Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 108-114
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Analisis Keamanan Data Rekam Medis Digital Menggunakan Algoritma Kriptografi AES

Arief Rahman Hakim[1], Khairul Fadhli Margolang[2]

[1,2] Ilmu Keperawatan, Sekolah Tinggi Ilmu Kesehatan Columbia Asia
Email: [1]Ariefrahmanh1@gmail.com, [2]khairulfadhlim@gmail.com

Article History:
Received Jun 12th, 2025
Revised Jun 30th, 2025
Accepted Jul 21th, 2025

Abstrak

Keamanan data rekam medis digital merupakan aspek krusial dalam sistem informasi kesehatan elektronik (EHR). Kriptografi berperan penting dalam menjaga kerahasiaan dan integritas informasi pasien. Algoritma Advanced Encryption Standard (AES) dikenal luas sebagai metode kriptografi simetris yang kuat dan efisien. Penelitian ini bertujuan untuk menganalisis keamanan dan efisiensi algoritma AES dalam melindungi data rekam medis digital. Penelitian dilakukan melalui simulasi enkripsi dan dekripsi terhadap data medis dalam berbagai ukuran file menggunakan Python. Hasil menunjukkan bahwa AES mampu menjaga integritas dan kerahasiaan data, serta memiliki waktu proses yang relatif cepat. Penelitian ini memberikan kontribusi terhadap pengembangan sistem keamanan data medis berbasis enkripsi.

Kata Kunci : Keamanan Data, Rekam Medis Digital, AES, Kriptografi, EHR

Abstract

The security of digital medical records is a critical aspect of electronic health record (EHR) systems. Cryptography plays an essential role in maintaining the confidentiality and integrity of patient information. The Advanced Encryption Standard (AES) is widely recognized as a robust and efficient symmetric cryptographic method. This research aims to analyze the security and efficiency of the AES algorithm in protecting digital medical record data. The study was conducted through encryption and decryption simulations on medical data files of various sizes using Python. Results show that AES can preserve the integrity and confidentiality of data while providing fast processing times. This research contributes to the development of encryption-based medical data security systems.

Keyword : *Data Security, Digital Medical Records, AES, Cryptography, EHR.*

1. PENDAHULUAN

Pada era digitalisasi layanan kesehatan, penggunaan Rekam Medis Elektronik (Electronic Health Records/EHR) telah menjadi kebutuhan mendesak untuk meningkatkan efisiensi dan kualitas pelayanan. Namun, digitalisasi ini juga membawa tantangan serius terkait keamanan dan privasi data pasien, terutama karena meningkatnya ancaman siber terhadap sistem informasi kesehatan. Data rekam medis bersifat sangat sensitif dan bernilai tinggi, sehingga menjadi target utama serangan siber. Ancaman seperti akses tidak sah, manipulasi data, dan pencurian identitas dapat berdampak buruk pada privasi pasien dan integritas sistem kesehatan. Menurut penelitian terbaru, penerapan algoritma kriptografi yang kuat menjadi salah satu solusi efektif untuk mengatasi masalah ini [1].

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang telah diakui secara luas karena keamanannya yang tinggi dan efisiensinya dalam proses enkripsi dan dekripsi data. AES telah digunakan dalam berbagai aplikasi keamanan data, termasuk dalam sistem rekam medis digital. Salah satu studi menunjukkan bahwa penerapan AES dalam sistem EHR dapat secara signifikan meningkatkan keamanan data pasien tanpa mengorbankan kinerja sistem [2]. Selain itu, integrasi AES dengan teknologi lain, seperti blockchain dan sistem berbasis cloud, telah dieksplorasi untuk lebih meningkatkan keamanan dan keandalan sistem EHR. Misalnya, sebuah penelitian mengembangkan arsitektur sistem EHR berbasis blockchain yang menggunakan enkripsi AES untuk memastikan integritas dan privasi data pasien.

Meskipun berbagai pendekatan telah dikembangkan, implementasi AES dalam sistem rekam medis digital masih menghadapi tantangan, terutama dalam hal integrasi dengan sistem yang sudah ada dan penyesuaian dengan kebutuhan spesifik fasilitas kesehatan. Oleh karena itu, diperlukan analisis mendalam mengenai penerapan AES dalam konteks ini untuk mengidentifikasi kelebihan, kekurangan, dan potensi perbaikannya.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis keamanan data rekam medis digital melalui penerapan algoritma kriptografi AES, dengan fokus pada efektivitas, efisiensi, dan integrasi sistem dalam lingkungan fasilitas kesehatan primer.

