5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI SISTEM PENGAMANAN RECORD DATABASE MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEBSITE PADA PT. JEJARING TIGA ARTHA

Rizky Febdriasyah Lexsi[1*], Dewi Kusumaningsih[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1*]2011510969@student.budiluhur.ac.id, [2]dewi.kusumaningsih@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT. Jejaring Tiga Artha, didirikan pada tahun 2017 di Jakarta Selatan, bergerak di bidang healthcare management berbasis teknologi untuk rumah sakit. Sebagai penyedia layanan manajemen berbasis web, perusahaan ini menghadapi tantangan utama dalam melindungi data sensitif, terutama informasi medis pasien. Ancaman terhadap data dapat berasal dari berbagai sumber, termasuk akses tidak sah, peretasan, dan kebocoran data. Penelitian ini bertujuan untuk merancang sistem pengamanan data record database berbasis website menggunakan algoritma Advanced Encryption Standard (AES) 256, guna membantu PT. Jejaring Tiga Artha mengamankan data sensitif. Sistem ini dikembangkan menggunakan PHP dan MySQL, dengan metode AES-256 untuk enkripsi dan dekripsi data. AES-256 adalah algoritma enkripsi yang sangat aman dan diakui secara luas, menggunakan kunci 256-bit untuk mengenkripsi data, sehingga sangat sulit ditembus oleh pihak tidak berwenang. Proses enkripsi mengubah data asli menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai, memastikan bahwa hanya pihak berwenang yang dapat mengakses informasi tersebut. Hasil pengujian menunjukkan bahwa sistem berhasil mengenkripsi dan mendekripsi data sensitif pada record database dengan baik. Data yang dienkripsi hanya dapat didekripsi oleh pengguna yang memiliki kunci yang benar, memastikan perlindungan maksimal terhadap akses tidak sah. Sistem ini juga dirancang agar mudah digunakan dalam lingkungan web, sehingga mendukung operasional PT. Jejaring Tiga Artha secara efektif. Dengan implementasi AES-256, tingkat keamanan data dalam sistem berhasil ditingkatkan, memberikan perlindungan yang diperlukan untuk informasi medis yang sensitif, dan mendukung PT. Jejaring Tiga Artha dalam menyediakan layanan manajemen kesehatan yang aman dan terpercaya.

Kata Kunci: Keamanan data, *Advanced Encryption Standard* 256, Enkripsi, *Healthcare management*, Informasi medis

IMPLEMENTATION OF A DATABASE RECORD SECURITY SYSTEM USING THE AES-256 ALGORITHM BASED ON A WEBSITE AT PT. JEJARING TIGA ARTHA

Abstract*-PT. Jejaring Tiga Artha, established in 2017 in South Jakarta, operates in the field of technology-based healthcare management for hospitals. As a provider of web-based management services, the company faces significant challenges in protecting sensitive data, particularly patient medical information. Data threats can come from various sources, including unauthorized access, hacking, and data breaches. This research aims to design a website-based database record security system using the Advanced Encryption Standard (AES) 256 algorithm to help PT. Jejaring Tiga Artha secure sensitive data. The system is developed using PHP and MySQL, with the AES-256 method employed for data encryption and decryption. AES-256 is a highly secure and widely recognized encryption algorithm, utilizing a 256-bit key to encrypt data, making it extremely difficult for unauthorized parties to penetrate. The encryption process converts the original data into a format that cannot be read without the appropriate decryption key, ensuring that only authorized personnel can access the information. Testing results show that the system successfully encrypts and decrypts sensitive data in the database records. The encrypted data can only be decrypted by users who possess the correct key, ensuring maximum protection against unauthorized access. The system is also designed to be user-friendly in a web environment, thereby effectively supporting PT. Jejaring Tiga Artha's operations. By implementing AES-256, the system's data security level has been significantly enhanced, providing the necessary protection for sensitive medical information and supporting PT. Jejaring Tiga Artha in delivering secure and reliable healthcare management services.*

Keywords*: Data security, Advanced Encryption Standard 256, Encryption, Healthcare management, Medical information*

