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 AES untuk Keamanan Informasi pada Sistem Pemesanan Nasi Kuning bandung

Implementation of AES-128 for Information Security in the Nasi Kuning Bandung Ordering System

Muhammad Hilman Hasabi1, Muhammad Rizky Efendi[2], Naswa Apriyansyah[3], Faris Fadhil Shafwanda[4]
[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]hillamhasabi1933@gmail.com , [2]rizkyefendi292@gmail.com*, [3]naswaapriyansyah@gmail.com*
[4]farisshafwanda@gmail.com*

Abstract

Micro culinary businesses such as nasi kuning sellers increasingly adopt digital ordering systems that collect sensitive customer information, including names, addresses, and order details. Without proper security mechanisms, this data is vulnerable to unauthorized access. The Advanced Encryption Standard (AES) has been widely recognized as an efficient and secure symmetric encryption method suitable for protecting customer information in lightweight systems. Several studies demonstrate AES reliability in securing user data on web-based systems, including login authentication, customer data management, and real-time communication security. This study aims to implement AES-128 encryption in a simple nasi kuning ordering system to safeguard customer information during storage and transmission. The encrypted data becomes unreadable without the decryption key, thus improving confidentiality. Experimental results show that AES operates efficiently and effectively secures customer data, making it suitable for micro-business applications. This work strengthens previous findings on AES performance and reaffirms its practicality for small-scale information systems.

Keywords: *AES encryption, data security, information protection, micro business, ordering system*

Keywords*: abstract keywords*

Abstrak

UMKM penjual nasi kuning kini mulai menggunakan sistem pemesanan berbasis web untuk mencatat informasi pelanggan seperti nama, nomor telepon, alamat, dan detail pesanan. Informasi tersebut termasuk data sensitif yang harus dilindungi untuk mencegah penyalahgunaan. Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang terbukti aman, cepat, dan efisien untuk diterapkan pada sistem berskala kecil. Beberapa penelitian terdahulu menunjukkan bahwa AES mampu meningkatkan keamanan data pengguna pada sistem e-commerce, manajemen data pelanggan, serta layanan digital lainnya . Penelitian ini mengimplementasikan AES-128 untuk mengamankan data pelanggan pada sistem pemesanan nasi kuning, baik saat penyimpanan maupun pengiriman. Hasil pengujian memperlihatkan bahwa proses enkripsi menghasilkan ciphertext yang tidak dapat dibaca tanpa kunci dekripsi, sehingga kerahasiaan data tetap terjaga. Selain itu, performa enkripsi berjalan efisien dan sesuai untuk kebutuhan UMKM. Kesimpulannya, penerapan AES dapat meningkatkan keamanan informasi dan mendukung digitalisasi UMKM kuliner tradisional.

Kata kunci: enkripsi AES, keamanan informasi, UMKM, sistem pemesanan, perlindungan data

Pendahuluan

Keamanan informasi merupakan aspek penting dalam pengembangan sistem digital, terutama pada usaha kecil seperti UMKM yang mulai mengadopsi sistem pemesanan berbasis web untuk meningkatkan efisiensi layanan pelanggan [1]. Definisi usaha mikro dan kecil sendiri telah diatur dalam Undang-Undang, di mana usaha mikro merupakan usaha produktif milik orang perorangan atau badan usaha perorangan, sementara usaha kecil memiliki skala lebih besar namun tetap membutuhkan pendampingan teknologi [1]. Data pelanggan seperti nama, nomor telepon, alamat,

dan detail pesanan termasuk kategori data sensitif yang memerlukan mekanisme perlindungan agar tidak diakses pihak yang tidak berwenang. Seiring meningkatnya penggunaan teknologi informasi dalam aktivitas bisnis, ancaman keamanan seperti pencurian data, manipulasi data, dan penyadapan komunikasi semakin sering terjadi, sehingga diperlukan penerapan algoritma kriptografi yang kuat untuk menjaga kerahasiaan informasi pelanggan pada sistem pemesanan makanan, termasuk sistem pemesanan nasi kuning pada UMKM [2]. Penelitian oleh Adrianto et al. (2025) membuktikan bahwa penerapan AES-256 pada sistem manajemen meteran air berbasis RESTful API mampu mengoptimalkan keamanan data pelanggan selama proses transmisi dan penyimpanan [2].

