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 Keamanan Data Pembeli Pada *Website* UMKM Pawnomis Official di Bekasi Menggunakan AES-256 CBC dan Laravel

Implementation of Buyer Data Security on the Pawnomis Official UMKM Website in Bekasi Using AES-256 CBC and Laravel

Sartika Agustin, Pranaja Widyadhana Wardana[2], Dzikry Eza Yusuf[3], Aldi Hermansyah[4]
[1]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[2]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]sartikaagustin3@gmail.com, [2]pranawardhana@gmail.com*, [3]ezayusuf2002@gmail.com*, [4]alher6555@gmail.com*

Abstract

Customer data security in UMKM transactions is often overlooked, leading to the risk of personal information stored in databases being leaked. This study raises the issue of data vulnerability on the Pawnomis Official website, which is still transparent. The purpose of this study is to implement a robust data protection system using AES-256 algorithm technology with Cipher Block Chaining (CBC) mode. The solution involves automatic encryption of sensitive data (name, phone number, and address) before it is stored in the database, as well as automatic decryption when the data is accessed by authorized parties through the dashboard. The test results show that the system successfully secures customer identities, as evidenced by an average Avalanche Effect (AE) test value of 50.23%. This figure meets the ideal cryptography standard, which indicates that small changes in plaintext result in drastic changes in ciphertext. Thus, the Pawnomis Official application is able to effectively guarantee the confidentiality of buyer data without reducing the operational efficiency of the system.

Keywords: *AES-256, CBC, Avalanche Effect, Cryptography, UMKM*

Abstrak

Keamanan data pelanggan pada transaksi UMKM sering kali terabaikan, sehingga menimbulkan risiko kebocoran informasi pribadi yang disimpan dalam basis data. Penelitian ini mengangkat permasalahan mengenai kerentanan data pada *website* Pawnomis Official yang masih bersifat transparan. Tujuan penelitian ini adalah mengimplementasikan sistem perlindungan data yang tangguh menggunakan teknologi algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC). Solusi yang diterapkan melibatkan proses enkripsi otomatis pada data sensitif (nama, nomor telepon, dan alamat) sebelum disimpan ke basis data, serta dekripsi otomatis saat data diakses oleh pihak berwenang melalui *dashboard*. Hasil pengujian menunjukkan bahwa sistem berhasil mengamankan identitas pelanggan, dibuktikan dengan nilai rata-rata pengujian *Avalanche Effect* (AE) sebesar 50,23%. Angka ini memenuhi standar ideal kriptografi, yang menunjukkan bahwa perubahan kecil pada *plaintext* menghasilkan perubahan drastis pada *ciphertext*. Dengan demikian, aplikasi Pawnomis Official mampu menjamin kerahasiaan data pembeli secara efektif tanpa mengurangi efisiensi operasional sistem.

Kata kunci: AES-256, CBC, Avalanche Effect, Kriptografi, UMKM

Pendahuluan

Perkembangan teknologi informasi yang pesat telah mendorong transformasi model bisnis konvensional menuju sistem *e-commerce* berbasis *website*. *Website* Pawnomis Official sebagai *platform* penjualan menghadapi tantangan besar dalam menjaga kerahasiaan data pembeli, seperti informasi pribadi dan detail transaksi. Sistem informasi penjualan yang tidak menggunakan cara mengenkripsi data membuat informasi sensitif seperti kata sandi dan data profil dikirim serta disimpan dalam bentuk teks biasa [1].

Hal ini secara signifikan meningkatkan risiko akses tidak sah dan modifikasi data oleh pihak luar. Fenomena penyadapan dan pencurian data pribadi menjadi ancaman nyata yang bisa merusak reputasi bisnis serta mengganggu privasi konsumen [2]. Masalah utama yang muncul adalah bagaimana membuat sistem perlindungan data yang kuat di dalam *database* sehingga jika terjadi kebocoran, data tersebut tetap tidak bisa dibaca tanpa kunci yang benar [3]. Berdasarkan situasi tersebut, masalah yang perlu diperhatikan adalah belum adanya mekanisme enkripsi data yang cukup kuat dalam sistem *database website* Pawnomis Official.

