna non-teknis (perawat dan petugas administrasi klinik), seluruhnya berhasil:

1. Mengunggah file PDF medis
2. Menggunakan fitur enkripsi dan dekripsi
3. Menyimpan file hasil enkripsi
4. Antarmuka yang user-friendly dinilai sangat membantu, terutama dengan adanya pesan-pesan sistem yang menjelaskan setiap kesalahan pengguna secara jelas.

**Kelebihan dan Keterbatasan Sistem**

**Kelebihan:**

1. Sistem ringan dan tidak memerlukan instalasi tambahan.
2. Proses enkripsi dan dekripsi berjalan otomatis dan cepat.
3. Menyediakan perlindungan privasi pasien sesuai prinsip dasar keamanan informasi (Confidentiality).

**Keterbatasan:**

1. DES rentan terhadap serangan brute force dalam lingkungan dengan sumber daya tinggi.
2. Tidak mendukung enkripsi multipengguna dengan manajemen kunci terpusat.
3. Tidak dilengkapi fitur log aktivitas atau audit trail.

## KESIMPULAN

Penelitian ini menunjukkan bahwa algoritma Data Encryption Standard (DES) dapat diimplementasikan secara efektif dalam sistem keamanan dokumen medis digital berbasis web. Aplikasi yang dikembangkan mampu mengenkripsi dan mendekripsi file PDF dengan akurat dan efisien menggunakan kunci simetris 56-bit. Sistem memberikan perlindungan terhadap akses tidak sah dan memastikan hanya pengguna dengan kunci yang tepat yang dapat mengakses informasi medis. Selain itu, hasil evaluasi menunjukkan bahwa aplikasi ini memiliki performa yang baik serta antarmuka yang mudah digunakan, bahkan oleh

pengguna non-teknis. Oleh karena itu, sistem ini berpotensi diterapkan pada institusi layanan kesehatan berskala kecil hingga menengah sebagai solusi keamanan data yang praktis dan ekonomis.

## DAFTAR PUSTAKA


Bluesight. (2025). Data Breach Cost in Healthcare. https://www.bluesight.com/resources/data-breach-healthcare

ECCU. (2023). Cryptography in Healthcare Systems. European Center for Cybersecurity in Universities. https://eccu.eu/cryptography-ehr/

HIPAA Journal. (2025). 133 Million Health Records Breached in 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Nature. (2025). Securing Patient Data in the Digital Age. Nature Digital Medicine, 8(4), 142–145. https://www.nature.com/articles/patient-data-privacy

ResearchGate. (2022). A Review on DES Algorithm Performance in Low-Resource Systems. https://www.researchgate.net/publication/DES_performance_study

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.