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 Enkripsi AES-256-CBC pada Sistem Manajemen Data Pelanggan UMKM SECOND AND DESTROY *Thrift Store* Berbasis Laravel

Implementation of AES-256-CBC Encryption in the Customer Data Management System of the SECOND AND DESTROY Thrift Store Based on Laravel

Ainun Dwi Permana1, Arya Wiratama[2], Farel Aryaduta Daniswara[3]
[1]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[2]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]aidahpermana27@gmail.com, [2]aryawiratama2401@gmail.com*, [3]farelaryaduta55@gmail.com*

Abstract

Customer data security is a critical challenge for Micro, Small, and Medium Enterprises (MSMEs) in Indonesia, particularly in managing sensitive information that is still commonly handled using conventional methods and is vulnerable to data breaches. This study aims to design and implement a secure web-based customer management system for Second and Destroy Thrift Store by applying field-level encryption using the Advanced Encryption Standard (AES) algorithm with a 256-bit key and Cipher Block Chaining (CBC) mode of operation. The system was developed using the Laravel framework and a MySQL database, with encryption and decryption processes implemented through the OpenSSL cryptographic library at the application model layer. Sensitive attributes, including customers' WhatsApp numbers and addresses, are encrypted before being stored in the database, while non-sensitive data are stored in plaintext to support operational requirements. The implementation results show that sensitive data are stored as Base64-encoded ciphertext containing encrypted payloads, an Initialization Vector (IV), and a Message Authentication Code (MAC), making the data unreadable without a valid decryption key. The use of randomly generated IVs ensures that identical plaintext values produce different ciphertexts, thereby eliminating statistical patterns. Avalanche effect testing produced an average value of 49.73%, which is close to the ideal value of 50%, indicating a very strong diffusion property. In terms of performance, the encryption and decryption processes operate efficiently without causing significant system latency. This study concludes that the implementation of the AES-256-CBC algorithm is effective, reliable, and suitable for protecting customer data in MSME customer management systems with limited computational resources.

Keywords: *AES-256-CBC encryption, customer data security, MSME digitalization, field-level encryption, Laravel framework, OpenSSL implementation*

Abstrak

Keamanan data pelanggan merupakan tantangan penting bagi UMKM di Indonesia, khususnya dalam pengelolaan informasi sensitif yang masih banyak dilakukan secara konvensional dan rentan terhadap kebocoran data. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem manajemen pelanggan berbasis web yang aman pada Second and Destroy *Thrift Store* dengan menerapkan enkripsi tingkat kolom (*field-level encryption*) menggunakan algoritma *Advanced Encryption Standard* (AES) 256-bit dengan mode operasi *Cipher Block Chaining* (CBC). Sistem dikembangkan menggunakan framework Laravel dan basis data MySQL, dengan proses enkripsi dan dekripsi diimplementasikan melalui pustaka kriptografi OpenSSL pada lapisan model aplikasi. Atribut sensitif berupa nomor WhatsApp dan alamat pelanggan dienkripsi sebelum disimpan ke basis data, sementara data non-sensitif disimpan dalam bentuk plaintext untuk mendukung kebutuhan operasional sistem. Hasil implementasi menunjukkan bahwa data sensitif tersimpan dalam bentuk ciphertext berformat Base64 yang mengandung payload terenkripsi, *Initialization Vector* (IV), dan *Message Authentication Code* (MAC), sehingga tidak dapat dibaca tanpa kunci dekripsi yang valid. Penggunaan IV acak memastikan *plaintext* identik menghasilkan *ciphertext* yang berbeda, sehingga

menghilangkan pola statistik. Pengujian *avalanche effect* menghasilkan nilai rata-rata sebesar 49,73%, mendekati nilai ideal 50%, yang menunjukkan tingkat difusi yang sangat baik. Dari sisi performa, proses enkripsi dan dekripsi berjalan efisien tanpa menimbulkan latensi signifikan. Penelitian ini menyimpulkan bahwa penerapan algoritma AES-256-CBC efektif, andal, dan layak diterapkan untuk melindungi data pelanggan pada sistem manajemen UMKM dengan sumber daya komputasi terbatas.

Kata kunci: enkripsi AES-256-CBC, keamanan data pelanggan, digitalisasi UMKM, enkripsi tingkat kolom, framework Laravel, implementasi OpenSSL

Pendahuluan

Setiap kali seseorang berbelanja di toko retail dan memberikan nomor teleponnya untuk program loyalitas, sebuah pertanyaan mendasar seharusnya muncul: apakah data pribadi saya aman? Dalam realitas bisnis UMKM Indonesia saat ini, pertanyaan ini seringkali tidak memiliki jawaban yang memuaskan. Data pelanggan nama, nomor WhatsApp, alamat tersimpan dalam spreadsheet sederhana, notebook fisik, atau bahkan catatan kertas yang rentan hilang, rusak, atau jatuh ke tangan yang salah.

Kondisi ini bukan hanya masalah teknis, melainkan cerminan dari *gap* fundamental antara adopsi digital dan kesadaran keamanan informasi di kalangan pelaku usaha kecil. Bahkan lebih memprihatinkan, banyak UMKM yang sama sekali tidak memiliki sistem pencatatan data pelanggan, sehingga kehilangan peluang untuk membangun hubungan jangka panjang dengan pelanggan mereka.

Indonesia menghadapi paradoks digitalisasi. Di satu sisi, transformasi digital membawa peluang besar bagi bisnis untuk meningkatkan efisiensi dan daya saing [1], termasuk bagi UMKM sebagai salah satu sektor yang paling diuntungkan dari percepatan adopsi teknologi digital. Namun di sisi lain, peluang ini diiringi oleh risiko yang tidak kalah signifikan. Ancaman siber di Indonesia menunjukkan peningkatan dari tahun ke tahun, dengan berbagai bentuk *cybercrime* seperti *phishing*, *malware*, peretasan akun, dan serangan berbasis jaringan yang terus berkembang dan menjadi ancaman serius bagi individu maupun bisnis [2].

Mayoritas UMKM tidak memiliki infrastruktur keamanan yang memadai untuk melindungi data pelanggan yang mereka kumpulkan. Hal ini menciptakan risiko ganda: kehilangan kepercayaan konsumen dan potensi pelanggaran regulasi perlindungan data pribadi.

SECOND AND DESTROY Thrift Store, sebuah UMKM retail pakaian bekas di Jl. Kp. Pasir Limus, RT.07/RW.04, Wangunharja, Kec. Cikarang Utara, Cikarang, Jawa Barat 17530, menghadapi permasalahan klasik ini. Toko yang menawarkan berbagai produk *fashion* seperti *t-shirt*, jaket, hoody, kemeja *casual*, berbagai jenis celana, dan topi ini sama sekali tidak memiliki *database* pelanggan. Ketika mendapatkan stok produk baru yang sesuai dengan preferensi pelanggan setia mereka, toko tidak memiliki cara untuk menghubungi pelanggan tersebut. Kondisi ini menyebabkan hilangnya peluang penjualan dan ketidakmampuan untuk melacak riwayat pembelian pelanggan guna mendukung strategi *Customer Relationship Management (CRM)* yang efektif [3].