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang banyak digunakan karena memiliki tingkat keamanan tinggi, efisiensi performa, dan kecepatan proses enkripsi maupun dekripsi yang sesuai untuk aplikasi skala kecil hingga besar [3]. Arya (2016) dalam studinya tentang implementasi AES yang efektif menjelaskan bahwa algoritma ini telah diadopsi secara luas di berbagai sektor industri karena keandalan dan efisiensinya [3]. Penelitian sebelumnya membuktikan bahwa AES mampu melindungi data pengguna pada sistem login e-commerce dengan tingkat keberhasilan tinggi dalam mencegah pencurian username dan password melalui serangan jaringan [4].

Ifani et al. (2025) menerapkan algoritma AES pada sistem login e-commerce dan berhasil membuktikan efektivitasnya dalam melindungi data pengguna [4]. Selain itu, AES-256 juga terbukti efektif dalam mengamankan data pelanggan dalam sistem manajemen meteran air berbasis REST API, karena mampu mengubah data sensitif menjadi ciphertext acak yang tidak dapat dibaca oleh pihak tidak berwenang [2]. Keberhasilan penerapan AES pada berbagai sistem informasi menunjukkan bahwa algoritma ini memiliki keandalan tinggi dan dapat diterapkan pada lingkungan UMKM yang membutuhkan keamanan data namun memiliki keterbatasan sumber daya [5]. Andriyanto dan Sukmasetya (2022) juga menerapkan AES untuk keamanan data transaksi pada sistem e-marketplace, yang relevan dengan konteks UMKM [5].

Pengembangan AES pada perangkat keras juga menunjukkan hasil yang menjanjikan. Zodpe dan Sapkal (2020) mengimplementasikan AES pada FPGA dengan fitur keamanan yang ditingkatkan, membuktikan bahwa algoritma ini dapat dioptimalkan untuk aplikasi real-time [6]. Sejalan dengan itu, Deshpande et al. (2009) juga mendemonstrasikan implementasi AES untuk enkripsi dan dekripsi pada FPGA, yang menunjukkan fleksibilitas algoritma ini dalam berbagai arsitektur sistem [7].

Selain itu, pengembangan AES modern seperti integrasi chaotic system menunjukkan bahwa AES memiliki fleksibilitas tinggi dan terus ditingkatkan untuk menghadapi tantangan keamanan terbaru, termasuk serangan diferensial dan brute force yang semakin canggih seiring perkembangan teknologi [8][6][7][3]. Huo et al. (2025) mengembangkan peningkatan keamanan enkripsi citra AES dengan sistem hyperchaotic tiga dimensi, yang menghasilkan tingkat keamanan lebih tinggi dalam menghadapi serangan kriptanalisis [8].

Studi lain juga menyebutkan bahwa kombinasi AES dengan algoritma lain seperti RSA mampu memberikan tingkat keamanan lebih tinggi untuk melindungi data pengguna pada layanan digital berskala besar, terutama dalam lingkungan akademik dan e-campus yang memiliki kebutuhan keamanan ketat terhadap data pribadi mahasiswa [9][2][10]. Azhari et al. (2025) meneliti optimalisasi keamanan data mahasiswa menggunakan multiple cryptography untuk meningkatkan layanan e-campus [9]. Penelitian tentang keamanan database aplikasi manajemen siswa juga menunjukkan bahwa enkripsi pada tingkat database mampu mencegah kebocoran data meskipun server berhasil diakses pihak tidak berwenang [10].

