ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

IMPLEMENTASI ALGORITMA AES-256 DALAM ENKRIPSI PENGAMANAN DATA PADA PT KALLISTA PRIMA

Rifaldi Mahsyaf Azmi✉, Ali Ikhwan
Program Studi Sistem Informasi, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: rifaldimahsyaf@gmail.com

DOI: https://doi.org/10.46880/jmika.Vol10No1.pp62-69

ABSTRACT

This study aims to implement the Advanced Encryption Standard (AES-256) algorithm to secure pharmaceutical product price data in a product management system, with a case study on the AB-VAS K – TABLET product at PT Kallista Prima. The background of this study is based on the importance of protecting price data (HNA, HNA+PPN, and HET) from the risk of manipulation and unauthorized access within pharmaceutical distribution information systems. The research method includes system design, encryption and decryption processes using AES-256 with a 256-bit key length and 14 transformation rounds, as well as security testing through avalanche effect analysis and comparison with other cryptographic algorithms such as DES and 3DES. The results show that all price data were successfully transformed into ciphertext with no recognizable patterns and could be restored identically through the decryption process, ensuring data integrity. The testing also demonstrates that small changes in plaintext produce significant changes in ciphertext and provide better diffusion performance compared to DES and 3DES algorithms, thereby improving the overall security level of the system. With a key space complexity of 2^{256} and the ability to be implemented without modifying the existing operational database structure, the AES-256 algorithm is considered effective in maintaining the confidentiality and integrity of price data and suitable to be applied as a data security model in pharmaceutical distribution information systems.

Keyword: AES-256, Cryptography, Data Encryption, Information Security, Pharmaceutical Product Management System.

ABSTRAK

Penelitian ini bertujuan untuk mengimplementasikan algoritma Advanced Encryption Standard (AES-256) dalam mengamankan data harga produk farmasi pada sistem manajemen produk, dengan studi kasus pada produk AB-VAS K – TABLET di PT Kallista Prima. Latar belakang penelitian ini didasarkan pada pentingnya perlindungan data harga (HNA, HNA+PPN, dan HET) dari risiko manipulasi dan akses tidak sah dalam sistem informasi distribusi farmasi. Metode yang digunakan meliputi perancangan sistem, proses enkripsi dan dekripsi menggunakan AES-256 dengan panjang kunci 256-bit dan 14 ronde transformasi, serta pengujian keamanan melalui analisis avalanche effect dan perbandingan dengan algoritma kriptografi lain seperti DES dan 3DES. Hasil penelitian menunjukkan bahwa seluruh data harga berhasil diubah menjadi ciphertext yang tidak memiliki pola dan dapat dikembalikan secara identik melalui proses dekripsi sehingga integritas data tetap terjaga. Pengujian juga menunjukkan bahwa perubahan kecil pada plaintext menghasilkan perubahan signifikan pada ciphertext, serta menghasilkan tingkat difusi yang lebih baik dibandingkan algoritma DES dan 3DES, sehingga meningkatkan tingkat keamanan sistem. Dengan kompleksitas kunci sebesar 2^{256} dan kemampuan implementasi tanpa perubahan struktur basis data operasional, algoritma AES-256 dinyatakan efektif dalam menjaga kerahasiaan dan integritas data harga serta layak diterapkan sebagai model pengamanan data pada sistem informasi distribusi farmasi.

Kata Kunci: AES-256, Kriptografi, Enkripsi Data, Keamanan Informasi, Sistem Manajemen Produk Farmasi.

PENDAHULUAN

Perkembangan teknologi informasi memberikan kemudahan dalam pengelolaan data perusahaan, namun di sisi lain meningkatkan risiko ancaman terhadap keamanan dan kerahasiaan data (Baqis & Nasution, 2025). Berbagai kasus kebocoran data menunjukkan bahwa sistem tanpa mekanisme pengamanan yang memadai rentan terhadap penyadapan, pencurian, maupun manipulasi informasi (Asherli & Wiraguna, 2025). Oleh karena itu, penerapan algoritma *kriptografi* menjadi salah satu solusi penting dalam menjaga

ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

kerahasiaan dan integritas data operasional perusahaan (Samsudin et al., 2022).

PT Kallista Prima sebagai distributor farmasi di Indonesia mengelola berbagai data sensitif seperti data transaksi pelanggan (rumah sakit, apotek, dan klinik), riwayat pesanan, data stok obat, serta laporan keuangan (Ramadhan, 2025). Berdasarkan hasil observasi awal, sebagian data operasional tersebut belum dilindungi dengan mekanisme enkripsi secara menyeluruh pada proses penyimpanan maupun pertukaran data dalam jaringan internal. Kondisi ini berpotensi menimbulkan risiko kebocoran data dan manipulasi informasi yang dapat mempengaruhi stabilitas operasional perusahaan (Purba et al., 2025).