Oleh karena itu, penelitian ini menyusun permasalahan terkait penerapan algoritma *Advanced Encryption Standard* (AES) 256-bit dengan mode *Cipher Block Chaining* (CBC) pada *framework* Laravel, serta sampai sejauh mana tingkat keamanan tersebut dapat diukur melalui metode *Avalanche Effect* [4]. Tujuan utama penelitian ini adalah membuat dan mengembangkan sistem perlindungan data pembeli yang terpasang di *website* Pawnomis Official. Dengan menggunakan metode AES-256 CBC, penelitian ini bertujuan memastikan semua data yang masuk ke dalam *database* telah melewati proses penyandian dengan 14 kali tahap perubahan yang rumit, yaitu *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey* [5].

Mode CBC dipilih karena bertujuan agar blok teks asli yang sama tidak menghasilkan blok teks rahasia yang sama, sehingga memperlihatkan lebih sulit bagi orang yang mencoba menganalisis pola dari data tersebut [6]. Selain itu, penelitian ini bertujuan untuk memvalidasi kinerja algoritma dengan cara melakukan pengujian efek *Avalanche*. Pengujian ini sangat penting karena membantu menunjukkan bahwa algoritma memiliki sensitivitas yang tinggi, yaitu perubahan satu bit di bagian input akan menyebabkan perubahan besar pada output. Hal ini menjadi tanda utama bahwa algoritma kriptografi tersebut cukup kuat dan efektif [7], [8]. Dengan mengintegrasikan *framework* Laravel yang menggunakan pustaka *OpenSSL*, diharapkan proses pengamanan dapat berjalan secara otomatis dan efisien tanpa mengurangi kecepatan akses pengguna pada situs web [9].

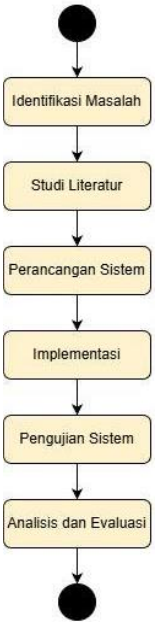
Relevansi penelitian ini terletak pada kebutuhkan perlindungan aset digital pembeli di tengah meningkatnya tindakan peretasan *database e-commerce* baik secara lokal maupun global. Seperti yang telah dijelaskan dalam penelitian yang dilakukan Jessa Syah Putra [10], keamanan data kini bukan hanya fitur tambahan, tetapi menjadi dasar penting dalam berkomunikasi secara digital dan menyimpan informasi sensitif agar tidak terjadi penyalahgunaan [11]. Kelebihan dari penelitian ini dibandingkan metode enkripsi lainnya adalah menggunakan panjang kunci 256-bit, yang sesuai dengan standar internasional dan dianggap sebagai tingkat perlindungan terbaik yang hampir tidak mungkin ditembus menggunakan metode *brute force* saat ini.

Selain itu, kombinasi antara kekuatan algoritma AES-256 CBC dengan kelebihan *framework* Laravel memberikan keuntungan dalam mengelola kunci secara lebih terstruktur dan aman bagi pengembang *website* [12]. Dengan adanya implementasi ini, *website* Pawnomis Official tidak hanya memudahkan proses transaksi, tetapi juga menjamin perlindungan data yang sangat baik, sehingga dapat meningkatkan rasa percaya dan ketetapan pelanggan terhadap *platform* tersebut.

Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah pendekatan *Research and Development* (R&D). *Research and Development* merupakan pendekatan sistematis yang digunakan untuk merancang produk baru sekaligus memvalidasi efektivitasnya [13]. Proses ini diawali dengan studi literatur dan observasi untuk menganalisis kebutuhan spesifik produk. Selanjutnya, dilakukan serangkaian pengujian teknis guna memastikan bahwa

produk tersebut layak dan berfungsi secara optimal sebelum diimplementasikan atau disebarluaskan kepada masyarakat [13] dengan tujuan utama untuk membuat sistem perlindungan data yang lebih baik pada platform perdagangan elektronik [13]. Alur penelitian ini dapat dilihat pada Gambar 1.