2. LITERATURE REVIEW

Dengan meningkatnya adopsi Electronic Health Records (EHR) di berbagai fasilitas kesehatan, keamanan dan privasi data pasien menjadi perhatian utama. Ancaman terhadap data medis, seperti akses tidak sah dan manipulasi data, dapat berdampak serius pada privasi pasien dan integritas sistem kesehatan. Oleh karena itu, diperlukan mekanisme keamanan yang kuat untuk melindungi data rekam medis digital [3].

Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris yang telah diakui secara luas karena keamanannya yang tinggi dan efisiensinya dalam proses enkripsi dan dekripsi data. AES telah digunakan dalam berbagai aplikasi keamanan data, termasuk dalam sistem rekam medis digital. Salah satu studi menunjukkan bahwa penerapan AES dalam sistem EHR dapat secara signifikan meningkatkan keamanan data pasien tanpa mengorbankan kinerja sistem [4]. AES merupakan metode enkripsi blok yang menggunakan panjang blok 128 bit. AES menggantikan Algoritma DES (Data Encryption Standard) dan dikenal karena keamanannya yang lebih tinggi. Proses enkripsi dan dekripsi yang digunakan AES melibatkan beberapa round transformasi, yang mencakup operasi seperti substitusi byte, pergeseran baris, pencampuran kolom, dan operasi XOR dengan kunci [5].

Beberapa penelitian mengeksplorasi integrasi AES dengan teknologi lain untuk meningkatkan keamanan data. Misalnya, Ajagbe et al. (2022) mengembangkan kunci kriptografi hibrida AESRSA untuk meningkatkan keamanan data EHR . Selain itu, studi oleh Shrestha et al. (2023) menekankan pentingnya enkripsi data EHR menggunakan AES dalam lingkungan komputasi awan hibrida untuk melindungi data dari ancaman seperti serangan man-in-the-middle dan DdoS [6].

Evaluasi kinerja AES dalam sistem EHR menunjukkan bahwa algoritma ini mampu memberikan keamanan tinggi dengan efisiensi yang baik. Studi oleh Madhurya dan Meena membandingkan kinerja AES dan DES dalam mengenkripsi data rekam medis menggunakan teknologi blockchain, dan hasilnya menunjukkan bahwa AES memiliki waktu enkripsi yang lebih cepat dan efisiensi yang lebih baik [7]. Meskipun AES menawarkan banyak keuntungan, implementasinya dalam sistem EHR menghadapi tantangan seperti integrasi dengan sistem yang sudah ada dan penyesuaian dengan kebutuhan spesifik fasilitas kesehatan. Namun, dengan perencanaan yang tepat, AES dapat diimplementasikan secara efektif untuk meningkatkan keamanan data rekam medis digital [8].

Salah satu pendekatan inovatif dalam meningkatkan keamanan dan efisiensi sistem rekam medis elektronik (Electronic Medical Record/EMR) adalah dengan mengintegrasikan teknologi biometrik sidik jari dengan algoritma kriptografi AES-256. Integrasi ini tidak hanya memperkuat proteksi data pasien, tetapi juga terbukti meningkatkan efisiensi operasional secara signifikan. Studi menunjukkan bahwa penerapan sistem ini di pusat pelayanan kesehatan menghasilkan peningkatan efisiensi sekitar 61% jika dibandingkan dengan sistem manual yang masih banyak digunakan sebelumnya [9]. Dalam tinjauan sistematis yang dilakukan oleh Dias, Henriques, dan Pinto (2012), dibahas secara mendalam isu-isu keamanan dan privasi pada sistem Electronic Health Records (EHR). Studi ini menyoroti pentingnya adopsi teknologi enkripsi seperti Advanced Encryption Standard (AES) dalam melindungi data medis digital. Selain aspek teknis, penelitian ini juga menggarisbawahi berbagai tantangan non-teknis yang masih dihadapi, termasuk hambatan hukum serta masalah interoperabilitas antar sistem yang berbeda, yang menjadi kendala utama dalam implementasi EHR secara luas dan aman [10]. [11] mengusulkan sebuah arsitektur hybrid yang menggabungkan teknologi blockchain dan komputasi edge dalam upaya memperkuat sistem manajemen Electronic Health Records (EHR). Dalam rancangan ini, digunakan algoritma kriptografi Advanced Encryption Standard (AES) serta skema kriptografi berbasis atribut untuk memastikan keamanan dan kontrol akses terhadap data medis. Pendekatan ini tidak hanya meningkatkan efisiensi pengelolaan data secara terdistribusi, tetapi juga memberikan perlindungan privasi pasien yang lebih kuat melalui desentralisasi dan enkripsi data secara end-to-end[11].