1. PENDAHULUAN

Dalam era teknologi yang berkembang dengan cepat, hampir semua aspek kehidupan modern mengandalkan teknologi informasi dan komunikasi, mulai dari aktivitas sehari-hari individu hingga operasi bisnis berskala besar dan layanan pemerintahan [1]. Bidang kesehatan, termasuk rumah sakit, tentunya berhubungan dengan privasi. Rekam medis adalah berkas yang mengandung catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, dan tindakan lain yang diberikan kepada pasien di fasilitas Kesehatan [2]. Keamanan dan kerahasiaan data menjadi tantangan utama, terutama dalam bidang kesehatan yang berhubungan dengan informasi sensitif seperti rekam medis. PT. Jejaring Tiga Artha, yang bergerak di bidang manajemen rumah sakit berbasis website, menghadapi risiko keamanan database yang signifikan.

Keberadaan sistem dengan keamanan yang masih standar, dapat menimbulkan risiko potensial serangan dari pihak-pihak yang tidak bertanggung jawab [3]. Cyber crime adalah tindak kejahatan yang dilakukan dengan memanfaatkan teknologi komputer sebagai alat kejahatan utama yang memanfaatakan perkembangan teknologi komputer khususnya internet [4]. Untuk melindungi data tersebut, diperlukan langkah-langkah keamanan yang efektif dan canggih, salah satunya adalah dengan menerapkan teknologi enkripsi yang kuat. Keamanan data tidak hanya penting untuk menjaga privasi pasien, tetapi juga untuk memenuhi standar hukum dan regulasi yang semakin ketat di bidang kesehatan. Seiring meningkatnya ancaman siber yang mengincar data sensitif, penggunaan metode kriptografi yang andal menjadi semakin penting. Crypto dan graphia adalah kata Yunani yang berarti "rahasia" dan "tulisan", masing-masing. Kriptografi, menurut definisinya, adalah seni dan ilmu untuk memastikan bahwa pesan atau data aman saat dikirim [5]. Kriptografi memiliki tujuan untuk memberi layanan keamanan, keempat aspek keamanan suatu system informasi menjadi tujuan utama dari kriptografi tersebut yaitu Kerahasiaan, Autentikasi, Integritas Data, dan Tidak ada penyangkalan [6].

Kunci kriptografi sendiri dibagi menjadi dua jenis yakni kunci simetris dan asimetris [7]. Pengirim dan penerima harus menyetujui kunci tertentu untuk menggunakan algoritma kriptografi simetris, yang sering dikenal sebagai algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci [8]. Algoritma asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi [9]. Dalam kriptografi terdiri dari enkripsi dan dekripsi [10]. Algoritma AES merupakan algoritma kunci simetrik yang dapat mengenkripsi dan dekripsi suatu informasi atau pesan [11]

Untuk itu, penerapan kriptografi untuk enkripsi menggunakan algoritma Advanced Encryption Standard (AES) 256 menjadi solusi penting. AES-256 dikenal dengan tingkat keamanannya yang tinggi, mampu melindungi data dari serangan kriptografi canggih. Karena diperlukan untuk mengamankan data pada perangkat penyimpanan, menjamin keamanan informasi yang dikirim, dan melindungi sistem informasi dari serangan siber, keamanan siber sangat penting untuk menjaga keamanan informasi [12].