Gambar 1 Alur Penelitian

Berikut adalah penjelasan tahapan dalam penelitian yang tertera pada Gambar 1 mengenai metode penelitian di atas:

1. Identifikasi Masalah

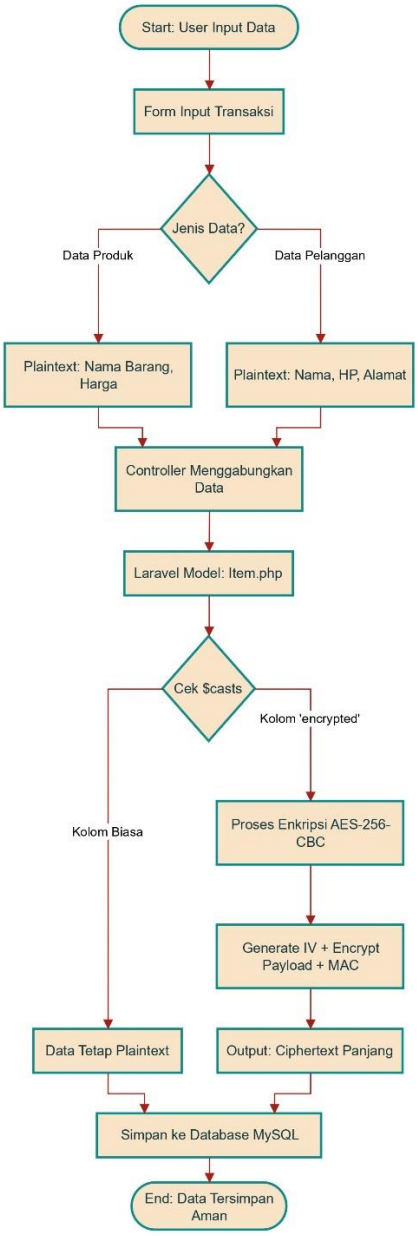
Tahap awal penelitian dilakukan dengan menganalisis celah keamanan data pada website Pawnomis Official. Fokus utama adalah mengidentifikasi kerentanan data pembeli yang masih tersimpan dalam bentuk teks asli *(plaintext)*.

2. Studi Literatur

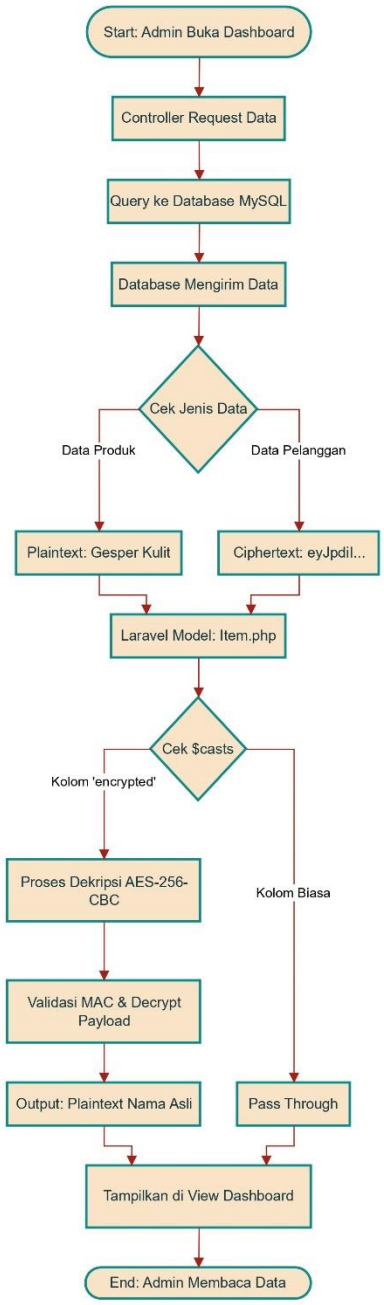
Melakukan kajian komprehensif melalui jurnal ilmiah dan literatur teknis mengenai algoritma kriptografi *Advanced Encryption Standard* (AES) 256-bit dengan mode operasi *Cipher Block Chaining* (CBC).