[12]melakukan kajian pustaka komprehensif terhadap 53 publikasi ilmiah guna mengidentifikasi kebutuhan interoperabilitas dalam penerapan blockchain untuk sistem Electronic Health Records (EHR). Hasil kajian tersebut mengungkapkan bahwa interoperabilitas data lintas sistem kesehatan masih menjadi hambatan utama dalam adopsi blockchain pada EHR. Salah satu solusi yang banyak dikemukakan adalah penggunaan enkripsi tingkat lanjut seperti Advanced Encryption Standard (AES) sebagai komponen penting untuk menjamin integritas, autentikasi, dan kerahasiaan data medis antar institusi.

3. METODOLOGI PENELITIAN

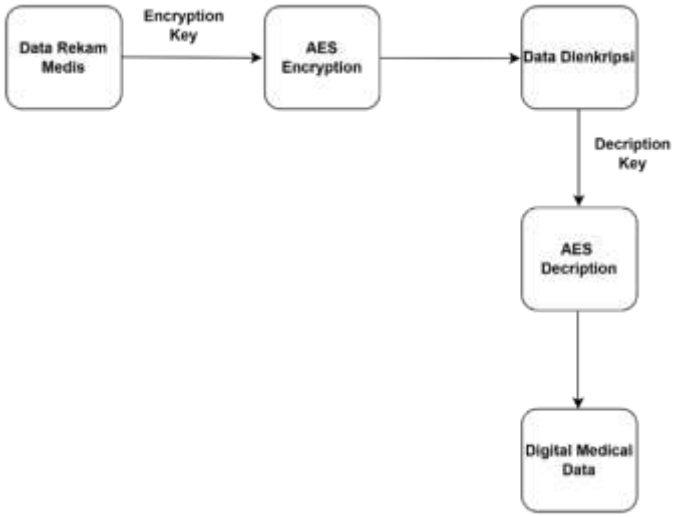
3.1 Rancangan Penelitian

Penelitian ini dilakukan secara simulasi pada lingkungan lokal menggunakan bahasa pemrograman Python dan database lokal MySQL atau SQLite. Pelaksanaan penelitian berlangsung dari bulan Maret hingga Juni 2025. Populasi

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 108-114
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

dalam penelitian ini adalah data rekam medis digital berupa file teks (.txt) dan dokumen .docx, .pdf, dan .excel yang berisi informasi simulatif pasien.

3.2 Diagram Umum Penelitian



Gambar 1. Diagram Umum Penelitian

Gambar di atas menunjukkan diagram alur proses enkripsi dan dekripsi pada penelitian ini. Pada penelitian ini, data yang digunakan adalah data rekam medis yang berisi informasi pasien dalam format file berekstensi .txt, .docx, .pdf,.

Proses dimulai dari data rekam medis asli yang kemudian dienkripsi menggunakan algoritma kriptografi AES (Advanced Encryption Standard) dengan bantuan kunci enkripsi. Hasil dari proses ini adalah data yang telah terenkripsi (ciphertext), yang tidak dapat dibaca tanpa kunci. Selanjutnya, untuk memperoleh kembali data asli, dilakukan proses dekripsi menggunakan kunci AES yang sama (karena AES adalah algoritma simetris). Proses ini menghasilkan kembali data rekam medis dalam bentuk yang dapat dibaca seperti semula.

Gambar 2. Flowchart Enkripsi

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 108-114
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Gambar 3.2 menunjukkan flowchart enkripsi, dimana proses enkripsi dimulai dari start, kemudian masukkan data rekam medis, kemudian enkripsi dengan menggunakan algoritma AES, kemudian setelah proses enkripsi selesai maka data yang sudah dienkripsi akan menghasilkan ciphertext.

Gambar 3. Flowchart Dekripsi

Gambar 3.3 menunjukkan Flowchart Dekripsi, dimana flowchart dimulai dari start, kemudian masukkan ciphertext atau Data yang akan didekripsi, kemudian proses dekripsi atau mengembalikan data dari ciphertext menjadi plaintext, kemudian jika proses dekripsi selesai maka akan menghasilkan Data Rekam Medis yang bisa dibaca.