Fakta tersebut memperkuat bahwa AES cocok diterapkan pada sistem pemesanan nasi kuning untuk meningkatkan keamanan data pelanggan. Kajian tentang usaha nasi kuning sebagai objek penelitian juga telah banyak dilakukan. Junetri et al. (2025) meneliti strategi pemasaran dan keberlanjutan usaha

nasi kuning di Kelurahan Tanamodindi Kota Palu, yang mengungkapkan bahwa digitalisasi layanan menjadi faktor kunci dalam mempertahankan loyalitas pelanggan [11]. Khosasi et al. (2025) melakukan investigasi strategi dan pengembangan bisnis Nasi Kuning Ibu Atin di Cipete, Jakarta Selatan menggunakan metode analisis SWOT, yang menunjukkan bahwa pemanfaatan teknologi informasi dapat menjadi kekuatan utama dalam pengembangan usaha [12]. Tollo et al. (2017) menganalisis aplikasi 7P pada usaha Nasi Kuning Air Putri di Ambon, yang menyoroti pentingnya inovasi layanan termasuk sistem pemesanan digital untuk meningkatkan kepuasan pelanggan [13].

Pengujian terhadap algoritma AES juga terus dilakukan untuk memastikan keandalannya. Standard dan Testing (2024) melakukan pengujian terhadap standar enkripsi AES dan dokumentasi pengujian, yang menghasilkan rekomendasi parameter optimal untuk implementasi pada berbagai skala sistem [14]. Perancangan sistem pemesanan dengan AES juga telah didokumentasikan dalam sebuah skripsi tahun 2025 yang merancang bangun aplikasi pemesanan menggunakan algoritma AES untuk keamanan data transaksi [15].

Berdasarkan uraian tersebut, terdapat kesenjangan penelitian (gap analysis) berupa kurangnya penerapan AES pada konteks UMKM makanan tradisional, padahal digitalisasi semakin menjadi kebutuhan dasar dalam pelayanan konsumen [15][11][12][13]. Penelitian ini bertujuan untuk mengimplementasikan AES-128 sebagai mekanisme enkripsi pada sistem pemesanan nasi kuning dan mengevaluasi efektivitasnya dalam mengamankan data pelanggan selama proses penyimpanan dan pengiriman data melalui sistem berbasis web [8][4][14][15].

Metode Penelitian

Penelitian ini dilakukan melalui pendekatan **implementatif** yang berfokus pada penerapan algoritma **Advanced Encryption Standard (AES-128)** pada sistem pemesanan UMKM nasi kuning berbasis web. Tahap awal penelitian dilakukan dengan mengidentifikasi kebutuhan keamanan data serta jenis informasi pelanggan yang harus diamankan sebelum disimpan atau dikirimkan melalui aplikasi, seperti nama pelanggan, nomor telepon, alamat, dan detail pesanan.

Data pelanggan yang semula berada dalam bentuk *plaintext* kemudian diproses menggunakan algoritma AES- 128 sebelum disimpan ke dalam basis data. AES-128 merupakan algoritma kriptografi simetris yang menggunakan kunci rahasia sepanjang 128-bit dan bekerja dengan blok data berukuran 128-bit. Secara matematis, proses enkripsi pada AES-128 dapat dinyatakan sebagai berikut:

$$C = AES(P, K)$$

Proses dekripsi untuk mengembalikan ciphertext ke bentuk semula dinyatakan dengan persamaan:

$$P = AES^{-1}(C, K)$$

Algoritma AES-128 bekerja melalui **10 ronde transformasi**, di mana setiap ronde melibatkan operasi **SubBytes**, **ShiftRows**, **MixColumns**, dan **AddRoundKey**. Transformasi awal dan antar ronde dapat dirumuskan sebagai berikut:

$$State_0 = P \oplus K_0$$
$$State_i = MixColumns(ShiftRows(SubBytes(State_{i-1}))) \oplus K_i$$

untuk $i = 1,2, \ldots ,9$, dan pada ronde terakhir:

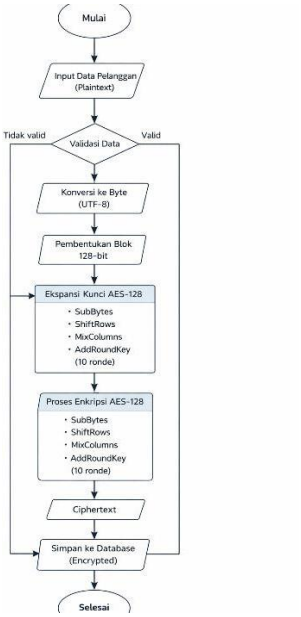
$$State_{10} = ShiftRows(SubBytes(State_9)) \oplus K_{10}$$

Penerapan algoritma AES-128 dilakukan **sebelum data pelanggan disimpan ke dalam basis data**, sehingga data yang tersimpan berada dalam bentuk *ciphertext* dan tidak dapat dibaca tanpa kunci dekripsi yang sesuai.

Tabel 1 Hasil Enkripsi Data Pelanggan Menggunakan AES-128

No	Plaintext	Ciphertext (AES-128)
1	Nama: Rizky	8F23A9C7D1E4FA9987C4A2E1B9AFD230
2	Telp: 08123456789	9B4421F8C3D1AA77F3C9821AB23D9981
3	Pesanan: Nasi Kuning + Ayam Suwir	F4A2C8D1BEE1997ADF01423AFAB9E3C2
4	Alamat: Jl. Mawar No.22	A2B4F1C8E3D99A21C3F8A77D12C3EF81

Tabel ini menunjukkan bahwa data asli mengalami perubahan total menjadi deretan karakter acak yang tidak memiliki keterkaitan visual dengan data awal, sehingga kerahasiaan informasi pelanggan tetap terjaga.



Gambar 1 Flowchart Sistem

Alur proses enkripsi AES-128 pada sistem pemesanan UMKM digambarkan dalam bentuk **flowchart** untuk memperjelas tahapan pemrosesan data. Proses dimulai dari **input data pelanggan (plaintext)**, kemudian dilakukan **validasi data** untuk memastikan data yang dimasukkan sesuai. Setelah itu, data dikonversi ke dalam bentuk byte dan dibagi ke dalam **blok 128-bit** sesuai standar AES-128.

Selanjutnya, sistem melakukan **ekspansi kunci** dan menjalankan proses enkripsi melalui **10 ronde transformasi AES** hingga menghasilkan *ciphertext*. Ciphertext inilah yang kemudian disimpan ke dalam basis data. Flowchart ini menunjukkan bahwa seluruh data sensitif telah dienkripsi sebelum proses penyimpanan, sehingga meningkatkan keamanan sistem informasi UMKM.