3. Perancangan Sistem

Perancangan sistem keamanan pada Pawnomis Official difokuskan pada perlindungan kerahasiaan data pembeli menggunakan algoritma AES-256 mode *Cipher Block Chaining* (CBC). Arsitektur perancangan ini mencakup dua proses utama, yaitu enkripsi data saat proses penyimpanan dan dekripsi data saat informasi akan ditampilkan kembali. Alur proses enkripsi dan dekripsi dapat dilihat pada Gambar 2 dan Gambar 3.



Gambar 2 Alur Proses Enkripsi



Gambar 3 Alur Proses Dekripsi

4. Implementasi

Tahap pengembangan sistem dilakukan menggunakan *framework* Laravel dengan mengimplementasikan fungsi kriptografi AES-256 dengan Mode CBC pada lapisan controller.

5. Pengujian Sistem

Melakukan uji coba keamanan dengan metode *Avalanche Effect*. Avalanche Effect merupakan salah satu karakteristik fundamental dalam kriptografi modern, di mana perubahan kecil pada data yang dimasukkan,

seperti mengubah satu bit pada *plaintext* atau kunci enkripsi, akan menghasilkan perubahan yang signifikan dan tidak bisa diprediksi pada hasil enkripsi yang dihasilkan [14], [15]. Skenario pengujian dilakukan dengan mengubah satu bit pada data input (plaintext) untuk melihat seberapa besar perubahan yang terjadi pada hasil enkripsi *(ciphertext)*.

Perhitungan *Avalanche Effect* (AE) dapat dihitung menggunakan persamaan (1):

$$AE = \frac{\text{Jumlah bit ciphertext yang berubah}}{\text{Total jumlah bit ciphertext}} \times 100\% \quad (1)$$

6. Analisis dan Evaluasi

Hasil pengujian Avalanche Effect dihitung secara matematis dan dianalisis apakah sudah mendekati nilai 50% yang ideal. Evaluasi ini dilakukan untuk mengetahui apakah implementasi AES-256 CBC pada Laravel sudah berjalan dengan efektif dan siap digunakan.

Hasil dan Pembahasan

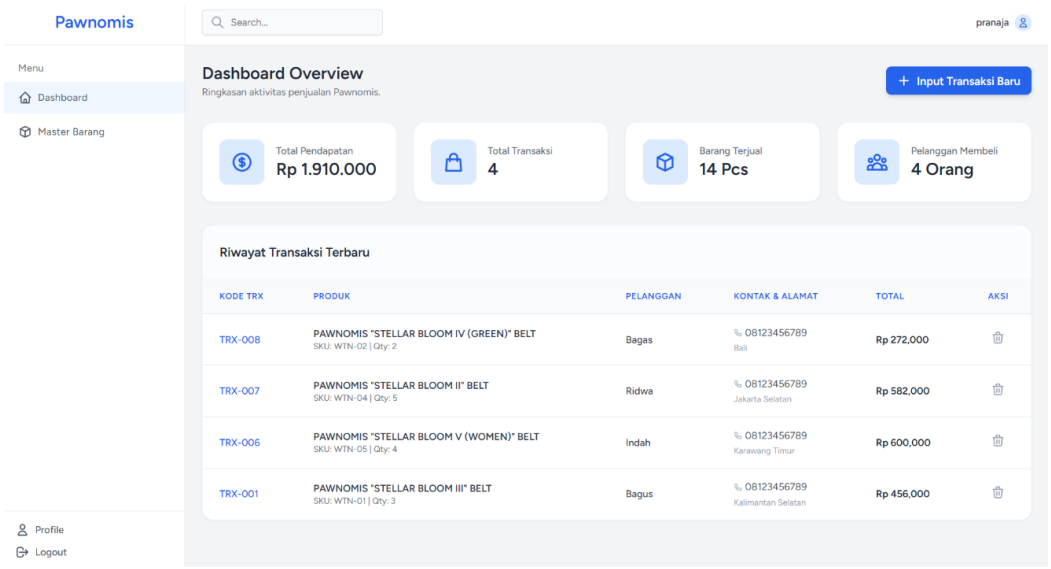
Tahap awal dari hasil penelitian ini adalah melakukan observasi dan identifikasi masalah pada objek penelitian guna mensinkronisasikan kebutuhan keamanan data dengan kondisi operasional di lapangan. Dokumentasi mengenai lingkungan fisik tempat penelitian ini ditampilkan pada Gambar 4.