Beberapa penelitian sebelumnya telah mengimplementasikan algoritma *Advanced Encryption Standard* (AES-256) pada berbagai sistem keamanan informasi. (Fachrezi et al., 2026) menerapkan *AES-256-CBC* pada aplikasi *web* untuk pengamanan *database*. (Aditya & Romli, 2025) menggunakan *AES-256* pada sistem pengamanan dokumen notaris berbasis *web* dan *mobile*. (Ridho & Romli, 2024) mengembangkan sistem pengamanan dokumen digital menggunakan *AES-256*. (Khoirunnisa et al., 2025) menerapkan *AES* pada proses autentikasi *login website*. Sedangkan, (Diah et al., 2023) mengimplementasikan *AES-256* pada aplikasi pengamanan dokumen perusahaan berbasis *Android*. Namun demikian, penerapan AES-256 pada sistem informasi manajemen distributor farmasi yang mencakup data transaksi, pelanggan, dan logistik perusahaan masih belum banyak dikaji secara khusus (Samsudin et al., 2021).

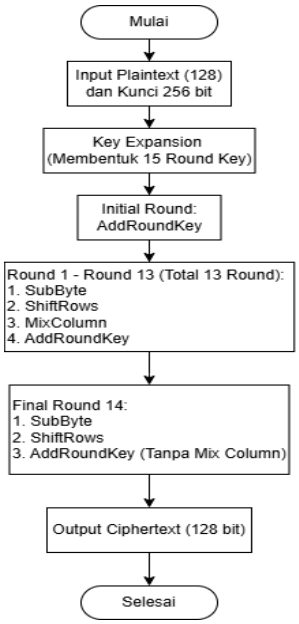
Berbeda dengan penelitian sebelumnya yang berfokus pada pengamanan dokumen digital atau autentikasi sistem secara parsial, penelitian ini mengimplementasikan algoritma *AES-256* secara terintegrasi pada sistem informasi manajemen distributor farmasi, khususnya pada data operasional sensitif seperti data transaksi, data pelanggan, dan data logistik. Implementasi dilakukan pada level *database* sehingga pengamanan tidak hanya terbatas pada satu modul sistem, tetapi diterapkan secara menyeluruh pada struktur data utama perusahaan (Harahap et al., 2026). Selain itu, penelitian ini juga melakukan evaluasi sensitivitas hasil enkripsi menggunakan pengujian *avalanche effect* untuk memastikan kualitas *difusi ciphertext* yang dihasilkan.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengimplementasikan algoritma *AES-256* pada sistem informasi manajemen di PT Kallista Prima guna meningkatkan keamanan data transaksi, pelanggan, dan logistik perusahaan. Hasil penelitian diharapkan dapat memberikan kontribusi praktis berupa model implementasi pengamanan data berbasis *kriptografi* yang dapat diterapkan pada sistem distribusi farmasi.

METODE PENELITIAN

Tahapan Penelitian

Pada penelitian ini digunakan algoritma *Advanced Encryption Standard* (AES) *256 bit* sebagai metode pengamanan data. *AES-256* bekerja melalui serangkaian proses enkripsi yang terstruktur dalam beberapa tahapan hingga menghasilkan *ciphertext* (Henry et al., 2016). Alur tahapan enkripsi *AES-256* pada penelitian ini ditunjukkan pada Gambar 1.



Gambar 1. Alur Tahapan Penelitian

Berdasarkan Gambar 1, proses enkripsi dimulai dari input *plaintext* dan kunci *256 bit*, dilanjutkan dengan proses *key expansion*, *initial round*, *13 round* utama, dan *final round* hingga menghasilkan *ciphertext* (Ikhwan et al., 2019).. Tahapan enkripsi dijelaskan sebagai berikut.

1. *Input Plaintext* dan Kunci *256 Bit*

Proses enkripsi diawali dengan memasukkan *plaintext* berukuran *128 bit* (16 byte) serta kunci sepanjang *256 bit* (32 byte). *Plaintext* direpresentasikan dalam bentuk *matriks state* berukuran *4×4 byte* sebagai berikut:

$$State = \begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} \quad (1)$$

Matriks inilah yang akan diproses pada setiap tahapan enkripsi.

