KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.6 Desember 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 433-444
DOI : https://doi.org/10.61722/jssr.v4i6.12917

PENGAMANAN DATA PASIEN PADA PUSKESMAS BATAHAN MENGGUNAKAN ALGORITMA AES-128 BERBASIS WEB

Charisya Silvara Maligan[1]*, Mhd. Basri[2]
[1]Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Indonesia
*Penulis Korespondensi: [charisyamaligan@gmail.com[1], mhdbasri@umsu.ac.id[2]]

Abstract. *This study aims to implement the Advanced Encryption Standard 128-bit (AES-128) algorithm to protect patient data at Puskesmas Batahan through a web-based information system. Patient identity and medical record data contain sensitive information that requires protection from unauthorized access. The system was developed using Next.js, React, Prisma, and MySQL 8.0. AES-128 was implemented using Cipher Block Chaining (CBC), PKCS#7 padding, and a randomly generated initialization vector (IV). The security mechanism was complemented by authentication, role-based access control, password hashing using bcrypt, and audit logging. Testing included black-box testing, validation against the NIST FIPS PUB 197 test vector, encryption-decryption round-trip testing, avalanche effect testing, and performance testing. The results show that all 38 black-box scenarios were successful, giving a 100% success rate. The average avalanche effect reached 50.70% for a one-bit plaintext change and 49.61% for a one-bit key change. The average encryption time for storing one patient record was 0.5329 ms, while decrypting 50 patient records for display took 17.5758 ms on average. These results indicate that AES-128 can be integrated into the developed system to strengthen patient-data confidentiality with relatively small processing overhead.*

Keywords*: AES-128; data security; medical records; patient data; web-based system.*

Abstrak. Penelitian ini bertujuan menerapkan algoritma Advanced Encryption Standard 128-bit (AES-128) untuk mengamankan data pasien pada Puskesmas Batahan melalui sistem informasi berbasis web. Data identitas dan rekam medis pasien mengandung informasi sensitif sehingga memerlukan perlindungan dari akses yang tidak berwenang. Sistem dikembangkan menggunakan Next.js, React, Prisma, dan MySQL 8.0. AES-128 diterapkan menggunakan mode Cipher Block Chaining (CBC), padding PKCS#7, dan Initialization Vector (IV) yang dibangkitkan secara acak. Mekanisme keamanan dilengkapi autentikasi, kontrol akses berbasis peran, hashing kata sandi menggunakan bcrypt, dan pencatatan audit. Pengujian meliputi black box testing, validasi terhadap vektor uji NIST FIPS PUB 197, pengujian bolak-balik enkripsi dan dekripsi, avalanche effect, dan pengujian kinerja. Hasil penelitian menunjukkan seluruh 38 skenario black box berhasil dengan tingkat keberhasilan 100%. Avalanche effect rata-rata mencapai 50,70% pada perubahan satu bit plaintext dan 49,61% pada perubahan satu bit kunci. Waktu enkripsi rata-rata untuk menyimpan satu data pasien sebesar 0,5329 ms, sedangkan dekripsi 50 data pasien untuk ditampilkan membutuhkan rata-rata 17,5758 ms. Hasil tersebut menunjukkan bahwa AES-128 dapat diterapkan untuk memperkuat kerahasiaan data pasien dengan overhead pemrosesan yang relatif kecil.

Kata kunci: AES-128; data pasien; keamanan data; rekam medis; sistem berbasis web.

1. LATAR BELAKANG

Perkembangan teknologi informasi mendorong fasilitas pelayanan kesehatan untuk memanfaatkan sistem informasi berbasis web dalam pengelolaan data pasien dan rekam medis. Digitalisasi memberikan kemudahan dalam pencatatan, pencarian, dan pengelolaan informasi, tetapi pada saat yang sama meningkatkan kebutuhan terhadap pengamanan data yang bersifat sensitif.

Naskah Masuk:01 Oktober 2026; Revisi: 02 Oktober 2026; Diterima: 04 Oktober 2026; Terbit: 05 Oktober 2026

Data pasien mencakup identitas pribadi dan informasi medis yang harus dijaga kerahasiaannya. Perlindungan data kesehatan juga menjadi bagian penting dalam penerapan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian terkait rekam medis elektronik menunjukkan bahwa kerahasiaan data perlu diperkuat melalui mekanisme keamanan yang sesuai dengan karakteristik informasi kesehatan (Puteri et al., 2024; Indriyajati et al., 2024).