Gambar 4 Dokumentasi Kegiatan Observasi lapangan pada UMKM Pawnomis Official

Gambar 4 merepresentasikan entitas bisnis Pawnomis Official yang berlokasi di Bekasi, Jawa Barat, sebagai objek penelitian primer. Dokumentasi ini memberikan konteks situasional mengenai infrastruktur operasional tempat sistem manajemen transaksi diintegrasikan. Melalui observasi di lokasi Bekasi ini, dilakukan pemetaan alur data konvensional untuk memastikan bahwa implementasi algoritma AES-256 CBC dapat berjalan selaras dengan kebutuhan keamanan data privasi pelanggan tanpa mengganggu efisiensi layanan di tempat tersebut.

Hasil Implementasi

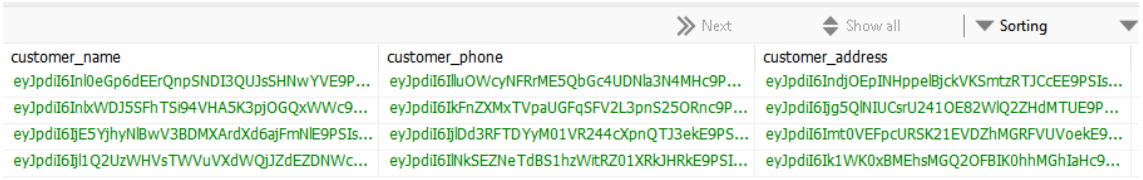
Setelah pemetaan kondisi lapangan selesai dilakukan, sistem informasi yang telah terintegrasi dengan modul kriptografi kemudian dioperasikan pada *website* Pawnomis Official. Tahap selanjutnya menampilkan halaman utama pada *website* Pawnomis Official. Halaman utama sistem Pawnomis Official dirancang sebagai pusat kendali operasional yang menyajikan ringkasan data statistik transaksi UMKM. Visualisasi data pada halaman ini merupakan hasil ekstraksi informasi yang telah diproses oleh sistem untuk memberikan gambaran cepat kepada pengguna mengenai aktivitas penjualan. Halaman ini menyajikan informasi umum seperti total pendapatan, total transaksi, barang terjual, dan jumlah pelanggan yang terdaftar. Tampilan halaman utama pada *website* Pawnomis Official ditampilkan pada Gambar 5.



Gambar 5 Halaman Home

Hasil Enkripsi Data

Pada tahap ini, dilakukan pengujian terhadap input data pembeli. Berdasarkan alur teknis, sistem membagi data ke dalam dua kategori sebelum disimpan di dalam basis data. Data publik berisi informasi seperti nama barang dan harga tetap dipertahankan dalam format *plaintext* agar dapat diproses secara efisien. Data sensitif berupa data nama, nomor telepon, dan alamat pembeli. Sistem secara otomatis menghidupkan *Initialization Vector* (IV) dan menggunakan kunci simetris 256-bit untuk mengubah data asli menjadi *ciphertext*. Hasil enkripsi dapat dilihat pada Gambar 6.