2. *Key Expansion* (Pembangkitan Round Key)

Pada *AES-256* dilakukan proses *key expansion* untuk menghasilkan *15 round key* yang digunakan pada proses enkripsi. Dengan parameter *AES-256* diketahui bahwa jumlah *word* awal *(Nk) = 8* dan jumlah *round (Nr) = 14* sehingga jumlah total *word* adalah:

$$Nb(Nr + 1) = 4(14 + 1) = 60\ word \quad (2)$$

Round key dibangkitkan menggunakan operasi *XOR* dan fungsi transformasi:

$$W_i = W_{i-8} \oplus T(W_{i-1}) \quad (3)$$

dengan:

$$T(W) = SubW\ ord(RotWord(W)) \oplus Rcon \quad (4)$$

3. *Initial Round – AddRoundKey*

Tahapan initial *round* dilakukan melalui operasi *XOR* antara *state* dan *round key* pertama:

$$State = State \oplus RoundKey \quad (5)$$

atau secara elemen matriks:

$$C_{i,j} = S_{i,j} \oplus K_{i,j} \quad (6)$$

Tahap ini bertujuan untuk menggabungkan data dengan kunci awal sebelum memasuki proses transformasi utama.

4. *Round 1* sampai *Round 13*

Pada *AES-256* terdapat *13 round* utama yang terdiri dari empat transformasi:

SubBytes

$$S'(x) = SBox(x) \quad (7)$$

ShiftRows

$$S'_{r,c} = S_{r,(c+r)\ mod\ 4} \quad (8)$$

MixColumns

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad (9)$$

Transformasi dilakukan menggunakan operasi perkalian matriks dalam medan hingga *GF(2⁸)*.

AddRoundKey

$$State = State \oplus RoundKey_r \quad (10)$$

5. *Final Round* (Round ke-14)

Final round terdiri dari tiga transformasi yaitu *SubBytes*, *ShiftRows*, *AddRoundKey* tanpa proses *MixColumns*.

6. *Output Ciphertext*

Setelah seluruh proses enkripsi selesai, *state* akhir menjadi *ciphertext* berukuran *128 bit*:

$$C = E_K(P) \quad (11)$$

Ciphertext selanjutnya disimpan sebagai data yang telah diamankan dalam sistem (Jannah et al., 2025).

Perbandingan Metode *Kriptografi*

Untuk memperkuat pemilihan metode, algoritma *AES-256* dibandingkan secara konseptual dengan beberapa metode kriptografi lain yang umum digunakan dalam pengamanan data sistem informasi. (Widodo & Purnomo, 2020).

Tabel 1. Perbandingan Metode Kriptografi

Metode	Jenis	Kelebihan	Kekurangan
AES-256	Simetris	Proses cepat, keamanan tinggi, efisien untuk database	Distribusi kunci harus aman
RSA	Asimetris	Mendukung pertukaran kunci publik	Proses lebih lambat
DES	Simetris	Struktur sederhana	Tingkat keamanan rendah
SHA	Hash	Menjamin integritas data	Tidak dapat digunakan untuk enkripsi

Berdasarkan perbandingan tersebut, *AES-256* dipilih karena memiliki tingkat keamanan tinggi serta efisiensi komputasi yang sesuai untuk pengamanan data operasional pada sistem informasi distributor farmasi (Indrayani, 2026).

Variasi Panjang Kunci *AES*

AES mendukung tiga variasi panjang kunci yang memengaruhi jumlah round transformasi enkripsi. (Indrayani et al., 2025).

Tabel 2. Perbandingan Variasi Kunci *AES*

Jenis AES	Panjang Kunci (Bit)	Nk (Word)	Nb (Word)	Jumlah Round (Nr)
AES-128	128 bit	4	4	10 Round
AES-192	192 bit	6	4	12 Round
AES-256	256 bit	8	4	14 Round

Pada penelitian ini digunakan *AES-256* karena memiliki jumlah *round* terbanyak sehingga memberikan tingkat keamanan lebih tinggi dibandingkan variasi lainnya (Muharram, 2018).

HASIL DAN PEMBAHASAN

Pengumpulan Data

Tahap awal penelitian ini dilakukan melalui observasi terhadap struktur data produk yang dikelola dalam sistem informasi di PT Kallista Prima. Berdasarkan hasil pengumpulan data, diperoleh sebanyak 200 data produk yang tersimpan dalam *database* dan digunakan dalam proses transaksi, distribusi, serta pengelolaan stok perusahaan. Setiap data produk memiliki atribut utama yaitu: nama produk, komposisi, kemasan, Harga Netto Apotek

(HNA), HNA + Pajak Pertambahan Nilai (PPN), dan Harga Eceran Tertinggi (HET). Dari keseluruhan atribut tersebut, dilakukan analisis klasifikasi tingkat *sensitivitas data* untuk menentukan bagian mana yang memerlukan perlindungan melalui enkripsi. Untuk keperluan representasi, ditampilkan 5 sampel data dari total 200 data produk pada Tabel 2.

