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

Pengamanan Data Pemesanan Pelanggan Menggunakan Algoritma AES-256-CBC: Studi Kasus pada UMKM Siti Furniture

Customer Order Data Security Using AES-256-CBC Algorithm: A Case Study at Siti Furniture MSME

Dita Tiara Putri1, Ifa Nurul Fauziah[2], Nur Laila[3], Suci Maolia[4]
[1]Informatika, Teknik, Universitas Pelita Bangsa
[2]Informatika, Teknik, Universitas Pelita Bangsa
[3]Informatika, Teknik, Universitas Pelita Bangsa
[4]Informatika, Teknik, Universitas Pelita Bangsa
[1]ditatiara654@gmail.com, [2]ifanurul270505@gmail.com*, [3]nurlailaa149@gmail.com*,
[4]maoliasuci@gmail.com*.

Abstract

Data security in e-commerce systems is a crucial aspect in protecting sensitive customer information and maintaining trust in digital platforms. This study implements the AES-256-CBC encryption algorithm with a field-level encryption approach on customer order data at Siti Furniture, a small and medium-sized enterprise (SME) in Cikarang, West Java. The implementation uses a 256-bit key and a random initialization vector (IV) generated automatically in each encryption process to prevent the formation of identical ciphertext patterns. Security evaluation was carried out through functional encryption-decryption testing and ciphertext randomness testing using Shannon Entropy. Functional testing showed that all sensitive customer data was successfully restored without changes. Shannon Entropy testing produced entropy values ranging from 7.9224 to 7.9845 bits/byte, equivalent to 99.03% to 99.81% of the ideal entropy value of 8 bits/byte, indicating a very high level of ciphertext randomness. The use of random IV ensures that identical plaintext produces different ciphertext in each encryption process. The results prove that AES-256-CBC with field-level encryption can be effectively applied to MSME e-commerce systems with limited resources without compromising data security and customer information integrity.

***Keywords**: AES-256-CBC, field-level encryption, Entropy Shannon, e-commerce security, MSME*

Abstrak

Keamanan data pada sistem *e-commerce* menjadi aspek krusial dalam melindungi informasi sensitif pelanggan dan menjaga kepercayaan terhadap platform digital. Penelitian ini mengimplementasikan algoritma enkripsi AES-256-CBC dengan pendekatan *field-level encryption* pada data pemesanan pelanggan di UMKM Siti *Furniture*, Cikarang, Jawa Barat. Implementasi menggunakan kunci 256-bit dan *initialization vector* (IV) acak yang dihasilkan secara otomatis pada setiap proses enkripsi untuk mencegah terbentuknya pola *ciphertext* yang identik. Evaluasi keamanan dilakukan melalui pengujian fungsional enkripsi-dekripsi dan pengujian tingkat keacakan *ciphertext* menggunakan Entropi Shannon. Pengujian fungsional menunjukkan bahwa seluruh data sensitif pelanggan berhasil dikembalikan tanpa perubahan. Pengujian Entropi Shannon menghasilkan nilai entropi berkisar antara 7,9224 hingga 7,9845 bit/byte, setara dengan 99,03% hingga 99,81% dari nilai entropi ideal yaitu sebesar 8 bit/byte, menunjukkan tingkat keacakan *ciphertext* yang sangat tinggi. Penggunaan IV acak memastikan plaintext yang identik menghasilkan *ciphertext* berbeda pada setiap proses enkripsi. Hasil membuktikan bahwa AES-256-CBC dengan enkripsi *field-level* dapat diterapkan efektif pada sistem *e-commerce* UMKM dengan sumber daya terbatas tanpa mengurangi keamanan data dan integritas informasi pelanggan.

Kata kunci: AES-256-CBC, Enkripsi *Field-level*, Entropi Shannon, Keamanan *E-Commerce*, UMKM

Pendahuluan

Transformasi digital telah membawa perubahan signifikan bagi Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia melalui peningkatan jangkauan pasar, efisiensi operasional, dan profitabilitas. UMKM berkontribusi sekitar 61% terhadap Produk Domestik Bruto (PDB) dan menyerap lebih dari 97% tenaga kerja, namun masih menghadapi berbagai tantangan dalam proses digitalisasi, seperti rendahnya literasi digital, keterbatasan sumber daya finansial, infrastruktur digital yang belum merata, serta dukungan regulasi yang belum optimal [1]. Industri *furniture* merupakan salah satu sektor UMKM yang mengalami transformasi digital melalui sistem pemesanan berbasis *online*, dimana platform *e-commerce* membuka peluang perluasan pasar melampaui batasan geografis konvensional [2].

