

Pengamanan Data Transaksi Menggunakan Metode AES pada UMKM Warung Nasi Ibu Engkod

Data Transaction Security Using the AES Method in the MSMEs “Warung Nasi Ibu Engkod”

Silfa Salsa Bila Putri¹, Laras Sakti², Hannifa Indah Rahayu³

Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

¹silfasalsabilaputri@gmail.com, ²larassakti167@gmail.com, ³hannifaindah11311@gmail.com*

Abstract

The development of information technology has encouraged Micro, Small, and Medium Enterprises (MSMEs) to adopt digital systems for managing transaction data; however, this digitalization also increases security risks such as data theft, manipulation, and unauthorized access. Transaction data are valuable assets for MSMEs because they are directly related to financial information and business sustainability. Therefore, an effective security method is required to ensure data confidentiality and integrity. This study aims to implement the Advanced Encryption Standard (AES) algorithm with a 256-bit key length to secure transaction data at Warung Nasi Ibu Engkod, an MSME case study. The research methodology includes transaction system analysis, security mechanism design, implementation of encryption and decryption processes using AES-256, and cryptographic text security testing using Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), and entropy. The test results show that the AES-256 algorithm produces an Avalanche Effect value of 56.25%, a CER of 84.09%, a BER of 56.25%, and an entropy value of 4.98. These results indicate that the generated ciphertext exhibits good diffusion, high sensitivity to input changes, and a level of randomness close to the maximum. Therefore, the implementation of the AES-256 algorithm is proven to be effective in enhancing transaction data security, minimizing the risk of data leakage, and suitable for securing transaction data in MSMEs.

Keywords: data security, transaction data, AES, cryptography, MSMEs

Abstrak

Perkembangan teknologi informasi mendorong pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) untuk memanfaatkan sistem digital dalam pengelolaan data transaksi, namun digitalisasi tersebut juga meningkatkan risiko terhadap keamanan data seperti pencurian, manipulasi, dan akses tidak sah. Data transaksi merupakan aset penting bagi UMKM karena berkaitan langsung dengan informasi keuangan dan keberlangsungan usaha, sehingga diperlukan metode pengamanan yang mampu menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menerapkan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 256 bit dalam pengamanan data transaksi pada UMKM Warung Nasi Ibu Engkod. Metode penelitian meliputi analisis sistem transaksi, perancangan mekanisme keamanan data, implementasi proses enkripsi dan dekripsi menggunakan AES-256, serta pengujian keamanan teks kriptografi menggunakan metode Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), dan entropi. Hasil pengujian menunjukkan bahwa algoritma AES-256 menghasilkan nilai Avalanche Effect sebesar 56.25%, CER sebesar 84.09%, BER sebesar 56.25%, serta nilai entropi sebesar 4.98. Nilai-nilai tersebut menunjukkan bahwa ciphertext yang dihasilkan memiliki tingkat difusi yang baik, sensitivitas tinggi terhadap perubahan input, dan tingkat keacakan yang mendekati maksimum. Dengan demikian, penerapan algoritma AES-256 terbukti efektif dalam meningkatkan keamanan data transaksi, meminimalkan risiko kebocoran data, serta layak diterapkan sebagai solusi pengamanan data transaksi pada UMKM.

Kata kunci: keamanan data, data transaksi, AES, kriptografi, UMKM

Pendahuluan

Perkembangan teknologi informasi yang semakin pesat telah mendorong pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) untuk memanfaatkan sistem digital dalam mengelola kegiatan usahanya[1]. Salah satu pemanfaatan teknologi tersebut adalah penggunaan sistem informasi transaksi untuk mencatat penjualan, pengeluaran, serta laporan keuangan. Digitalisasi transaksi ini memberikan kemudahan dalam pengelolaan data, namun di sisi lain juga menimbulkan risiko terhadap keamanan data, seperti pencurian, manipulasi, dan penyalahgunaan informasi transaksi[2].

Data transaksi merupakan aset penting bagi UMKM karena memuat informasi keuangan yang bersifat rahasia dan strategis[2][3]. Kebocoran atau manipulasi data transaksi dapat menyebabkan kerugian finansial, kesalahan pengambilan keputusan, serta menurunkan kepercayaan pemilik usaha terhadap sistem yang digunakan. Pada UMKM skala kecil seperti Warung Nasi Ibu Engkod, sistem pencatatan transaksi umumnya masih memiliki keterbatasan dalam penerapan mekanisme keamanan data yang memadai. Hal ini menyebabkan data transaksi rentan terhadap akses tidak sah, baik akibat kelemahan sistem maupun faktor human error[4][5].

Keamanan data menjadi aspek yang sangat penting dalam pengelolaan sistem informasi transaksi. Salah satu teknik yang dapat digunakan untuk melindungi data adalah kriptografi, yaitu proses pengamanan data dengan cara mengubah informasi asli menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang[6]. *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi simetris yang telah diakui secara internasional dan banyak digunakan dalam berbagai sistem keamanan informasi[7][8]. Algoritma AES juga telah ditetapkan sebagai standar enkripsi oleh National Institute of Standards and Technology (NIST) karena memiliki tingkat keamanan yang tinggi serta efisiensi dalam proses enkripsi dan dekripsi [15]. Algoritma AES memiliki keunggulan dalam hal tingkat keamanan yang tinggi, kecepatan proses enkripsi dan dekripsi, serta efisiensi dalam penggunaan sumber daya sistem[9].

Beberapa penelitian sebelumnya telah menunjukkan bahwa penerapan algoritma AES mampu meningkatkan keamanan data pada berbagai sistem, seperti sistem transaksi penjualan, sistem informasi keuangan, dan basis data. Meskipun demikian, penerapan metode AES pada sistem transaksi UMKM masih belum banyak dibahas secara spesifik, terutama pada usaha kecil yang memiliki keterbatasan sumber daya dan infrastruktur teknologi. Oleh karena itu, diperlukan penelitian yang mengkaji penerapan algoritma AES secara praktis dan sederhana agar dapat diimplementasikan pada UMKM.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menerapkan metode *Advanced Encryption Standard* (AES) dalam pengamanan data transaksi pada UMKM Warung Nasi Ibu Engkod. Penelitian ini diharapkan dapat memberikan solusi keamanan data yang efektif dan mudah diterapkan, serta menjadi referensi bagi UMKM lain dalam meningkatkan keamanan sistem informasi transaksi yang digunakan.

