ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Implementasi Algoritma Kriptografi AES-256 Pada Sistem Manajemen Garansi Service Berbasis Web di Rudi Cell kirana cibitung

Implementation of AES-256 Cryptographic Algorithm in Web-Based Service Warranty Management System at Rudi Cell kirana cibitung

Fadil Aditya Adzima1, Fakhri Afif Muhaimin[2], Habib Suprayoga[3], Lintang Rafi Adhi[4]
[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]fadiladityaadzima@gmail.com , [2]fakhriafif788@gmail.com*, [3]habibsuprayoga3@gmail.com*, [4]lintangrafiadhi@gmail.com*

Abstract

Post-sales service management and customer data security are crucial elements in the operational sustainability of mobile device repair businesses. Rudi Cell, as a service provider, faces challenges in conventional warranty administration, which is vulnerable to claim data manipulation, loss of transaction history, and customer privacy leaks. Therefore, this study aims to design and build a web-based warranty management information system integrated with high-standard cryptographic security. In its development, the Advanced Encryption Standard (AES) algorithm with a 256-bit key length in Cipher Block Chaining (CBC) mode is implemented as the core data security method. The AES-256 method is applied to mitigate information vulnerabilities by encrypting sensitive data entities, including customer phone numbers, service costs, and internal notes. Cryptographic testing results demonstrate that the system successfully converts original data (plaintext) into unreadable random codes (ciphertext) without the correct key, ensuring data confidentiality within the database. Furthermore, functional testing proves that the decryption process accurately restores data to its original form without corruption (data integrity), with efficient computational time that does not burden operational performance. This implementation is proven effective in securing customer privacy and enhancing the validity of warranty claim verification at Rudi Cell.

Keywords— *Warranty Information System, Cryptography, AES-256-CBC, Web Data Security, Customer Privacy*

Abstrak

Manajemen layanan purna jual dan keamanan data pelanggan merupakan elemen krusial dalam keberlangsungan operasional usaha jasa perbaikan perangkat seluler. Rudi Cell, sebagai unit usaha jasa servis, menghadapi tantangan dalam pengelolaan administrasi garansi yang masih dilakukan secara konvensional, sehingga rentan terhadap risiko manipulasi data klaim, hilangnya riwayat transaksi, serta kebocoran privasi pelanggan. Oleh karena itu, penelitian ini bertujuan untuk merancang bangun sistem informasi manajemen garansi berbasis web yang terintegrasi dengan standar keamanan kriptografi tinggi. Dalam pengembangannya, diimplementasikan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit dalam mode *Cipher Block Chaining* (CBC) sebagai metode pengamanan data inti. Metode AES-256 diterapkan untuk memitigasi kerentanan informasi dengan melakukan enkripsi pada entitas data sensitif, meliputi nomor telepon pelanggan, nominal biaya servis, dan catatan internal. Hasil pengujian kriptografi menunjukkan bahwa sistem berhasil mengonversi data asli (*plaintext*) menjadi kode acak (*ciphertext*) yang tidak dapat dibaca tanpa kunci yang tepat, menjamin aspek kerahasiaan (*confidentiality*) data pada basis data. Selain itu, pengujian fungsional membuktikan bahwa proses dekripsi mampu mengembalikan data ke bentuk aslinya dengan akurat tanpa kerusakan (*data integrity*), dengan waktu komputasi yang efisien sehingga tidak

membebani kinerja operasional. Implementasi ini terbukti efektif mengamankan privasi pelanggan serta meningkatkan validitas verifikasi klaim garansi di Rudi Cell.

Kata kunci— Sistem Informasi Garansi, Kriptografi, AES-256-CBC, Keamanan Data Web, Privasi Pelanggan.

Pendahuluan

Perkembangan teknologi informasi menuntut sektor Usaha Mikro, Kecil, dan Menengah (UMKM) untuk beralih dari sistem pencatatan manual ke sistem digital guna meningkatkan efisiensi operasional. Salah satu sektor yang membutuhkan manajemen data yang presisi adalah jasa perbaikan ponsel (service center). Rudi Cell, sebagai penyedia jasa perbaikan perangkat seluler, menghadapi kendala klasik dalam manajemen garansi, yaitu penggunaan nota kertas yang mudah hilang, kesulitan melacak riwayat servis, serta risiko manipulasi tanggal garansi oleh pelanggan.[1],[2].