Algoritma Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang menggunakan blok berukuran 128 bit. AES-128 menggunakan kunci 128 bit dan menjalankan 10 ronde transformasi (Evans et al., 2022). Penelitian sebelumnya menunjukkan bahwa AES dapat digunakan untuk pengamanan database dan data rekam medis, termasuk penerapan AES-128 pada file rekam medis pasien (Ramadhani & Cobantoro, 2022; Hakim & Margolang, 2025; Tamin & Hendrik, 2025).

Penelitian mengenai mode operasi AES juga menunjukkan bahwa CBC dapat menghasilkan difusi yang baik dan mencegah plaintext yang sama menghasilkan ciphertext identik ketika digunakan bersama IV yang berbeda (Prabowo & Nizirwan, 2025). Namun, penelitian yang secara khusus mengimplementasikan AES-128 pada pengelolaan data pasien di tingkat puskesmas seperti Puskesmas Batahan masih terbatas. Oleh karena itu, penelitian ini membangun sistem informasi pasien berbasis web dengan penerapan AES-128 serta kontrol akses dan audit log.

Penelitian ini bertujuan membangun sistem informasi pasien berbasis web dengan penerapan AES-128 serta mengevaluasi hasil implementasinya melalui pengujian fungsional, validasi terhadap standar NIST FIPS PUB 197, pengujian avalanche effect, pengujian keamanan, dan pengujian kinerja.

2. KAJIAN TEORITIS

Data Pasien dan Rekam Medis

Data pasien merupakan informasi yang berkaitan dengan identitas individu yang menerima pelayanan kesehatan, sedangkan rekam medis memuat informasi mengenai pemeriksaan dan pelayanan yang diberikan. Dalam penelitian ini, data identitas dan atribut rekam medis diperlakukan sebagai data yang perlu dilindungi ketika tersimpan dalam basis data.

Keamanan Data

Keamanan informasi berkaitan dengan kerahasiaan, integritas, dan ketersediaan. Penelitian ini berfokus pada kerahasiaan melalui enkripsi AES-128, serta memperkuat pengamanan melalui autentikasi, Role-Based Access Control (RBAC), hashing kata sandi, dan audit log. Perlindungan data kesehatan juga berkaitan dengan kewajiban menjaga data pribadi spesifik sebagaimana diatur dalam UU No. 27 Tahun 2022 (Alaikha Annan, 2024).

Algoritma AES-128

AES ditetapkan sebagai standar kriptografi oleh NIST dan menggunakan ukuran blok 128 bit. AES-128 menggunakan kunci sepanjang 128 bit dengan 10 ronde. Transformasi utama meliputi SubBytes, ShiftRows, MixColumns, dan AddRoundKey (Evans et al., 2022; Ganesh et al., 2025).

Mode CBC dan Initialization Vector

Cipher Block Chaining (CBC) menghubungkan blok plaintext dengan ciphertext sebelumnya sebelum proses enkripsi. Blok pertama menggunakan IV. Sistem penelitian membangkitkan IV acak sepanjang 16 byte setiap kali record disimpan atau diubah sehingga plaintext yang sama tidak menghasilkan ciphertext yang sama.

Role-Based Access Control dan Audit Log

RBAC membatasi fungsi berdasarkan peran pengguna. Sistem memiliki tiga peran, yaitu admin, dokter, dan petugas. Audit log digunakan untuk mencatat pengguna, jenis aksi, tabel yang diakses, record, alamat IP, dan waktu kejadian.

3. METODE PENELITIAN

Penelitian ini merupakan penelitian rekayasa perangkat lunak dengan model pengembangan Waterfall. Model tersebut digunakan karena pengembangan dilakukan secara bertahap melalui pengumpulan kebutuhan, perancangan, implementasi, pengujian, dan evaluasi (Bakri et al., 2024; Saravanos, 2023).