Selain penerapan algoritma kriptografi, evaluasi tingkat keamanan algoritma menjadi aspek penting dalam memastikan efektivitas pengamanan data. Pengujian kriptografi diperlukan untuk menilai tingkat difusi, sensitivitas terhadap perubahan input, serta tingkat keacakan data hasil enkripsi. Beberapa metode pengujian yang umum digunakan antara lain Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), dan entropi. Pengujian ini digunakan untuk memastikan bahwa algoritma AES yang diterapkan benar-benar mampu menghasilkan ciphertext yang sulit ditebak dan memiliki tingkat keamanan yang tinggi. Oleh karena itu, penelitian ini tidak hanya berfokus pada implementasi AES-256, tetapi juga pada pengujian kualitas keamanan hasil enkripsi data transaksi.

Metode Penelitian

Penelitian ini menggunakan desain penelitian *deskriptif* dengan pendekatan *eksperimental*, yang bertujuan untuk menerapkan dan menguji metode *Advanced Encryption Standard* (AES) dalam pengamanan data transaksi[10]. Rancangan kegiatan penelitian dimulai dengan analisis sistem transaksi yang digunakan oleh

UMKM, dilanjutkan dengan perancangan mekanisme pengamanan data, implementasi algoritma AES-256, serta pengujian hasil enkripsi dan dekripsi data transaksi.

Objek penelitian adalah data transaksi penjualan pada UMKM Warung Nasi Ibu Engkod yang meliputi data tanggal transaksi, jumlah transaksi, harga, dan total pembayaran. Ruang lingkup penelitian dibatasi pada pengamanan data transaksi yang tersimpan dalam basis data menggunakan algoritma AES dengan panjang kunci 256 bit.

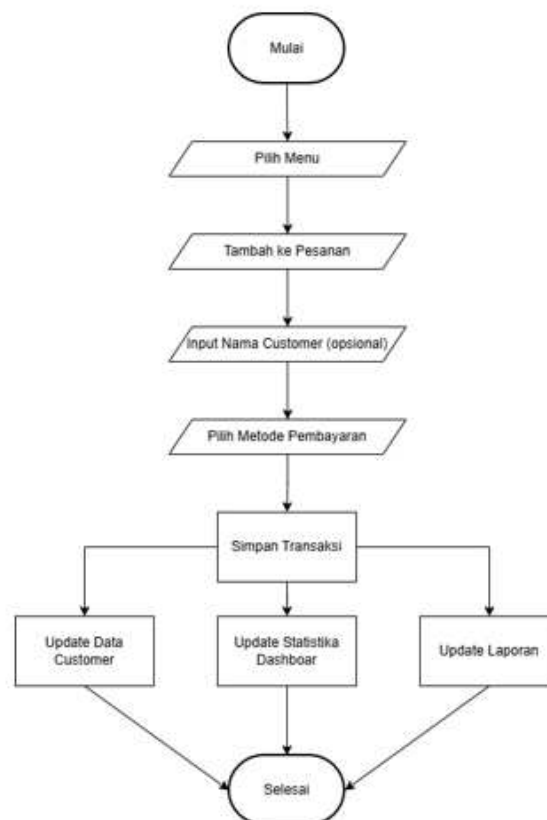
Penelitian ini dilaksanakan di UMKM Warung Nasi Ibu Engkod, dengan fokus pada sistem pencatatan transaksi yang digunakan dalam kegiatan operasional harian. Teknik pengumpulan data dilakukan melalui observasi langsung terhadap sistem transaksi yang berjalan serta studi dokumentasi terhadap data transaksi yang digunakan sebagai sampel penelitian.

Teknik analisis penelitian dilakukan dengan membandingkan data transaksi sebelum dan sesudah proses enkripsi menggunakan algoritma AES-256. Analisis difokuskan pada keberhasilan proses enkripsi dan dekripsi, serta kemampuan sistem dalam menjaga kerahasiaan data transaksi. Data hasil pengujian digunakan untuk menilai efektivitas penerapan metode AES dalam pengamanan data transaksi pada UMKM.

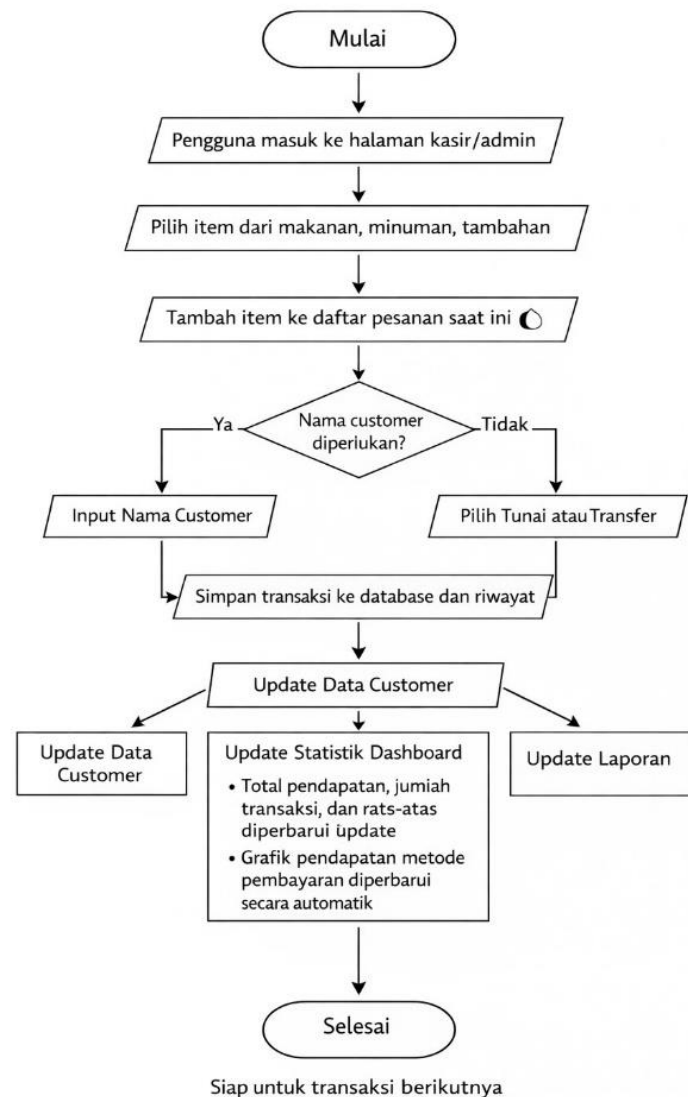
Hasil dan Pembahasan

Flowchart Pengamanan Data Transaksi Menggunakan AES-256

Flowchart ini menggambarkan alur pengamanan data transaksi menggunakan algoritma AES-256. Data transaksi yang dimasukkan ke dalam sistem akan dienkripsi terlebih dahulu sebelum disimpan ke dalam basis data. Data yang tersimpan hanya berupa ciphertext dan tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Ketika data diperlukan, sistem melakukan proses dekripsi untuk mengembalikan data ke bentuk aslinya.