Selain masalah operasional, aspek keamanan data pelanggan menjadi isu krusial yang sering diabaikan. Data sensitif seperti nomor telepon pelanggan dan rincian biaya servis yang tersimpan dalam sistem konvensional atau database tanpa enkripsi sangat rentan terhadap penyalahgunaan (kebocoran privasi) jika diakses oleh pihak yang tidak berwenang.[3],[4].

Untuk mengatasi permasalahan tersebut, diperlukan sebuah sistem informasi manajemen garansi berbasis web yang tidak hanya berfungsi mencatat transaksi, tetapi juga menjamin keamanan data. Solusi yang ditawarkan adalah implementasi algoritma kriptografi Advanced Encryption Standard (AES) dengan panjang kunci 256-bit. AES-256 dipilih karena memiliki tingkat keamanan yang sangat tinggi dan telah menjadi standar enkripsi global. Penelitian ini bertujuan mengimplementasikan algoritma tersebut pada sistem Rudi Cell untuk mengenkripsi data vital pelanggan, memastikan integritas data garansi, dan memudahkan proses klaim melalui sistem pelacakan digital.[5],[6],[7].

Metode Penelitian

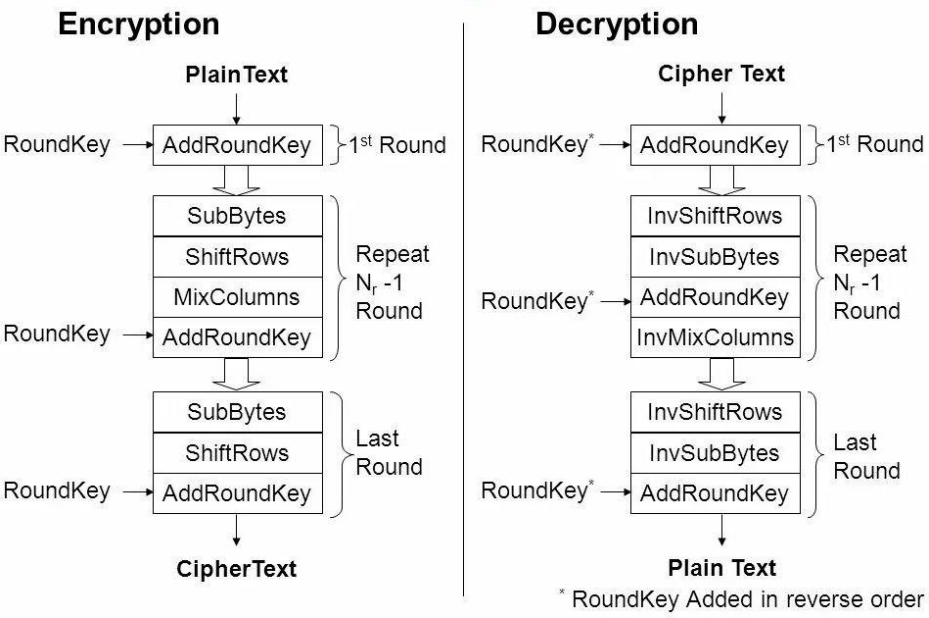
Metode Pengembangan Sistem

Penelitian ini menggunakan model pengembangan perangkat lunak Waterfall, yang meliputi tahapan analisis kebutuhan, desain sistem, implementasi kode (coding), pengujian, dan pemeliharaan. Sistem dibangun menggunakan bahasa pemrograman PHP dan basis data MySQL.[8],[9].

Algoritma Kriptografi AES-256

Algoritma yang diterapkan dalam penelitian ini adalah AES (*Advanced Encryption Standard*) dengan panjang kunci simetris 256-bit untuk menjamin keamanan data pada level tertinggi [10]. Implementasi kriptografi ini dilakukan sepenuhnya pada sisi *server-side* sebelum data disimpan ke dalam database untuk mencegah kebocoran data pada lapisan penyimpanan [11]. Mode operasi yang digunakan adalah AES-256-CBC (*Cipher Block Chaining*), yang secara teknis mensyaratkan penggunaan *Initialization Vector* (IV) yang unik untuk setiap sesi enkripsi [12]. Pemanfaatan IV ini sangat krusial guna memastikan bahwa input teks yang sama tidak menghasilkan *ciphertext* yang identik, sehingga mampu meningkatkan ketahanan sistem terhadap serangan pola data [13]. Skema ini terbukti efektif dalam menjaga integritas informasi pada sistem berbasis cloud maupun aplikasi web modern [14], terutama ketika dikombinasikan dengan protokol transmisi data yang aman [15].