Seiring meningkatnya pemanfaatan sistem *e-commerce*, keamanan data menjadi isu krusial karena platform digital mengelola informasi sensitif pelanggan dalam jumlah besar. Pelanggaran data tidak hanya berpotensi mengekspos informasi pribadi, tetapi juga menurunkan kepercayaan konsumen terhadap sistem digital [3]. Secara global, biaya pelanggaran data terus meningkat dan berdampak signifikan terhadap operasional bisnis [4]. Selain itu, insiden kebocoran data dilaporkan dapat memengaruhi keberlanjutan hubungan bisnis antara konsumen dan penyedia layanan digital akibat menurunnya tingkat kepercayaan [5].

Sebagai upaya pengamanan data, *Advanced Encryption Standard* (AES) telah banyak diadopsi sebagai standar enkripsi global. Panduan CISA dan NIST menyatakan bahwa algoritma AES dengan ukuran kunci 128, 192, dan 256 bit masih aman digunakan dalam jangka panjang [6]. AES-256 direkomendasikan untuk skenario yang menuntut tingkat keamanan tinggi [7]. AES-CBC adalah skema enkripsi yang menggabungkan algoritma *Advanced Encryption Standard* (AES) sebagai *block cipher* dengan mode operasi *Cipher Block Chaining* (CBC), dimana data dienkripsi dalam bentuk blok-blok berurutan. Pada mode ini, setiap blok *plaintext* terlebih dahulu dikombinasikan dengan *ciphertext* dari blok sebelumnya menggunakan operasi XOR sebelum dienkripsi menggunakan algoritma AES, dengan *Initialization Vector* (IV) acak digunakan pada blok pertama untuk mencegah terbentuknya pola *ciphertext* yang identik [8].

Meskipun menawarkan tingkat keamanan yang lebih baik dibandingkan *Electronic Codebook* (ECB), mode CBC memiliki tantangan berupa ketergantungan antar blok data yang berpotensi memengaruhi efisiensi sistem apabila tidak dirancang dengan tepat [9]. Di sisi lain, AES-256 dikenal memiliki efisiensi *lightweight* dan kompatibilitas yang baik dengan sistem yang ada [10], serta terbukti efektif dalam pengamanan data login dan data pelanggan pada sistem *e-commerce* dengan kebutuhan memori yang relatif kecil [11]. Namun, sebagian besar implementasi tersebut masih berfokus pada sistem berskala besar, sehingga belum sepenuhnya merepresentasikan karakteristik dan keterbatasan sumber daya UMKM.

Penggunaan *initialization vector* (IV) yang dihasilkan secara acak pada setiap proses enkripsi merupakan praktik esensial dalam implementasi AES-CBC untuk mencegah terbentuknya pola *ciphertext* yang identik pada *plaintext* yang sama [12]. Studi terbaru menunjukkan bahwa implementasi AES-CBC dengan IV acak mampu menghasilkan *ciphertext* dengan tingkat keacakan yang tinggi, dimana efektivitas enkripsi dapat dievaluasi menggunakan metrik Entropi Shannon untuk memastikan distribusi *ciphertext* yang optimal [13]. Pendekatan ini menjadi pertimbangan penting dalam perancangan sistem enkripsi *field-level* untuk aplikasi *e-commerce* yang memproses data pelanggan dalam jumlah besar dengan keterbatasan sumber daya.

Berdasarkan kondisi dan kesenjangan (gap) tersebut, masih terbatas kajian yang membahas implementasi AES-256-CBC pada sistem *e-commerce* UMKM *furniture* di Indonesia dengan mempertimbangkan aspek efisiensi, kemudahan implementasi, dan keterbatasan sumber daya. Oleh karena itu, untuk menjawab kesenjangan ini, penelitian ini mengusulkan implementasi praktis AES-256-CBC pada sistem pemesanan UMKM *furniture* berbasis PHP dan MariaDB. Kebaruan penelitian secara spesifik terletak pada penerapan enkripsi *field-level* terhadap data sensitif pelanggan, seperti nama, nomor telepon, dan alamat pengiriman, yang dipilih karena kemampuannya mengoptimalkan kinerja sistem dibandingkan pendekatan enkripsi seluruh basis data.

Evaluasi keamanan dilakukan menggunakan metrik Entropi Shannon untuk mengukur tingkat keacakan *ciphertext* yang dihasilkan, dimana nilai entropi yang tinggi menunjukkan distribusi *ciphertext* yang baik dan tingkat keamanan yang kuat [14]. Dalam teori informasi, entropi merupakan besaran yang digunakan untuk mengukur tingkat ketidakpastian atau ketidakteraturan suatu variabel acak. Konsep entropi berawal dari gagasan konten informasi dan kemudian diformalkan oleh Claude E. Shannon sebagai ukuran kuantitatif dari banyaknya informasi yang terkandung dalam suatu data. Entropi Shannon menggambarkan tingkat keacakan distribusi simbol, di mana nilai entropi yang semakin besar menunjukkan distribusi data yang semakin merata dan sulit diprediksi. Oleh karena itu, Entropi Shannon banyak digunakan sebagai metrik evaluasi pada berbagai bidang, termasuk keamanan informasi dan kriptografi, untuk menilai kualitas dan karakteristik keacakan data yang dihasilkan[15].

