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

Penerapan Algoritma Enkripsi AES-256-CBC pada Sistem Informasi Penjualan Website Aqilah Cakes

Implementation of the AES-256-CBC Encryption Algorithm in the Aqilah Cakes Website Sales Information System

Aaqilah Aathirah Sutisna1, Eka Juliyana Rahayu[2], Dita Aulia[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]aqilahaathiras22@gmail.com, [2]eka610407@gmail.com*, [3]ditaaul05@gmail.com*

Abstract

The development of information technology has driven digitalization in various sectors, including the culinary industry, which now utilizes sales websites to support online transactions. However, the increasing use of web-based systems also poses serious challenges related to customer data and transaction security. This study aims to implement the AES-256-CBC encryption algorithm in the Aqilah Cakes sales information system to ensure data confidentiality and integrity. The research method uses an applied experimental approach with stages of needs analysis, encryption module design, system implementation, and performance and security testing. The implementation results show that sensitive customer data (name, telephone number, address) is successfully encrypted before being stored in the MongoDB database. Cryptographic testing resulted in an Avalanche Effect value of 53.12%, a Bit Error Rate of 0.5312, a Character Error Rate of 93.18%, and an Entropy of 7.98 bits, which proves that AES-256-CBC has excellent diffusion and confusion and produces near-ideal random ciphertext. Thus, the Aqilah Cakes sales information system has proven capable of enhancing data security without sacrificing performance and can be relied upon to support the continuity of online business.

Keywords: *AES-256-CBC, cryptography, data security, information systems, sales, web encryption.*

Abstrak

Perkembangan teknologi informasi telah mendorong digitalisasi di berbagai sektor, termasuk industri kuliner yang kini banyak memanfaatkan website penjualan untuk mendukung transaksi daring. Namun, meningkatnya penggunaan sistem berbasis web juga menimbulkan tantangan serius terkait keamanan data pelanggan dan transaksi. Penelitian ini bertujuan untuk menerapkan algoritma enkripsi AES-256-CBC pada sistem informasi penjualan Aqilah Cakes guna menjamin kerahasiaan dan integritas data. Metode penelitian menggunakan pendekatan eksperimental terapan dengan tahapan analisis kebutuhan, perancangan modul enkripsi, implementasi sistem, serta pengujian performa dan keamanan. Hasil implementasi menunjukkan bahwa data sensitif pelanggan (nama, nomor telepon, alamat) berhasil dienkripsi sebelum disimpan ke dalam basis data MongoDB. Pengujian kriptografi menghasilkan nilai *Avalanche Effect* sebesar 53,12%, *Bit Error Rate* 0,5312, *Character Error Rate* 93,18%, dan *Entropi* 7,98 bit, yang membuktikan bahwa AES-256-CBC memiliki difusi dan konfusi yang sangat baik serta menghasilkan ciphertext acak mendekati ideal. Dengan demikian, sistem informasi penjualan Aqilah Cakes terbukti mampu meningkatkan keamanan data tanpa mengorbankan performa, serta dapat diandalkan untuk mendukung keberlangsungan bisnis daring.

Kata kunci: AES-256-CBC, kriptografi, keamanan data, sistem informasi, penjualan, enkripsi web.

Pendahuluan

Perkembangan teknologi informasi telah mendorong digitalisasi di berbagai sektor, termasuk industri kuliner yang kini banyak memanfaatkan website penjualan untuk mendukung transaksi daring. Namun, meningkatnya penggunaan sistem berbasis web juga menimbulkan tantangan serius terkait keamanan data pelanggan dan transaksi. Ancaman seperti pencurian data, *man-in-the-middle attack*, maupun eksploitasi celah keamanan menuntut penerapan algoritma kriptografi yang kuat dan efisien[1], [2].

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang ditetapkan oleh NIST pada tahun 2001 sebagai pengganti Data Encryption Standard (DES). AES memiliki keunggulan berupa struktur Substitution-Permutation Network (SPN), penggunaan aritmetika Galois Field, serta fleksibilitas panjang kunci 128, 192, dan 256 bit[3]. Di antara variasi tersebut, AES-256 dipandang paling aman karena mampu memberikan tingkat kerahasiaan tinggi terhadap ancaman brute-force maupun serangan kuantum di masa depan[3], [4], [5].

Dalam implementasi praktis, AES digunakan bersama *mode of operation* untuk meningkatkan keamanan. *Cipher Block Chaining* (CBC) adalah salah satu mode populer yang menambahkan *initialization vector (IV)* sehingga setiap blok ciphertext bergantung pada blok sebelumnya, mencegah pola berulang pada data terenkripsi[4]. Kombinasi AES-256 dengan CBC terbukti memberikan keseimbangan antara keamanan dan performa, serta banyak digunakan pada aplikasi web security, VPN, dan cloud storage. Selain itu, penelitian terbaru menunjukkan bahwa integrasi AES dengan mekanisme tambahan seperti Hash-based Message Authentication Code (HMAC) maupun Residue Number System (RNS) dapat meningkatkan integritas dan efisiensi sistem[4], [6]. Penelitian lain juga menegaskan efektifitas AES-256-CBC dalam pengamanan data akademik berbasis web[2] dan login sistem e-commerce[7]. Namun, untuk aplikasi penjualan berbasis web skala menengah seperti Aqilah Cakes, penerapan AES-256-CBC sudah cukup untuk menjamin kerahasiaan data transaksi, melindungi informasi pelanggan, serta menjaga kepercayaan konsumen.