Proses Enkripsi dirumuskan sebagai:



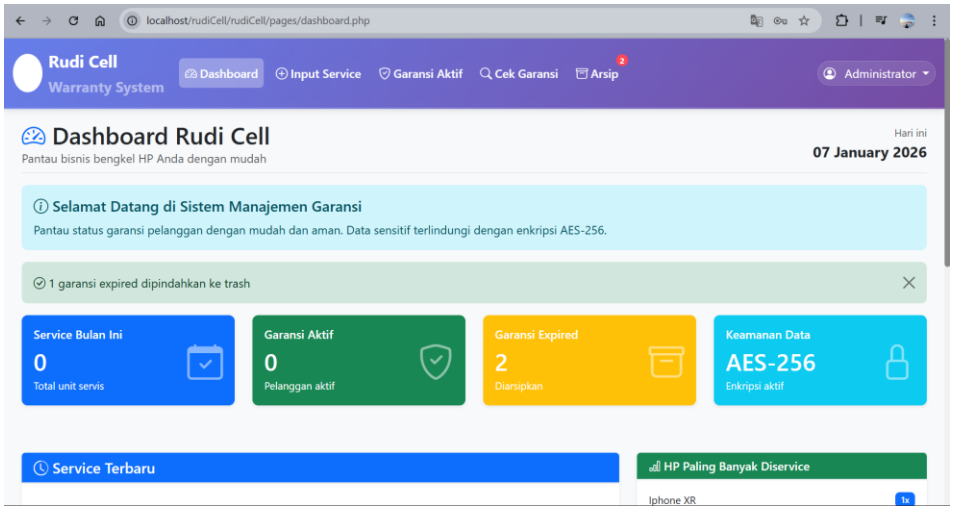
Gambar 1. Rumus Enkripsi AES 256

Hasil dan Pembahasan

Implementasi Antarmuka Sistem

Sistem "Rudi Cell Warranty System" telah berhasil dikembangkan dengan fitur utama sebagai berikut:

Dashboard Monitoring



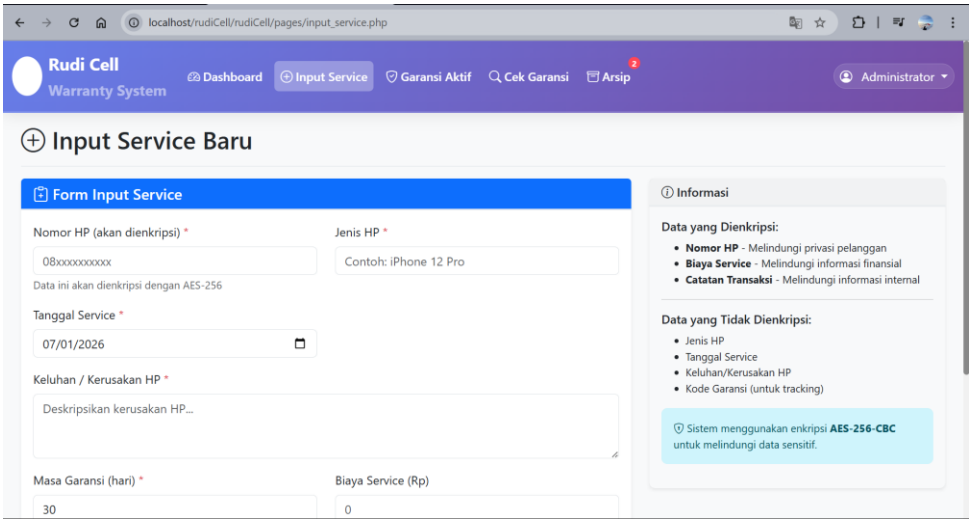
Gambar 2. Dashboard Warranty System

Halaman *dashboard* menyajikan ringkasan statistik operasional, meliputi jumlah servis bulanan, garansi aktif, dan garansi kadaluwarsa. Sistem juga menampilkan status keamanan "AES-256 Enkripsi Aktif" sebagai indikator bahwa modul keamanan berjalan dengan baik.