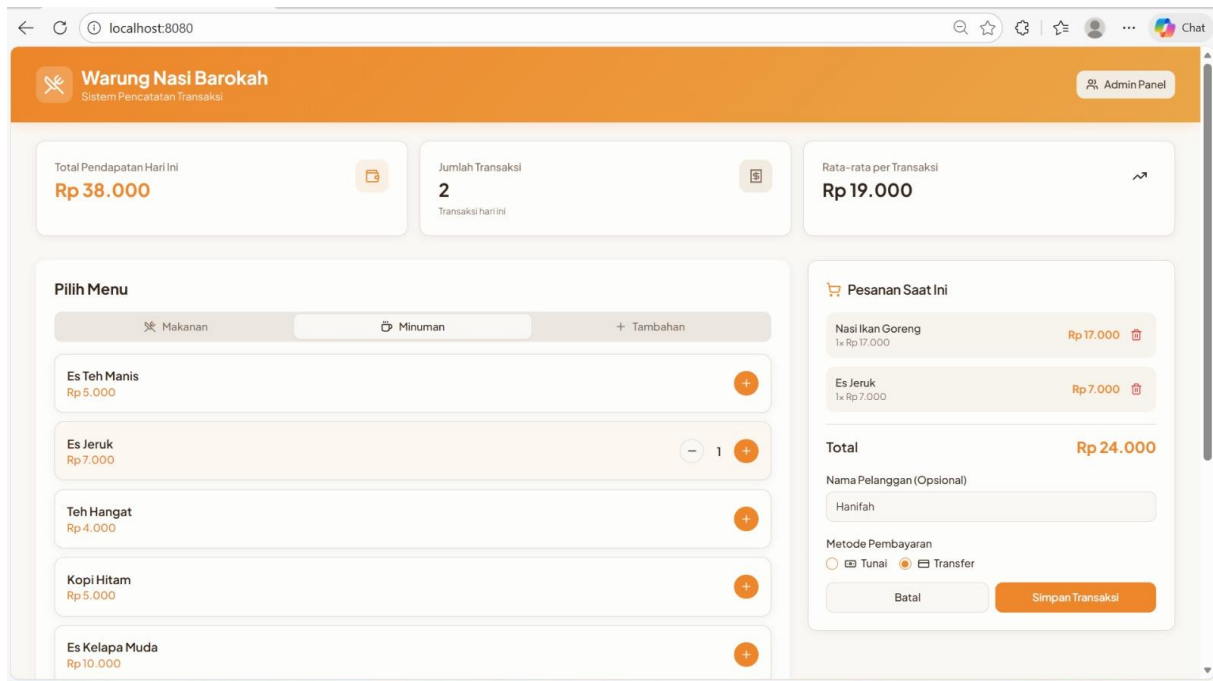
Gambar 1 Flowchart Proses Enkripsi Data Transaksi



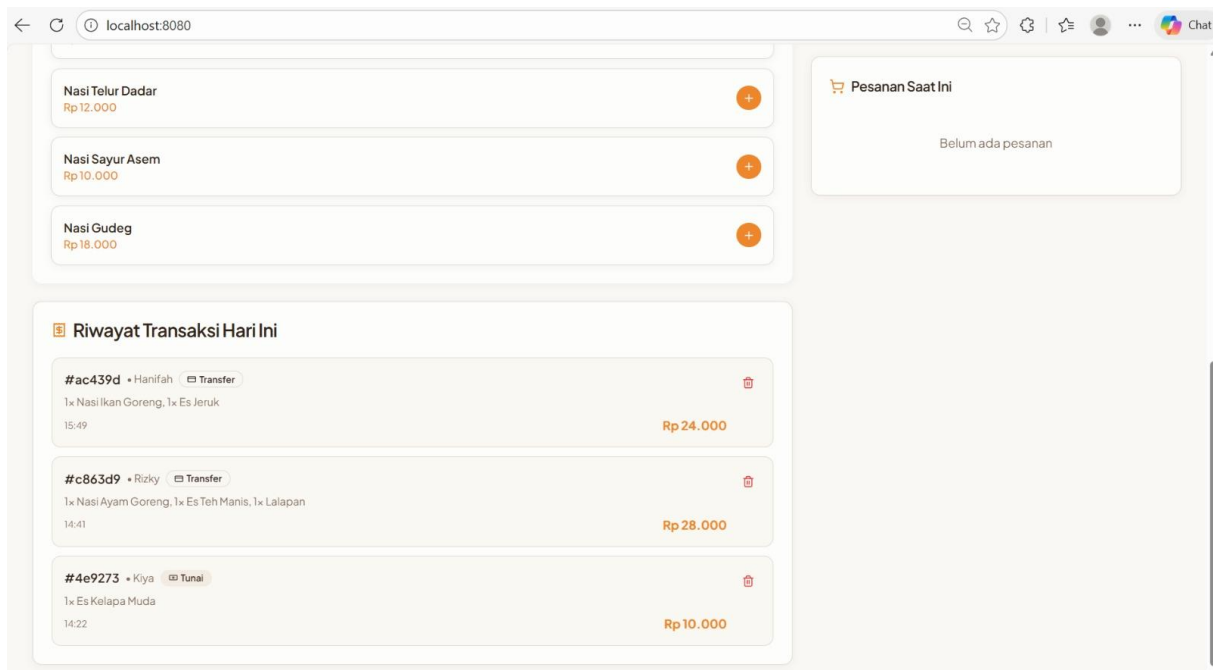
Gambar 2 Flowchart Proses Deskripsi Data Transaksi

Sistem Transaksi UMKM Warung Nasi Ibu Engkod

Gambar ini menampilkan keseluruhan alur sistem transaksi pada aplikasi web UMKM Warung Nasi Ibu Engkod, mulai dari input transaksi, dashboard, hingga riwayat transaksi harian. Kasir memasukkan data transaksi melalui halaman input, termasuk pilihan menu, jumlah pesanan, nama pelanggan, dan metode pembayaran. Data transaksi yang dimasukkan akan dienkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam basis data. Dashboard menampilkan ringkasan informasi transaksi seperti total pendapatan, pendapatan harian, jumlah transaksi, jumlah pelanggan, dan rata-rata transaksi. Bagian riwayat transaksi harian menampilkan daftar transaksi lengkap beserta nomor transaksi, nama pelanggan, metode pembayaran, waktu transaksi, dan total pembayaran. Seluruh data yang ditampilkan di dashboard dan riwayat transaksi hanya dapat diakses oleh sistem melalui proses dekripsi, sehingga keamanan dan kerahasiaan informasi transaksi tetap terjaga.