Beberapa penelitian sebelumnya juga menegaskan bahwa sistem informasi berbasis web rentan terhadap kebocoran data apabila tidak dilengkapi dengan mekanisme enkripsi yang memadai. Implementasi algoritma kriptografi simetris seperti AES pada berbagai sistem berbasis web terbukti mampu meningkatkan perlindungan terhadap data sensitif dan transaksi pengguna[8], [9] . Selain itu, penerapan metode enkripsi pada sistem informasi penjualan dan layanan digital menunjukkan peningkatan signifikan dalam aspek kerahasiaan dan keamanan penyimpanan basis data[10].

Berdasarkan penjelasan diatas, penelitian ini bertujuan untuk menganalisis dan menerapkan algoritma enkripsi AES-256-CBC pada sistem informasi penjualan Aqilah Cakes. Fokus utama adalah bagaimana algoritma ini dapat mengamankan data transaksi, menjaga integritas informasi, serta mendukung keberlangsungan bisnis dengan sistem yang aman, efisien, dan dapat diandalkan.

Metode Penelitian

Desain Penelitian

Penelitian ini menggunakan pendektan eksperimental terapan dengan fokus pada implementasi algoritma enkripsi AES-256-CBC dalam sistem informasi penjualan berbasis web. Desain penelitian dirancang untuk membandingkan kondisi sitem sebelum dan sesudah penerapan enkripsi, khususnya pada aspek keamanan data transaksi dan performa sistem[3], [4].

Rancangan Kegiatan

Tahapan penelitian meliputi analisis kebutuhan sistem untuk mengidentifikasi data sensitive yang harus diamankan, perancangan modul enkripsi berbasis AES-256-CBC yang terintegrasi dengan sistem penjualan, implementasi sistem ke dalam website *Aqilah Cakes*, pengujian sistem dengan scenario transaksi nyata, dan evaluasi hasil berdasarkan indicator keamanan dan performa.

Ruang Lingkup/Objek Penelitian

Objek penelitian adalah website penjualan Aqilah Cakes, dengan ruang lingkup meliputi proses login, penyimpanan data pelanggan, dan transaksi penjualan yang melibatkan data sensitive.[1], [11]

Tempat Penelitian

Penelitian dilakukan di Aqilah Cakes, Cikarang Selatan, Jawa Barat. Sistem uji cob aini berbasis server local dan simulasi akses melalui jaringan internet.

Teknik Analisis Penelitian

Analisis dilakukan dengan pendekatan komparatif dan deksriptif. **Komperatif** membandingkan performa sistem sebelum dan sesudah penerapan AES-256-CBC. **Deskriptif** menjelaskan hasil pengujian keamanan, termasuk keberhasilan algoritma dalam mencegah akses tidak sah. Validasi keamanan simulasi serangan sederhana untuk memastikan data terenkripsi tidak dapat dibaca tanpa kunvi yang sah.

Teknologi yang Digunakan

Dalam pengembangan website sistem informasi penjualan Aqilah Cakes, teknologi frontend dipilih untuk mendukung tampilan antarmuka pengguna yang interaktif, responsif, serta mudah dikembangkan. Teknologi yang digunakan pada sisi frontend disesuaikan dengan kebutuhan pengelolaan data, performa aplikasi, dan kemudahan integrasi dengan backend. Daftar teknologi frontend yang digunakan pada penelitian ini disajikan pada Tabel 1.

Tabel 1. Frontend

No	Teknologi	Keterangan
1	React.js	Library UI berbasis komponen.
2	Vite	Build tool modern untuk pengembangan cepat
3	TypeScript	Bahasa dengan static typing untuk keandalan kode.
4	React Query	Pengelolaan data server state.
5	Axios	HTTP client untuk komunikasi REST API.
6	Tailwind CSS	Framework CSS berbasis utility-first.
7	Shadcn UI	Komponen UI siap pakai berbasis Tailwind.
8	Lucide Icons	Library ikon berbasis SVG.

Selain teknologi frontend, pengembangan sistem juga melibatkan teknologi backend yang berfungsi untuk mengelola logika aplikasi, pengolahan data, serta komunikasi antara frontend dan basis data. Pemilihan teknologi backend didasarkan pada kebutuhan skalabilitas, efisiensi pengolahan data, serta kemudahan integrasi dengan mekanisme keamanan yang diterapkan. Rincian teknologi backend yang digunakan dalam penelitian ini ditunjukkan pada Tabel 2.