Untuk mengatasi permasalahan keamanan data ini, kriptografi modern menawarkan solusi yang telah terbukti efektif. *Advanced Encryption Standard (AES)* telah menjadi standar enkripsi global sejak adopsinya oleh *National Institute of Standards and Technology (NIST)* pada tahun 2001, menggantikan *Data Encryption Standard (DES)* yang sudah tidak memadai [4][5]. Tidak hanya mengandalkan kekuatan algoritma dan ukuran kunci, penerapan AES dalam sistem ini juga diperkuat melalui penggunaan mode operasi *Cipher Block Chaining* (CBC).

Mode CBC memastikan bahwa setiap blok *plaintext* diolah secara saling terkait dengan *ciphertext* blok sebelumnya sehingga tidak ada pola yang muncul dalam *ciphertext*, bahkan ketika format datanya seragam. Dengan memanfaatkan IV (*Initialization Vector*) acak pada blok pertama, CBC mencegah terjadinya kemiripan *ciphertext* meskipun *plaintext*-nya identik, sehingga tingkat keamanan data pelanggan dapat ditingkatkan secara signifikan[4]. AES dipilih melalui kompetisi ketat yang melibatkan 15 algoritma dari

seluruh dunia, dengan algoritma Rijndael karya Joan Daemen dan Vincent Rijmen keluar sebagai pemenang karena kombinasi optimal antara keamanan kriptografis, efisiensi komputasi, dan fleksibilitas implementasi [5].

AES-256, varian dengan kunci 256-bit, menawarkan keamanan tertinggi dengan 14 putaran enkripsi [6]. Setiap putaran melibatkan empat transformasi matematis: *SubBytes* untuk substitusi non-linear menggunakan *S-box*, *ShiftRows* untuk permutasi baris data, *MixColumns* untuk pencampuran kolom guna mencapai difusi yang optimal, dan *AddRoundKey* untuk pencampuran kunci putaran [7]. Dengan ruang kunci sebesar 2^{256}, AES-256 secara praktis tidak mungkin dipecahkan menggunakan serangan *brute force* bahkan dengan teknologi komputasi paling canggih saat ini [8].

Studi empiris menunjukkan bahwa AES-256 memiliki performa enkripsi dan dekripsi yang sangat efisien. Satria dan Sutabri menemukan bahwa AES dapat mengenkripsi pesan teks dalam 0,05 detik dan file multimedia dalam 0,2 detik tanpa membebani sumber daya perangkat secara signifikan [9]. Temuan ini mengindikasikan bahwa penggunaan AES-256 tetap layak untuk diterapkan pada aplikasi dengan kapasitas komputasi terbatas.

Dalam konteks sistem berbasis web seperti yang digunakan UMKM, kebutuhan komputasi untuk operasi *CRUD* relatif ringan sehingga waktu proses enkripsi maupun dekripsi tidak akan menghambat performa aplikasi secara keseluruhan. Efisiensi ini menegaskan bahwa AES-256 dapat digunakan untuk menjamin keamanan data pelanggan tanpa mengorbankan kecepatan akses maupun respons sistem, sekaligus memberikan perlindungan yang kuat terhadap potensi serangan siber.

Dalam konteks sistem manajemen pelanggan, implementasi *field-level encryption* menggunakan AES-256 memberikan perlindungan *robust* terhadap data sensitif. Baso dan Anriani menunjukkan bahwa implementasi AES-256 menggunakan *OpenSSL* efektif dalam melindungi informasi dari akses tidak sah dan meningkatkan tingkat keamanan data [10]. Bahkan jika terjadi kebocoran *database* atau akses tidak sah ke sistem penyimpanan, data pelanggan tetap tidak dapat dibaca tanpa kunci dekripsi yang valid.

Namun, keamanan sistem tidak hanya bergantung pada enkripsi data saja. Mekanisme autentikasi yang kuat diperlukan untuk memastikan hanya pengguna berwenang yang dapat mengakses sistem. Fungsi *hash* kriptografis seperti SHA-256 menghasilkan output 256-bit dengan karakteristik *one-way* yang ideal untuk penyimpanan *password* [11][12]. Penambahan *salt string* acak unik untuk setiap pengguna—sebelum *hashing* memberikan proteksi terhadap serangan *rainbow table* dan memastikan *password* yang sama menghasilkan *hash* berbeda [12].

Dalam implementasi praktis, framework Laravel menyediakan mekanisme autentikasi bawaan yang menggunakan algoritma *bcrypt*, yaitu algoritma hashing yang dirancang khusus untuk pengamanan *password*. *Bcrypt* memiliki karakteristik yang memenuhi prinsip dasar kriptografi modern seperti irreversibility, penggunaan *salt* secara otomatis pada setiap proses hashing, serta tingkat resistensi yang tinggi terhadap serangan *brute force*. Penelitian oleh Febrian et al. menunjukkan bahwa implementasi algoritma *bcrypt* pada framework Laravel menghasilkan nilai hash konstan sepanjang 60 karakter, dengan *cost factor* yang memengaruhi waktu proses hashing dan verifikasi hash [13]. Selain itu, penelitian Zulma et al. membuktikan bahwa kombinasi algoritma AES sebagai enkripsi data dan *bcrypt* sebagai hashing *password* dapat diimplementasikan secara efektif pada sistem berbasis web, serta mampu meningkatkan keamanan data pengguna [14].

Framework Laravel menyediakan ekosistem ideal untuk mengimplementasikan sistem dengan keamanan terintegrasi. Sebagai *PHP framework* dengan arsitektur *MVC*, Laravel menawarkan *built-in encryption* menggunakan OpenSSL dengan AES-256-CBC, *Eloquent ORM* untuk interaksi database yang aman melalui *prepared statements*, serta fitur autentikasi yang *robust*. Hasirun menunjukkan bahwa framework Laravel dapat meningkatkan keamanan perpustakaan digital, di mana pengujian menggunakan *OWASP ZAP 2* tidak

menemukan ancaman yang memiliki risiko tinggi [15]. Tahir menunjukkan bahwa sistem informasi *encrypt* dan *decrypt* menggunakan algoritma AES dengan framework Laravel dapat diimplementasikan secara efektif untuk mengamankan teks maupun file [16]. Fitur keamanan bawaan Laravel seperti proteksi terhadap *SQL Injection*, *automatic escaping* untuk XSS, dan *CSRF token protection* memberikan fondasi keamanan yang solid untuk aplikasi web.