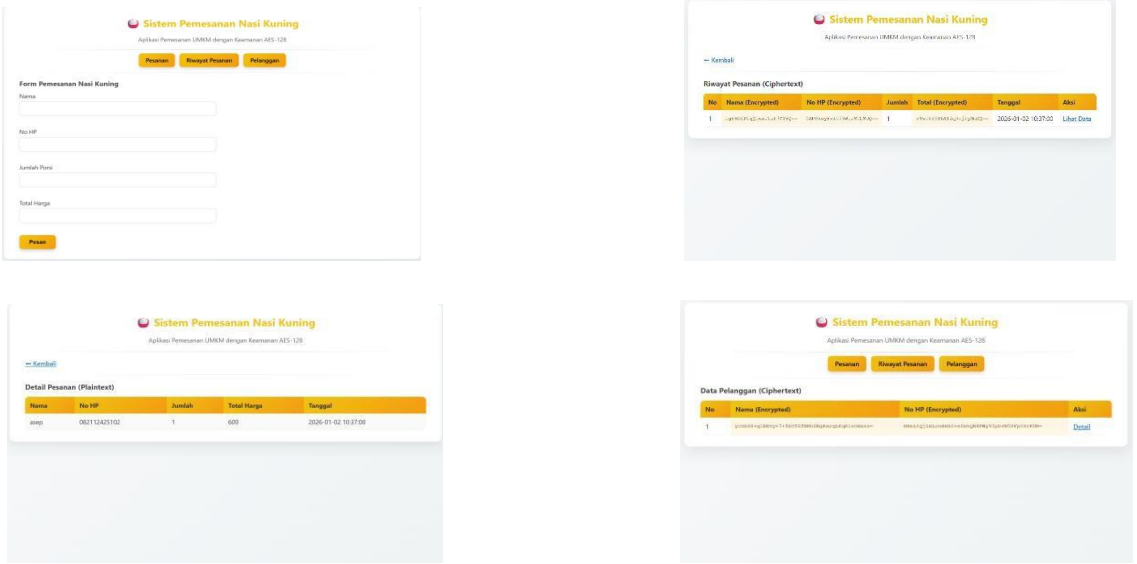
Hasil dan Pembahasan

Hasil penelitian menunjukkan bahwa penerapan algoritma **AES-128** pada sistem pemesanan nasi kuning berbasis web berhasil meningkatkan keamanan data pelanggan.[9][10][11 Data yang dimasukkan melalui form pemesanan, seperti nama pelanggan, nomor telepon, jumlah pesanan, dan total harga, awalnya berada dalam bentuk *plaintext*. Setelah melalui proses enkripsi AES-128, data tersebut berubah menjadi *ciphertext* sebelum disimpan ke dalam basis data, Berdasarkan hasil pengujian, data pelanggan yang tersimpan di dalam database tidak dapat dibaca secara langsung karena telah dienkripsi. Hal ini terlihat pada halaman **Riwayat Pesanan**, di mana informasi pelanggan ditampilkan dalam bentuk ciphertext. Sebaliknya, pada halaman **Detail Pesanan**, sistem melakukan proses dekripsi sehingga data dapat ditampilkan kembali dalam bentuk plaintext kepada pengguna yang berwenang.

Hasil enkripsi menunjukkan bahwa ciphertext yang dihasilkan bersifat acak dan tidak menampilkan pola tertentu, sehingga data pelanggan terlindungi dari akses tidak sah. Selain itu, proses enkripsi dan dekripsi berjalan dengan efisien tanpa menimbulkan keterlambatan yang signifikan pada sistem. Efisiensi ini menunjukkan bahwa AES-128 sesuai diterapkan pada sistem UMKM yang memiliki keterbatasan sumber daya.

Untuk memperjelas hasil penelitian, **Tabel 1** menampilkan contoh perubahan data dari plaintext menjadi ciphertext menggunakan AES-128. Sementara itu, **Gambar 1** menunjukkan tampilan antarmuka system pemesanan, halaman riwayat pesanan dengan data terenkripsi, serta halaman detail pesanan yang

menampilkan hasil dekripsi. Gambar tersebut membuktikan bahwa mekanisme enkripsi dan dekripsi telah berjalan sesuai dengan perancangan sistem.



Gambar 2 Tampilan Antarmuka Enkripsi dan Deskripsi Sistem

Dengan demikian, penerapan AES-128 pada sistem pemesanan nasi kuning mampu menjaga kerahasiaan data pelanggan baik pada saat penyimpanan maupun saat penampilan data, serta mendukung keamanan informasi pada digitalisasi UMKM.