Tabel 2. Backend

No	Teknologi	Keterangan
1	Node.js	Runtime JavaScript berbasis event-driven.
2	Express.js	Framework minimalis untuk RESTful API
3	MongoDB	Basis data NoSQL fleksibel.
4	Mongoose	ODM untuk interaksi dengan MongoDB.
5	REST API	Arsitektur komunikasi fronted-backend.

Untuk menjamim kemanan data transaksi pada sistem informasi penjualan Aqilah Cakes, penelitian ini menerapkan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256 bit dan mode operasi *Cipher Block Chaining* (CBC). AES merupakan algoritma enkripsi simetris yang dipilih oleh NIST pada tahun

2001 sebagai standar pengganti DES. Algoritma ini menggunakan struktur *Substitution-Permutation Network* (SPN) dengan operasi berbaris aritmatika *Galois Field* untuk mencapai tingkat keamanan tinggi terhadap serangan kriptanalisis[1], [12].

Dalam penelitian ini, pemilihan algoritma enkripsi AES-256 dengan mode operasi *Cipher Block Chaining* (CBC) didasarkan pada pertimbangan tingkat keamanan, ketahanan terhadap perkembangan ancaman komputasi, serta efisiensi implementasi pada sistem informasi berbasis web. Beberapa alasan utama yang melatarbelakangi pemilihan AES-256-CBC sebagai mekanisme pengamanan data pada sistem informasi penjualan Aqilah Cakes dijelaskan sebagai berikut:

Kekuatan kunci, panjang kunci 256 bit memberikan ruang pencarian yang sangat besar, sehingga tahan terhadap brute-force attack[3], [12].

Ketahanan terhadap ancaman kuantum, AES-256 dianggap lebih aman disbanding AES-128 karen Grover's Algorithm hanya mamou mengurangi kompleksitas pencarian menjadi $2^{n/2}$, sehingga AES-256 tetap memiliki tingkat keamanan setara 128 bis di era komputasi kuantum[4], [13].

Efisiensi implementasi, AES dapat dijalankan dengan baik pada perangkat lunak maupun perangkat keras, termasuk sistem berbasis web.

Sejumlah penelitian eksperimental juga menunjukkan bahwa AES dengan panjang kunci tinggi memberikan tingkat keamanan yang lebih baik dibandingkan variasi kunci yang lebih pendek, khususnya pada sistem berbasis web dan aplikasi transaksi digital[14]. Hasil tersebut memperkuat pemilihan AES-256-CBC dalam penelitian ini sebagai solusi pengamanan data pelanggan.

Mode CBC digunakan karena siap blok plaintext dienkripsi dengan cara di-XOR dengan ciphertext blok sebelumnya menggunakan *Intialization Vectro* (IV) acak. Hal ini mencegah pola berulang pada cipher text dan meningkatkan difusi data, dengan kombinasi AES-256 dan CBC, sistem penjualan *Aqilah Cakes* mampus menjaga kerahasiaan data pelanggan, transaksi, serta informasi pembayaran dari akses tidak sah.

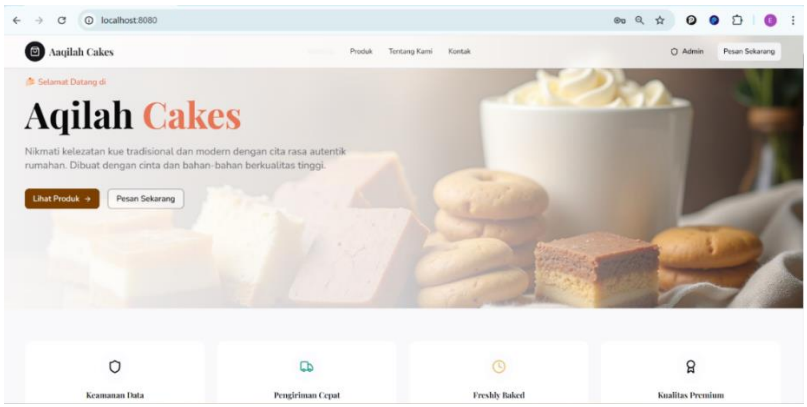
Hasil dan Pembahasan

Hasil Implementasi Sistem

Website Aqilah Cakes berhasil dibangun sebagai sistem informasi penjualan berbasis web yang mendukung promosi produk, pemesanan online, serta pengamanan data pelanggan menggunakan algoritma AES-256-CBC. Impelemntasi website dari beberapa halaman utama sebagai berikut.