Secara operasional, penelitian ini bertujuan untuk: (1) merancang dan mengimplementasikan sistem enkripsi AES-256-CBC pada data pemesanan serta (2)mengevaluasi tingkat keamanannya menggunakan Entropi Shannon. Hasil penelitian diharapkan dapat menjadi rujukan praktis bagi UMKM sejenis dalam menerapkan solusi keamanan data yang efektif dan efisien, serta meningkatkan kepercayaan pelanggan terhadap sistem pemesanan *online*.

Metode Penelitian

Penelitian ini menggunakan pendekatan studi kasus pada UMKM Siti *Furniture* dan dirancang sebagai penelitian eksperimental untuk menganalisis implementasi algoritma AES-256-CBC pada sistem pemesanan. Pengumpulan data dilakukan melalui observasi langsung ke lokasi penelitian dan diskusi dengan pihak UMKM guna memperoleh kebutuhan sistem pemesanan dan pengamanan data. Penelitian ini dilaksanakan pada UMKM Siti *Furniture* yang berlokasi di Cikarang, Jawa Barat. Dokumentasi kegiatan observasi dan pengumpulan data ditunjukkan pada Gambar 1.

Gambar 1. Dokumentasi kegiatan observasi lapangan di UMKM Siti *Furniture*

Objek penelitian berupa data pemesanan pelanggan yang diperoleh melalui sistem pemesanan UMKM Siti *Furniture*. Dari data tersebut, informasi yang diklasifikasikan sebagai data sensitif meliputi nama pelanggan, alamat pengiriman, dan nomor telepon. Data sensitif tersebut menjadi fokus utama penelitian dalam penerapan mekanisme pengamanan menggunakan algoritma AES-256-CBC.

Implementasi sistem dilakukan menggunakan bahasa pemrograman PHP dengan memanfaatkan *library OpenSSL* untuk menerapkan algoritma AES-256-CBC, kunci berukuran 256-bit, dan *initialization vector* (IV)

yang dihasilkan secara acak. Data sensitif dienkripsi terlebih dahulu sehingga menghasilkan *ciphertext*, kemudian *ciphertext* tersebut disimpan ke dalam basis data MySQL.

Pengujian dilakukan dengan menghitung nilai Entropi Shannon dari *ciphertext* hasil enkripsi untuk menilai tingkat keacakan data. Perhitungan tingkat keacakan *ciphertex*t dilakukan menggunakan rumus Entropi Shannon sebagaimana ditunjukkan pada Persamaan (1) [16].

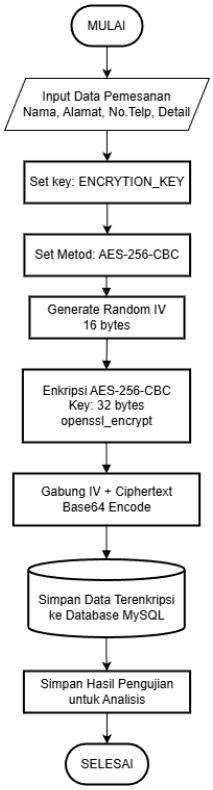
Persamaan (1):

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

Dengan Hmenyatakan nilai entropi, p_i menyatakan probabilitas kemunculan simbol ke-i, dan n menyatakan jumlah total simbol yang diamati.

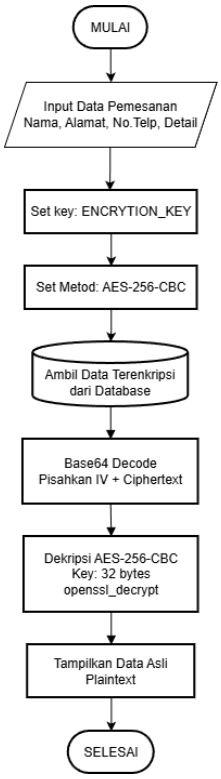
Teknik analisis data dilakukan secara deskriptif dan komparatif. Analisis deskriptif digunakan untuk menggambarkan karakteristik tingkat keacakan *ciphertext* hasil enkripsi, sedangkan analisis komparatif dilakukan dengan membandingkan nilai entropi berdasarkan variasi input data, panjang data, serta pengaruh penggunaan *initialization vector* (IV) acak untuk menilai efektivitas implementasi algoritma AES-256-CBC.