Meskipun kebutuhan ideal UMKM dapat mencakup sistem CRM komprehensif dengan berbagai fitur lanjutan, penelitian ini secara khusus berfokus pada pembangunan sistem sederhana berbasis *CRUD* yang dilengkapi dengan enkripsi AES-256 untuk melindungi data pelanggan. Ruang lingkup difokuskan pada pencatatan data pelanggan nama, nomor WhatsApp, alamat dan riwayat transaksi secara aman sesuai kebutuhan operasional UMKM. Implementasi AES-256 pada sistem ini dilakukan melalui fungsi enkripsi dan dekripsi yang dirancang menggunakan pustaka kriptografi OpenSSL pada PHP, memberikan kontrol penuh terhadap proses kriptografi tanpa bergantung sepenuhnya pada fungsi bawaan Laravel.

Penelitian ini bertujuan merancang dan mengimplementasikan sistem manajemen pelanggan berbasis web yang sederhana namun aman untuk SECOND AND DESTROY Thrift Store. Sistem yang dibangun memungkinkan pemilik toko untuk mencatat data pelanggan secara terstruktur, melakukan operasi *CRUD (Create, Read, Update, Delete)*, dan mengakses data melalui autentikasi yang aman dengan semua data sensitif terenkripsi menggunakan AES-256 sebelum disimpan ke database. Dengan mendemonstrasikan implementasi kriptografi pada UMKM melalui aplikasi yang praktis dan langsung dapat digunakan, penelitian ini memberikan kontribusi praktis berupa sistem yang siap *deploy* serta kontribusi teoritis sebagai studi kasus *applied cryptography* pada konteks bisnis riil.

Metode Penelitian

Metodologi Metodologi penelitian ini merinci tahapan sistematis dalam merancang dan mengimplementasikan sistem manajemen pelanggan berbasis web dengan mekanisme *field-level encryption* menggunakan algoritma *Advanced Encryption Standard (AES) 256-bit* pada mode operasi *Cipher Block Chaining (CBC)*. Sistem dibangun menggunakan *framework Laravel*, namun penelitian ini tidak memanfaatkan fungsi enkripsi bawaan seperti *Crypt::encrypt()* atau *encryptString()*. Sebaliknya, proses enkripsi dan dekripsi diterapkan melalui fungsi manual yang ditulis sendiri oleh peneliti sehingga seluruh tahapan kriptografi mulai dari pemrosesan *plaintext*, operasi XOR, hingga pemanggilan mesin AES dapat diamati dan dikendalikan secara langsung. Walaupun fungsi enkripsi ditulis manual, penelitian tetap memanfaatkan pembangkit *Initialization Vector (IV)* dari Laravel melalui *random_bytes()* guna menghasilkan IV acak sepanjang 16 byte sesuai standar CBC. Pendekatan ini memadukan fleksibilitas Laravel sebagai *framework* dengan kontrol penuh terhadap mekanisme kriptografi, memungkinkan pengujian keamanan dilakukan lebih komprehensif dalam konteks kebutuhan UMKM.

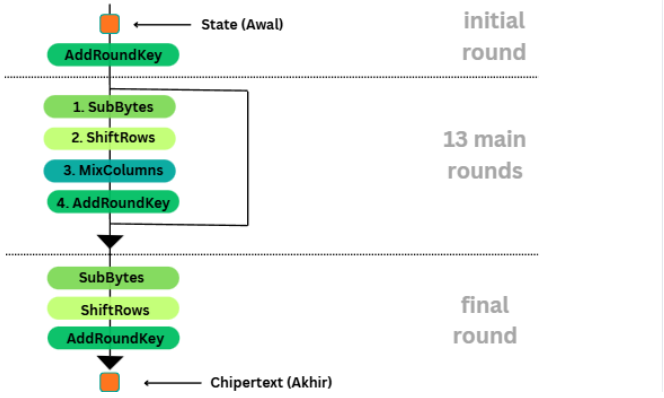
Pengembangan sistem dilakukan menggunakan metode *Agile* dengan pola iteratif melalui serangkaian *sprint*, di mana setiap sprint mencakup aktivitas analisis kebutuhan, perancangan komponen, implementasi fitur, pengujian fungsi dan keamanan, serta refleksi sebelum melanjutkan ke tahap berikutnya. Pendekatan ini dipilih karena sifatnya yang adaptif terhadap perubahan kebutuhan dan kemampuannya dalam mengintegrasikan mekanisme enkripsi secara bertahap tanpa mengganggu fungsionalitas sistem yang sedang berjalan. Dengan model iteratif ini, proses enkripsi–dekripsi dapat dievaluasi pada setiap siklus sehingga potensi kesalahan dapat diperbaiki sejak dini.

Penelitian ini berfokus pada implementasi sistem untuk *SECOND AND DESTROY Thrift Store*, sebuah UMKM yang membutuhkan sistem pencatatan pelanggan yang aman dan terstruktur. Ruang lingkup pengembangan mencakup pembuatan fitur dasar seperti pencatatan pelanggan, pengelolaan data melalui operasi CRUD, penerapan enkripsi AES-256-CBC pada kolom yang menyimpan informasi sensitif seperti nomor WhatsApp dan alamat, serta pengamanan autentikasi menggunakan mekanisme hashing. Penelitian

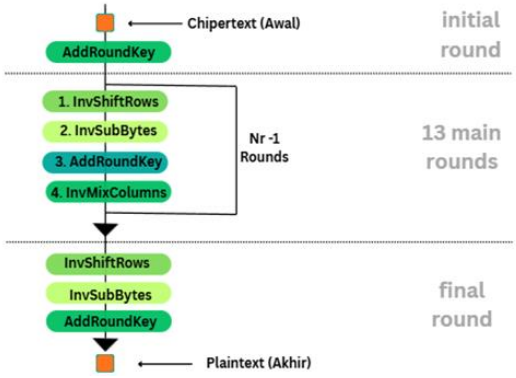
tidak mencakup integrasi modul analitik maupun fitur CRM lanjutan agar fokus tetap tertuju pada ketepatan penerapan enkripsi dan peningkatan keamanan data pelanggan.

Data penelitian dikumpulkan melalui observasi langsung terhadap proses pencatatan pelanggan pada UMKM dan identifikasi berbagai permasalahan keamanan yang muncul akibat metode konvensional. Wawancara dengan pemilik usaha dilakukan untuk menggali kebutuhan fungsional sistem serta tingkat urgensi perlindungan data. Selain itu, studi literatur digunakan untuk memperkuat landasan teoretis dengan menelaah algoritma kriptografi, mode operasi AES, serta praktik keamanan aplikasi web yang relevan, khususnya implementasi yang didukung oleh Laravel.