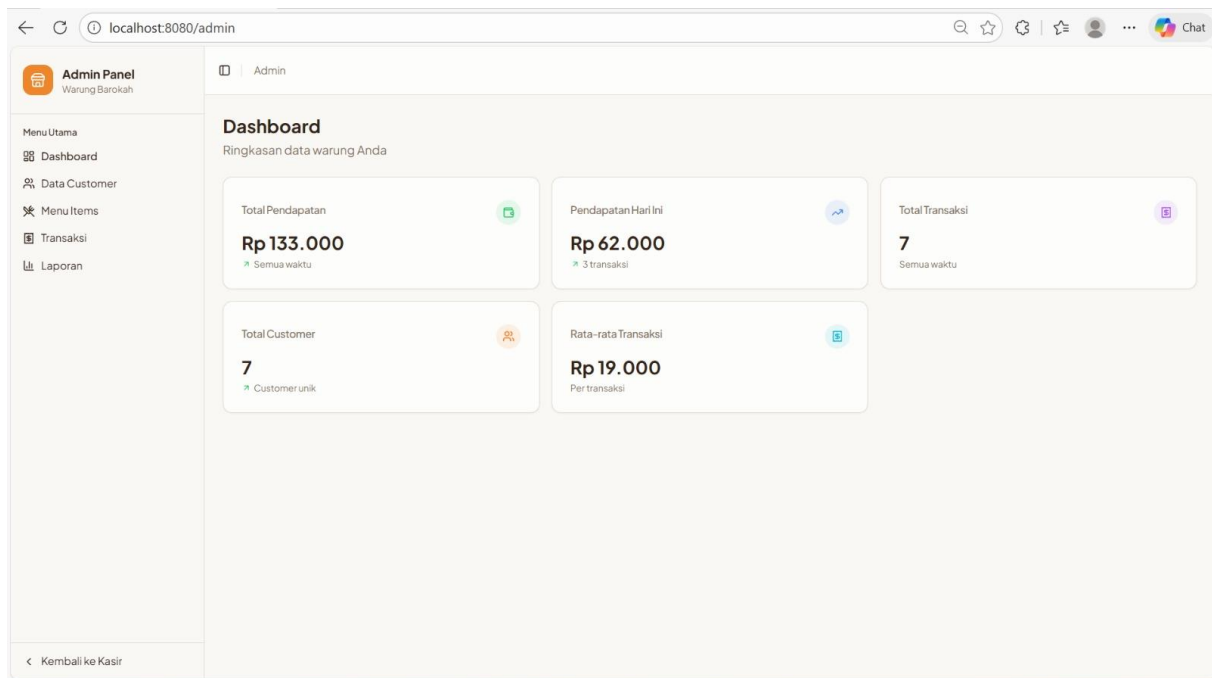
Gambar 3 Dashboard Admin Sistem Transaksi



Gambar 4 Halaman Riwayat Transaksi Harian

Dashboard Ringkasan Transaksi UMKM Warung Nasi Ibu Engkod

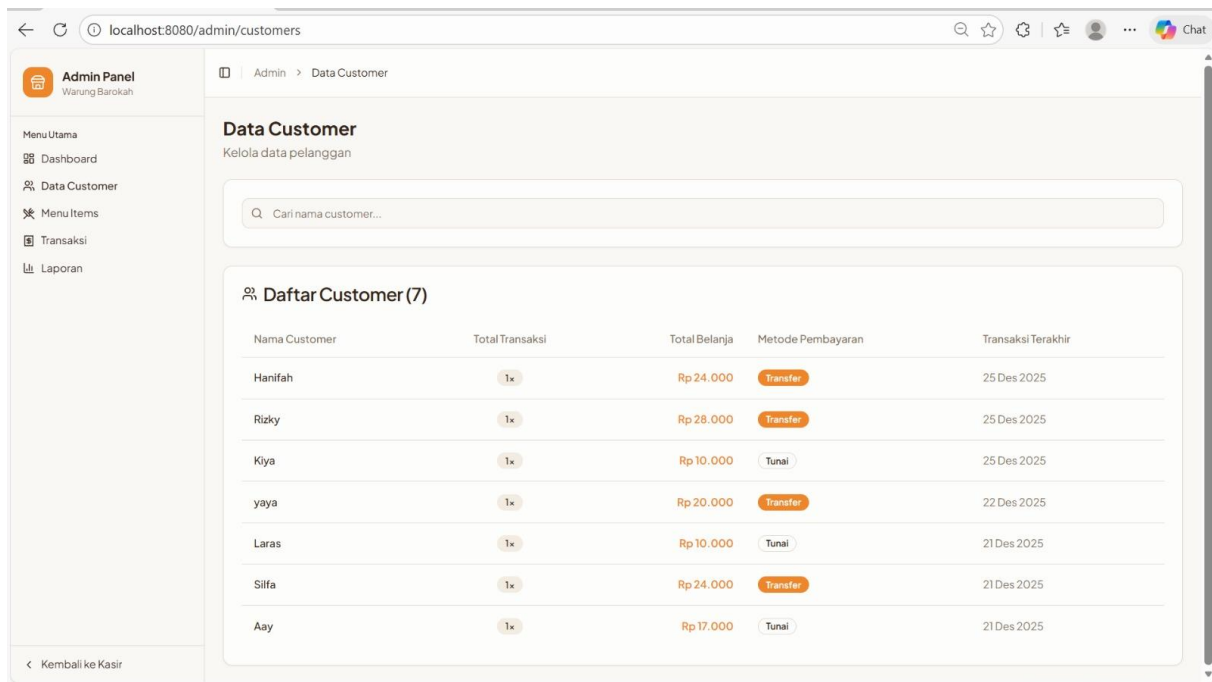
Gambar ini menampilkan ringkasan transaksi harian warung, termasuk total pendapatan, pendapatan harian, jumlah transaksi, jumlah pelanggan, dan rata-rata transaksi. Data yang ditampilkan berasal dari basis data transaksi yang telah diamankan menggunakan algoritma AES-256. Dengan tampilan ini, pemilik warung dapat memantau kinerja usaha secara cepat dan data tetap terjaga kerahasiaannya karena hanya dapat diakses melalui sistem yang sah.