Alur kerja sistem enkripsi divisualisasikan dalam bentuk *flowchart* pada Gambar 2. Proses enkripsi dimulai dengan menerima *input* data pemesanan yang mencakup nama, alamat, nomor telepon, dan detail pesanan dari formulir pemesanan. Sistem kemudian menetapkan kunci enkripsi (*ENCRYPTION_KEY*) dan metode enkripsi AES-256-CBC. Selanjutnya, sistem membangkitkan *initialization vector* (IV) secara acak berukuran 16 bytes untuk setiap proses enkripsi guna memastikan *ciphertext* yang unik. Data *plaintext* dienkripsi menggunakan algoritma AES-256-CBC dengan kunci 32 bytes melalui fungsi *openssl_encrypt*. Hasil enkripsi berupa IV dan *ciphertext* kemudian digabungkan dan di-*encode* ke format *Base64* sebelum disimpan ke dalam basis data MySQL. Sistem juga menyimpan hasil pengujian untuk analisis keamanan.



Gambar 2. *Flowchart* Proses Enkripsi

Sementara itu, alur kerja dekripsi divisualisasikan pada Gambar 3. Proses dekripsi dimulai ketika administrator mengakses data pemesanan yang mencakup nama, alamat, nomor telepon, dan detail pesanan. Sistem menetapkan kunci dekripsi yang sama (*ENCRYPTION_KEY*) dan metode AES-256-CBC. Data terenkripsi diambil dari basis data, kemudian dilakukan *decode* dari format *Base*64 untuk memisahkan IV dan *ciphertext*. Sistem mengekstraksi IV dari 16 bytes pertama data terenkripsi. Dengan menggunakan IV yang telah diekstraksi dan kunci dekripsi 32 bytes, sistem melakukan dekripsi menggunakan fungsi *openssl_decrypt* untuk mengembalikan data ke bentuk *plaintext* yang dapat dibaca.

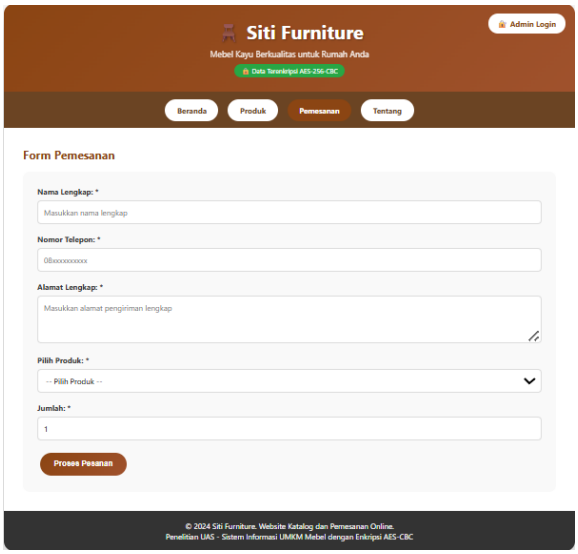


Gambar 3. *Flowchart* Proses Dekripsi

Hasil dan Pembahasan

Desain Antarmuka Formulir Pemesanan Pelanggan

Sistem informasi yang dikembangkan pada UMKM Siti *Furniture* menyediakan fitur pemesanan *daring* yang memungkinkan pelanggan mengisi formulir pemesanan sebagaimana ditunjukkan pada Gambar 4. Formulir tersebut mencakup data nama lengkap, nomor telepon, alamat pengiriman, pilihan produk, dan jumlah pesanan. Dari seluruh data yang diinputkan, informasi berupa nama pelanggan, nomor telepon, dan alamat pengiriman diklasifikasikan sebagai data sensitif. Oleh karena itu, ketiga data tersebut dienkripsi terlebih dahulu sehingga menghasilkan *ciphertext*, kemudian *ciphertext* tersebut disimpan ke dalam basis data sistem, sedangkan data lainnya disimpan tanpa melalui proses enkripsi.



Gambar 4. Desain Antarmuka Formulir Pemesanan Pelanggan

Implementasi Enkripsi Data Pemesanan

Hasil pengujian menunjukkan bahwa data sensitif pada kolom *customer_name*, *customer_phone*, dan *customer_address* tidak lagi tersimpan dalam bentuk teks asli, melainkan dalam bentuk *ciphertext* yang tidak dapat dibaca secara langsung. Kondisi ini ditunjukkan pada Gambar 5 yang memperlihatkan hasil penyimpanan data setelah proses enkripsi diterapkan. Proses enkripsi dilakukan pada sisi server sebelum data disimpan ke dalam basis data, sehingga hanya *field* data sensitif yang tersimpan dalam bentuk *ciphertext*, sementara *field non-sensitif* tetap disimpan dalam bentuk *plaintext* untuk mendukung kebutuhan operasional sistem.