Secara teoretis, *Advanced Encryption Standard (AES)* merupakan algoritma kriptografi kunci simetris modern yang diadopsi *National Institute of Standards and Technology (NIST)* pada tahun 2001 sebagai pengganti DES. AES bekerja pada blok data 128-bit dan mendukung panjang kunci 128, 192, dan 256 bit; penelitian ini menggunakan varian 256-bit yang menawarkan tingkat keamanan tertinggi karena melibatkan 14 putaran pemrosesan. Tahapan kerja enkripsi dan dekripsi AES-256-CBC divisualisasikan melalui gambar 1 dan gambar 2 yang menggambarkan alur proses enkripsi dan dekripsi AES-256-CBC.



Gambar 1. Tahapan Kerja Enkripsi AES-256-CBC

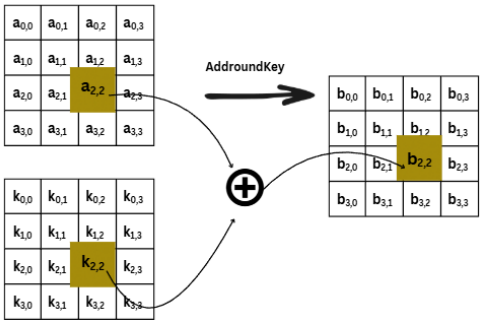


Gambar 2. Tahapan Kerja Dekripsi AES-256-CBC

Setiap putaran dalam algoritma AES tersusun atas beberapa transformasi utama yang bekerja secara berurutan dalam memodifikasi state. Agar proses ini dapat dipahami secara utuh, uraian berikut menjelaskan fungsi dan prinsip kerja dari setiap transformasi tersebut, disertai gambar ilustrasi untuk memperjelas mekanismenya.

AddRoundKey (Initial Round)

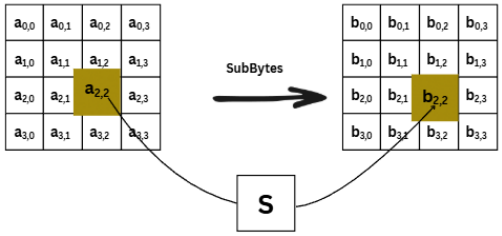
Tahap awal pada AES, di mana setiap byte pada state hasil pemetaan *plaintext* digabungkan dengan *byte* yang bersesuaian dari *round key* pertama melalui operasi XOR. Tahap ini berfungsi mengikat data dengan kunci rahasia sejak awal proses enkripsi, sehingga tanpa kunci yang benar, seluruh transformasi selanjutnya tidak dapat menghasilkan *plaintext* yang valid. Dengan melibatkan kunci secara langsung pada tahap awal, *AddRoundKey* menjadi elemen fundamental dalam memastikan keamanan setiap blok *ciphertext* yang dihasilkan.



Gambar 3. Ilustrasi Transformasi *AddRoundKey*

SubBytes / InvSubByte

Tahap Kedua, yaitu substitusi non-linear terhadap setiap *byte* menggunakan tabel S-Box. Fungsi utamanya adalah menambahkan sifat non-linearitas yang mencegah hubungan langsung antara *plaintext, ciphertext*, dan *key*. Prinsip kerjanya memanfaatkan transformasi matematis dalam Galois Field GF(2^8) sehingga setiap byte diganti dengan nilai lain yang tidak memiliki pola sederhana. Pada proses dekripsi, digunakan *Inverse S-Box* untuk memetakan kembali nilai tersebut secara tepat.



Gambar 4. Ilustrasi Transformasi *SubBytes / InvSubByte*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
A	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

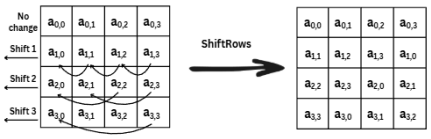
Gambar 5. S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
7	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
A	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
B	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
C	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
D	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
E	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
F	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 6. Inversi S-box

ShiftRows / InvShiftRows

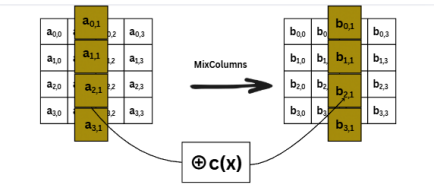
Tahap ketiga, yaitu operasi pergeseran baris secara sirkular ke kiri pada proses enkripsi dan ke kanan pada proses dekripsi. Fungsi utama tahap ini adalah menciptakan difusi horizontal dengan menggeser posisi *byte* dalam setiap baris sehingga kolom-kolom baru terbentuk dan bercampur dengan byte lain pada putaran selanjutnya. Prinsip kerjanya sederhana tetapi sangat penting karena menghilangkan struktur berulang yang dapat dimanfaatkan dalam serangan kriptanalisis.



Gambar 7. Ilustrasi Transformasi *ShiftRows / InvShiftRows*

MixColumns / InvMixColumn

Tahap keempat, yaitu *MixColumns*, merupakan transformasi linier yang bekerja pada level kolom *state*. Setiap kolom *state* diperlakukan sebagai sebuah vektor dan dikalikan dengan matriks tetap yang didefinisikan dalam medan hingga *Galois Field* GF(2^8). Transformasi ini bertujuan untuk meningkatkan difusi dengan mencampurkan setiap *byte* dalam satu kolom, sehingga perubahan kecil pada data masukan akan memengaruhi keempat *byte* dalam kolom tersebut secara bersamaan. Melalui mekanisme ini, setiap byte hasil setelah beberapa putaran tidak lagi memiliki keterkaitan langsung dengan *byte* asalnya. Pada proses dekripsi, transformasi ini dibalik menggunakan matriks invers (*InvMixColumns*) untuk mengembalikan struktur data ke kondisi sebelum enkripsi.