Gambar 5 Dashboard Ringkasan Transaksi Warung

Tampilan Data Customer UMKM Warung Nasi Ibu Engkod

Gambar ini menampilkan daftar pelanggan warung beserta informasi penting, yaitu nama pelanggan, total transaksi yang telah dilakukan, total belanja, metode pembayaran yang digunakan, dan tanggal transaksi terakhir. Seluruh data customer yang tersimpan dalam sistem telah melalui proses enkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam basis data, sehingga hanya dapat diakses kembali melalui sistem dengan kunci dekripsi yang sah. Mekanisme ini menjamin kerahasiaan informasi pelanggan sekaligus memudahkan pemilik warung dalam memantau aktivitas dan riwayat transaksi tiap pelanggan.



Data Customer
Kelola data pelanggan

Cari nama customer...

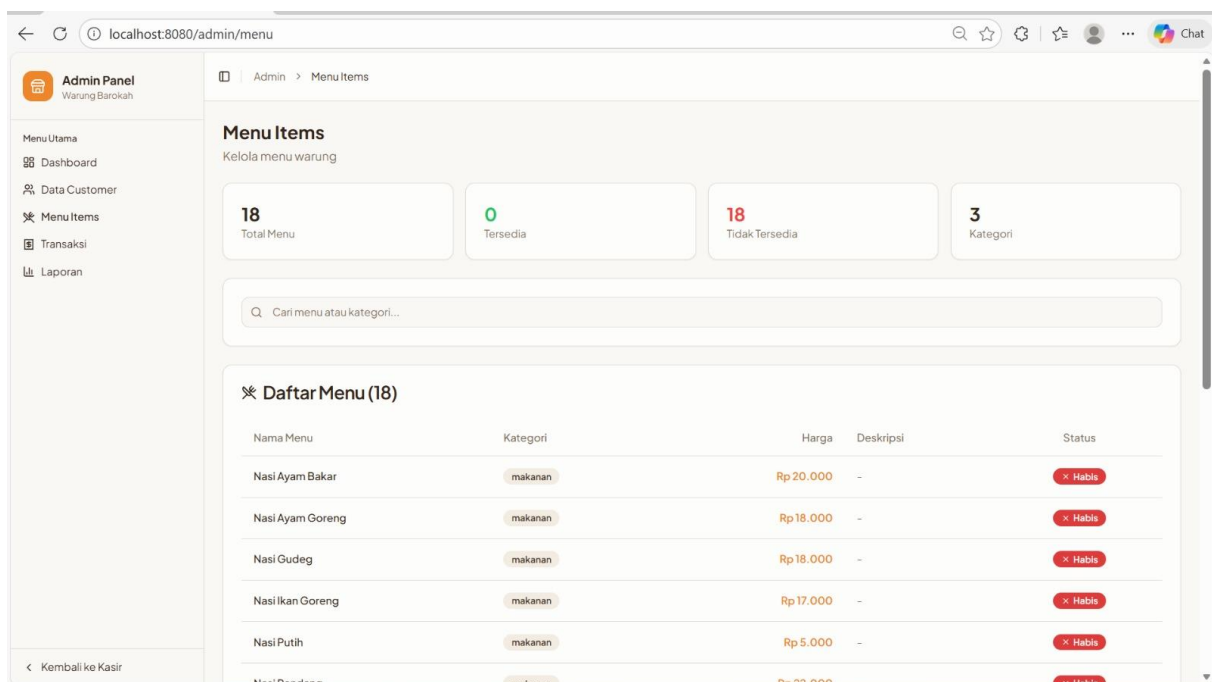
Daftar Customer (7)

Nama Customer	Total Transaksi	Total Belanja	Metode Pembayaran	Transaksi Terakhir
Hanifah	1x	Rp 24.000	Transfer	25 Des 2025
Rizky	1x	Rp 28.000	Transfer	25 Des 2025
Kiya	1x	Rp 10.000	Tunai	25 Des 2025
yaya	1x	Rp 20.000	Transfer	22 Des 2025
Laras	1x	Rp 10.000	Tunai	21 Des 2025
Silfa	1x	Rp 24.000	Transfer	21 Des 2025
Aay	1x	Rp 17.000	Tunai	21 Des 2025

Gambar 6 Data Customer Warung

Tampilan Menu Items UMKM Warung Nasi Ibu Engkod

Gambar ini menampilkan daftar menu yang tersedia di warung beserta harga masing-masing item. Menu items yang dipilih oleh kasir akan dimasukkan ke dalam transaksi, yang kemudian dienkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam basis data. Dengan mekanisme ini, seluruh informasi transaksi yang melibatkan menu items tetap aman dan tidak dapat diakses secara tidak sah, sambil memudahkan pemilik warung dalam pengelolaan stok dan penjualan.



Menu Items
Kelola menu warung

18 Total Menu

0 Tersedia

18 Tidak Tersedia

3 Kategori

Cari menu atau kategori...