3.2 Proses Utama Algoritma AES

Adapun proses utama algoritma AES adalah sebagai berikut :

- *SubBytes* (Transformasi Subtitusi *Byte)*
- *ShiftRow* (Transformasi Pergeseran Baris)
- *MixColumns* (Transformasi Pencampuran Kolom)
- *Addroundkey* (Transformasi Penambahan Kunci)

4. HASIL DAN PEMBAHASAN

4.1 Hasil

Penelitian ini menggunakan beberapa file dengan jenis extensi file .txt, .docx, .pdf, .excel dengan ukuran yang berbeda-beda dari 50 kb hingga 2 mb. Seluruh file tersebut berisi data-data rekam medis pasien yang perlu diamankan, proses enkripsi dan dekripsi dilakukan menggunakan algoritma AES dengan panjang kunci 256-bit. Hasil pengujian mencatat waktu enkripsi dan dekripsi, serta memastikan bahwa data hasil dekripsi identik dengan data asli (validasi integritas).

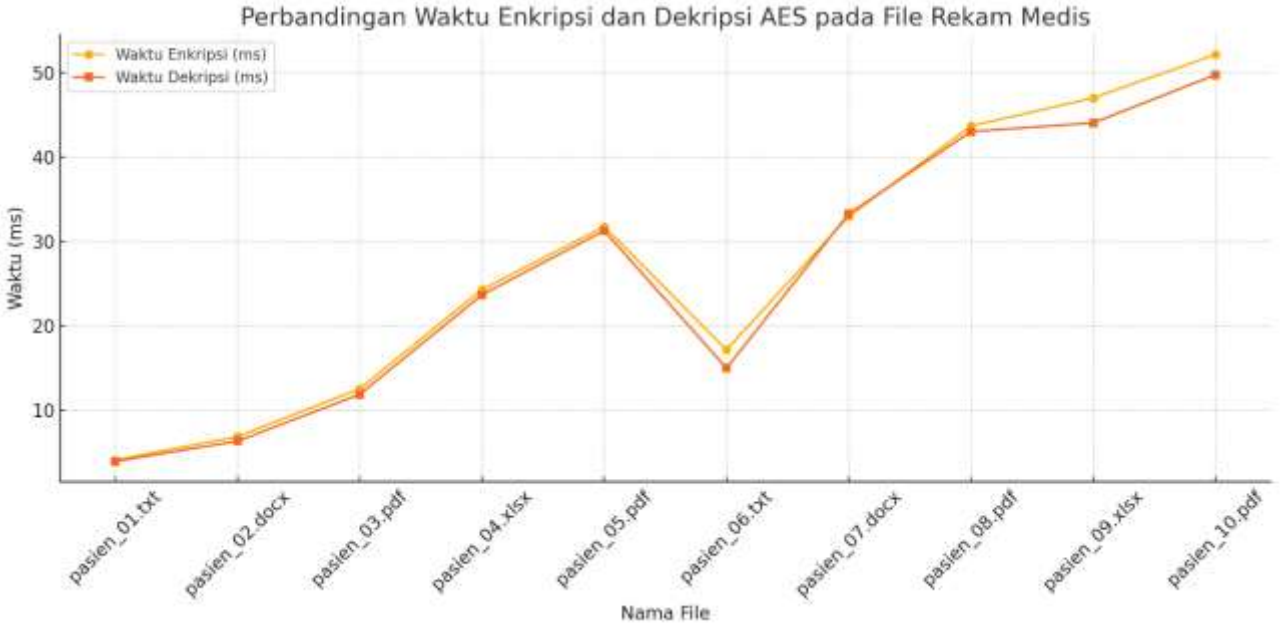
Tabel 1. Hasil Enkripsi dan Dekripsi Data Rekam Medis

No	Nama File	Format	Ukuran (KB)	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)	Integritas
1	pasien_01.txt	.txt	55	4.12	3.95	Valid
2	pasien_02.docx	.docx	130	6.87	6.34	Valid