MixColumns

$$b_{0,0} = (02 \cdot a_{0,0}) \oplus (03 \cdot a_{1,0}) \oplus (01 \cdot a_{2,0}) \oplus (01 \cdot a_{3,0})$$
$$b_{1,0} = (01 \cdot a_{0,0}) \oplus (02 \cdot a_{1,0}) \oplus (03 \cdot a_{2,0}) \oplus (01 \cdot a_{3,0})$$
$$b_{2,0} = (01 \cdot a_{0,0}) \oplus (01 \cdot a_{1,0}) \oplus (02 \cdot a_{2,0}) \oplus (03 \cdot a_{3,0})$$
$$b_{3,0} = (03 \cdot a_{0,0}) \oplus (01 \cdot a_{1,0}) \oplus (01 \cdot a_{2,0}) \oplus (02 \cdot a_{3,0})$$

InvMixColumn

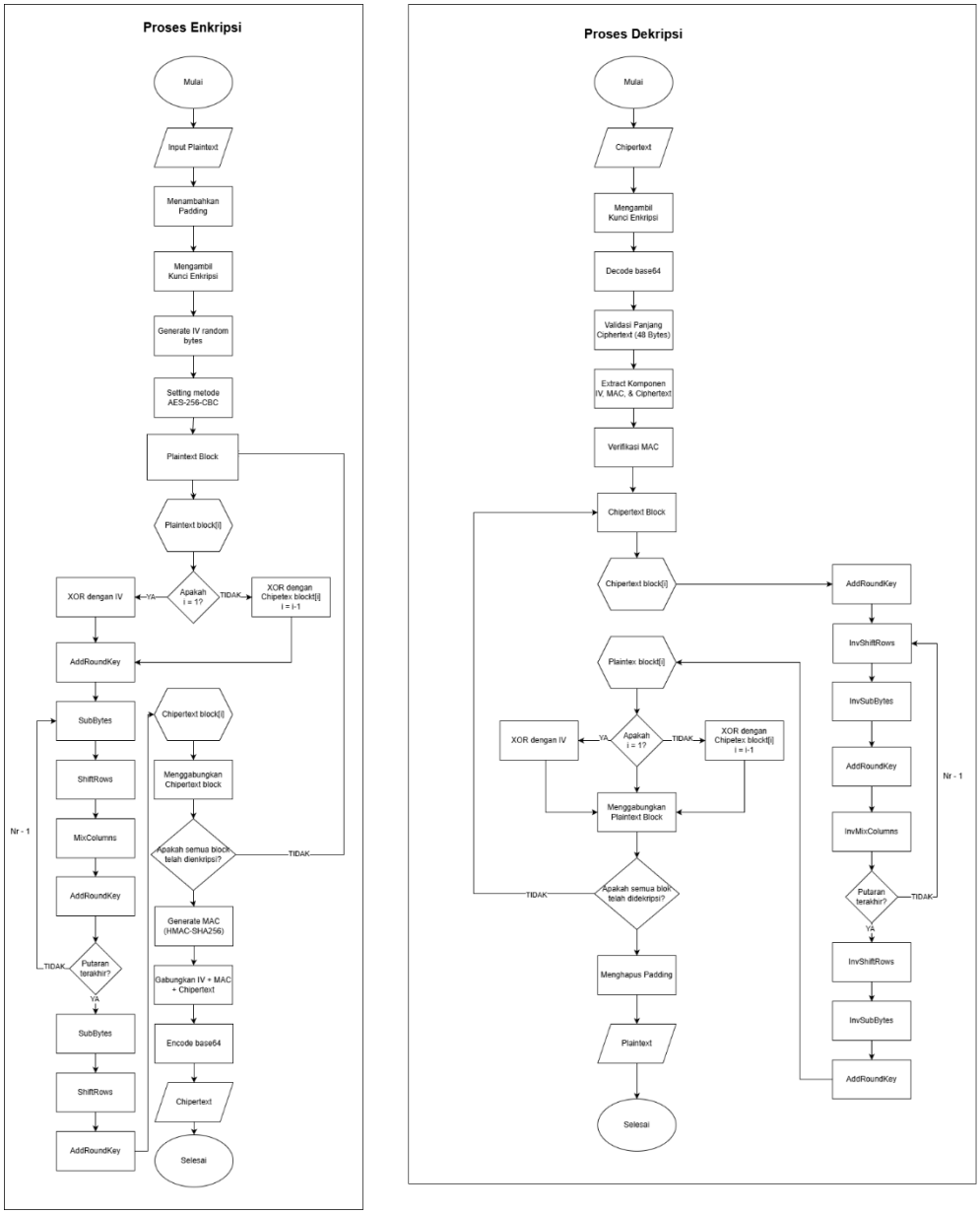
$$a_{0,0} = (0E \cdot b_{0,0}) \oplus (0B \cdot b_{1,0}) \oplus (0D \cdot b_{2,0}) \oplus (09 \cdot b_{3,0})$$
$$a_{1,0} = (09 \cdot b_{0,0}) \oplus (0E \cdot b_{1,0}) \oplus (0B \cdot b_{2,0}) \oplus (0D \cdot b_{3,0})$$
$$a_{2,0} = (0D \cdot b_{0,0}) \oplus (09 \cdot b_{1,0}) \oplus (0E \cdot b_{2,0}) \oplus (0B \cdot b_{3,0})$$
$$a_{3,0} = (0B \cdot b_{0,0}) \oplus (0D \cdot b_{1,0}) \oplus (09 \cdot b_{2,0}) \oplus (0E \cdot b_{3,0})$$

Gambar 8. Ilustrasi Transformasi *MixColumns*

AddRoundKey

Di akhir setiap putaran, proses kembali melakukan *AddRoundKey* untuk menggabungkan *state* yang telah dimodifikasi dengan *round key* berikutnya. Langkah ini mengunci kembali hasil transformasi sebelumnya sehingga setiap putaran menghasilkan kombinasi unik antara data dan kunci. Pada putaran terakhir, *MixColumns* dihilangkan sesuai desain AES, tetapi *AddRoundKey* tetap menjadi tahap penutup yang memastikan keamanan *ciphertext* secara keseluruhan.

Setelah penjabaran setiap transformasi AES, alur lengkap proses enkripsi dan dekripsi divisualisasikan melalui flowchart pada Gambar 9. Pada sisi kiri, flowchart menunjukkan bagaimana *plaintext* dipersiapkan, dibagi per blok, lalu diproses melalui putaran AES-256-CBC hingga menghasilkan *ciphertext*. Sementara itu, sisi kanan menggambarkan proses dekripsi yang berlangsung secara terbalik, di mana *ciphertext* dipulihkan kembali blok demi blok hingga membentuk *plaintext* semula. Setelah seluruh blok selesai diproses, padding dihapus sehingga data asli dapat diperoleh kembali secara utuh.