id	customer_name	customer_phone	customer_address	product_name	quantity	price	total_price	order_date
1	0rNRheRVXG1KNpvLAM/IOhAYvfKi9Hp,tj7inyPsBeSd7r5SsOarYty05zRjFMpS0	MuZIZUS346ins9pIH5vFTOspMQ1QYVKJNTGXv01Cyv!=	v16zQ3zfAOk/rMaCUOWbsGoj2FNGlbClBiYv1oDPL6Mx9aJ5x44Aw76I1L6qO6gbdy3zV9DDuOJv6/pSXkB/HjdD0XWB38twYzT01qxmOXA9Uva6d9+ yo0i7gt1StpwSG7h3FSzjcpFow3Y27s2KM88HFjZ+ INx2jTFRVsnCEkk1O1FmIeGVGNqdZQeAmiOeIK8E4LxTclTjEbzH9zt9nQ= =	Kursi Makan Minimalis	1	450000.00	450000.00	2025-12-20 13:19:59
2	2U2zRwqtYBdp+ h68b+ CIR9X5jGttQYKHWFhMTwL80IjgR+ Qxf08eUtlSkg1ViUwA	C3WYpOtcYtpLt+ FcE/wSeHrUcksoECCTkvD6h+ ACyO0=	g1B/s3KC9po2RoVFA71pHDqjMSoPW7e1sYuQB+ wgqyviHetnFdoTOksdc/0W7/JHZiSDzq8b6Lby/e36DS44InuaBvF,JwaUTAMethRtcEjHnILDkkgS+ OKZGAf6BTAzQMkckTb/Jen1JuhDMOkjIOoiEHeLOzk7yensfCnTYTWTWdOVwwqm7ZeiILyR1+ aMvwuncvv/BtkHJBxftTQ= =	Kursi Teras Klasik	2	550000.00	1100000.00	2025-12-20 13:21:29

Gambar 5. Implementasi Enkripsi Data Pemesanan

Selain itu, dilakukan juga uji coba enkripsi terhadap data pelanggan yang memiliki nilai *plaintext* yang sama, khususnya pada atribut nama pelanggan, untuk memastikan konsistensi penerapan *initialization vector* (IV) acak. Pada pengujian ini, *plaintext* dengan nilai yang sama dienkripsi lebih dari satu kali menggunakan kunci enkripsi yang sama. Hasil pengujian tersebut dapat dilihat pada Tabel 1.

Tabel 1 Implementasi Enkripsi Data Pemesanan

Plaintext	IV	**Kunci**	**Ciphertext**
Rizal Fahmi Kurniawan	IV-1(acak)	Tetap	2U2zRwqtYBdp+h68b+CIR9X5jGttQYKHWFhMTwL80IjgR+Qxf08eUtlSkg1ViUwA
Rizal Fahmi Kurniawan	IV-2(acak)	Tetap	avdgQYe1W8S5JdZNN1ZeecgrqclUvYGnQ0fsXat98WpKsLZn0zI0mVz76VKDgnJj

Berdasarkan Tabel 1, terlihat bahwa meskipun *plaintext* yang digunakan identik ("Rizal Fahmi Kurniawan"), *ciphertext* yang dihasilkan berbeda pada setiap proses enkripsi. Kedua *ciphertext* memiliki panjang yang sama,

yaitu 68 karakter dalam format *Base64*, namun dengan komposisi karakter yang berbeda. Penggunaan format *Base64* dilakukan untuk merepresentasikan data *ciphertext* yang bersifat biner ke dalam bentuk teks, sehingga dapat disimpan dan dikelola dengan aman pada basis data berbasis PHP–MySQL tanpa kehilangan integritas data hasil enkripsi. Perbedaan *ciphertext* tersebut terjadi akibat penggunaan *initialization vector* (IV) yang dihasilkan secara acak pada setiap proses enkripsi dan digabungkan bersama hasil *ciphertext* sebelum disimpan ke dalam basis data.

Hasil Implementasi Dekripsi Data Pemesanan

Administrator diberikan akses ke *dashboard* untuk melihat dan mengelola data pemesanan pelanggan. Data yang tersimpan dalam basis data tetap berada dalam kondisi terenkripsi dan hanya didekripsi secara otomatis pada sisi aplikasi setelah proses autentikasi berhasil. Proses dekripsi dilakukan dengan mengekstraksi *initialization vector* (IV) dari data terenkripsi, sehingga IV tidak perlu disimpan secara terpisah. Dengan mekanisme ini, data pelanggan tetap aman di dalam basis data dan hanya ditampilkan dalam bentuk *plaintext* pada saat diperlukan, sebagaimana ditunjukkan pada Gambar 6.