Halaman Beranda

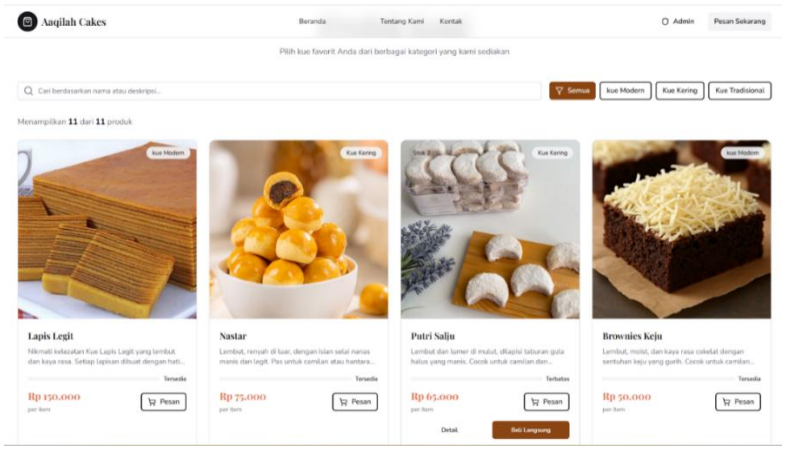
Halaman ini menampilkan informasi umum mengenai usaha Aqilah Cakes, produk unggulan, serta penjelasan singkat mengenai komitmen keamanan data pelanggan melalui penerapan enkripsi AES-256. Halaman ini menjadi pintu utama bagi pengguna untuk mengenal layanan yang disediakan. Gambar 1 menunjukkan tampilan halaman beranda website Aqilah Cakes.



Gambar 1. Halaman Beranda Aqilah Cakes

Halaman Produk

Halaman ini menampilkan daftar kue yang tersedia, meliputi kue tradisional, kue modern, dan kue kering. Setiap produk dilengkapi dengan informasi deskripsi, harga, serta status ketersediaan stok, data produk diambil dari backend dan ditampilkan secara dinamis pada halaman ini. Tampilan halaman produk ditunjukkan pada Gambar 2.



Gambar 2. Halaman Produk Website Aqilah Cakes

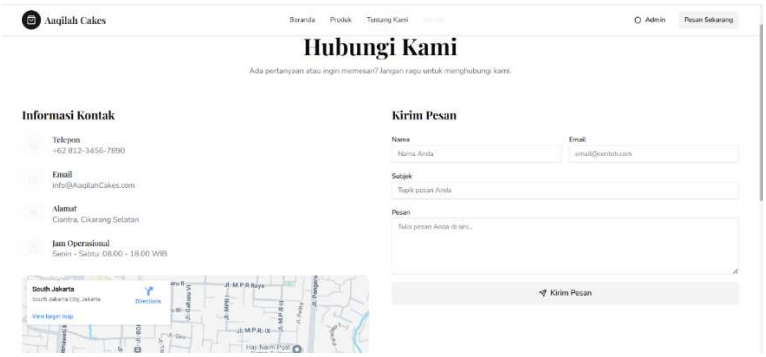
Halaman Tentang Kami

Berisi narasi singkat mengenai perjalanan usaha Aqilah Cakes yang telah berdiri sejak tahun 2015. Selain menekankan kualitas produk, halam ini juga menampilkan komitmen usaha dalam menjaga keamanan data pelanggan melalui sistem yang aman dan terenkripsi. Gambar 3 memperlihatkan tampilan halaman *Tentang Kami* pada website Aqilah Cakes.

Gambar 3. Tentang Kami pada Website Aqilah Cakes

Halaman Kontak

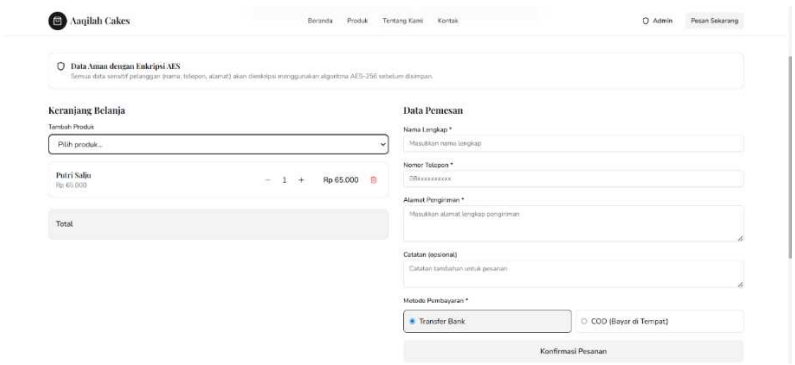
Menyediakan informasi berupa alamat usaha, nomor telepon, jam operasional, serta formular kontak yang dapat digunakan pelanggan untuk mengirim pesan secara langsung. Data yang dikirimkan melalui formular ini diproses oleh sistem backend secara aman. Tampilan halaman kontak ditunjukkan pada Gambar 4.



Gambar 4. Halaman Kontak Website Aqilah Cakes

Form Pemesanan Online

Memungkinkan pelanggan untuk memilih produk, mengisi data pribadi seperti nama, nomor telepon, dan alamat, serta memilih metode pembayaran. Seluruh data sensitive yang dimasukkan oleh pelanggan akan dienkripsi menggunakan algoritma AES-256-CBC sebelum disimpan ke dalam basisi data, yang akan ditampilkan pada Gambar 5.