Pengumpulan Data

Data penelitian diperoleh melalui observasi, wawancara, dan studi literatur. Observasi digunakan untuk memahami proses pengelolaan data pasien, wawancara

digunakan untuk menggali kebutuhan sistem, sedangkan studi literatur digunakan untuk memperoleh landasan mengenai keamanan data, AES-128, dan sistem informasi kesehatan.

Perancangan dan Implementasi

Sistem dibangun menggunakan Next.js dan React pada sisi aplikasi, Prisma sebagai ORM, dan MySQL 8.0 sebagai basis data. Sistem mencakup autentikasi, dashboard, data pasien, rekam medis, manajemen pengguna, log aktivitas, dan demo enkripsi.

Atribut yang Dienkripsi

Atribut yang dienkripsi pada tabel pasien meliputi nama, NIK, tanggal lahir, alamat, dan nomor telepon. Pada tabel rekam_medis, atribut yang dienkripsi meliputi keluhan, diagnosa, tindakan, dan resep. AES-128 diterapkan menggunakan mode CBC, padding PKCS#7, dan IV acak sepanjang 16 byte.

Pengujian

Pengujian terdiri atas black box testing terhadap 38 skenario yang mencakup 17 kebutuhan fungsional, validasi AES-128 menggunakan vektor uji NIST FIPS PUB 197, pengujian bolak-balik terhadap 10 data uji, pengujian avalanche effect pada perubahan satu bit plaintext dan satu bit kunci, pengujian keamanan, serta pengujian kinerja dengan 30 iterasi per skenario. Pengujian black box digunakan untuk memastikan keluaran sistem sesuai dengan kebutuhan fungsional yang ditetapkan (Utomo et al., 2020).

Alur Kerja Sistem

Alur pengamanan dimulai ketika pengguna melakukan login. Sistem memverifikasi kredensial dan role pengguna. Ketika data pasien atau rekam medis disimpan, atribut sensitif dienkripsi menggunakan AES-128 CBC dan hasilnya disimpan sebagai ciphertext. Ketika data diminta oleh pengguna yang berwenang, ciphertext dan IV diambil dari basis data kemudian didekripsi sebelum ditampilkan. Aktivitas penting dicatat pada audit log.

4. HASIL DAN PEMBAHASAN

Pengumpulan data dilakukan melalui observasi, wawancara, dan studi literatur untuk memahami proses pengelolaan data pasien serta kebutuhan pengamanan sistem.

Penelitian dilaksanakan di Puskesmas Batahan, Kecamatan Batahan, Kabupaten Mandailing Natal, Provinsi Sumatera Utara. Waktu pelaksanaan penelitian berlangsung dari Januari hingga Juni 2026, yang mencakup pengumpulan data awal, analisis sistem, perancangan, implementasi, pengujian, dan penyusunan laporan.

Hasil Implementasi dan Hak Akses

Hasil implementasi menunjukkan bahwa sistem memiliki tujuh halaman utama dengan pembagian hak akses berdasarkan role. Pembagian hak akses tersebut diringkas pada Tabel 1. Rekam medis hanya dapat diakses oleh admin dan dokter, sedangkan manajemen pengguna dan log aktivitas hanya dapat diakses oleh admin. Pembatasan tersebut menjadi bagian dari mekanisme perlindungan data selain enkripsi.

Tabel 1. Daftar Halaman Sistem dan Hak Akses

No	Halaman	Admin	Dokter	Petugas
1	Login	✓	✓	✓
2	Dashboard	✓	✓	✓
3	Data Pasien	✓	✓	✓
4	Rekam Medis	✓	✓	—
5	Manajemen Pengguna	✓	—	—
6	Log Aktivitas	✓	—	—
7	Demo Enkripsi	✓	✓	✓

Sumber: Hasil pengujian, 2026.

Hasil Pengumpulan dan Penyimpanan Data

Hasil observasi dan perancangan diterjemahkan ke dalam mekanisme penyimpanan yang mengenkripsi atribut sensitif sebelum disimpan. Data identitas pasien dan data rekam medis yang dipilih tidak disimpan sebagai plaintext pada atribut yang dilindungi. Mekanisme ini mendukung tujuan kerahasiaan data karena isi informasi tidak dapat dibaca secara langsung dari penyimpanan tanpa proses dekripsi menggunakan kunci yang sesuai.