ID	Tanggal	Nama	Telepon	Alamat	Produk	Qty	Total
#3	20/12/2025 13:25	Rizal Fahmi Kurniawan	081212121212	Jl. Flamboyan Indah No. 456, RT 22/RW 14, Kelurahan Kenari Baru, Kecamatan Aurora, Kota Pelita, Provinsi Harapan, Kode Pos 98765	Kursi Kerja Ergonomis	2	**Rp 1.300.000**
#2	20/12/2025 13:21	Rizal Fahmi Kurniawan	080808080808	Jl. Anggrek Timur No. 123, RT 12/RW 08, Kelurahan Melur Abadi, Kecamatan Falsafah, Kota Mandiri, Provinsi Makmur, Kode Pos 54321	Kursi Teras Klasik	2	**Rp 1.100.000**
#1	20/12/2025 13:19	Sari Lestari Dewi Putri	081234567890	Jl. Kenanga Permai Blok Z/12, RT 15/RW 10, Kelurahan Mawar Sari, Kecamatan Imaginary, Kota Tirta, Provinsi Nusantara, Kode Pos 12345	Kursi Makan Minimalis	1	**Rp 450.000**

Gambar 6. Tampilan Dekripsi Data Pemesanan

Data pelanggan yang disajikan dalam tabel dan visualisasi hasil pengujian telah dianonimkan dan dimodifikasi, sehingga tidak merepresentasikan data pribadi pelanggan yang sebenarnya. Seluruh data yang digunakan dalam penelitian ini bertujuan untuk kepentingan pengujian sistem dan tidak mengandung informasi yang dapat mengidentifikasi individu secara langsung.

Pengujian Fungsional Enkripsi dan Dekripsi Data Pemesanan

Untuk memastikan bahwa mekanisme enkripsi dan dekripsi yang diimplementasikan berjalan dengan benar dan konsisten, dilakukan pengujian fungsional terhadap proses enkripsi–dekripsi data pemesanan. Pengujian fungsional ini dilakukan melalui beberapa tahapan. Pertama, data pemesanan pelanggan disimpan ke dalam basis data setelah melalui proses enkripsi menggunakan algoritma AES-256-CBC. Data yang tersimpan berada dalam bentuk *ciphertext* yang telah digabungkan dengan *initialization vector* (IV) dan direpresentasikan dalam format *Base64*.

Selanjutnya, sistem mengambil kembali *ciphertext* tersebut dari basis data untuk dilakukan proses dekripsi. Pada pengujian ini, proses dekripsi dilakukan terhadap salah satu data pemesanan pelanggan yang tersimpan di dalam basis data, yaitu data dengan ID = 1, sebagai sampel pengujian. Pada tahap ini, *initialization vector* (IV) diekstraksi secara otomatis dari bagian awal *ciphertext*, kemudian digunakan bersama kunci enkripsi yang sama untuk mengembalikan data ke bentuk *plaintext*.

Hasil dekripsi kemudian dibandingkan dengan data *plaintext* awal yang dimasukkan ke dalam sistem. Apabila data hasil dekripsi identik dengan *plaintext* awal tanpa mengalami perubahan, maka proses enkripsi dan dekripsi dinyatakan berjalan secara konsisten dan sejalur. Hasil pengujian menunjukkan bahwa seluruh data sensitif pelanggan yang terenkripsi dapat dikembalikan ke bentuk *plaintext* semula secara utuh tanpa perubahan, sebagaimana ditunjukkan pada Gambar 7. Hal ini membuktikan bahwa mekanisme enkripsi–dekripsi AES-256-CBC yang diterapkan telah berjalan dengan baik, konsisten, dan sejalur.

Data	Ciphertext (Database)	Hasil Dekripsi (Plaintext)	Status
Nama	0rNRheRVXG1KNpvLAM/IOhAYvfKi9HpJq7inyPsBeSd7r5Ss0arYty05zRjFMpS0	Sari Lestari Dewi Putri	Valid
Telepon	MuZlZUS346ins9plH5vFTOspMQ1QYVKJNTGXv01CyvI=	081234567890	Valid
Alamat	v16zQ3zfAOk/rMaCUOWbsGoj2FNGIbCIBiYv1oDPL6Mx9aJSx44Aw76l1L6qO6gbdy3zV9DDuOJv6/pSXkB/HjdD0XWB38twYzT01qxmOXA9Uva6d9+yo0i7gt1StpwSG7h3FSzjcpFow3Y27s2KM88HFjZ+lNx2jTFRVsnCEkk1O1FmleGVGNqdZQeAmiOelK8E4LxTclTjEbzH9zt9nQ==	Jl. Kenanga Permai Blok Z/12, RT 15/RW 10, Kelurahan Mawar Sari, Kecamatan Imaginary, Kota Tirta, Provinsi Nusantara, Kode Pos 12345	Valid