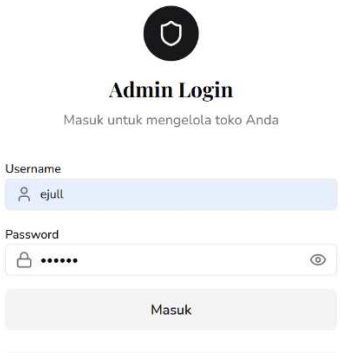


Gambar 5. Form Pemesanan Online

Hasil Implementasi Admin Panel

Dashboard Admin

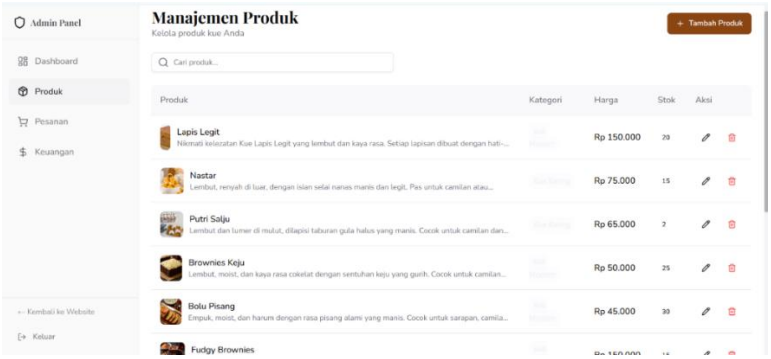
Menampilkan ringkasan informasi sistem, seperti jumlah produk, jumlah pemesanan, serta pendapatan harian dan total. Informasi ini membantu admin dalam emantau kondisi usaha secara cepat, dashboard ini akan ditampilkan pada Gambar 6.



Gambar 6. Dashboard Admin

Manajemen Produk

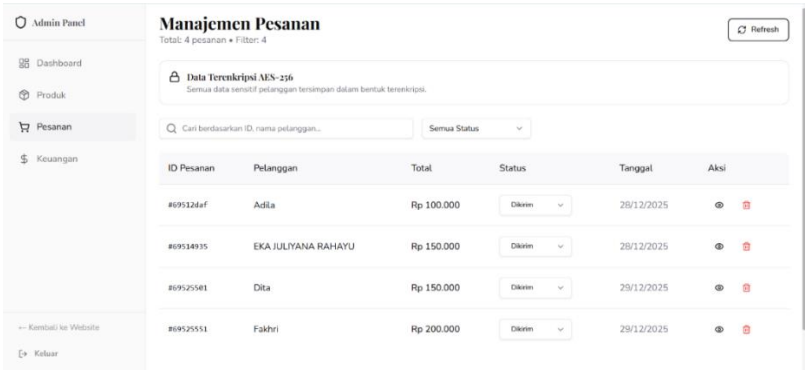
Memungkinkan admin untuk menambahk, mengedit, dan menghapus data produk, setiap produk dapat dikelola berdasarkan harga, stok, dan kategori, sehingga memudahkan pengelolaan katalog produk, halaman ini akan ditampilkan pada Gambar 7.



Gambar 7. Manajemen Produk

Manajemen Pesanan

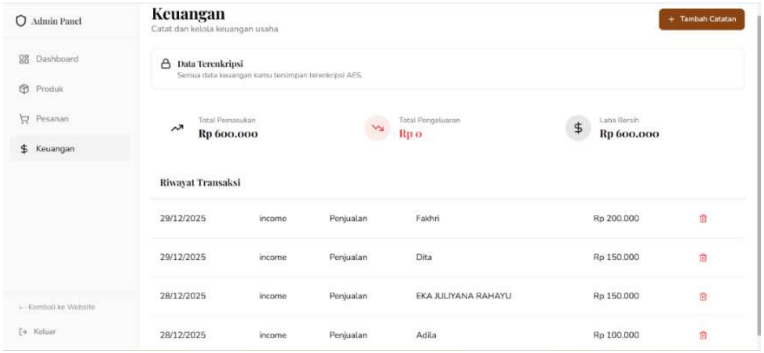
Menampilkan daftar pesanan pelanggan lengkap dengan status pemesanan, total harga, dan tanggal transaksi. Data pelanggan yang tersimpan di database berada dalam bentuk terenkripsi menggunakan AES-256, namum dapat didekripsi oleh sistem untuk keperluan tampilan admin. Halaman ini akan ditampilkan pada Gambar 8.



Gambar 8. Manajemen Pemesanan

Manajemen Keuangan

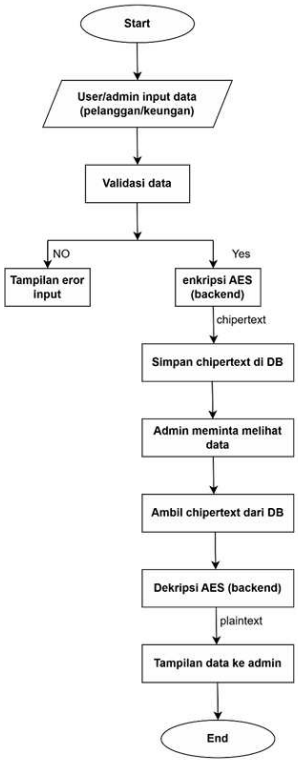
Menampilkan data pemasukkan, pengeluaran, serta perhitungan laba bersih. Riwayat transaksi ditampilkan secara rinci berdasarkan nama pelanggan, kategori transaksi, dan jumlah pembayaran, sehingga membantu admin dalam melakukan evaluasi keuangan. Halaman ini ditampilkan pada Gambar 9.