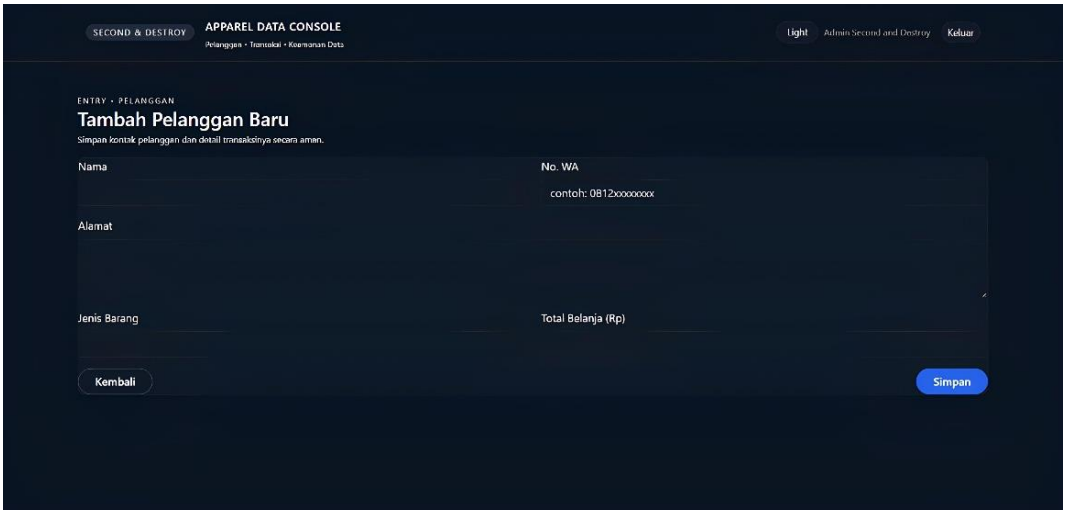


Gambar 9. Flowchart Enkripsi(Kiri) dan Dekripsi(Kanan) AES 256bit mode CBC

Hasil dan Pembahasan

Hasil Implementasi sistem manajemen data pelanggan pada Second and Destroy Thrift Store telah berhasil dikembangkan menggunakan kerangka kerja Laravel dengan fokus utama pada pengamanan privasi data. Berbeda dengan sistem pencatatan konvensional yang rentan terhadap kebocoran informasi, sistem yang dibangun menerapkan mekanisme enkripsi tingkat kolom (*field-level encryption*) sebelum data disimpan ke dalam basis data MySQL. Dalam arsitektur sistem ini, data diklasifikasikan menjadi dua kategori: data publik dan data rahasia. Atribut identitas umum seperti nama pelanggan dan total belanja disimpan dalam format teks asli (plaintext) untuk memfasilitasi pencarian dan operasi aritmatika, sedangkan atribut sensitif yang mencakup nomor WhatsApp dan alamat pelanggan diwajibkan melalui proses enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit.

Proses input data dimulai pada antarmuka admin, di mana pengguna memasukkan data pelanggan secara normal. Pada tahap ini, sistem belum melakukan enkripsi hingga tombol simpan ditekan, seperti yang terlihat pada antarmuka input data di bawah ini.



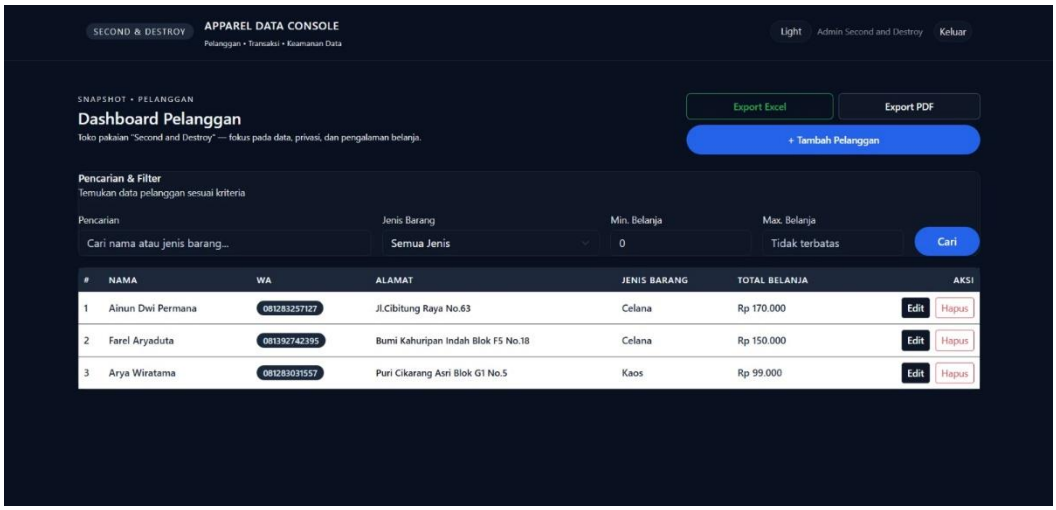
Gambar 10. Interface Input Data

Setelah data disubmit, mekanisme enkripsi berjalan secara otomatis pada lapisan model aplikasi memanfaatkan pustaka *OpenSSL* yang terintegrasi dalam fitur casting *Eloquent ORM Laravel*. Hal ini menjamin bahwa data sensitif tidak pernah menyentuh media penyimpanan dalam bentuk yang dapat dibaca. Efektivitas penerapan kriptografi ini dibuktikan melalui pemeriksaan langsung pada penyimpanan basis data MySQL. Sebagaimana ditunjukkan pada Gambar 11, atribut nomor WhatsApp dan alamat telah bertransformasi menjadi ciphertext berupa string acak yang panjang, semenetara nama tetap terbaca.

id	nama	wa	alamat	jenis_barang	total_belanja	created_at	updated_at
14	Arya Wiratama	mQy4Bjf+NcA5RdKpYejNBbIfokVBU/XUQsQVduwFq/9T5y4C6i...	ums58JlyvGOVCAJc2UkJgLUlfTlR8CLTgp9gd7BAgtiAJEzz67...	Kaos	99000.00	2025-12-09 14:29:01	2025-12-09 14:29:01
15	Farel Aryaduta	tcwtPaPBhfBEbhwgjwZJ9vs43iw260Q24WB8pFQbwv8J3zx5fD...	m2YFfUXepPF452tt9duhJbKebrw/mNO8e/PajDvhvk7eZbd9dF...	Celana	150000.00	2025-12-09 14:29:42	2025-12-09 14:29:55
16	Ainun Dwi Permana	8W8zgQ0ZU6aHUwiTDEfl68haK2EVYV8cfc3UsXpmrnyF7N81mF...	FGVPdOVGxD8uu3ADcuPCRTS6NHrfDxCwtes+YS1J2H0TsVuzRl...	Celana	170000.00	2025-12-09 14:30:45	2025-12-09 14:30:45

Gambar 11. Basis Data Pelanggan

String acak tersebut merupakan hasil enkripsi Base64 yang mengandung payload terenkripsi, *Initialization Vector* (IV), dan *Message Authentication Code* (MAC). Hal ini menegaskan bahwa jika terjadi insiden keamanan seperti akses ilegal ke basis data (*SQL Injection*), pihak yang tidak berwenang tidak akan dapat mengekstraksi informasi kontak pelanggan tanpa memiliki kunci dekripsi yang valid. Namun, bagi pengguna yang memiliki otorisasi (Admin), sistem secara otomatis melakukan dekripsi saat data dipanggil kembali ke halaman dashboard, mengembalikan informasi ke format aslinya yang dapat dibaca.