Perbandingan mode operasi juga dilakukan untuk memastikan alasan penggunaan CBC. Hasil ringkas pada Tabel 2 menunjukkan bahwa plaintext yang sama pada mode ECB menghasilkan keluaran ciphertext yang identik, sedangkan pada CBC dengan IV acak menghasilkan keluaran yang berbeda. Temuan tersebut sesuai dengan prinsip CBC dan mendukung penggunaan IV acak pada setiap proses penyimpanan.

Tabel 2. Ringkasan Perbandingan Mode ECB dan CBC

Mode	Kondisi Pengujian	Hasil
ECB	Plaintext sama digunakan kembali	Ciphertext identik
CBC	Plaintext sama dengan IV acak	Ciphertext berbeda
CBC	Penyimpanan ulang record	IV dibangkitkan kembali

Sumber: Hasil pengujian, 2026.

Validasi Implementasi AES-128

Validasi implementasi AES-128 dilakukan menggunakan vektor uji resmi NIST FIPS PUB 197. Tabel 3 menyajikan hasil dalam bentuk ringkasan, bukan data mentah. Ciphertext yang dihasilkan sistem sama dengan keluaran referensi NIST dan proses dekripsi mengembalikan plaintext uji. Hasil tersebut menunjukkan bahwa implementasi transformasi AES-128 pada sistem sesuai dengan standar yang digunakan sebagai acuan (Evans et al., 2022).

Tabel 3. Hasil Validasi Implementasi AES-128

Aspek Validasi	Hasil Sistem	Interpretasi
Vektor uji NIST FIPS PUB 197	Sesuai dengan nilai referensi	Implementasi AES-128 valid
Enkripsi	Ciphertext sesuai referensi	Transformasi enkripsi sesuai
Dekripsi	Plaintext kembali seperti semula	Proses bolak-balik berhasil

Sumber: Hasil pengujian, 2026.

Hasil Black Box Testing

Pengujian black box dilakukan terhadap 38 skenario yang mencakup 17 kebutuhan fungsional. Pengujian mencakup autentikasi, hak akses, pengelolaan data pasien, rekam medis, manajemen pengguna, audit log, dan kondisi negatif. Ringkasan hasil pengujian disajikan pada Tabel 4.

Tabel 4. Ringkasan Hasil Black Box Testing

Aspek Pengujian	Jumlah Skenario	Hasil
Autentikasi dan hak akses	10	Valid
Manajemen pengguna	5	Valid
Data pasien	12	Valid
Rekam medis	6	Valid
Log aktivitas dan fitur pendukung	5	Valid
Total	38	100% valid

Sumber: Hasil pengujian, 2026.

Seluruh 38 skenario menghasilkan keluaran sesuai dengan yang diharapkan sehingga tingkat keberhasilan pengujian mencapai 100%. Hasil ini menunjukkan bahwa fungsi utama dan pembatasan akses yang dirancang dapat berjalan pada skenario pengujian yang digunakan.

Hasil Pengujian Avalanche Effect

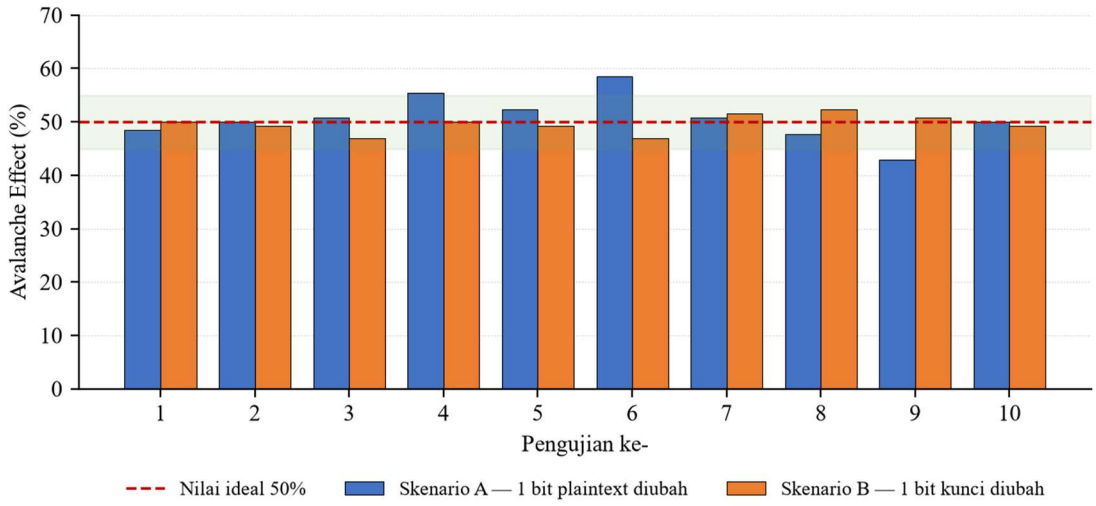
Avalanche effect digunakan untuk mengukur perubahan ciphertext ketika satu bit masukan diubah. Pengujian dilakukan pada dua skenario, yaitu perubahan satu bit plaintext dengan kunci tetap dan perubahan satu bit kunci dengan plaintext tetap. Masing-masing skenario dilakukan sebanyak sepuluh percobaan. Ringkasan hasil ditampilkan pada Tabel 5.