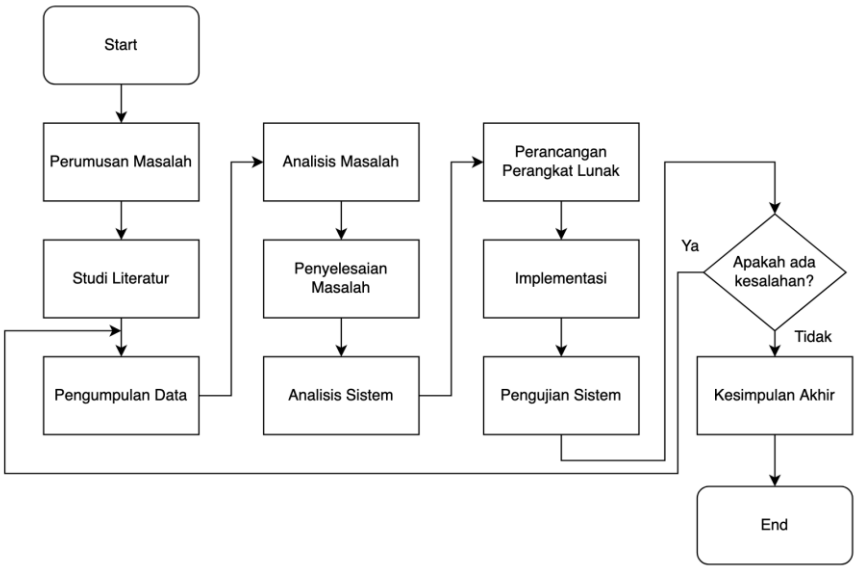
Pada Penelitian yang dilakukan sebelumnya oleh Wahyu Hidayat dan Budi Triandi (2023). “Aplikasi Sistem Keamanan Data Absensi Guru SMK Tarbiyah Islamiyah Berbasis Web Dengan Metode Algoritma AES”, menjelaskan bahwa algoritma AES dapat diterapkan pada sistem yang digunakan oleh SMK Tarbiyah Islamiyah untuk mengamankan isi data absensi guru. Hasil dari penelitian tersebut menunjukan bahwa algoritma AES berhasil melakukan enkripsi dan dekripsi, sehingga dapat mengamankan data - data absensi guru.

Penelitian lainnya, Ni Putu Ayu Astriyani, Danang Rimbawa, Budi Raharjo (2024). “Studi Perbandingan AES 128 dan 256 untuk Pengamanan Sistem Informasi Manajemen Rumah Sakit Dr. Mintoharjo”. Menjelaskan terkait peningkatan ancaman serangan siber di Indonesia adalah hal yang harus diantisipasi dengan serius. Berdasarkan pengujian yang telah dilakukan, penerapan keamanan data menggunakan algoritma AES-256 adalah solusi yang diperlukan dalam sistem manajemen Rumah Sakit Dr. Mintoharjo dikarenakan dari hasil pengujian, AES-256 lebih unggul dari segi performa dan pengamanan dibanding AES-128.

Dalam penelitian ini, terdapat perbedaan signifikan dibandingkan dengan penelitian sebelumnya. Fokus dalam penelitian ini adalah pada pengamanan data di PT. Jejaring Tiga Artha, yang mencakup data pengguna, pasien, dan rekam medis. Dan penelitian ini secara khusus mengimplementasikan algoritma AES-256 dalam konteks sistem database berbasis web pada keamanan data di bidang kesehatan. Hasil dari penelitian sebelumnya juga mendukung bahwa AES-256 adalah metode yang lebih unggul dibandingkan dengan varian lainnya, seperti AES-128, dalam hal performa dan keamanan data. Dengan adanya sistem ini, data sensitif dapat disimpan dan diakses dengan aman, memberikan perlindungan yang diperlukan dalam menjaga privasi dan keamanan informasi di sektor kesehatan.

2. METODE PENELITIAN

Metode penelitian ini berfungsi sebagai peta jalan untuk prosedur yang harus dilakukan untuk menjamin bahwa penelitian ini tetap sesuai dengan tujuan awalnya. Tahapan-tahapan yang digambarkan pada Gambar 1 berikut ini.



Gambar 1. Tahapan Penelitian

2.1 Data Penelitian

Data yang digunakan sebagai bahan penyusunan tugas akhir ini adalah Data User, Data Pasien, dan Data Resume Medis Pasien yang didapatkan dari PT. Jejaring Tiga Artha.

2.2 Penerapan Metode

Skema enkripsi Rijndael, yang dikembangkan oleh Vincent Rijmen dan John Daemen dari Belgia, berhasil memenangkan kompetisi untuk menggantikan DES. Pada tanggal 26 November 2001, National Institute of Standards and Technology (NIST), sebuah organisasi pemerintah Amerika Serikat, menyelenggarakan kompetisi ini.

Teknik kriptografi yang disebut Advanced Encryption Standard (AES) dirancang untuk melindungi data. Salah satu jenis cipher blok simetris yang dapat digunakan untuk mengenkripsi dan mendekode data adalah AES. Enkripsi mengubah data menjadi ciphertext—bentuk yang sulit dipahami—dan bentuk aslinya, yang dikenal sebagai plaintext, dikembalikan melalui dekripsi.