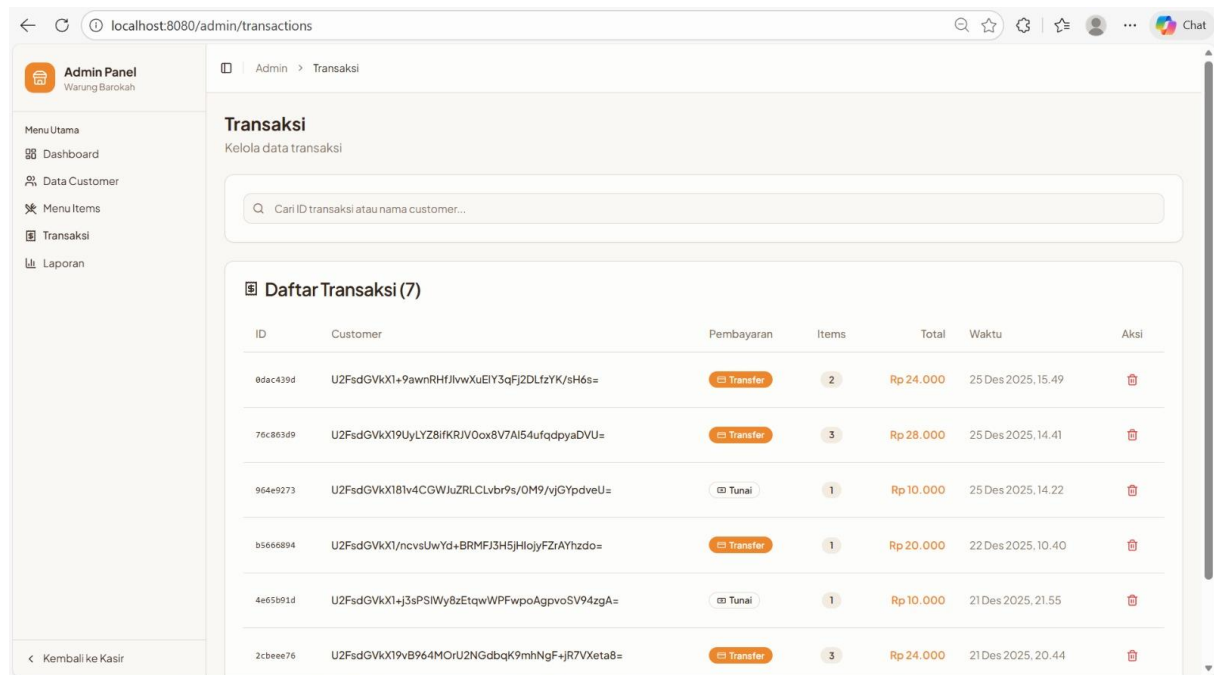
Daftar Menu (18)

Nama Menu	Kategori	Harga	Deskripsi	Status
Nasi Ayam Bakar	makanan	Rp 20.000	-	Habis
Nasi Ayam Goreng	makanan	Rp 18.000	-	Habis
Nasi Gudeg	makanan	Rp 18.000	-	Habis
Nasi Ikan Goreng	makanan	Rp 17.000	-	Habis
Nasi Putih	makanan	Rp 5.000	-	Habis
Nasi Rendang	makanan	Rp ?? 000	-	Habis

Gambar 7 Menu Items Warung

Tampilan Detail Transaksi Pelanggan UMKM Warung Nasi Ibu Engkod

Gambar ini menampilkan rincian transaksi pelanggan yang mencakup kolom ID transaksi, nama pelanggan, metode pembayaran, items yang dibeli, total pembayaran, dan waktu transaksi. Setiap data transaksi yang tercatat di sistem telah melalui proses enkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam basis data. Data hanya dapat dibaca kembali melalui proses dekripsi dengan kunci yang sah, sehingga menjamin keamanan dan kerahasiaan informasi transaksi sekaligus memudahkan pemilik warung dalam memantau riwayat transaksi secara rinci.

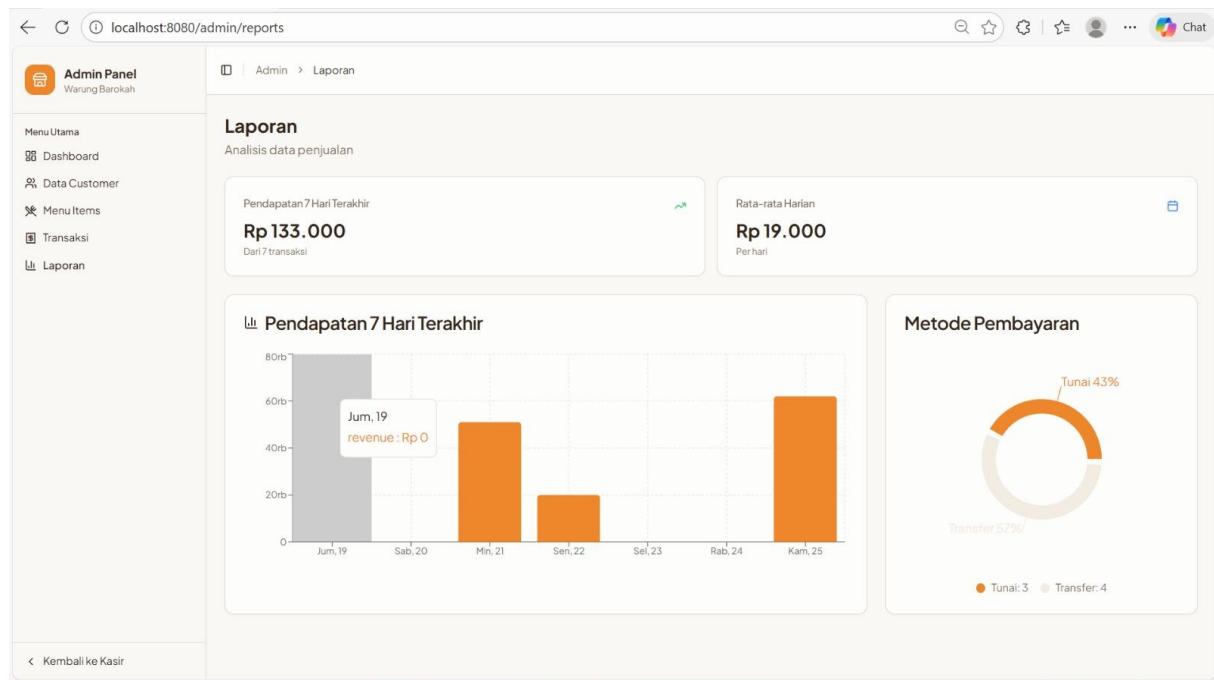


ID	Customer	Pembayaran	Items	Total	Waktu	Aksi
04ac439d	U2FsdGVkX1+9awnRHfJlwwXuEY3qFj2DLfzYK/sH6s=	Transfer	2	Rp 24.000	25 Des 2025, 15.49	[Aksi]
76c863d9	U2FsdGVkX19UyLYZ8ifKRJV0ox8V7Al54ufqdpyaDVU=	Transfer	3	Rp 28.000	25 Des 2025, 14.41	[Aksi]
964e9273	U2FsdGVkX18lv4CGWJuzRLCLvbr9s/0M9/ajGYpdveU=	Tunai	1	Rp 10.000	25 Des 2025, 14.22	[Aksi]
b5668894	U2FsdGVkX1ncvsUwYd+BRMFJ3H5jHlojyFZrAYhzdo=	Transfer	1	Rp 20.000	22 Des 2025, 10.40	[Aksi]
4e65b91d	U2FsdGVkX1+j3sPSIWY8zEtqwWPFwpoAgpvoSV94zgA=	Tunai	1	Rp 10.000	21 Des 2025, 21.55	[Aksi]
2cbeee76	U2FsdGVkX19vB964MOuU2NGdbqK9mhNgF+jR7VXeta8=	Transfer	3	Rp 24.000	21 Des 2025, 20.44	[Aksi]