Tabel 5. Ringkasan Hasil Pengujian Avalanche Effect

Skenario	Rata-rata AE	Terendah	Tertinggi
Perubahan 1 bit plaintext	50,70%	42,97%	58,59%
Perubahan 1 bit kunci	49,61%	46,88%	52,34%

Sumber: Hasil pengujian, 2026.

Gambar 1 memperlihatkan hasil pengujian avalanche effect. Rata-rata avalanche effect sebesar 50,70% pada perubahan plaintext dan 49,61% pada perubahan kunci berada dekat dengan nilai ideal 50%. Hasil tersebut menunjukkan bahwa perubahan kecil pada input menghasilkan perubahan pada sekitar setengah bit ciphertext, sehingga difusi pada implementasi AES-128 yang diuji dapat dikatakan baik. Temuan ini sejalan dengan penelitian mengenai AES-128 yang menggunakan parameter avalanche effect sebagai indikator difusi kriptografi (Pinuyut et al., 2024; Prabowo & Nizirwan, 2025).



Gambar 1. Grafik Hasil Pengujian Avalanche Effect

Sumber: Hasil pengujian, 2026.

Hasil Pengujian Kinerja

Pengujian kinerja dilakukan untuk mengetahui waktu proses enkripsi dan dekripsi pada beberapa panjang data. Hasil pengukuran diringkas pada Tabel 6. Waktu enkripsi meningkat seiring bertambahnya panjang data, sedangkan waktu dekripsi pada skenario yang diuji tetap berada pada rentang yang relatif rendah.

Tabel 6. Waktu Enkripsi dan Dekripsi Berdasarkan Panjang Data

Panjang Data	Operasi	Rata-rata (ms)	Minimum (ms)	Maksimum (ms)
16 karakter	Enkripsi	0,2024	0,1453	0,5734
16 karakter	Dekripsi	0,1423	0,0928	0,9313
64 karakter	Enkripsi	0,1986	0,1453	0,9803
64 karakter	Dekripsi	0,1163	0,1001	0,1917
256 karakter	Enkripsi	0,2445	0,1680	1,1799
256 karakter	Dekripsi	0,1023	0,0955	0,1168
1024 karakter	Enkripsi	0,4593	0,3261	1,0875
1024 karakter	Dekripsi	0,1435	0,1374	0,1982

Sumber: Hasil pengujian, 2026.