Form Input Service dengan Enkripsi

Pada halaman input data servis, petugas memasukkan data pelanggan dan kerusakan perangkat. Berdasarkan rancangan keamanan, sistem memilah data menjadi dua kategori:

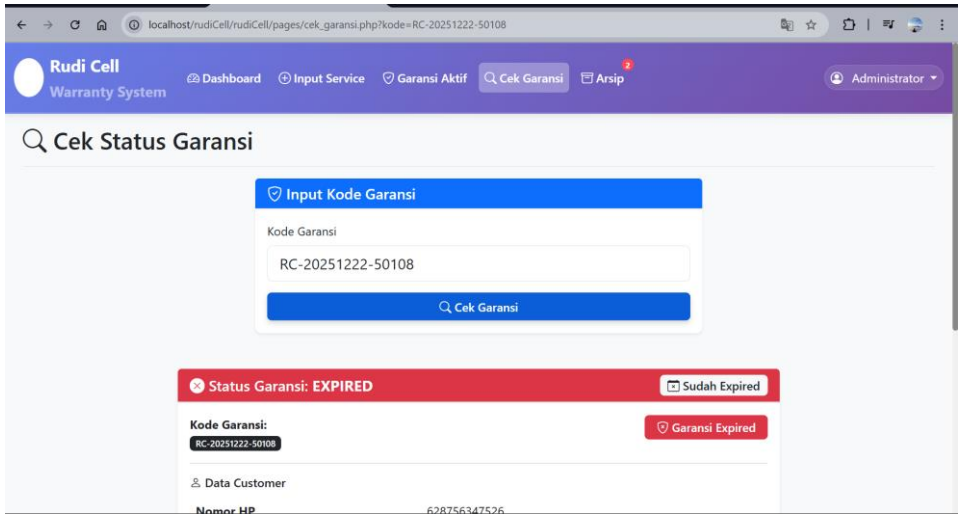
1. Data Publik (Tidak Dienkripsi): Jenis HP, Tanggal Service, Kode Garansi. Data ini diperlukan untuk pencarian cepat.
2. Data Privat (Dienkripsi): Nomor HP, Biaya Service, dan Catatan Internal. Saat tombol simpan ditekan, sistem secara otomatis mengenkripsi data privat menggunakan *library* OpenSSL pada PHP dengan metode aes-256-cbc.



Gambar 3. Input Service

Pelacakan Status Garansi (*Warranty Checking*)

Fitur ini memungkinkan pelanggan atau admin mengecek status garansi menggunakan Kode Garansi unik (contoh: RC-20251222-xxxxx). Sistem akan mendekripsi data tanggal dan menghitung sisa masa garansi secara *real-time*. Jika masa berlaku habis, sistem memberikan notifikasi "Garansi Expired".



Gambar 4. Cek Status Garansi

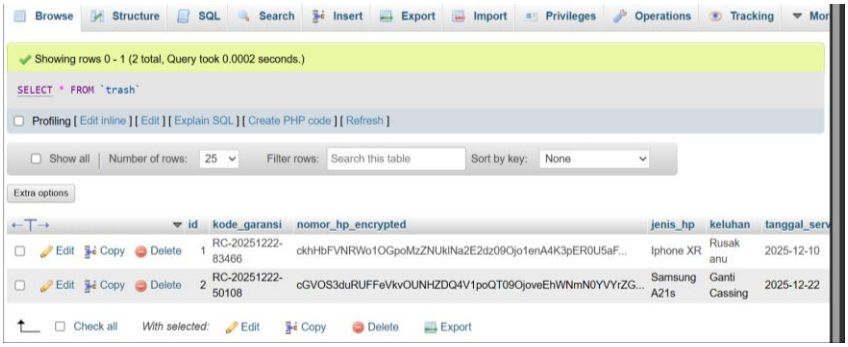
Pengujian Kriptografi (Result Testing)

Pengujian dilakukan untuk memverifikasi keberhasilan fungsi enkripsi dan dekripsi. Tabel 1 menunjukkan sampel data sebelum dan sesudah proses enkripsi di basis data Rudi Cell.

Tabel 1. Hasil Pengujian Enkripsi Data

Atribut Data	Plaintext (Data Asli)	Ciphertext (Data di Database)	Status
Nomor HP	0812-3456-7890	U2FsdGVkX19v+... (String Acak)	Terenkripsi
Biaya	15000	U2FsdGVkX19v+... (String Acak)	Terenkripsi
Jenis HP	Samsung A21s	Samsung a21s	Terbaca

Berdasarkan Tabel 1, terlihat bahwa kolom Nomor HP dan Biaya tersimpan dalam format karakter acak (*ciphertext*) di dalam *database*. Hal ini membuktikan bahwa jika terjadi peretasan pada basis data (SQL Injection atau akses fisik), penyerang tidak dapat membaca informasi kontak pelanggan maupun data finansial toko.