Gambar 12. Dashboard Admin Second and Destroy

Perbandingan representasi data pada kedua gambar di atas diringkas dalam tabel berikut untuk memperjelas status keamanan pada setiap tahapan proses.

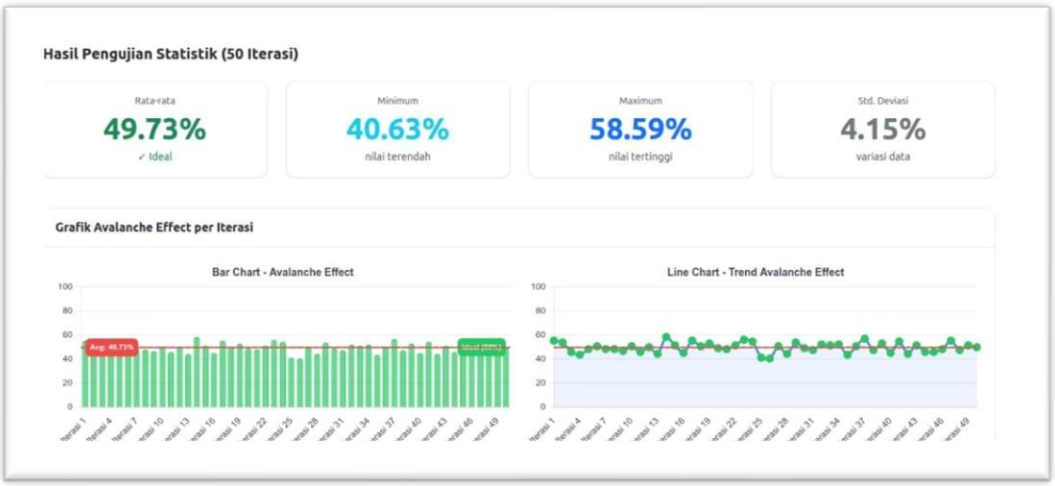
Tabel 1. Gambaran Perbandingan Representasi Data pada Antarmuka dan Basis Data

Atribut Data	Input Admin (Plain Text)	Penyimpanan Database MySQL (Ciphertext)	Tampilan Dashboard (Decrypted)
Nama	Budi Santoso	Budi Santoso	Budi Santoso
No. WA	0812-3456-7890	ESS6UN7eG/uU…	0812-3456-7890
Alamat	Jl. Pasir Limus...	doLu+Q+AEs5Y…	Jl. Pasir Limus...

Analisis lebih lanjut terhadap hasil enkripsi pada Gambar 11 menunjukkan peran krusial dari mode operasi *Cipher Block Chaining* (CBC). Dalam pengujian teknis, penggunaan *Initialization Vector* (IV) yang dibangkitkan secara acak menyebabkan dua entri data dengan nilai plaintext yang sama akan menghasilkan ciphertext yang sepenuhnya berbeda di dalam basis data. Mekanisme ini secara efektif menghilangkan pola statistik dalam data terenkripsi, sehingga menutup celah bagi serangan kriptanalisis. Keamanan ini didukung oleh kekuatan matematis algoritma AES-256, membuat serangan brute force menjadi mustahil dilakukan secara komputasi dengan teknologi saat ini. Dari sisi performa operasional, implementasi enkripsi AES-256 terbukti efisien dan tidak membebani kinerja sistem secara signifikan. Sesuai dengan studi literatur yang menyebutkan bahwa AES mampu mengenkripsi data teks dalam waktu yang sangat singkat, pengujian pada aplikasi menunjukkan bahwa proses transisi data dari plaintext ke ciphertext dan sebaliknya berjalan mulus tanpa latensi yang mengganggu pengalaman pengguna. Hal ini mengonfirmasi bahwa AES-256 layak diterapkan pada sistem UMKM dengan sumber daya komputasi terbatas, memberikan solusi manajemen yang tidak hanya fungsional tetapi juga aman.

Untuk memastikan bahwa algoritma AES-256 tidak hanya aman secara teoretis tetapi juga kuat secara kriptografis dalam implementasi nyata, dilakukan pengujian lanjutan menggunakan metode *avalanche effect*. Pengujian dilakukan sebanyak 50 iterasi dengan pasangan plaintext yang hanya mengalami perubahan kecil pada satu atau dua karakter.

Berdasarkan hasil yang ditampilkan pada Gambar 13, diperoleh nilai *avalanche effect* dengan rata-rata sebesar 49,73%, yang sangat mendekati nilai ideal 50%. Nilai minimum tercatat sebesar 40,63%, sedangkan nilai maksimum mencapai 58,59%, dengan simpangan baku sebesar 4,15%. Hasil ini menunjukkan bahwa perubahan kecil pada plaintext mampu menghasilkan perubahan bit yang signifikan pada ciphertext.



Gambar 13. Hasil Pengujian *Avalanche Effect* Algoritma AES-256-CBC

Nilai *avalanche effect* yang berada pada rentang 46,09% hingga 51,17% menunjukkan bahwa algoritma AES-256-CBC memiliki tingkat difusi yang sangat baik. Artinya, setiap perubahan kecil pada data masukan akan memengaruhi hampir setengah dari keseluruhan bit keluaran. Karakteristik ini sangat penting dalam sistem keamanan data karena mampu mencegah penyerang melakukan analisis hubungan antara *plaintext* dan *ciphertext* secara statistik maupun diferensial.

Grafik batang dan grafik garis pada Gambar 13 memperlihatkan bahwa distribusi nilai *avalanche effect* relatif stabil di sekitar nilai rata-rata. Tidak terlihat fluktuasi ekstrem atau pola anomali yang mengindikasikan kelemahan difusi. Konsistensi ini menegaskan bahwa algoritma AES-256-CBC memiliki karakteristik difusi yang baik, di mana hampir setengah dari bit keluaran berubah akibat modifikasi kecil pada data masukan.

Karakteristik tersebut sangat penting dalam sistem keamanan data karena mampu mencegah penyerang melakukan analisis statistik maupun diferensial terhadap hubungan antara *plaintext* dan *ciphertext*. Dengan demikian, hasil pengujian ini membuktikan bahwa implementasi algoritma AES-256-CBC telah berjalan dengan benar, stabil, dan memenuhi prinsip kriptografi modern.

Berdasarkan hasil pengujian visual dan numerik tersebut, dapat disimpulkan bahwa penggunaan algoritma AES-256 dengan mode operasi *Cipher Block Chaining* (CBC) pada sistem manajemen pelanggan UMKM aman, andal, dan layak diterapkan untuk melindungi data sensitif dari berbagai potensi serangan kriptografi.

Sejalan dengan kesimpulan tersebut, Gambar 14 menampilkan dokumentasi kegiatan penelitian yang dilakukan di lokasi UMKM sebagai bagian dari proses observasi, implementasi, dan pengujian sistem secara langsung. Dokumentasi ini menunjukkan keterlibatan aktif peneliti dalam memastikan bahwa sistem manajemen pelanggan yang dikembangkan dapat berjalan sesuai dengan rancangan serta kebutuhan operasional UMKM di lapangan.