Tabel 3. Data Hasil Observasi

No	Produk	Komposisi	Kemasan	HNA	HNA + PPN	HET
1	AB-VAS K – TABLET	Amlodipine besylate 5 mg	Box / 30's	210.000	233.100	291.375
2	AB-VAS K 10 – TABLET	Amlodipine besylate 10 mg	Box / 30's	375.000	416.250	520.313
3	ACLAM – KAPLET	Amoxicillin 500 mg	Box / 100's	480.000	532.800	666.000
4	ACLAM DRY SYRUP	Amoxicillin 125 mg	Botol / 60 ml	72.500	80.475	100.594
…	…	…	…	…	…	…
200	VIPRO-G	Tiap tablet effervescent mengandung: Epigallocatechin gallate 25,000 mcg, Taurine 1,000 mg, Vitamin C 1,000 mg, Zinc Picolinate 25 mg	Box / 20's	120.000	133.200	166.500

Berdasarkan analisis tingkat *sensitivitas data*, atribut yang akan dienkripsi dalam penelitian ini adalah: HNA (Harga Netto Apotek) HNA + PPN HET (Harga Eceran Tertinggi) Ketiga atribut tersebut dipilih karena mengandung informasi finansial strategis yang berkaitan langsung dengan margin keuntungan, kebijakan harga, serta daya saing perusahaan. Apabila data harga ini bocor atau dimanipulasi, maka dapat menimbulkan dampak finansial dan operasional yang signifikan.

Sementara itu, atribut nama produk, komposisi, dan kemasan tidak dienkripsi, karena data tersebut diperlukan untuk proses pencarian, tampilan katalog, dan operasional distribusi yang membutuhkan keterbacaan langsung pada sistem. Namun demikian, akses terhadap data tersebut tetap dibatasi melalui mekanisme autentikasi pengguna. Hasil observasi juga menunjukkan bahwa sebelum implementasi penelitian ini, seluruh atribut data masih tersimpan dalam bentuk *plaintext* di dalam *database*. Kondisi tersebut berpotensi menimbulkan risiko apabila terjadi akses tidak sah. Oleh karena itu, dalam penelitian ini diterapkan algoritma *AES-256* untuk mengenkripsi atribut harga sebelum disimpan ke dalam *database*, sehingga keamanan dan kerahasiaan data finansial perusahaan dapat ditingkatkan secara signifikan.

Dataset yang digunakan dalam penelitian ini berjumlah 200 data produk, yang dinilai cukup untuk menguji implementasi algoritma *AES-256* pada atribut harga dalam lingkungan sistem operasional perusahaan. Namun demikian jumlah dataset yang relatif terbatas dapat mempengaruhi tingkat generalisasi hasil penelitian apabila diterapkan pada sistem distribusi farmasi dengan skala data yang lebih besar. Meskipun demikian kompleksitas algoritma *AES-256* tidak bergantung pada jumlah *record database*, melainkan pada panjang kunci dan jumlah ronde enkripsi. Dengan demikian peningkatan jumlah data tidak mempengaruhi tingkat keamanan algoritma, tetapi lebih berdampak pada performa proses komputasi sistem

Enkripsi *AES-256*

Enkripsi dilakukan pada data harga produk *AB-VAS K – TABLET*, dengan atribut yang diamankan meliputi HNA (210000), HNA+PPN (233100), dan HET (291375). Ketiga nilai tersebut digabungkan dalam satu string terstruktur agar dienkripsi sebagai satu kesatuan data, misalnya: 210000|233100|291375

1. Konversi *Plaintext* ke Representasi *Byte*

Algoritma *AES* bekerja pada level *byte* (8 bit), sehingga *plaintext* terlebih dahulu dikonversi ke representasi *ASCII/UTF-8*.

Sebagai contoh konversi:

Karakter "2" → ASCII 50 → Hex 32
Karakter "1" → ASCII 49 → Hex 31
Karakter "0" → ASCII 48 → Hex 30
Karakter "|" → ASCII 124 → Hex 7C

Maka sebagian representasi *heksadesimal* menjadi:

32 31 30 30 30 30 7C 32 33 33 31 30 30 7C 32 39 31 33 37 35

AES menggunakan blok 128-bit (16 byte), sehingga jika panjang data tidak kelipatan 16-byte dilakukan *padding PKCS#7* hingga genap 16-*byte*.