Gambar 8 Detail Transaksi Pelanggan

Laporan Transaksi dan Statistik UMKM Warung Nasi Ibu Engkod

Gambar ini menampilkan ringkasan laporan transaksi harian warung, termasuk pendapatan 7 hari terakhir dan rata-rata pendapatan harian. Selain itu, terdapat diagram yang menunjukkan perbandingan pendapatan berdasarkan 7 hari terakhir dan metode pembayaran yang digunakan pelanggan. Seluruh data transaksi yang digunakan dalam laporan telah melalui proses enkripsi menggunakan algoritma AES-256 sebelum disimpan ke dalam basis data, sehingga hanya dapat diakses melalui proses dekripsi oleh sistem yang sah. Visualisasi ini membantu pemilik warung dalam memantau performa penjualan dan metode pembayaran secara aman dan efektif.



Gambar 9 Laporan Transaksi dan Statistik Warung

Pengujian Teks Kriptografi

Pengujian kriptografi pada penelitian ini dilakukan untuk mengetahui tingkat keamanan algoritma AES dalam mengamankan data teks pada sistem yang dikembangkan. Parameter pengujian yang digunakan meliputi Avalanche Effect, Character Error Rate (CER), Bit Error Rate (BER), dan Entropi. Keempat parameter tersebut digunakan untuk mengevaluasi tingkat difusi, sensitivitas perubahan, serta tingkat keacakan ciphertext yang dihasilkan.

Avalanche Effect

Avalanche Effect adalah salah satu metode pengujian dalam kriptografi yang menentukan seberapa baik suatu algoritma dengan mencari besar persentase pengubahan pesan pada saat proses enkripsi dilakukan. Hal ini dilakukan dengan melihat rasio antara jumlah bit pada ciphertext yang berubah dan jumlah bit dari plaintext sebelum diubah. Perubahan bit sebesar 45-60% menunjukkan bahwa pengujian Avalanche Effect dianggap baik, dimana 50% adalah hasil yang dianggap baik dalam pengujian. Perhitungan avalanche effect dapat dilihat dalam persamaan[14].

$$AE = \frac{\text{Jumlah Perubahan Bit}}{\text{Jumlah Total Bit}} \times 100\%$$

Jika diketahui dalam sebuah proses enkripsi memiliki jumlah perubahan bit sebesar 198 bit dari total bit pada ciphertext sebesar 352 bit, maka persentase Avalanche Effect adalah sebagai berikut :

$$AE = \frac{198}{352} \times 100\% = 56.25\%$$

Berdasarkan hasil perhitungan, algoritma AES menghasilkan nilai Avalanche Effect sebesar 56.25%, yang menunjukkan bahwa perubahan kecil pada plaintext menyebabkan perubahan besar pada ciphertext. Hal ini membuktikan bahwa algoritma AES memiliki tingkat difusi yang baik dan layak digunakan untuk pengamanan data teks.

Character Error Rate

Character Error Rate (CER) merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mengukur tingkat perubahan karakter antara plaintext dan ciphertext hasil proses enkripsi. Pengujian ini bertujuan untuk mengetahui seberapa sensitif algoritma enkripsi terhadap perubahan input. Semakin besar nilai CER yang dihasilkan, maka semakin tinggi tingkat perubahan karakter yang terjadi, sehingga menunjukkan bahwa algoritma memiliki tingkat keamanan yang baik.

Perhitungan CER dilakukan dengan membandingkan jumlah karakter yang berbeda antara plaintext dan ciphertext terhadap jumlah total karakter yang dikirim. Rumus Character Error Rate dituliskan sebagai berikut:

$$CER = \frac{\text{Jumlah Karakter Berbeda}}{\text{Jumlah Karakter yang Dikirim}} \times 100\%$$

Jika terdapat 37 karakter yang berbeda dari total karakter yang dikirim sebanyak 44 karakter, maka didapatkan perhitungan sebagai berikut :

$$CER = \frac{37}{44} \times 100\% = 84.09\%$$

Nilai CER yang tinggi menunjukkan ciphertext sangat sensitif terhadap perubahan input.

Bit Error Rate

Bit Error Rate merupakan salah satu metode pengujian dalam kriptografi yang digunakan untuk mencari besar persentase bit yang dilakukan dengan cara membandingkan jumlah bit yang salah dengan total bit pada saat melakukan penyisipan. BER dikatakan baik jika nilainya mendekati 0, yang menyatakan tidak adanya perbedaan antara ciphertext dan plaintext. Perhitungan BER dinyatakan dalam persamaan [11].

$$BER = \frac{\text{Jumlah Bit Error}}{\text{Jumlah Total Bit}} \times 100\%$$

Misalnya terdapat 198 bit yang salah dari total 352 bit, maka diperoleh perhitungan sebagai berikut:

$$BER = \frac{198}{352} \times 100\% = 56.25\%$$

Nilai BER di atas 50% menunjukkan tingkat difusi AES sangat baik dan memenuhi standar kriptografi.

Entropi

Entropi merupakan sebuah konsep kriptografi yang berfungsi untuk memperkirakan jumlah bit rata-rata dalam pengkodean pesan [12]. Besaran entropi dinyatakan dalam satuan bit. Cara menghitung entropi dituliskan dalam persamaan [13] berikut.

$$H = - \sum_{i=1}^n p(k) \log_2 (p(k))$$

Rumus menghitung probabilitas setiap karakter:

$$P(k) = \frac{\text{Jumlah kemunculan karakter ke } - i}{\text{Jumlah Total Karakter}}$$

Jika terdapat karakter U muncul 3 kali dengan jumlah total karakter 32, maka diperoleh perhitungan sebagai berikut:

$$P(k) = \frac{3}{32} = 0.09375$$

$$H = - \sum_{i=1}^3 p(k) \log_2 (p(k)) = -(0.09375 \times \log_2 0.09375) = 0.318$$

$$H = 0.318 + 0.295 + 0.281 = 4.98$$

Hasil pengujian entropi menunjukkan bahwa ciphertext hasil enkripsi menggunakan algoritma AES memiliki nilai entropi sebesar 4.98, yang mendekati nilai maksimum. Hal ini menunjukkan bahwa data hasil enkripsi bersifat acak dan sulit diprediksi, sehingga meningkatkan tingkat keamanan sistem.