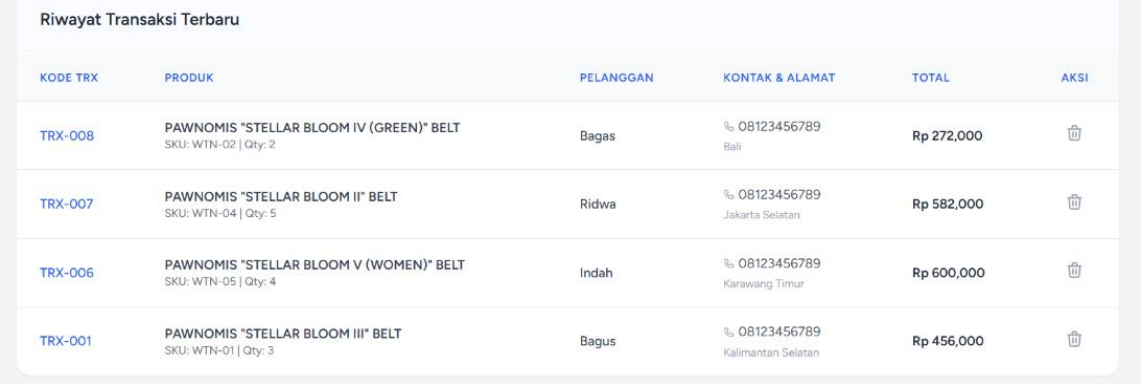


Gambar 6 Hasil Enkripsi Data Pembeli

Langkah ini memastikan bahwa data yang tersimpan pada tabel *items* tidak dapat dibaca oleh pihak yang tidak berwenang, meskipun dapat mengakses basis data.

Hasil Dekripsi Data

Proses dekripsi terjadi di latar belakang *(background),* saat data didapatkan dari database untuk ditampilkan pada *Dashboard*. Ketika Admin membuka halaman *Dashboard*, sistem memanggil data di mana Laravel secara otomatis melakukan transformasi kembali dari *ciphertext* menjadi *plaintext* menggunakan kunci yang sama. Hasil dekripsi ditampilkan pada Gambar 7.



Riwayat Transaksi Terbaru

KODE TRX	PRODUK	PELANGGAN	KONTAK & ALAMAT	TOTAL	AKSI
TRX-008	PAWNOMIS "STELLAR BLOOM IV (GREEN)" BELT SKU: WTN-02 | Qty: 2	Bagas	08123456789 Bali	Rp 272,000	
TRX-007	PAWNOMIS "STELLAR BLOOM II" BELT SKU: WTN-04 | Qty: 5	Ridwa	08123456789 Jakarta Selatan	Rp 582,000	
TRX-006	PAWNOMIS "STELLAR BLOOM V (WOMEN)" BELT SKU: WTN-05 | Qty: 4	Indah	08123456789 Karawang Timur	Rp 600,000	
TRX-001	PAWNOMIS "STELLAR BLOOM III" BELT SKU: WTN-01 | Qty: 3	Bagus	08123456789 Kalimantan Selatan	Rp 456,000	

Gambar 7 Hasil Dekripsi Data Pembeli

Hasil dekripsi menunjukkan bahwa data pelanggan kembali muncul secara utuh pada antarmuka Admin. Membuktikan bahwa proses dekripsi CBC berjalan tanpa kesalahan atau kehilangan karakter.