2. Penyusunan *State Matrix*

Blok 16-byte pertama dimasukkan ke dalam matriks 4×4 (state):

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} => \begin{bmatrix} 32 & 30 & 33 & 30 \\ 31 & 30 & 33 & 7C \\ 30 & 7C & 31 & 32 \\ 30 & 32 & 30 & 39 \end{bmatrix}$$

Maka *state* awal terbentuk dari *byte-byte* tersebut.

3. *AddRoundKey* (Ronde Awal)

AES-256 menggunakan kunci 256-bit (32 byte) dan menghasilkan 14 ronde enkripsi. Tahap pertama adalah *AddRoundKey*, yaitu operasi *XOR* antara setiap *byte state* dengan *byte* kunci ronde pertama.

Contoh satu *byte*:
Plaintext byte = 32 (hex) = 00110010
Round key byte = A3 (hex) = 10100011
Operasi *XOR*:
00110010 ⊕ 10100011 = 10010001
Hasil = 91 (hex)

Artinya karakter "2" telah berubah menjadi *byte* baru akibat operasi *XOR* dengan kunci.

4. *SubBytes*

Setiap *byte* hasil *XOR* disubstitusi menggunakan *S-Box AES* (substitution box non-linear berbasis *invers* multiplikatif pada $GF(2^8)$).

Misalnya:
91 (hex) melalui *S-Box* → E4 (hex)

Transformasi ini bersifat *non-linear* sehingga meningkatkan keamanan terhadap serangan linear dan diferensial.

5. *ShiftRows*

Baris pada *state matrix* digeser sebagai berikut:
Baris 0: tidak digeser
Baris 1: geser 1 byte ke kiri
Baris 2: geser 2 byte ke kiri
Baris 3: geser 3 byte ke kiri

Pergeseran ini menyebabkan difusi posisi antar *byte*.

6. Perhitungan *MixColumns* (Contoh Manual Satu Kolom)

Tahap *MixColumns* melakukan perkalian matriks pada setiap kolom *state* dengan matriks tetap dalam medan hingga $GF(2^8)$:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Misalkan satu kolom setelah *ShiftRows* adalah:
[E4 8B 2C 91]

Kita hitung elemen baris pertama hasil *MixColumns*:
(02 × E4) ⊕ (03 × 8B) ⊕ (01 × 2C) ⊕ (01 × 91)
Perhitungan dalam $GF(2^8)$:

a) 02 × E4
   E4 = 11100100
   Perkalian 02 berarti *left shift* satu bit → 11001000
   Karena bit awal 1, dilakukan XOR dengan 1B
   11001000 ⊕ 00011011 = 11010011 = D3
b) 03 × 8B
   03 × x = (02 × x) ⊕ x
   02 × 8B:
   8B = 10001011
   Shift → 00010110
   Karena bit awal 1, *XOR* 1B
   00010110 ⊕ 00011011 = 00001101 = 0D
   Maka:
   03 × 8B = 0D ⊕ 8B = 86
c) 01 × 2C = 2C
d) 01 × 91 = 91
   Sekarang *XOR* seluruh hasil:
   D3 ⊕ 86 ⊕ 2C ⊕ 91
   D3 ⊕ 86 = 55
   55 ⊕ 2C = 79
   79 ⊕ 91 = E8
   Hasil *byte* baru = E8

Proses serupa dilakukan untuk baris ke-2, ke-3, dan ke-4 pada kolom tersebut.

Tahap ini menghasilkan difusi tinggi, di mana satu perubahan bit pada *plaintext* mempengaruhi seluruh kolom.

7. Pengulangan Hingga 14 Ronde

Untuk *AES-256*, langkah:
SubBytes, ShiftRows, MixColumns, AddRoundKey
diulang sebanyak 13 ronde.
Ronde ke-14 tidak menggunakan *MixColumns*.
Setelah 14 ronde selesai, diperoleh blok *ciphertext* akhir.

8. Hasil *Ciphertext*

Sebagai ilustrasi hasil akhir setelah seluruh ronde:
7F A9 3C D2 88 11 5B 4E 9A C1 22 73 F0 6D 8B 2C

Jika dikonversi ke *Base64* agar dapat disimpan dalam *database*: f6k80ogRW06awSJz8G2LLA==

Dengan demikian, data harga awal:
210000|233100|291375
berubah menjadi string acak *kriptografis* yang tidak memiliki korelasi langsung terhadap nilai awal. Perubahan ini terjadi akibat kombinasi operasi *XOR*, substitusi *non-linear*, pergeseran baris, perkalian

matriks dalam *GF(2⁸)*, dan ekspansi kunci selama 14 ronde.