Gambar 7. Tampilan Pengujian Fungsional Enkripsi - Dekripsi Data Pemesanan

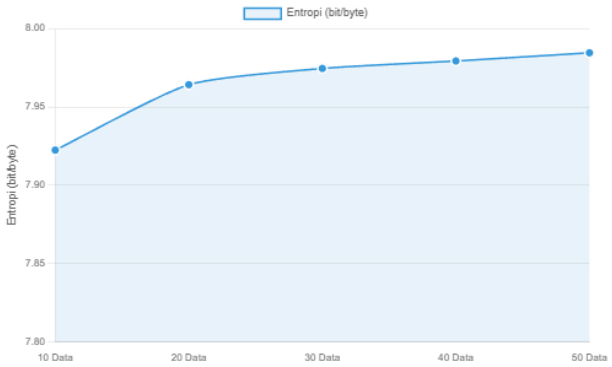
Pengujian Entropi Shannon

Pengujian entropi shannon dilakukan untuk mengevaluasi tingkat keacakan *ciphertext* hasil enkripsi menggunakan algoritma AES-256-CBC sebagai indikator kualitas keamanan data. Pengujian dilakukan dengan menghitung nilai entropi shannon dari *ciphertext* gabungan data sensitif pelanggan, meliputi nama, nomor telepon, dan alamat, dengan variasi jumlah data sebanyak 10 hingga 50 data. Hasil perhitungan nilai entropi shannon terhadap *ciphertext* gabungan tersebut disajikan pada Tabel 2.

Tabel 2 Pengujian Entropi Shannon

Jumlah Data	Total *Field* Terenkripsi	Total Byte	Entropi (bit/byte)	Persentase Ideal (%)
10	30 *field*	2,304 byte	7.9224	99.03%
20	60 *field*	4,624 byte	7.9641	99.55%
30	90 *field*	6,880 byte	7.9745	99.68%
40	120 *field*	9,104 byte	7.9792	99.74%
50	150 *field*	11,376 byte	7.9845	99.81%

Berdasarkan Tabel 2, nilai entropi menunjukkan peningkatan seiring dengan bertambahnya jumlah data yang diuji. Pada pengujian dengan 10 data, nilai entropi sebesar 7,9224 bit/byte atau 99,03% dari nilai ideal, dan meningkat hingga mencapai 7,9845 bit/byte atau 99,81% pada pengujian dengan 50 data. Nilai tersebut mendekati entropi maksimum sebesar 8 bit/byte, yang mengindikasikan tingkat keacakan *ciphertext* yang sangat tinggi. Seluruh nilai entropi yang diperoleh berada di atas 7,9 bit/byte, yang menunjukkan bahwa *ciphertext* memiliki kualitas keacakan yang baik dan sesuai dengan karakteristik algoritma kriptografi simetris modern. Tren peningkatan dan kestabilan nilai entropi tersebut juga diperkuat melalui visualisasi pada Gambar 8.



Gambar 8. Grafik Pengujian Entropi Shannon

Gambar 8 memperlihatkan tren nilai entropi *ciphertext* yang meningkat dan kemudian stabil mendekati nilai maksimum. Pola kurva yang cenderung mendatar pada jumlah data yang lebih besar menunjukkan bahwa tingkat keacakan telah mencapai kondisi optimal dan tidak mengalami fluktuasi signifikan. Hasil ini membuktikan bahwa penerapan algoritma AES-256-CBC mampu menghasilkan *ciphertext* dengan karakteristik keacakan yang tinggi dan konsisten, sehingga efektif dalam melindungi keamanan data pemesanan pelanggan.

Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan sistem enkripsi AES-256-CBC pada data pemesanan UMKM Siti Furniture dengan menerapkan pendekatan enkripsi *field-level* terhadap data sensitif pelanggan, yang meliputi nama, nomor telepon, dan alamat pengiriman. Implementasi dilakukan menggunakan kunci 256-bit dan *initialization vector* (IV) acak yang dihasilkan secara otomatis pada setiap proses enkripsi, sehingga *plaintext* yang identik menghasilkan *ciphertext* yang berbeda dan mampu mencegah terbentuknya pola yang berpotensi dieksploitasi.

Pengujian fungsional enkripsi–dekripsi menunjukkan bahwa seluruh data sensitif yang tersimpan dalam basis data dapat dikembalikan ke bentuk *plaintext* semula secara utuh tanpa mengalami perubahan. Hasil ini membuktikan bahwa mekanisme enkripsi dan dekripsi berjalan secara konsisten dan sejalur, serta tidak memengaruhi keakuratan data yang dikelola oleh sistem.

Selanjutnya, evaluasi keamanan menggunakan entropi shannon menunjukkan tingkat keacakan *ciphertext* yang sangat tinggi, dengan nilai entropi berkisar antara 7,9224 bit/byte hingga 7,9845 bit/byte, atau setara dengan 99,03% hingga 99,81% dari nilai ideal sebesar 8 bit/byte. Hasil tersebut mengindikasikan bahwa algoritma AES-256-CBC mampu menghasilkan *ciphertext* dengan karakteristik keacakan yang optimal dan konsisten, sehingga efektif dalam melindungi keamanan data pemesanan pelanggan.