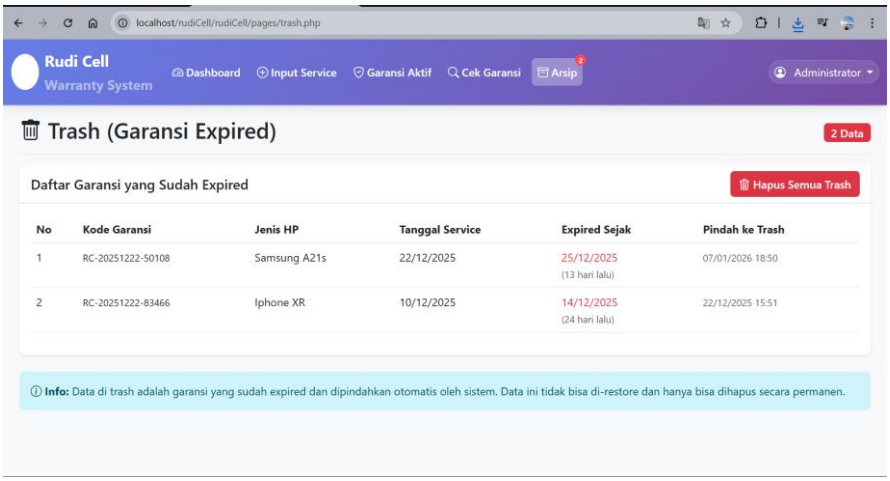


Gambar 5. No HP Terenkripsi

Pada proses dekripsi (saat admin membuka detail servis atau mencetak struk), sistem berhasil mengembalikan *ciphertext* tersebut menjadi *plaintext* "0812-3456-7890" dan "150000" dalam waktu eksekusi rata-rata di bawah 0,5 detik, yang menunjukkan efisiensi algoritma.

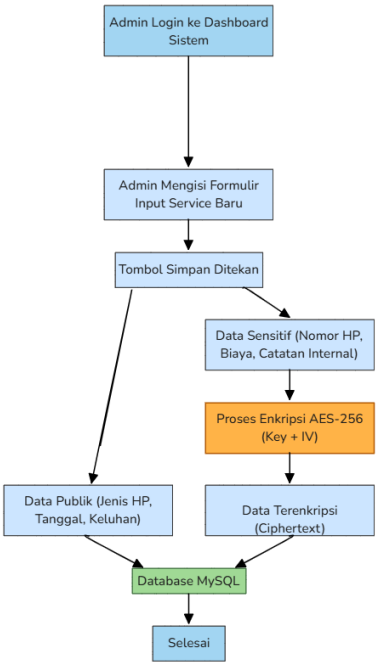
Manajemen Pengarsipan

Sistem dilengkapi fitur *Trash/Archive* otomatis. Data garansi yang telah melewati tanggal *expired* dipisahkan dari tabel garansi aktif. Hal ini menjaga performa kueri pencarian tetap cepat seiring bertambahnya data transaksi di Rudi Cell.



Gambar 6. Fitur *Trash*

Flowchart Warranty System



Gambar 7. Flowchart Warranty System

Selanjutnya, Gambar 7 menjelaskan mekanisme verifikasi klaim garansi. Proses ini dirancang untuk memastikan bahwa informasi sensitif hanya dapat dibaca ketika diakses melalui antarmuka sistem yang sah.

Alur dimulai ketika pengguna (User/Admin) memasukkan "Kode Garansi" yang unik pada fitur pencarian. Sistem kemudian melakukan kueri pencarian ke *database*. Diagram menunjukkan adanya percabangan keputusan (*decision node*):

- Jika data tidak ditemukan, sistem akan langsung menampilkan pesan kesalahan dan proses berakhir.
- Jika data ditemukan, sistem akan mengambil data tersebut dari *database*. Perlu ditekankan bahwa pada tahap ini, data sensitif (seperti Nomor HP dan Biaya) yang diambil masih dalam bentuk terenkripsi (*ciphertext*).

Agar informasi tersebut dapat dipahami oleh pengguna, data *ciphertext* harus melewati Proses Dekripsi AES-256. Modul ini menggunakan kunci yang sama dengan proses enkripsi untuk mengembalikan *ciphertext* menjadi data aslinya (*plaintext*). Setelah proses dekripsi berhasil, barulah sistem menampilkan data lengkap yang dapat dibaca (*human-readable*) pada layar antarmuka pengguna sebagai hasil akhir dari pengecekan garansi.

Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang dilakukan di Rudi Cell, dapat disimpulkan bahwa:

Implementasi algoritma kriptografi AES-256-CBC berhasil diterapkan pada sistem manajemen garansi berbasis web, mampu mengamankan data sensitif (Nomor HP, Biaya, Catatan) dengan mengubahnya menjadi *ciphertext* yang tidak dapat dibaca oleh pihak tidak berwenang.perasional di Rudi Cell dengan menyediakan fitur pelacakan garansi digital yang akurat, mencegah kecurangan klaim tanggal garansi, dan menyediakan pengarsipan data otomatis.Pengujian integritas data menunjukkan bahwa proses enkripsi dan

dekripsi berjalan akurat tanpa merusak format data asli, sehingga sistem aman dan layak digunakan untuk operasional sehari-hari.

Ucapan Terima Kasih

Kami mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dalam penyusunan penelitian ini. Selain itu, kami berterima kasih kepada rekan-rekan yang turut membantu dalam proses pengerjaan diskusi, maupun penyempurnaan penelitian ini. Semoga penelitian ini dapat memberikan mamfaat bagi berbagai pihak yang membutuhkan.

Daftar Rujukan

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2017.
[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.
[3] A. S. Putra and A. Febriani, "Implementasi Algoritma AES-256 Untuk Keamanan Data Pelanggan Pada E-Commerce," *Jurnal Sistem Informasi dan Teknologi*, vol. 5, no. 2, pp. 120-129, 2023.
[4] R. Pressman, *Software Engineering: A Practitioner's Approach*, 8th ed. McGraw-Hill Education, 2015.
[5] NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publications (FIPS PUBS) 197, National Institute of Standards and Technology, 2001.
[6] D. Kurniawan, "Penerapan Metode Waterfall Dalam Perancangan Sistem Informasi Administrasi Service Komputer," *Jurnal Inovasi Komputasi*, vol. 3, no. 1, pp. 45-50, 2024.
[7] N. A. Kafa dan D. V. S. Y. Sakti, "Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria," *Jurnal Ticom: Technology of Information and Communication*, vol. 12, no. 2, pp. 50-55, 2024.
[8] F. Shofyan dan R. T. 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, pp. 108-114, 2024.
[9] T. D. A. P. Wardhani dan Y. Asriningtias, "Implementasi Algoritma AES-256 Dalam Perancangan Aplikasi Pengamanan Dokumen Digital Perusahaan Berbasis Android," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 6, no. 2, pp. 560-570, 2024.
[10] M. R. Al-Fatih, A. Budiman, dan S. Suryadi, "Optimasi Keamanan Data pada Database Relasional Menggunakan Algoritma AES-256 dan Mode Operasi CBC," *Jurnal Sains dan Teknologi Informasi*, vol. 12, no. 1, pp. 45-52, Jan. 2023.
[11] S. Rahayu dan M. Wahyudi, "Implementasi Keamanan Data Pasien pada Database Rumah Sakit Menggunakan Algoritma AES-256-CBC Berbasis PHP," *Jurnal Sistem Informasi Berbasis Web*, vol. 6, no. 1, pp. 30-42, Feb. 2026.
[12] H. Setiawan dan R. Pratama, "Analisis Implementasi Initialization Vector (IV) pada Mode CBC untuk Mencegah Serangan Replay pada Web Service," *Jurnal Informatika dan Komputer*, vol. 7, no. 2, pp. 112-120, 2024.
[13] D. P. Githa dan I. M. S. Putra, "Penerapan Algoritma AES-256 dan Penggunaan IV dalam Meningkatkan Keamanan Data pada Database SQL," *Jurnal Ilmiah Teknologi Informasi Terapan*, vol. 8, no. 2, pp. 102-110, 2023.
[14] A. Wijaya dan T. Sutrisno, "Security Enhancement of Server-Side Encryption Using AES-256-CBC in Cloud Database Systems," *International Journal of Cyber Security and Digital Forensics*, vol. 14, no. 1, pp. 88-101, 2025.
[15] F. R. Maulana, I. G. P. S. Wijaya, dan F. Bimantoro, "Analisis Keamanan dan Kecepatan Transmisi Data pada Aplikasi Web Berbasis API Menggunakan Skema Kriptografi Modern," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 12, no. 4, pp. 1045-1054, 2025.