Algoritma AES mendukung tiga ukuran kunci: 128-bit, 192-bit, dan 256-bit. Algoritma ini dirancang untuk menggunakan blok input enkripsi minimal 128-bit [13]. Proses enkripsi dan dekripsi pada AES melibatkan beberapa putaran transformasi yang mencakup substitusi, pergantian, dan pencampuran data, yang dirancang untuk memberikan keamanan yang tinggi terhadap berbagai jenis serangan kriptanalisis. Penyandian AES menggunakan proses yang berulang yang disebut dengan ronde [14]

2.3 Rancangan Pengujian

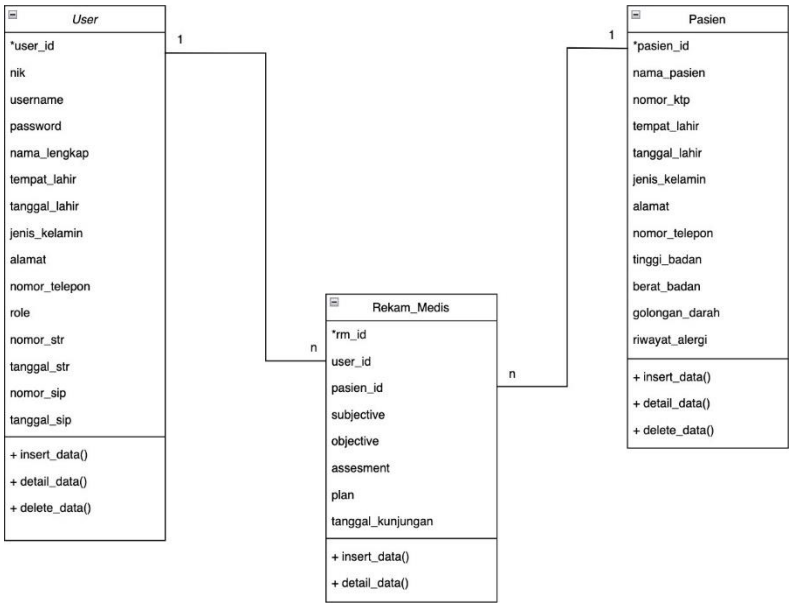
Rancangan Pengujian yang dilakukan pada penelitian ini adalah dengan menggunakan metode Black box. Black box testing adalah teknik untuk mengevaluasi aplikasi berdasarkan fiturnya, termasuk tampilan aplikasi, fungsi-fungsi yang ditawarkannya, dan sejauh mana alur fungsi tersebut sesuai dengan sistem yang diinginkan oleh pengembang [15]. Penguji hanya mengetahui input yang diberikan dan output yang diharapkan, serta berusaha untuk memastikan bahwa perangkat lunak berfungsi sesuai dengan spesifikasi yang telah ditentukan. Tujuan utama dari black box testing adalah untuk memvalidasi bahwa semua fitur perangkat lunak bekerja dengan benar dan untuk mendeteksikesalahan atau bug yang mungkin ada dalam sistem.

2.4 Rancangan Basis Data

Berikut ini adalah desain basis data yang digunakan.

a. Class Diagram

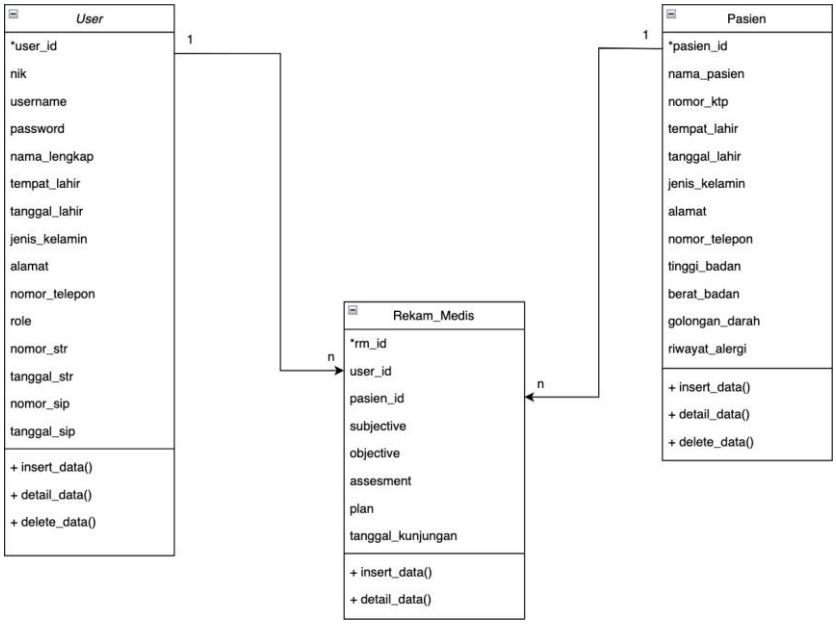
Berikut adalah gambar *Class Diagram* yang digunakan.