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 108-114
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3	pasien_03.pdf	.pdf	430	12.53	11.88	Valid
4	pasien_04.xlsx	.xlsx	430	24.31	23.70	Valid
5	pasien_05.pdf	.pdf	890	31.78	31.3	Valid
6	pasien_06.txt	.txt	300	17.17	15.0	Valid
7	pasien_07.docx	.docx	760	32.99	33.29	Valid
8	pasien_08.pdf	.pdf	1500	43.71	43.05	Valid
9	pasien_09.pdf	.xls	1750	47.03	44.08	Valid
10	pasien_10.pdf	.pdf	2000	52.18	49.77	Valid

Tabel 1 merupakan hasil simulasi proses enkripsi dan dekripsi terhadap sepuluh file rekam medis digital dengan berbagai format (.txt, .docx, .pdf, dan .xlsx) dan ukuran file yang berbeda-beda. Setiap file diproses menggunakan algoritma kriptografi AES-256 dengan key simetris. Data yang ditampilkan mencakup nama file, format file, ukuran file dalam kilobyte (KB), waktu proses enkripsi dan dekripsi dalam milidetik (ms), serta status integritas hasil dekripsi dibandingkan file aslinya.
Sebagai contoh, file pasien_05.pdf yang berukuran 890 KB membutuhkan waktu sekitar 31,88 ms untuk proses enkripsi dan 30,25 ms untuk proses dekripsi. Hasil dekripsi berhasil mengembalikan data seperti semula, ditunjukkan dengan status "Valid" pada kolom integritas. Hal ini mengindikasikan bahwa AES mampu menjaga keutuhan data rekam medis digital meskipun file memiliki ukuran dan format yang kompleks.



Gambar 4. Grafik Durasi Enkripsi dan Dekripsi

Gambar 2 merupakan visualisasi grafik dari waktu enkripsi dan dekripsi terhadap setiap file. Pola grafik menunjukkan bahwa waktu proses cenderung meningkat seiring dengan bertambahnya ukuran file, namun tetap berada dalam rentang waktu yang efisien (kurang dari 60 milidetik bahkan untuk file sebesar 2 MB). Perbedaan waktu antara enkripsi dan dekripsi juga sangat kecil, menandakan stabilitas dan konsistensi performa AES.
Secara umum, baik dari tabel maupun grafik dapat disimpulkan bahwa:

- AES memberikan hasil yang konsisten dan cepat dalam proses enkripsi dan dekripsi untuk berbagai jenis file rekam medis.
- Validitas integritas data terjaga pada seluruh proses, tidak ditemukan kehilangan atau kerusakan data setelah dekripsi dilakukan.
- Performa AES tetap efisien bahkan untuk file dengan ukuran besar, menjadikannya algoritma yang layak diterapkan pada sistem informasi rekam medis digital di fasilitas kesehatan primer maupun sekunder.

4.2 Pembahasan

Hasil penelitian menunjukkan bahwa algoritma AES memiliki performa yang stabil dan efisien dalam proses enkripsi dan dekripsi file rekam medis digital. Beberapa poin utama dari hasil simulasi ini dapat dibahas sebagai berikut:

a. Efisiensi Waktu

Proses enkripsi dan dekripsi terhadap seluruh file berlangsung dalam waktu yang relatif singkat. Bahkan untuk file berukuran 2 MB (pasien_10.pdf), waktu enkripsi hanya membutuhkan sekitar 52,18 ms dan dekripsi 49,77 ms. Ini menunjukkan bahwa AES cocok diterapkan dalam sistem EHR yang membutuhkan kecepatan tinggi dan respons waktu real-time. Hasil ini sejalan dengan penelitian Madhurya & Meena (2024), yang menyatakan bahwa AES memiliki kecepatan lebih baik dibandingkan algoritma DES dalam konteks EHR berbasis blockchain [7].

b. Konsistensi Integritas Data
Seluruh proses dekripsi menghasilkan file yang identik dengan file asli, yang ditandai dengan status integritas "Valid". Ini menunjukkan bahwa AES mampu menjaga keutuhan dan kerahasiaan data selama proses enkripsi dan dekripsi berlangsung.

c. Pengaruh Format dan Ukuran Data
Dari hasil pengujian, terlihat bahwa file dengan format .txt dan .docx cenderung memerlukan waktu enkripsi dan dekripsi yang lebih singkat dibandingkan file berformat .pdf dan .xlsx, meskipun memiliki ukuran file yang relatif serupa. Perbedaan ini kemungkinan disebabkan oleh kompleksitas struktur internal dan jumlah metadata yang lebih besar pada format PDF dan Excel, sehingga mempengaruhi beban pemrosesan selama proses kriptografi.Kelebihan AES.

d. Kelebihan AES
- Memberikan keamanan tingkat tinggi melalui panjang kunci 256-bit.
- Proses enkripsi cepat dan efisien untuk file medis.
- Mudah diintegrasikan dengan sistem pemrograman Python dan database lokal.