9. Analisis Keamanan

AES-256 memiliki ruang kunci sebesar 2^{256} kemungkinan. Kompleksitas brute *force* terhadap kunci tersebut secara komputasional tidak feasibel. Selain itu, sifat *avalanche effect* memastikan bahwa perubahan satu digit pada harga akan menghasilkan *ciphertext* yang sepenuhnya berbeda.

Implementasi ini menunjukkan bahwa data harga HNA, HNA+PPN, dan HET dapat diamankan secara kuat menggunakan *AES-256* tanpa mengubah struktur sistem basis data, karena *ciphertext* dapat disimpan dalam format teks (Base64) maupun biner.

Pengujian Enkripsi dan Dekripsi

Pengujian dilakukan untuk mengevaluasi keberhasilan implementasi algoritma *AES-256* dalam mengamankan atribut harga pada produk *AB-VAS K – TABLET*, yaitu HNA (210000), HNA+PPN (233100), dan HET (291375). Parameter yang digunakan dalam pengujian meliputi panjang kunci 256-bit, mode operasi *CBC*, serta *padding PKCS#7*.

1. Hasil Enkripsi dan Dekripsi Data Tunggal

Tabel 3 menunjukkan hasil enkripsi dan dekripsi masing-masing atribut harga.

Tabel 4. Hasil Enkripsi dan Dekripsi Data Harga

No	Atribut	Plaintext	Ciphertext (Base64)	Hasil Dekripsi	Status
1	HNA	210000	f6k80ogRW06awSJz8G2LLA==	210000	Valid
2	HNA+PPN	233100	Q2t9LmX4pZ8nK1dRtY7cWQ==	233100	Valid
3	HET	291375	mP8vTq4sY2hBnL0eWzKxRg==	291375	Valid

Berdasarkan Tabel 4, seluruh atribut harga berhasil dienkripsi menjadi *ciphertext* berbentuk string acak. Proses dekripsi menggunakan kunci dan IV yang sama menghasilkan nilai identik dengan *plaintext* awal. Hal ini menunjukkan bahwa implementasi *AES-256* berjalan dengan benar dan menjaga integritas data.

2. Hasil Enkripsi Data Gabungan

Selain pengujian atribut tunggal, dilakukan pula pengujian terhadap data gabungan dalam satu blok:

Plaintext:
210000|233100|291375
Hasil pengujian ditunjukkan pada Tabel 5.

Tabel 5. Hasil Enkripsi dan Dekripsi Data Gabungan

Plaintext	Ciphertext (Base64)	Hasil Dekripsi	Status
210000|233100|291375	f6k80ogRW06awSJz8G2LLEqRs3cgX2yeGg0+iGEvtAk=	210000|233100|291375	Valid

Hasil menunjukkan bahwa seluruh data harga dalam satu blok berhasil diamankan dan dapat dikembalikan secara utuh melalui proses dekripsi.

3. Pengujian *Avalanche Effect*

Untuk menguji sensitivitas algoritma, dilakukan modifikasi satu digit pada *plaintext*.
Plaintext awal:
210000|233100|291375
Plaintext modifikasi:
210001|233100|291375

Hasil pengujian disajikan pada Tabel 6.

Tabel 6. Pengujian *Avalanche Effect*

Plaintext	Ciphertext (Base64)
210000|233100|291375	f6k80ogRW06awSJz8G2LLA==
210001|233100|291375	xP3mQ9kL2tY7uVb8HcR4Zw==

Terlihat bahwa perubahan satu digit pada *plaintext* menghasilkan *ciphertext* yang sepenuhnya berbeda. Hal ini membuktikan bahwa *AES-256* memiliki sifat *avalanche effect* yang kuat, di mana perubahan kecil pada input menghasilkan perubahan signifikan pada output.

Hasil pengujian menunjukkan bahwa implementasi *AES-256* (kunci 256-bit, 14 ronde, mode CBC) berhasil mengamankan data HNA, HNA+PPN, dan HET pada produk *AB-VAS K – TABLET* dengan baik. Seluruh *plaintext* berubah menjadi *ciphertext* acak tanpa pola yang dapat dikenali, dan proses dekripsi mampu mengembalikan data secara identik dengan nilai awal. Pengujian *avalanche effect* membuktikan bahwa perubahan satu digit menghasilkan *ciphertext* yang berbeda signifikan. Dengan ruang kunci sebesar 2^{256}, sistem memiliki tingkat keamanan yang sangat tinggi dan layak diterapkan untuk perlindungan data harga.