Berdasarkan hasil penelitian tersebut, dapat disimpulkan bahwa penerapan enkripsi *field-level* menggunakan AES-256-CBC dapat diterapkan secara efektif pada sistem *e-commerce* UMKM dengan sumber daya terbatas tanpa mengorbankan keamanan dan integritas data. Untuk penelitian selanjutnya, disarankan dilakukan perbandingan kinerja antara enkripsi *field-level* dan *database-level encryption*, serta pengujian ketahanan sistem terhadap berbagai skenario serangan kriptografi guna memperoleh evaluasi keamanan yang lebih komprehensif.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada pemilik dan manajemen UMKM Siti *Furniture*, Cikarang, Jawa Barat, yang telah memberikan izin dan dukungan penuh dalam pelaksanaan penelitian ini. Apresiasi juga disampaikan kepada seluruh tim yang telah membantu dalam proses pengumpulan data dan implementasi sistem. Ucapan terima kasih juga ditujukan kepada para *reviewer* dan editor yang telah memberikan masukan konstruktif untuk penyempurnaan artikel ini.

Daftar Rujukan

[1] P. S. Sitompul, M. M. Sari, C. M. Br Lumban Gaol, and L. M. Harahap, "Transformasi digital UMKM Indonesia: Tantangan dan strategi adaptasi di era ekonomi digital," J. Manaj. Bisnis Digit. Terkini, vol. 2, no. 2, pp. 9–18, Apr. 2025.

[2] M. Chaidir, Ruslaini, and D. Irawan, "Transformasi digital dalam manajemen keuangan (Studi kasus pada UMKM Indonesia di era ekonomi digital)," JUMMA'45: J. Mahasiswa Manaj. dan Akuntansi, vol. 4, no. 1, pp. 239–249, Apr. 2025.

[3] E. A. Otieno, "Data protection and privacy in e-commerce environment: Systematic review," GSC Adv. Res. Rev., vol. 22, no. 1, pp. 238–271, Jan. 2025.

[4] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, Armonk, NY, USA, July 2024.

[5] A. Strzelecki and M. Rizun, "Consumers' change in trust and security after a personal data breach in online shopping," Sustainability, vol. 14, no. 10, p. 5866, May 2022.

[6] Cybersecurity and Infrastructure Security Agency (CISA), "Transition to Advanced Encryption Standard (AES)," U.S. Department of Homeland Security, Washington, DC, USA, Tech. Rep., May 2024.

[7] N. Mouha, "Review of the Advanced Encryption Standard," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Interagency Rep. 8319, Jul. 2021.

[8] N. Mouha and M. Dworkin, "Recommendation for block cipher modes of operation in the NIST SP 800-38 series," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Interagency Rep. 8459, Sep. 2024.

[9] K. C. Chang, Y. T. Teng, and W. L. Chin, "High-throughput CBC mode crypto circuit," Elect. Sci. Eng., vol. 5, no. 1, pp. 20–30, Apr. 2023.

[10] N. Sharma and P. Yadav, "Efficient implementation of AES-256 for secure machine learning datasets: A performance and compatibility study," Int. J. Eng. Trends Technol., vol. 73, no. 9, pp. 91–99, Sep. 2025.

[11] R. P. Shete, A. M. Bongale, and D. Dharrao, "Lightweight cryptographic and scalable IoT systems for encryption across GSM-MQTT architectures in resource-constrained aquaculture environment," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25133-25139, Aug. 2025.

[12] B. Zolfaghari, K. Bibak, and T. Koshiba, "The odyssey of entropy: Cryptography," *Entropy*, vol. 24, no. 2, p. 266, Feb. 2022.

[13] K. Haria, R. Shah, V. Jain, A. Chawla, S. Jain, and H. S. Kushwaha, "Enhanced image encryption using AES algorithm with CBC mode: a secure and efficient approach," Iran J. Comput. Sci., vol. 7, pp. 589–605, 2024.

[14] R. S. Sutar and V. K. Shandliya, "A Novel Approach for Information Security using AES Algorithm and Shannon Entropy," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 1, pp. 642–648, 2022.

[15] E. Renyi, R. Raafi, and I. P. Solihin, "Simulasi Entropi Shannon, Entropi Renyi, dan informasi pada kasus Spin Wheel 1," vol. 12, no. 1, pp. 120–128, 2021.

[16] S.-W. Lee and K.-B. Sim, "Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security," Electronics, vol. 10, no. 9, Art. no. 1127, May 2021.