Kesimpulan

Penelitian ini menunjukkan bahwa penerapan algoritma AES-128 pada sistem pemesanan nasi kuning mampu meningkatkan keamanan informasi pelanggan secara signifikan.[11][10] Proses enkripsi berhasil mengubah data asli seperti nama, nomor telepon, alamat, dan detail pesanan menjadi ciphertext yang tidak dapat dibaca tanpa kunci dekripsi sehingga mampu menjaga kerahasiaan data pada saat penyimpanan maupun pengiriman. Hasil pengujian memperlihatkan bahwa proses enkripsi berjalan efisien tanpa menimbulkan keterlambatan pada sistem, sehingga cocok digunakan dalam lingkungan UMKM yang memiliki keterbatasan sumber daya. Implementasi AES dalam sistem pemesanan juga memberikan lapisan perlindungan yang esensial untuk menghadapi risiko penyalahgunaan data, sekaligus mendukung proses digitalisasi UMKM agar dapat menyediakan layanan yang lebih aman dan dapat dipercaya oleh pelanggan. Penelitian ini pada akhirnya membuktikan bahwa AES merupakan solusi enkripsi yang efektif, ringan, dan layak digunakan dalam pengamanan data pelanggan pada skala usaha kecil seperti penjual nasi kuning

Daftar Rujukan

[1] A. E. Loho, "Usaha Mikro, Kecil, dan Menengah: Definisi dan Kriteria," vol. XI, no. September, pp. 63–72, 2015.

[2] S. Adrianto, B. A. Herlambang, and R. Renaldy, "Optimizing Customer Data Security in Water Meter Data Management Based on RESTful API and Data Encryption Using AES-256 Algorithm," vol. 9, no. 3, pp. 876–882, 2025.

[3] A. Arya, "Effective AES Implementation," vol. 7, no. 1, pp. 1–9, 2016.

[4] A. Z. Ifani, R. Nurul, and J. S. Intam, "Application of Advanced Encryption Standard (AES) Algorithm in E-Commerce Login System for User Data Security," vol. 6, no. 1, pp. 1–9, 2025.

[5] 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.

[6] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *Journal of King Saud University - Engineering Sciences*, vol. 32, no. 2, pp. 115–122, 2020, doi: 10.1016/j.jksues.2018.07.002.

[7] A. M. Deshpande, M. S. Deshpande, and D. N. Kayatanavar, "FPGA Implementation of AES Encryption and Decryption," no. June, pp. 1–6, 2009.

[8] M. Huo, Y. Zheng, and J. Huang, "Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency," pp. 1–22, 2025, doi: 10.1371/journal.pone.0328297.

[9] M. Azhari, F. Riza, and H. Maulana, "Student Data Security Optimization using Multiple Cryptography to Improve E-Campus Services," 2025.

[10] F. Teknik, M. I. Komputer, and U. T. Indonesia, "Keamanan Database Aplikasi Manajemen Siswa," vol. 4, no. 2, pp. 111–119, 2025.

[11] J. Junetri et al., "Strategi Pemasaran Dan Keberlanjutan Usaha: Studi Pada Usaha Nasi Kuning Di Kelurahan Tanamodindi Kota Palu," vol. 3, no. 1, pp. 51–56, 2025.

[12] A. M. Khosasi, F. Ekonomi, and U. Pamulang, "Investigasi Strategi dan Pengembangan Bisnis Nasi Kuning Ibu Atin Cipete, Jakarta Selatan Menggunakan Metode Analisis SWOT," vol. 2, no. 1, pp. 1–15, 2025.

[13] F. Tollo, P. M. Bisnis, P. S. Manajemen, U. K. Petra, and J. Siwalankerto, "Analisis Aplikasi 7P Pada Usaha Nasi Kuning Air Putri Di Ambon," vol. 5, no. 1, 2017.

[14] A. E. Standard, K. Dokumen, and B. B. Testing, "Pengujian dan Standarisasi Algoritma AES," no. November 2018, pp. 1044–1052, 2024.

[15] T. A. Skripsi, "Rancang Bangun Aplikasi Pemesanan Menggunakan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi," 2025.