Kegiatan observasi dan implementasi yang dilakukan secara langsung memungkinkan peneliti untuk menyesuaikan sistem dengan kondisi nyata, termasuk pola pengelolaan data pelanggan dan proses operasional yang berlangsung. Dengan demikian, penerapan algoritma AES-256 dengan mode operasi *Cipher Block Chaining* (CBC) tidak hanya diuji melalui pengujian teknis dan analisis numerik, tetapi juga divalidasi dalam lingkungan penggunaan sesungguhnya.

Melalui dokumentasi ini, dapat ditegaskan bahwa hasil penelitian tidak hanya bersifat teoritis, tetapi juga aplikatif dan relevan untuk diterapkan pada sistem manajemen pelanggan UMKM. Implementasi sistem

keamanan data yang telah diuji secara langsung di lapangan diharapkan mampu meningkatkan kepercayaan pelaku UMKM dalam melindungi data sensitif pelanggan dari berbagai potensi risiko keamanan informasi.

Gambar 13. Dokumentasi Kegiatan Penelitian

Kesimpulan

Sistem manajemen pelanggan Second and Destroy *Thrift Store* berhasil mengimplementasikan *field-level encryption* menggunakan algoritma AES-256-CBC, memastikan data sensitif seperti nomor WhatsApp dan alamat pelanggan terenkripsi dengan aman di basis data. Pengujian *avalanche effect* menunjukkan perubahan minor pada *plaintext* menghasilkan perubahan bit *ciphertext* rata-rata mendekati 50%, menandakan tingkat difusi optimal. Dengan demikian, sistem ini terbukti aman, andal, dan layak diterapkan pada UMKM dengan sumber daya komputasi terbatas, sekaligus melindungi data pelanggan dari potensi serangan kriptografi.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada **Bapak Muhammad Najamuddin Dwi Miharja, S.Kom, M.Kom**, selaku dosen mata kuliah Kriptografi, atas bimbingan, arahan, dan ilmu yang telah diberikan. Ilmu dan pengalaman yang Bapak bagikan sangat membantu penulis dalam memahami konsep enkripsi, penerapan AES-256, dan pengujian *avalanche effect*, sehingga penelitian ini dapat terselesaikan dengan baik.

Daftar Rujukan

[1] D. Sinaga and P. Peniarsih, "Menghadapi perubahan dunia melalui transformasi digital menuju kesuksesan pada era digitalisasi," JSI (Jurnal Sistem Informasi) Universitas Suryadarma, vol. 11, no. 2, pp. 51–58, 2024. doi: 10.35968/jsi.v11i2.1240.

[2] R. D. Hapsari and K. G. Pambayun, "Ancaman cybercrime di Indonesia: Sebuah tinjauan pustaka sistematis," Jurnal Konstituen, vol. 5, no. 1, pp. 1–17, 2023. doi: 10.33701/jk.v5i1.3208.

[3] N. A. Nabilah, "Customer Relationship Management (CRM) pada UMKM Indonesia – Literature review," Manajemen Inovasi Bisnis dan Strategi, vol. 7, no. 1, pp. 54–66, Jul. 2023.

[4] A. Satria, D. Nanda, R. Herlambang, and N. Pravitasari, "Penerapan kriptografi AES untuk keamanan data aplikasi pemesanan bibit ternak pada BPSI UAT," Remik, vol. 8, pp. 29–44, 2024.

[5] N. Mouha, "Review of the Advanced Encryption Standard," NIST Interagency Report (NISTIR) 8319, National Institute of Standards and Technology, May 2021.

[6] R. Indrayani, P. Ferdiansyah, and M. Koprawi, "Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format," *Digital Transformation Technology (Digitech)*, vol. 4, no. 2, pp. 1245–1251, 2025, doi: 10.47709/digitech.v4i2.5457.

[7] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis keamanan data dengan menggunakan kriptografi modern algoritma Advance Encryption Standard (AES)," Jurnal Media Informatika, vol. 4, no. 2, pp. 97–101, Jun. 2023. doi: 10.55338/jumin.v4i2.435.

[8] J. S. Putra, "Tinjauan terhadap implementasi Advanced Encryption Standard 256 dalam keamanan data," DEVICE: Journal of Information System, Computer Science and Information Technology, vol. 5, no. 2, pp. 45–53, Dec. 2024.

[9] A. Satria, B. Piwari and T. Sutarbi, "Implementasi Algoritma Kriptografi AES untuk Keamanan Data pada Aplikasi Pesan Instan Berbasis Android," *Jurnal Ilmiah Teknik Informatika dan Komunikasi*, vol. 5, no. 2, pp. 541–547, 2025. doi: 10.55606/juitik.v5i2.1167.

[10] F. Baso and N. Anriani L, "Implementasi teknik kriptografi dengan metode AES 256 untuk keamanan file," Information Technology Education Journal, vol. 3, no. 3, pp. 84–87, Sep. 2024.

[11] S. A. Rahmah et al., "Analisis terhadap keamanan password menggunakan hash SHA-256," Jurnal Quancom: Quantum Computer Jurnal, vol. 2, no. 2, pp. 9–16, 2024.

[12] H. Herman, R. Wijaya, and S. Miharja, "Implementasi algoritma AES-128 dan SHA-256 dalam perancangan aplikasi pengamanan file dokumen," Jurnal TIMES, vol. 10, no. 2, pp. 80–87, Jan. 2022.

[13] D. Febrian, Yuhandri, and Sumijan, "Implementation of Bcrypt Algorithm on Website-Based Hashing Generator Using Laravel Framework," J. Inf. Syst. Informatics Comput. (JISICOM), vol. 7, no. 2, pp. 199–212, Dec. 2023, doi: 10.52362/jisicom.v7i2.1130.

[14] G. D. M. Zulma, H. B. Seta, and T. Yuniati, "Implementasi Algoritma AES dan Bcrypt untuk Pengamanan File Dokumen," Inform. J. Ilmu Komput., vol. 18, no. 2, pp. 163–172, 2022, doi: 10.52958/iftk.v18i2.4667.

[15] Hasirun, "Implementasi framework Laravel dan enkripsi IONCUBE encode untuk meningkatkan keamanan pada perpustakaan digital," Jurnal Borneo Informatika dan Teknik Komputer, vol. 4, no. 1, pp. 32–43, 2024.

[16] T. B. Tahir, "Sistem informasi encrypt dan decrypt dengan algoritma AES menggunakan framework Laravel," Patria Artha Technological Journal, vol. 4, no. 1, pp. 38–45, Apr. 2020.