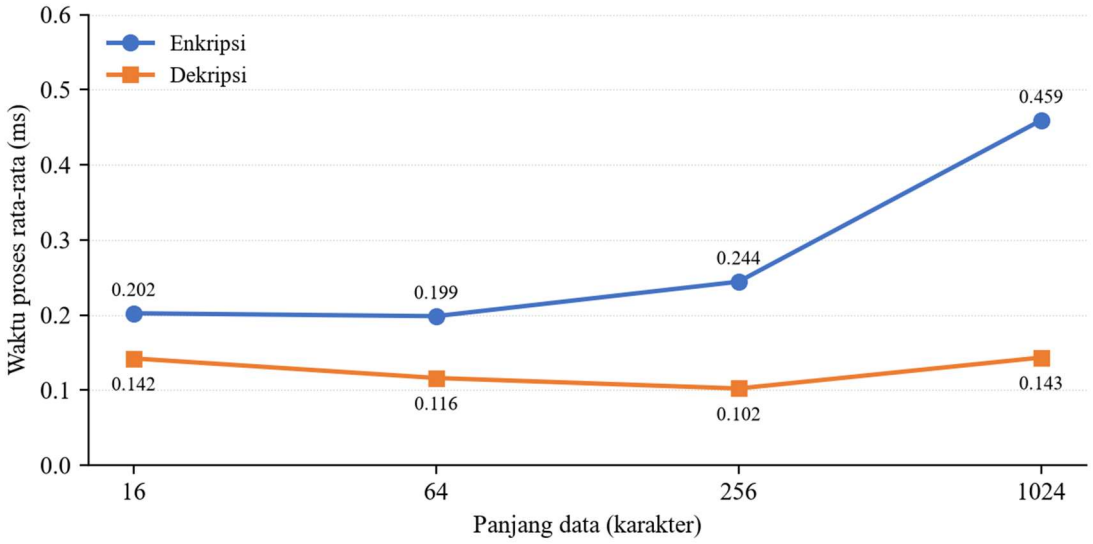
Pada tingkat record, Tabel 7 menunjukkan bahwa enkripsi satu record pasien yang terdiri atas lima atribut memiliki rata-rata waktu 0,5329 ms. Dekripsi satu record memiliki rata-rata 0,3953 ms, sedangkan dekripsi 50 record untuk ditampilkan memiliki rata-rata 17,5758 ms. Hasil ini menunjukkan bahwa proses kriptografi memberikan tambahan waktu pemrosesan yang relatif kecil pada skenario pengujian.

Tabel 7. Waktu Proses pada Tingkat Record Data Pasien

Skenario	Rata-rata (ms)	Minimum (ms)	Maksimum (ms)
Enkripsi 1 record pasien (5 atribut)	0,5329	0,4580	0,9899
Dekripsi 1 record pasien (5 atribut)	0,3953	0,3390	1,6478
Dekripsi 50 record pasien	17,5758	14,7433	24,2393

Sumber: Hasil pengujian, 2026.

Gambar 2 memperlihatkan kecenderungan waktu proses berdasarkan panjang data. Grafik menunjukkan bahwa waktu enkripsi meningkat pada panjang data 1024 karakter dibandingkan panjang data yang lebih kecil. Pola tersebut konsisten dengan bertambahnya data yang harus diproses, sedangkan variasi waktu dekripsi relatif kecil pada skenario pengujian.



Gambar 2. Grafik Panjang Data terhadap Waktu Proses

Sumber: Hasil pengujian, 2026.

Hasil Pengujian Keamanan

Pengujian keamanan dilakukan untuk memeriksa kerahasiaan data, kegagalan dekripsi dengan kunci yang salah, pembatasan endpoint berdasarkan role, penyimpanan kata sandi, dan akses halaman tanpa autentikasi. Ringkasan hasil ditampilkan pada Tabel 8.

Tabel 8. Hasil Pengujian Keamanan Sistem

Skenario	Hasil Pengujian	Keterangan
Basis data diakses langsung	Atribut sensitif hanya tersimpan sebagai ciphertext	Aman
Dekripsi dengan kunci salah	Data asli tidak berhasil dipulihkan	Aman
Endpoint admin oleh role lain	Akses ditolak dengan HTTP 403	Aman
Kata sandi pada basis data	Tersimpan menggunakan bcrypt	Aman
Akses halaman tanpa autentikasi	Dialihkan ke halaman login	Aman

Sumber: Hasil pengujian, 2026.

Hasil tersebut menunjukkan bahwa perlindungan sistem tidak hanya bergantung pada enkripsi, tetapi juga pada autentikasi dan pembatasan hak akses. Penerapan RBAC memastikan fungsi administratif tidak dapat dipanggil oleh role yang tidak sesuai, sedangkan audit log menyediakan rekam aktivitas yang dapat digunakan untuk penelusuran kejadian.