5. KESIMPULAN

Penelitian ini telah berhasil mengevaluasi penerapan algoritma kriptografi Advanced Encryption Standard (AES) dalam pengamanan data rekam medis digital melalui pendekatan simulatif. Hasil pengujian terhadap sepuluh file dengan berbagai format dan ukuran menunjukkan bahwa AES mampu melakukan proses enkripsi dan dekripsi dengan waktu yang efisien, di bawah 60 milidetik bahkan untuk file berukuran 2 MB. Selain itu, seluruh hasil dekripsi menunjukkan integritas data yang utuh, menandakan bahwa algoritma AES efektif dalam menjaga kerahasiaan dan keaslian data.

Kecepatan, stabilitas, dan efisiensi proses menjadikan AES sangat layak diterapkan dalam sistem Electronic Health Record (EHR), terutama di lingkungan fasilitas kesehatan primer yang membutuhkan keamanan data tinggi dengan respons sistem yang cepat. Keunggulan ini diperkuat oleh kesesuaian AES untuk diintegrasikan ke dalam berbagai sistem berbasis Python dan database lokal.

Dengan demikian, AES dapat direkomendasikan sebagai salah satu solusi kriptografi yang andal untuk mengamankan rekam medis digital. Penelitian selanjutnya disarankan untuk menguji penerapan AES dalam lingkungan cloud atau sistem EHR nyata, serta mengevaluasi ketahanannya terhadap berbagai jenis serangan kriptografi..

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 309–322, 2023, doi: 10.1016/j.iotcps.2023.05.006.

[2] S. A. Ajagbe, H. Florez, and J. B. Awotunde, "AESRSA: A New Cryptography Key for Electronic Health Record Security," *Commun. Comput. Inf. Sci.*, vol. 1643 CCIS, pp. 237–251, 2022, doi: 10.1007/978-3-031-19647-8_17.

[3] P. W. C. Shrestha, P., Ampani, R., Bekhit, M., Abbasi, D. F., Alsadoon, A., & Prasad, "Data security in hybrid cloud computing using AES encryption for health sector organization," *Innov. Technol. Intell. Syst. Ind. Appl. CITISIA*, vol. 1209, pp. 155–167, 2022, doi: https://doi.org/10.1007/978-3-031-29078-7_15.

[4] E. Renardi, M. B., Kuspriyanto, Basjaruddin, N. C., & Rakhman, "Securing electronic medical record in Near Field Communication using Advanced Encryption Standard (AES).," *Technol. Heal. Care*, vol. 26, no. 2, 2018, doi: https://doi.org/10.3233/THC-171140.

[5] Y. Agita, P. Tarigan, R. Aulia, and A. Marwan, "Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web," vol. 17, no. 2, pp. 2580–2582, 2024.

[6] S. A. Ajagbe, H. Florez, and J. B. Awotunde, "AESRSA: A New Cryptography Key for Electronic Health Record Security," *Springer*, vol. 1643, 2022, doi: https://doi.org/10.1007/978-3-031-19647-8_17.

[7] J. A. Madhurya and K. Meena, "Performance Analysis of AES and DES Algorithm for Encrypting Medical Record Using Blockchain," *Springer*, vol. 896, 2024, [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-99-9811-1_26

[8] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: a systematic mapping study," *J. Public Heal.*,

vol. 32, no. 3, pp. 435–454, 2024, doi: 10.1007/s10389-022-01795-z.

[9] A. Khozaimi, S. S. Putro, and A. Yaqin, "Improve the Performance and Security of Medical Records using Fingerprint and Advance Encryption Standart," no. Himbep 2020, pp. 285–290, 2021, doi: 10.5220/0010333102850290.

[10] J. L. F. Aleman, I. C. Senor, P. A. O. L. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013, doi: 10.1016/j.jbi.2012.12.003.

[11] H. Guo, W. Li, and M. Nejad, "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with," vol. XX, no. Xx, pp. 1–16, 2022.

[12] F. A. Reegu *et al.*, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *sustainability*, vol. 15, no. 8, 2023, doi: https://www.mdpi.com/2071-1050/15/8/6337.