Hasil Pengujian

Hasil perhitungan *Avalanche Effect* menggunakan persamaan (1):

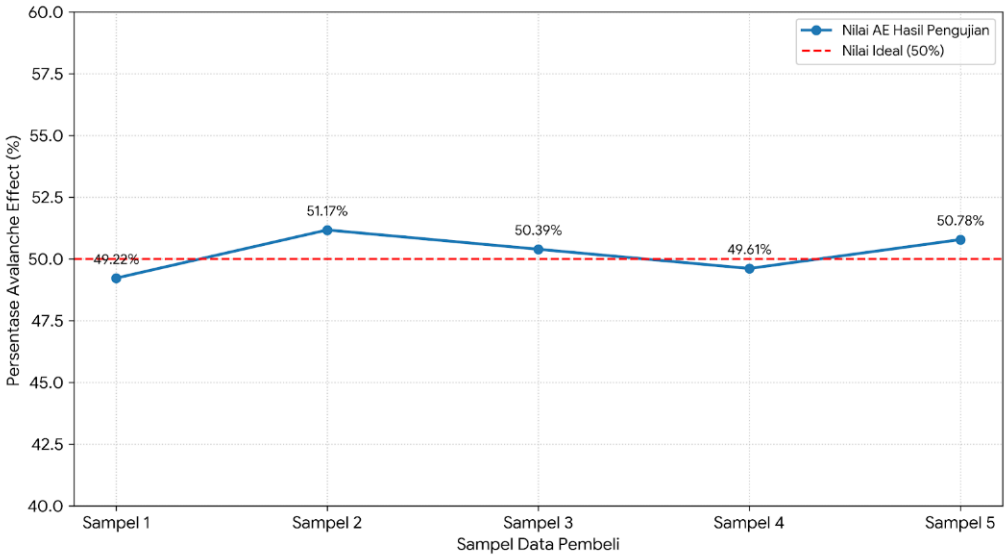
$$AE = \frac{129}{256} \times 100\% = 50{,}39\% \quad (1)$$

Berdasarkan rumus persentase *Avalanche Effect* (AE) yang telah ditetapkan, dilakukan pengujian terhadap 5 sampel data pembeli. Hasil pengujian menunjukkan tingkat perubahan bit yang sangat signifikan pada *ciphertext* meskipun hanya terdapat perubahan minimal pada *plaintext*. Hasil pengujian dapat dilihat pada Tabel 1.

Tabel 1 Hasil Pengujian Persentase Avalanche Effect

No	Sampel Data	Bit Berubah	Total Bit	Perhitungan	Hasil AE (%)
1	Data Pembeli 1	126	256	$\left(\frac{126}{256}\right) \times 100\%$	49,22%
2	Data Pembeli 2	131	256	$\left(\frac{131}{256}\right) \times 100\%$	51,17%
3	Data Pembeli 3	129	256	$\left(\frac{129}{256}\right) \times 100\%$	50,39%
4	Data Pembeli 4	127	256	$\left(\frac{127}{256}\right) \times 100\%$	49,61%
5	Data Pembeli 5	130	256	$\left(\frac{130}{256}\right) \times 100\%$	50,78%
	Nilai Rata-rata				50,23%

Untuk mempermudah analisis, nilai AE dari kelima sampel divisualisasikan dalam grafik garis di bawah ini. Garis putus-putus merah merepresentasikan nilai ideal (50%) dalam standar keamanan kriptografi. Hasil pengujian dapat dilihat pada grafik hasil *Avalanche Effect* yang ditampilkan pada Gambar 7.



Gambar 8 Grafik Hasil Pengujian

Kesimpulan

Berdasarkan hasil penelitian, implementasi algoritma AES-256 mode CBC pada *website* Pawnomis Official berhasil mengamankan data sensitif dalam bentuk ciphertext pada *database*. Ketangguhan sistem terbukti secara ilmiah melalui nilai rata-rata *Avalanche Effect* sebesar 50,23% yang memenuhi standar ideal kriptografi. Selain itu, sistem tetap fungsional karena mampu melakukan dekripsi otomatis secara akurat untuk menampilkan kembali data asli pada *Dashboard* Admin tanpa kerusakan data. Untuk melanjutkan penelitian selanjutnya disarankan untuk melakukan pengujian sistem menggunakan metode *Black Box Testing* guna memvalidasi seluruh fungsionalitas antarmuka. Selain itu, diperlukan pengembangan mekanisme manajemen kunci yang lebih dinamis, seperti penerapan rotasi kunci *(key rotation)* secara periodik, untuk memperkuat lapisan keamanan kunci rahasia dari potensi ancaman akses ilegal di masa depan.