Pembahasan

Secara keseluruhan, hasil penelitian menunjukkan bahwa AES-128 dapat diintegrasikan ke dalam sistem pengelolaan data pasien berbasis web tanpa menghilangkan fungsi utama aplikasi. Dari sisi fungsionalitas, seluruh 38 skenario pengujian berhasil. Dari sisi kebenaran algoritma, hasil sistem sesuai dengan vektor uji NIST dan pengujian bolak-balik berhasil mengembalikan data ke bentuk semula. Hasil tersebut mendukung penelitian sebelumnya mengenai penerapan AES-128 pada pengamanan database dan rekam medis (Ramadhani & Cobantoro, 2022; Hakim & Margolang, 2025; Tamin & Hendrik, 2025).

Pada aspek kerahasiaan, atribut sensitif disimpan dalam bentuk ciphertext sehingga tidak dapat dibaca langsung ketika basis data diakses. Penggunaan CBC dengan IV acak juga mencegah plaintext yang sama menghasilkan ciphertext yang sama pada proses penyimpanan yang berbeda. Hasil ini sejalan dengan penelitian Prabowo dan Nizirwan (2025) mengenai difusi pada AES-128 mode CBC.

Nilai avalanche effect sebesar 50,70% untuk perubahan plaintext dan 49,61% untuk perubahan kunci menunjukkan bahwa perubahan satu bit pada masukan menghasilkan perubahan pada sekitar setengah bit ciphertext. Hasil tersebut berada dekat dengan nilai ideal 50% dan konsisten dengan temuan penelitian AES sebelumnya (Pinuyut et al., 2024; Sidqon & Nafis, 2024). Dari sisi kinerja, rata-rata enkripsi satu record pasien sebesar 0,5329 ms dan dekripsi 50 record sebesar 17,5758 ms menunjukkan overhead pemrosesan yang relatif kecil pada skenario pengujian.

Secara teoritis, hasil penelitian memperkuat penerapan prinsip kerahasiaan melalui kriptografi simetris pada data kesehatan. Secara terapan, sistem memberikan mekanisme perlindungan berlapis melalui enkripsi, RBAC, bcrypt, dan audit log. Namun, mode CBC berfokus pada kerahasiaan dan tidak menyediakan autentikasi integritas ciphertext secara langsung. Oleh karena itu, pengembangan berikutnya dapat mempertimbangkan authenticated encryption seperti AES-GCM serta pengelolaan dan rotasi kunci yang lebih kuat.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil membangun sistem informasi berbasis web untuk pengamanan data pasien pada Puskesmas Batahan menggunakan algoritma AES-128 mode CBC dengan padding PKCS#7 dan IV acak. Data identitas pasien dan rekam medis yang dipilih disimpan dalam bentuk ciphertext, sedangkan akses pengguna dibatasi menggunakan RBAC dan aktivitas dicatat melalui audit log. Seluruh 38 skenario black box berhasil dengan tingkat keberhasilan 100%, validasi implementasi sesuai dengan vektor uji NIST FIPS PUB 197, dan avalanche effect rata-rata mencapai 50,70% pada perubahan satu bit plaintext serta 49,61% pada perubahan satu bit kunci. Pengujian kinerja menunjukkan waktu enkripsi rata-rata 0,5329 ms untuk satu record pasien dan dekripsi rata-rata 17,5758 ms untuk 50 record. Hasil tersebut menunjukkan bahwa mekanisme AES-128 yang diterapkan dapat digunakan untuk memperkuat kerahasiaan data pasien dengan overhead pemrosesan yang relatif kecil pada skenario pengujian. Pengembangan selanjutnya dapat meningkatkan perlindungan integritas melalui authenticated encryption dan memperkuat pengelolaan kunci.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Puskesmas Batahan yang telah memberikan kesempatan dan informasi yang diperlukan dalam pelaksanaan penelitian, serta kepada Universitas Muhammadiyah Sumatera Utara yang telah mendukung proses akademik penelitian ini. Artikel ini merupakan bagian dari penelitian skripsi penulis.

DAFTAR REFERENSI

Alaikha Annan. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. Jurnal Ilmiah Multidisiplin, 1(4), 247–254.