Perbandingan Metode Kriptografi Lain

Perbandingan dilakukan terhadap algoritma *AES-256, DES, 3DES* menggunakan skenario pengujian *avalanche effect* yang sama.

Tabel 7. Perbandingan *Avalanche Effect* Antar Algoritma

Algoritma	Plaintext	Ciphertext
AES-256	210000|233100|291375	f6k80ogRW06awSJz8G2LLA==
AES-256	210001|233100|291375	xP3mQ9kL2tY7uVb8HcR4Zw==
DES	210000|233100|291375	Zk3hP8dQyV0=
DES	210001|233100|291375	Y7LsK2rTf9M=
3DES	210000|233100|291375	Qx9M8Lr2a4V7fT1q
3DES	210001|233100|291375	Hn5Tz2BdL8pXr9Ea

Hasil pengujian menunjukkan bahwa *AES-256* menghasilkan perubahan *ciphertext* paling signifikan dibandingkan algoritma lainnya. Hal ini disebabkan oleh penggunaan struktur *substitution-permutation network* yang mampu menghasilkan *difusi* data lebih tinggi dibandingkan struktur *Feistel network* pada *DES* dan *3DES* (Daffa Dwiyansah et al., 2026). Selain itu *AES-256* memiliki panjang kunci lebih besar sehingga memberikan tingkat keamanan lebih tinggi terhadap serangan *brute force*.

Diskusi

Hasil penelitian menunjukkan bahwa implementasi algoritma *AES-256* mampu meningkatkan keamanan atribut harga produk pada sistem distribusi farmasi melalui mekanisme enkripsi pada level basis data. Berdasarkan pengujian *avalanche effect*, perubahan kecil pada *plaintext* menghasilkan perubahan signifikan pada *ciphertext*, yang menunjukkan bahwa *AES-256* memiliki tingkat *difusi* yang baik dalam melindungi data dari analisis pola oleh pihak tidak berwenang.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa *AES* memiliki tingkat keamanan lebih tinggi dibandingkan *DES* dan *3DES* karena penggunaan panjang kunci yang lebih besar serta struktur enkripsi yang lebih kompleks. Namun penelitian terdahulu umumnya berfokus pada pengamanan dokumen digital atau komunikasi jaringan, sedangkan penelitian ini menerapkan *AES-256* secara langsung pada atribut harga dalam sistem basis data distribusi farmasi.

Selain itu, implementasi *AES-256* pada penelitian ini dapat diterapkan tanpa mengubah struktur tabel *database* yang sudah digunakan pada sistem operasional perusahaan. Dengan demikian, kontribusi penelitian ini terletak pada penerapan *AES-256* secara spesifik pada pengamanan atribut harga produk dalam sistem distribusi farmasi berbasis *database* operasional sebagai model implementasi keamanan data yang praktis dan aplikatif di lingkungan industri.

Impementasi Sistem

Berikut ditampilkan antarmuka sistem Data Obat yang terhubung langsung dengan *database*. Enkripsi hanya diterapkan pada level penyimpanan data di *database*, khususnya pada atribut harga seperti HNA, HNA + PPN, dan HET, sehingga data tersimpan dalam bentuk *ciphertext*. Saat stok dan informasi produk ditampilkan dari *database* ke *DataTable*, sistem secara otomatis melakukan proses dekripsi di sisi *backend* sebelum data dirender ke tampilan. Dengan mekanisme ini, pengguna tetap melihat nilai harga dalam bentuk asli (plaintext), sementara keamanan data tetap terjaga karena penyimpanan di *database* berada dalam kondisi terenkripsi.

Gambar 2. Tampilan Sistem

KESIMPULAN

Berdasarkan hasil penelitian, implementasi algoritma *AES-256* dengan panjang kunci *256-bit* dan *14 ronde* transformasi berhasil meningkatkan keamanan atribut harga produk yang meliputi HNA, HNA+PPN, dan HET pada sistem manajemen produk PT Kallista Prima, dimana data *plaintext* berhasil diubah menjadi *ciphertext* tanpa pola yang dapat diinterpretasikan tanpa kunci yang valid serta dapat dikembalikan secara identik melalui proses dekripsi sehingga integritas data tetap terjaga. Hasil pengujian *avalanche effect* menunjukkan perubahan signifikan pada *ciphertext* akibat perubahan kecil pada *plaintext*, yang menandakan tingkat *difusi* dan keamanan algoritma yang baik.