Gambar 9. Manajemen Keuangan

Flowchart Sistem

Flowchart digunakan untuk menggambarkan alur kerja utama pada sistem informasi penjualan website Aqilah Cakes, mulai dari proses autentikasi pengguna hingga data transaksi ditampilkan kembali kepada admin. Flowchart ini menunjukkan tahapan pemrosesan data serta posisi penerapan algoritma enkripsi AES-256-CBC dalam sistem. Data tersebut selanjutnya diproses oleh backend untuk dilakukan enkripsi menggunakan AES-256-CBC sebelum dikirim dan disimpan ke dalam basis data MongoDB. Setelah data tersimpan, admin dapat mengakses dan melihat data transaksi melalui sistem yang secara otomatis melakukan proses dekripsi untuk keperluan tampilan. Gambar 10.



Gambar 10. Flowchart AES

Flowchart ini menegaskan bahwa setiap data sensitif selalu melalui proses enkripsi sebelum disimpan, sehingga sistem memiliki mekanisme pengamanan yang konsisten dan terstruktur terhadap potensi kebocoran data.

Hasil Implementasi Enkripsi Data pada Basis Data

Berdasarkan hasil implementasi sistem, penerapan algoritma AES-256-CBC dapat diamati secara langsung pada data yang tersimpan di babsis data MongDB. Data sensitive tidak disimpan dalam bentuk *plaintext*, melainkan telah melalui proses enkripsi sehingga hanya tersimpan dalam bentuk *ciphertext*.

Pendekatan penyimpanan data dalam bentuk ciphertext ini juga diterapkan pada beberapa sistem informasi berbasis database yang menekankan pentingnya perlindungan terhadap data pelanggan guna mencegah penyalahgunaan apabila terjadi akses ilegal ke server [8], [10].

Penyimpanan Data Terenkripsi

Pada Gambar 11, ditunjukkan contoh data yang tersimpan di basis data dengan satu field utama berupa nilai terenkripsi. Nilai tersebut merupakan hasil enkripsi menggunakan AES-256-CBC yang menghasilkan rangkaian karakter acak. Struktur data ini menunjukkan bahwa sistem tidak menyimpan informasi asli secara langsung, sehingga aman apabila terjadi akses tidak sah ke database.

Gamabar 11. Contoh Data Terenkripsi Menggunakan AES-256-CBC di MongoDB

Konsistensi Hasil Enkripsi pada Waktu Berbeda

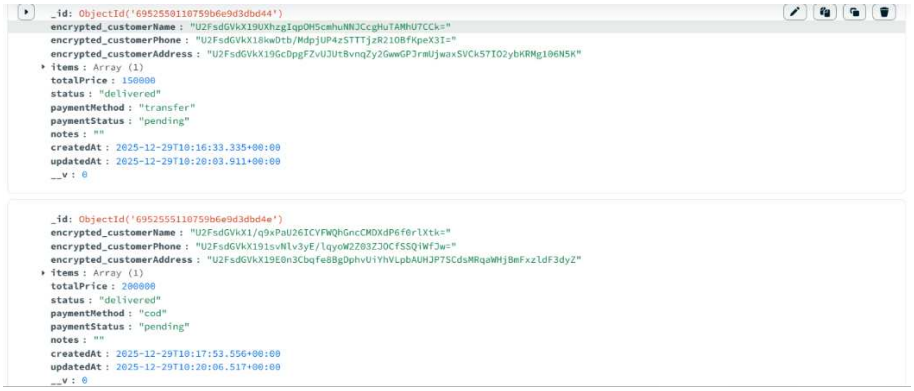
Pada Gambar 12 dan Gambar 13, terlihat bahwa data terenkripsi yang dihasilkan pada waktu yang berbeda memiliki nilai ciphertext yang berbeda, meskipun struktur data yang disimpan serupa. Hal ini terjadi karena pengguna *Intialization Vector* (IV) acak pada mode CBC. Mekaniske ini memastikan setiap proses enkripsi menghasilkan *ciphertext* yang unik dan tidak dapat dianalisis berdasarkan pola tertentu.

Gambar 12. Hasil Enkripsi Data pada Waktu Penyimpanan Berbeda

Gambar 13. Variasi Ciphertext Akibat Pengguna IV Acak

Enkripsi Data Pelanggan pada Transaksi Penjualan

Pada Gambar 14, ditampilkan data transaksi pelanggan yang tersimpan di basis data. Informasi sensitive seperti nama pelanggan, nomor telepon, dan lamat disimpan dalam field *encrypted_customerName*, *encrypted_customerPhone*, dan *encrypted_customerAddress*. Seluruh field tersebut berisi *ciphertext* hasil enkripsi AES-256-CBC, sedangkan data non-sensitif seperti total harga, status pemesanan, dan metode pembayaran disimpan dalam bentuk *plaintext*. Pendekatan ini menunjukkan bahwa sistem hanya mengenkripsi data yang bersifat sensitive, sehingga tetap menjaga efisiensi pengolahan data tanpa mengorbankan keamanan.