Bakri, S. N., Irwan, M., Nasution, P., Islam, U., & Sumatera, N. (2024). Penerapan Metodologi Rekayasa Perangkat Lunak untuk Efisiensi Pengembangan Sistem. Jurnal Sistem Informasi Dan Teknologi Informasi Komputer, 3(1), 53–66. https://doi.org/10.53624/jsitik.v3i1.542

Basri, M., & Sulaiman, K. (2024). Encryption of URL Address (Uniform Resource Locator) on PHP Web Base with MD5 Algorithm. Proceeding of International Conference on Science and Technology UISU, 7929, 12–16.

Candra Aditya Pinuyut, E., Utami, E., & Muhammad, A. H. (2024). Analisis Kinerja Algoritma Advanced Encryption Standard (AES) Termodifikasi dalam Enkripsi dan Dekripsi Data. TEKNIMEDIA: Teknologi Informasi dan Multimedia, 5(2), 132–137. https://doi.org/10.46764/teknimedia.v5i2.200

Evans, D. L., Bond, P. J., & Burr, K. H. (2022). Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. https://doi.org/10.6028/NIST.FIPS.197-upd1

Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. (2025). A panoramic survey of the advanced encryption standard: From architecture to security analysis, key management, real-world applications, and post-quantum challenges. International Journal of Information Security, 24(5). https://doi.org/10.1007/s10207-025-01116-x

Hakim, A. R., & Margolang, K. F. (2025). Analisis Keamanan Data Rekam Medis Digital Menggunakan Algoritma Kriptografi AES. Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, 8, 108–114. https://doi.org/10.53513/jsk.v8i2.11461

Hidayatuloh, F., Amila, Y., Naufal, M., Akbar, N., & Maesaroh, S. (2026). Komparasi Performa dan Keamanan Algoritma AES-128 dan Blowfish pada Enkripsi Berkas Teks. Jurnal Ilmiah Multidisiplin, 2(1), 1674–1677.

Indriyajati, F., Margarith, M., Damiana, S., Utomo, H., et al. (2024). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. Sanskara Manajemen dan Bisnis, 02(01), 59–66. https://doi.org/10.58812/smb.v2i01

Prabowo, W., & Nizirwan, A. (2025). Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC. Jurnal Ikraith-Informatika, 9(1), 178–186.

Puteri, D., Pramesti, A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan Kerahasiaan Data Medis Pasien dalam Implementasi Rekam Medis Elektronik. Jurnal Kesehatan Masyarakat, 8, 7691–7702. https://doi.org/10.31004/prepotif.v8i3.38445

Ramadhani, T. A., & Cobantoro, A. F. (2022). Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem. Jurnal Informatika Polinema, 10(4), 521–526. https://doi.org/10.33795/jip.v10i4.5619

Rospita Adelina Siregar, H. S. R. S. (2025). Aspek Hukum Perlindungan Data Pasien Dalam. Jurnal Hukum To-Ra: Hukum Untuk Mengatur dan Melindungi Masyarakat, 11(1), 106–116.

Saravanos, A. (2023). Simulating the Software Development Lifecycle: The Waterfall Model. Applied System Innovation. https://doi.org/10.3390/asi6060108

Sidqon, M., & Nafis, R. O. (2024). Rancang Bangun Sistem E-Arsip Berbasis Website Menggunakan Metode Enkripsi AES (Advanced Encryption Standard) Studi Kasus KPU Sidoarjo. Jurnal Rekayasa Sistem Informasi dan Teknologi, 2(1), 488–497.

Siregar, F. A., Informasi, T., & Utara, M. S. (2024). Implementation of the Arnold Catmap on a Combination of Symmetric and Asymmetric Cryptography. Jurnal dan Penelitian Teknik Informatika, 8(1), 174–182.

Tamin, Z., & Hendrik, B. (2025). Penerapan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan File Rekam Medis Pasien. Jurnal KomtekInfo, 12, 22–30. https://doi.org/10.35134/komtekinfo.v12i1.592

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Utomo, A., Sutanto, Y., Tiningrum, E., & Susilowati, E. M. (2020). Menggunkan Black Box Testing Boundary. Jurnal Bisnis Terapan, 04, 133–140. https://doi.org/10.24123/jbt.v4i2.2170

Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. International Journal of Advanced Computer Science and Applications, 12(2).