Daftar Rujukan

[1] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.

[2] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 1, no. 02, pp. 108–114, 2021, doi: 10.30998/jrkt.v1i02.4096.

[3] dan E. R. Dian Sri Purwanti, Muhammad Fadli, Muhammad Surono, "PERANCANGAN PENERAPAN ALGORITMA KRIPTOGRAFI AES 256 UNTUK KEAMANAN DATABASE APLIKASI MANAJEMEN SISWA," *J. Ilm. Tek. dan Ilmu Komput.*, vol. 4, no. 2, pp. 111–119, 2025, doi: 10.55123.

[4] T. W. Lingga, O. K. Sulaiman, and K. Nasution, "Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data pada Aplikasi E-Pariwisata," *sudo J. Tek. Inform.*, vol. 3, no. 4, pp. 201–216, 2025, doi: 10.56211/sudo.v3i4.923.

[5] D. Fahrizal, "Implementasi Kriptografi Aes 256 Bit Pada Aplikasi Pesan Di Android Dengan Raspberry Pi Server Berbasis Open Source," *TECHSI - J. Tek. Inform.*, vol. 14, no. 2, p. 107, 2023, doi: 10.29103/techsi.v14i2.12456.

[6] C. Lung and R. Munir, "Studi dan Implementasi Advanced Encryption Standard dengan Empat Mode Operasi Block Cipher," *Sekol. Tek. Elekto dan Tek. Inform. ITB Bandung*, pp. 1–10, 1997, [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/TA/Makalah_TA Chan Lung.pdf

[7] A. Rosyadi, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES UNTUK ENKRIPSI DAN DEKRIPSI EMAIL," *Transient*, vol. 1, no. 3, pp. 2–6, 2012.

[8] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[9] Y. V. Euaggelion and R. Somya, "Analisis Dan Implementasi Aplikasi Penjualan Kosmetik Di Bmc Berbasis Website Menggunakan Framework Laravel," *INOVTEK Polbeng - Seri Inform.*, vol. 7, no. 1, p. 36, 2022, doi: 10.35314/isi.v7i1.2359.

[10] J. S. Putra, R. Ardianto, and P. Purwono, "Tinjauan Terhadap Implementasi Advanced Encryption Standard 256 Dalam Keamanan Data," *Device J. Inf. Syst. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 335–355, 2024, doi: 10.46576/device.v5i2.4621.

[11] A. R. Z. Rakhmadi Rahman, "Keamanan data terenkripsi: studi kasus enkripsi AES dalam pengembangan web formulir aduan PPKS ITH Rakhmadi," *Technol. Sci. Insights J.*, vol. 1, pp. 0–3, 2024.

[12] F. A. Naimnule *et al.*, "Implementation of AES Encryption for Data Security on Web-Based Information Systems in Fafinesu A Village," *Sist. Kendali Jaringan) E-ISSN*, vol. 4, no. 3, pp. 2808–3520, 2025, doi: https://doi.org/10.58982/krisnadana.v4i3.836.

[13] Mohammad Sidik, "Perancangan dan Pengembangan E-commerce dengan Metode Research and Development," *J. Tek. Inform. Unika St. Thomas*, vol. 04, Nomor, pp. 99–107, 2021.

[14] W. Prabowo and A. Nizirwan, "Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC," *J. ikraith-infromatika*, vol. 1, no. 9, pp. 178–186, 2025.

[15] Imam Fauzy Muldani Rachmat, "PENERAPAN ADVANCED ENCRYPTION STANDARD UNTUK SISTEM LOGIN DAN REGISTRASI PADA SISTEM INFORMASI PENJUALAN (STUDI KASUS:TOKO ILHAM BANJAR)," *IPSIKOM*, vol. 12, no. February, pp. 4–6, 2024.