Gambar 14. Penyimpanan Data Transaksi dengan Field Pelanggan Terenkripsi

Analisis Hasil Implementasi Enkripsi

Dari hasil pengujian menunjukkan bahwapenerapan AES-256-CBC telah berjalan dengan baik dan konssistensi pada seluruh data sensitive dalam sistem. Tidak ditemukan data pelanggan yang tersimpan dalam bentuk *plaintext* di basis data. Selain itu, penggunaan IV acak pada mode CBC berhasil meningkatkan keamanan dengan menghasilkan *ciphertext* yang unik untuk setiap transaksi-Nya.

Dengan demikian, sistem informasi penjualan Aqilah Cakes berbasis website telah memenuhi prinsip dasar kemanan informasi, yaitu kerahasian (*confidentiality*) dan integritas (*integrity*) data, tanpa mengganggu performa dan fungsi utama sistem.

Hasil Pengujian Teks Kriptografi AES-256-CBC

Avalanche Effect (AE)

Rumus Avalanche Efferct, $AE = \frac{Jumlah\ bit\ berubah}{Jumlah\ total\ bit} \times 100\%$

(panjang ciphertext: 128 bit, bit berubah setelah perubahan 1 karakter pada plaintext: 68 bit)

$AE = \frac{68}{128} \times 100\% = 53{,}12\%$; Nilai Avalanche Effect **53,12% (Sangat Baik)**

Bit Errir Rate (BER)

Rumus $BER = \frac{Jumlah\ bit\ berbeda}{Jumlah\ total\ bit}$

(Jumlah bit berbeda: 68 bit, total bit ciphertext: 128 bit)

$BER = \frac{68}{128} = 0{,}5312$; Nilai Bit Error Rate **0,5312 (Sangat Aman)**

Character Error Rate (CER)

Rumus $CER = \frac{Jumlah\ karakter\ berbeda}{Jumlah\ total\ karakter} \times 100\%$

(Panjang ciphertext (Base64): 44 karakter, Karakter berbeda setelah perubahan 1 karakter plaintext: 41 karakter)

$CER = \frac{41}{44} \times 100\% = 93{,}18\%$; Nilai Character Error Rate **93,18% (Sangat Baik)**

Entropi (Entropy)

Rumus $H = -\sum_{i=1}^{n} p_i log_2(p_i)$

(Jumlah kemungkikanan symbol byte: $n = 256$, probabilitas kemunculan setiap byte: $p_i \approx \frac{1}{256} = 0{,}00390625$)

$H = -\sum_{i=1}^{256}(0{,}0039 log_2(0{,}0039) \approx 7{,}98\ bit$; Nilai Entropi **7,98 bit (Mendekati Ideal)**

Interpretasi: Entropi maksimum untuk data byte = **8 bit**, Nilai &,98 menunjukkan ciphertext **sangat acak**, dan hampir tidak ada pola yang dapat diananlisis.

Nilai Avalanche Effect di atas 50% serta entropi mendekati 8 bit menunjukkan bahwa ciphertext memiliki tingkat keacakan yang tinggi dan sesuai dengan karakteristik algoritma kriptografi yang baik. Temuan ini sejalan dengan penelitian terdahulu yang menguji performa AES pada sistem informasi digital dan memperoleh hasil difusi serta konfusi yang optimal [9], [15].

Ringkasan Nilai Pengujian Kriptografi

Tabel 3. Nilai Pengujian

Parameter	Nilai	Kriteria	Status
Avalanche Effect (AE)	53,12%	$\geq 50\%$	Sangat Baik
Bir Error Rate (BER)	0,5312	$\approx 0{,}5$	Aman
Character Error Rate (CER)	93,18%	$\geq 80\%$	Sangat Baik
Entropi (Entropy)	7,98 bit	$\leq 8\ bit$	Mendekati Ideal

Berdasarkan hasil pengujian *Avalanche Effect*, *Bit Error Rate*, *Character Error Rate*, dan *Entropi*, algoritma AES-256-CBC yang diterapkan pada sistem informasi penjualan website Aqilah Cakes terbukti memiliki **difusi dan konfusi yang sangat baik**, menghasilkan ciphertext yang **sangat acak**, tahan terhadap **analisis statistic dan kriptanalisis sederhana**, dan layak digunakan untuk **pengamanan data sensitive berbasis web**.