Gambar 2. *Class Diagram*

b. *Logical Record Structure* (LRS)

Berikut adalah gambar LRS yang digunakan



Gambar 3. LRS *(Logical Record Structure)*

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Perangkat Keras dan Perangkat Lunak

Untuk memastikan aplikasi kriptografi yang menggunakan algoritma AES 256 dapat berfungsi dengan optimaldan sesuai dengan harapan, diperlukan spesifikasi perangkat keras dan perangkat lunak yang memadai. Berikut adalah spesifikasi yang diperlukan untuk mendukung implementasi aplikasi ini :

a. Perangkat Keras

Berikut penggunaan Perangkat Keras yang digunakan :

1) Processor M2

2) Memory 8 GB
3) Hard disk 256 GB

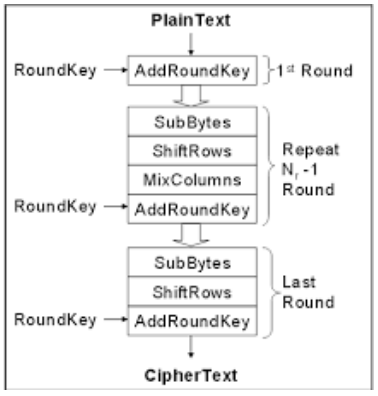
b. Perangkat Lunak

Berikut penggunaan Perangkat Lunak yang digunakan :

1) Mac OS Sonoma
2) Mamp
3) c. PHP 7.4.33
4) MySQL
5) Visual Studio Code
6) Browser (Google Chrome/Mozilla Firefox)

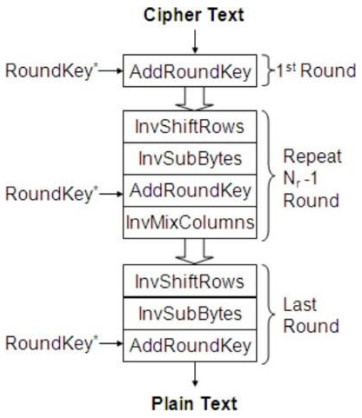
3.2 Implementasi Metode

SubBytes, ShiftRows, MixColumns, dan AddRoundKey adalah beberapa tahap kunci dalam proses enkripsi pada implementasi Advanced Encryption Standard (AES) untuk enkripsi dan dekripsi data. Setelah input diubah menjadi state, AddRoundKey digunakan untuk melakukan transformasi byte pada state tersebut pada tahap enkripsi pertama. Setelah itu, state ini secara berulang melalui tahap AddRoundKey, MixColumns, SubBytes, dan ShiftRows selama N putaran. Dalam algoritma AES, prosedur ini disebut sebagai fungsi round. Perlu diingat, pada putaran terakhir terdapat perbedaan dengan putaran sebelumnya, di mana state tidak mengalami perubahan MixColumns.



Gambar 4. Enkripsi AES-256

Dalam proses dekripsi menggunakan Advanced Encryption Standard (AES), langkah-langkah yang dilakukan adalah kebalikan dari proses enkripsi. Tahapan dekripsi meliputi InvShiftRows, InvSubBytes, InvAddRoundKey,dan InvMixColumns.