Kesimpulan

Penerapan algoritma Advanced Encryption Standard (AES) dengan panjang kunci 256 bit pada sistem transaksi UMKM Warung Nasi Ibu Engkod terbukti efektif dalam menjaga keamanan dan kerahasiaan data transaksi serta data pelanggan. Sistem web yang terintegrasi, meliputi fitur input transaksi, dashboard ringkasan, pengelolaan data pelanggan, menu items, serta laporan statistik, mampu memproses dan menyimpan data dalam bentuk terenkripsi sehingga informasi yang tersimpan di dalam basis data tidak dapat dibaca tanpa kunci dekripsi yang sah. Hal ini memastikan kerahasiaan dan integritas data tetap terjaga sekaligus mendukung kemudahan pengelolaan transaksi secara real-time.

Hasil pengujian keamanan teks kriptografi menunjukkan bahwa algoritma AES-256 menghasilkan ciphertext dengan tingkat keamanan yang tinggi. Nilai Avalanche Effect sebesar 56.25% menunjukkan tingkat difusi yang baik, di mana perubahan kecil pada plaintext menghasilkan perubahan signifikan pada ciphertext. Selain itu, nilai Character Error Rate (CER) sebesar 84.09% dan Bit Error Rate (BER) sebesar 56.25% mengindikasikan tingginya sensitivitas algoritma terhadap perubahan input, yang mencerminkan kekuatan proses enkripsi. Pengujian entropi menghasilkan nilai 4.98, yang mendekati nilai maksimum, menandakan bahwa ciphertext bersifat acak dan sulit diprediksi.

Berdasarkan hasil implementasi dan pengujian tersebut, algoritma AES-256 dapat disimpulkan sebagai solusi pengamanan data yang efektif dan efisien untuk sistem transaksi UMKM. Algoritma ini mampu menggabungkan tingkat keamanan yang tinggi dengan implementasi yang ringan, sehingga layak diterapkan pada sistem digital UMKM. Penelitian ini diharapkan dapat menjadi acuan bagi pengembangan sistem informasi UMKM lainnya serta sebagai dasar untuk penambahan mekanisme keamanan lanjutan di masa mendatang.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada dosen mata kuliah Kriptografi Program Studi Teknik Informatika Universitas Pelita Bangsa yang telah memberikan arahan, masukan, dan proses penelaahan (review) terhadap penelitian ini. Selain itu, penulis juga menyampaikan apresiasi kepada pihak UMKM Warung Nasi Ibu Engkod atas dukungan dan ketersediaan data yang digunakan dalam penelitian. Terima kasih juga kepada rekan-rekan yang telah berpartisipasi dan berkontribusi dalam proses penyusunan jurnal ini, baik dalam pengumpulan data, perancangan sistem, implementasi algoritma, maupun penyempurnaan penulisan, sehingga penelitian ini dapat diselesaikan dengan baik. Semoga hasil penelitian ini dapat memberikan kontribusi bagi pengembangan penerapan kriptografi pada sistem informasi UMKM.

Daftar Rujukan

- [1] S. Transaction and D. Security, "Penerapan Advanced Encryption Standard pada Aplikasi Payment Gateway untuk Keamanan Data Transaksi Penjualan," vol. 24, no. 1, pp. 248–259, 2025.

- [2] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," vol. 4, no. 1, 2022, doi: 10.47065/josyc.v4i1.2451.
- [3] M. I. Rifki and N. Syamia, "Message Security Application Using Mobile-Based AES Algorithm," vol. 5, no. 2, pp. 595–606, 2024, doi: 10.30596/jcositte.v5i2.20834.
- [4] P. S. Ramadhan, M. Syahril, R. Kustini, H. Winata, and R. D. Gea, "CESS Pengamanan Data Transaksi Menggunakan AES dan RC4 Transaction Data Security Using AES and RC4," vol. 8, no. January, pp. 60–70, 2023.
- [5] E. Alvizar Dayusman, A. Alimudin, and T. Hidayat, "Kemanusiaan Dan Kesejahteraan Sosial Dalam Pemikiran Islam Kontemporer," *TAJDID J. Pemikir. Keislam. dan Kemanus.*, vol. 7, no. 1, pp. 118–134, 2023, doi: 10.52266/tajdid.v7i1.1759.
- [6] U. S. Utara and U. S. Utara, "JITE (Journal of Informatics and Telecommunication Engineering)," vol. 8, no. January, pp. 152–164, 2025.
- [7] M. Tania, T. S. Alasi, and R. Yap, "Algoritma Aes Untuk Keamanan Data Digital Berbasis Web Di Kantor Desa Aman Damai," *J. TIMES*, vol. 13, no. 2, pp. 142–149, 2024, doi: 10.51351/jtm.13.2.2024781.
- [8] 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," *J. Syst. Comput. Eng.*, vol. 6, no. 1, pp. 1–9, 2025, doi: 10.61628/jsce.v6i1.1511.
- [9] A. Farissi, A. Pradata, and K. Miraswan, "Securing Messages Using AES Algorithm and Blockchain Technology on Mobile Devices," *Sinkron*, vol. 8, no. 2, pp. 1166–1171, 2023, doi: 10.33395/sinkron.v8i2.12381.
- [10] J. L. Calpito, P. L. Olanday, and A. C. Gallarde, "Application of Advanced Encryption Standard in the computer or handheld online year-round registration system," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 2, pp. 922–935, 2022, doi: 10.11591/ijeecs.v27.i2.pp922-935.
- [11] C. A. Sari and W. S. Sari, "Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna," vol. 13, no. 1, pp. 45–58, 2022.
- [12] L. B. Handoko and C. Umam, "Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting," *Pros. Sains Nas. dan Teknol.*, vol. 12, no. 1, p. 390, Nov. 2022.
- [13] E. H. Rachmawanto and C. A. Sari, "Gabungan Advanced Encryption Standard Dan Vigenere Cipher Untuk Pengamanan Dokumen Digital," *J. Inform. Polinema*, vol. 8, no. 4, pp. 1–8, 2022.
- [14] Karima, N. A., Aisyah, A. N., Silla, H. V., Handoko, L. B., & Sani, R. R. (2024). Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit. *Jurnal Masyarakat Informatika*, 15(1), 1-13.
- [15] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19 like pandemics," *IEEE Network*, vol. 34, no. 4, pp. 126–132, 2020.