Kesimpulan

Penetilian ini membuktikan bahwa penerapan algoritma AES-256-CBC pada sistem informasi penjualan Aqilah Cakes mampu meningkatkan keamanan data pelanggan dan transaksi. Data sensitif berhasil disimpan dalam bentuk terenkripsi sehingga tidak dapat diakses tanpa kunci yang sah. Pengujian kriptografi menunjukkan hasil yang sangat baik dengan nilai *Avalanche Effect* di atas 50%, *Character Error Rate* di atas 90%, serta *entropi* mendekati ideal, yang menandakan *ciphertext* acak dan sulit dianalisis. Selain itu, performa sistem tetap efisien dengan waktu enkripsi dan dekripsi yang singkat, sehingga tidak mengganggu pengalaman pengguna. Dengan demikian, sistem ini telah memenuhi prinsip dasar keamanan informasi yaitu kerahasiaan (*confidentiality*) dan integritas (*integrity*), serta dapat dijadikan solusi praktis untuk pengamanan data pada aplikasi penjualan berbasis web.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada pihak-pihak yang telah memberikan dukungan, masukan, dan bantuan selama proses penelitian ini berlangsung. Apresiasi diberikan kepada rekan sejawat, rekan tim, serta mitra yang terlibat dalam pengembangan dan pengujian sistem. Dukungan moral maupun teknik dari berbagai pihak sangat membantu sehingga penelitian ini dapat terselesaikan dengan baik.

Daftar Rujukan

[1] C. Yadav, R. Dhakad, M. Panchal, and E. Bhupinder Kaur, "Revolutionizing Near-by Accommodation: An in-depth Analysis of React.js, Node.js, MongoDB, and Express.js Integration for Website Development." [Online]. Available: https://ssrn.com/abstract=4932790

[2] A. Z. Ifani, R. N. J. S.Intam, A. I. Syair, and H. Husnawati, "Application of Advanced Encryption Standard (AES) Algorithm in E-Commerce Login System for User Data Security," *Journal of System and Computer Engineering (JSCE)*, vol. 6, no. 1, pp. 1–9, Jan. 2025, doi: 10.61628/jsce.v6i1.1511.

[3] R. Ganesh, B. U. I. Khan, A. R. Khan, and A. Bin Kamsin, "A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges," *Int. J. Inf. Secur.*, vol. 24, no. 5, Oct. 2025, doi: 10.1007/s10207-025-01116-x.

[4] S. Akobre, J. K. Wiredu, M. I. Daabo, and M. A. Agebure, "An Enhanced RNS-AES Encryption Scheme with CBC Mode and HMAC for Secure and Authenticated Data Protection," *Earthline Journal of Mathematical Sciences*, pp. 1091–1112, Oct. 2025, doi: 10.34198/ejms.15625.10911112.

[5] Z. Hayat Arka Putri, Y. Arye Yustraini, R. Ariansyah, N. Choirun Nisa, E. Dyar Wahyuni, and A. Brastama Putra, "Pengamanan Data Akademik Berbasis Web dengan Enkripsi AES-256 (Studi Kasus pada Pendataan Digital SMA XYZ)," *JNATIA*, vol. 3, no. 3, p. 2025.

[6] G. A. Fauzi, K. Aes, D. Hmac, G. A. Fauzi, and A. Rahmatulloh, "Kombinasi AES dan HMAC SHA-256 untuk Pengamanan Parameter URL dari Serangan SQL Injection," *JURNAL INFORMATIKA & MULTIMEDIA*, vol. 17, no. 1, 2025.

[7] A. I. Suranta, D. Virgian, and S. Y. Sakti, "Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 1, pp. 1–10, 2022.

[8] C. A. Pinuyut, E. Utami, and A. H. Muhammad, "ANALISIS KINERJA ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) TERMODIFIKASI DALAM ENRKIPSI DAN DEKRIPSI DATA (PERFORMANCE ANALYSIS OF MODIFIED ADVANCED ENCRYPTION STANDART (AES) ALGORITHM FOR ENCRYPTING AND DECRYPTING DATA)."

[9] A. Djunaidy and M. Husni, "PENERAPAN AES UNTUK OTENTIKASI AKSES CLOUD COMPUTING," vol. 4, no. 1, 2014.

[10] M. Fajar, A. Billy Kambodji, I. Alwiah Musdar, and J. Algoritma STMIK Kharisma Makassar Jl Baji, "Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle." [Online]. Available: https://jurnal.itg.ac.id/

[11] C. Sravani, P. Kumar, S. Priya, S. K. Yadav, M. J. Rao, and U. D. Prasan, "Constructing a Study Buddy Using MERN (MongoDB, Express.js, React, Node.js) Stack Technologies †," *Engineering Proceedings*, vol. 66, no. 1, 2024, doi: 10.3390/engproc2024066027.

[12] J. S, Prof. P. O. Sarangamath, and Dr. S. H. Ali, "Implementation of AES-256 in Virtual Private Network with Secure Communication," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 9, pp. 807–812, Sep. 2025, doi: 10.22214/ijraset.2025.74065.

[13] "PCB Design and Development for Multipurpose Robots," 2025.

[14] J. Dan Analisis Algoritma Enkripsi Untuk Pengamanan Komunikasi Jaringan, S. Asri, T. Peryanto, E. Malays, U. Yai, and J. Pusat, "Perbandingan Implementasi Algoritma Aes Dalam Pemrograman", doi: 10.37817/tekinfo.v25i2.

[15] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, 2016, [Online]. Available: http://ejournal.unisba.ac.id