Gambar 5. Dekripsi AES-256

3.3 Hasil Pengujian

Teknik black box, yang fokus pada penilaian fungsi program berdasarkan input dan outputnya tanpa memperhatikan atau memahami struktur internal kode sumber, digunakan untuk menguji perangkat lunak ini. Fokus utama dari pengujian ini adalah bagaimana program menangani data yang diberikan dan apakah hasil yang diperoleh sesuai dengan hasil yang diharapkan. Dengan kata lain, perangkat lunak diuji sebagai "kotak hitam," dengan hanya reaksi eksternalnya terhadap berbagai kondisi yang diperiksa. Pengujian fungsional ini dijelaskan lebih lanjut melalui Tabel 1, yang menggunakan metode black box untuk memastikan bahwa setiap fungsi program beroperasi sesuaidengan spesifikasi yang telah ditentukan.

Tabel 1 Tabel Pengujian Fungsi

No.	Skenario Pengujian	Hasil Pengujian
1	Fungsi tambah User / Pasien	Fungsi tambah data User / Pasien berjalan dengan baik untuk mengenkripsi teks ke dalam database
2	Fungsi Edit User / Pasien	Fungsi edit data User / Pasien berjalan dengan baik untuk mengenkripsi teks ke dalam database
3	Fungsi Detail User / Pasien	ngsi detail User / Pasienberjalan dengan baik untuk mendekripsi teks dari dalam database
4	Fungsi Hapus User / Pasien	Fungsi hapus User / Pasien berjalan dengan baik untuk menghapus data dari database
5	Fungsi isi data rekam medis pasien	Fungsi isi data rekam medis pasien berjalan dengan baik untuk mengenkripsi teks ke dalam database

Dalam pengujian perhitungan akurasi yang dilakukan saat proses enkripsi dan dekripsi, dengan menggunakan data penelitian yaitu data user, pasien, dan rekam medis. Ditemukan bahwa ke 15 data tersebut kembali sama persis dengan data aslinya sehingga keakuratan perhitungan mencapai 100%.

Tabel 2 Tabel Pengujian Enkripsi dan Dekripsi

No.	Input Nama	Hasil Enkripsi	Hasil Dekripsi
1	DR. ADITYA AGUSTIAN. MM. MARS	RyULBvteY37bVxC/ZISp/2j9w2TZdMr1dIlrJWY5y6A=	DR.ADITYA AGUSTIAN. MM.MARS
2	dr. SALAS PUTRI RAHAYU	PXQUHDndAl1VI+QWlGn1se7fU34sH+IL0171f7gW7K8=	dr. SALAS PUTRIRAHAYU
3	ADE BUDIAWAN	1I25WJTLhruIjT67iqqeww==	ADE BUDIAWAN
4	AYUDYA FINORYITA	SqKD9Y+tbweEp/AqpRLLZg==	AYUDYA FINORYITA
5	Drg. AMI KRISMIATI	VQR+fYkqO+isn3KSKH8pRvOo2hT79e5dNIQlBD1uR4o=	Drg. AMI KRISMIATI
6	Karnadi	FNq7jTWvSHxTcFV1KD5fFw==	Karnadi
7	Restu Wijanarko	a8SDVgavrbIMeLsZXEKSyQ==	Restu Wijanarko
8	Khaeruddin	yP5wyNsSfSaThjnPlZ3U0A==	Khaeruddin
9	Diana Hamidah	NgxcseE2xJU563TvjUQiOw==	Diana Hamidah
10	Nurul Damiyati	C4J2z34h2zNBb9QATvLxuw==	Nurul Damiyati

11	Husnaini	P4Vioj4ItWUqH22w0jxnkA==	Husnaini
12	Abdul Fatah	qZW1Pr3qjl2jXSpGaDQvPQ==	Abdul Fatah
13	Hidayat	lKEkHnITZPwhi7uR3U1uMQ==	Hidayat
14	Haris Ismail	7/srUhEl28B6++Wir8B7aQ==	Haris Ismail
15	Jamharudin	znNdrbCuMCKDVU8duDLz5A==	Jamharudin

4. KESIMPULAN

Setelah mempelajari permasalahan serta dari hasil pengujian yang telah dilakukan dapat disimpulkan bahwa:

a. Perancangan dan implementasi keamanan sistem informasi dengan menggunakan metode kriptografiAdvanced Encryption Standard (AES) 256 dapat secara efektif mengamankan record database di PT.Jejaring Tiga Artha. Dengan mengimplementasikan AES 256, data sensitif yang tersimpan dalam database menjadi lebih aman dari akses tidak sah dan potensi serangan, sehingga meningkatkan keandalan dan integritas sistem informasi perusahaan.
b. Dari hasil pengujian yang dilakukan terhadap data yang diambil dari data penelitian, diperoleh bahwa hasil enkripsi dan dekripsi 15 data yang dihasilkan sudah cukup akurat dengan text yang sebelum dienkripsi dan setelah didekripsi tidak ada perbedaan atau kehilangan konsistensi.
c. Berdasarkan pengujian yang dilakukan dengan mengikuti alur pengujian pada tabel pengujian fungsi. Sistem yang telah dibuat dapat berfungsi untuk melakukan enkripsi dan dekripsi data pada record database tanpa kendala.
d. Serta penelitian ini perlu dilanjutkan kembali agar dapat diimplementasikan pada tabel database yang lainnya serta dapat dikembangkan menjadi sistem enkripsi versi *mobile*.

DAFTAR PUSTAKA

[1] D. Ramalinda and A. R. Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," *Journal of International Multidisciplinary Research*, vol. 2, no. 6, pp. 665–671, 2024
[2] S. Sofia, E. Tri Ardianto, and N. Muna, "Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan," *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, vol. 1, no. 2, pp. 2829–4777, 2022.
[3] F. Shofyan and R. Tahara Shita, "Implementasi Web Service Restful API dengan Autentikasi Personal Access Tokens dan Algoritma AES 256," *Jurnal TICOM: Technology of Information and Communication*, vol. 12, no. 3, 2024.
[4] Y. Putra, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting," *Jurnal Sistim Informasi dan Teknologi*, vol. 3, no. 2, pp. 56–63, 2021.
[5] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," JIKOMSI: *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 4, no. 2, p. 75-85, 2021.
[6] U. Wahyuningsih *et al.*, "Analisis Proses Enkripsi Algoritma Kriptografi Modern Advanced Encryption Standard (AES)," *Jurnal Multidisiplin*, vol. 1, no. 2, pp. 380–387, 2023.
[7] M. B. Aryanto, M. Tahir, S. I. Devita, Z. N. Mustofa, Q. Ainiyah, and S. Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *JUISIK*, vol. 3, no. 1, 2023, [Online]. Available: http://journal.sinov.id/index.php/juisik/indexHalamanUTAMAJurnal:https://journal.sinov.id/index.php
[8] N. Amalya, S. M. S. Silalahi, D. F. Nasution, M. Sari, and I. Gunawaan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *Jurnal Media Informatika* , vol. 4, no. 2, pp. 90–93, 2023.
[9] R. Febrianto and S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (Aes-256) Untuk Mengamankan Database Penilaian Karyawan Pada Kjpp Ndr," *BIT(Fakultas Teknologi Informasi Universitas Budi Luhur)*, vol. 20, no. 1, pp. 44–49, 2023.
[10] K. Gusnanda, N. Ulfadillah, and T. Sumarni, "Struktur Basis Data Di Era Digital (Implementasi Pengamanan Basis Data Di Era Global)," *Jurnal Multidisiplin Saintek*, vol. 3, no. 7, pp. 100–111, 2024.
[11] Mhd. Fachrul Fachrozi and H. Fahmi, "Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint," *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]* , vol. 3, no. 3, pp. 1–8, 2021.
[12] D. A. Sudarmadi and A. J. S. Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *Article 7 Ketahanan Nasional*, vol. 2, no. 2, 2019.
[13] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digital Transformation Technology (Digitech)* | *e*, vol. 3, no. 1, 2023.

[14] Y. Luruk Ulu, Y. R. Kaesmetan, and I. Artikel Abstrak, "Perbandingan Metodedata Encryption Standard (DES) Dan Advanced Encryption Standard (AES) Pada Keamanan Jaringan Komputer Di SMK Willibrodus Betun," *KETIK: Jurnal Informatika*, vol. 1, no. 5, pp. 26-32, 2024.

[15] U. Uminingsih, M. N. Ichsanudin, M. Yusuf, , and Suraya, "Pengujian Fungsional Perangkat Lunak Sistem Informasi Perpustakaan Dengan Metode Black Box Testing Bagi Pemula Info Artikel Abstrak," STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer, vol. 1, no. 2, pp. 1–8, 2022.