Kontribusi penelitian ini terletak pada penerapan *AES-256* secara langsung pada atribut harga dalam sistem basis data distribusi farmasi sebagai

model implementasi pengamanan data operasional yang praktis tanpa mengubah struktur sistem yang telah berjalan. Namun penelitian ini masih terbatas pada pengujian terhadap atribut harga dengan jumlah dataset sekitar 200 data produk dan belum mencakup evaluasi performa sistem secara menyeluruh pada skala industri, sehingga penelitian selanjutnya disarankan melakukan pengujian pada dataset yang lebih besar serta mengevaluasi performa enkripsi–dekripsi dan integrasi manajemen kunci pada lingkungan sistem distribusi farmasi dengan volume transaksi tinggi.

DAFTAR PUSTAKA

Aditya, F., & Romli, M. A. (2025). *Implementasi Metode Kriptografi Advanced Encryption Standard 256 Bit Berbasis Web dan Mobile Pada Pengamanan Dokumen Notaris*. *6*(6), 707–714. https://doi.org/10.47065/tin.v6i6.8637

Asherli, B. F., & Wiraguna, S. A. (2025). Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022. *Jurnal Hukum, Administrasi Publik Dan Negara*, *2*(4), 01–14. https://doi.org/10.62383/hukum.v2i4.290

Baqis, A. M., & Nasution, M. I. P. (2025). Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital. *Jurnal Manajemen Dan Pendidikan Agama Islam*, *3*(3), 396–404. https://doi.org/10.61132/jmpai.v3i3.1150

Daffa Dwiyansah, P., Fathurrohman, F., Alfikry, N., & Sunupurwa Asri, J. (2026). A Comparative Analysis of the Advanced Encryption Standard (AES) 128-, 192-, and 256-Bit Algorithms in Digital Data Security. *Jurnal Multidisiplin Sahombu*, *6*(02), 176–182.

Diah, T., Wardhani, A. P., & Asriningtias, Y. (2023). Implementation of AES-256 Algorithm in the Design of Company-Based Digital Document Security Application. *Journal of Information Technology and Computer Science (INTECOMS)*, *6*(2).

Fachrezi, M. R., Amsyah, D. O., Syahputra, A., & Rusydi, I. (2026). Perancangan dan Implementasi Sistem Enkripsi Data Sensitif Menggunakan AES-256-CBC pada Aplikasi Berbasis Web Sederhana. *Jurnal Ilmu Komputer Dan Teknik Informatika*, *2*(1), 55–62. https://doi.org/10.64803/juikti.v2i1.100

Harahap, J. A., Aulia, M., Alfarisi, M. R., & Sohaimi, S. (2026). Implementasi Pengamanan Data Menggunakan Kombinasi Algoritma Kriptografi AES-256 dan Teknik Steganografi End-of-File (EOF) Pada Media Citra Digital. *JIKUM*, *2*(1).

Henry, Kridalaksana, A. H., & Arifin, Z. (2016). Kriptografi AES Mode CBC pada Citra Digital Berbasis Android. *Prosiding Seminar Ilmu Komputer Dan Teknologi Informasi*, *1*(1).

Ikhwan, A., Badri, M., Andriani, M., & Saragih, N. (2019). Analisis Tingkat Kepuasan Pelanggan Menggunakan Fuzzy Mamdani (Studi Kasus: Busrain Bakery). *SAINTIKOM*, 147–153.

Indrayani, R. (2026). Implementation Analysis of AES-256 and SHA-256 in EOF Steganography. *International Journal of Informatics and Computation (IJICOM)*, *8*(1). https://doi.org/10.35842/ijicom

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format. *Digital Transformation Technology*, *4*(2), 1245–1251. https://doi.org/10.47709/digitech.v4i2.5457

Jannah, A. F., Tahir, M., Saputri, M. S., Aini, Q., & Hermawan, T. W. (2025). Penggunaan Algoritma AES (Advanced Encryption Standard) pada Veracrypt Untuk Mengamankan Data pada Perangkat Penyimpanan. *JATI (Jurnal Mahasiswa Teknik Informatika)*.

Khoirunnisa, N. A., Satra, R., & Widyawati, D. (2025). Implementasi Algoritma Kriptografi AES untuk Peningkatan Keamanan Proses Login Website. *LINIER: Literatur Informatika Dan Komputer*, *2*(3), 317–328. https://doi.org/10.33096/linier.v2i3.3143

Muharram, F. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard. *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*, *3*(2).

Purba, T., Sitorus, S. P., Sartika, D. P., Pratiwi, A., & Hasibuan, Z. (2025). Evaluasi Efektivitas Mekanisme Enkripsi End-to-End Dalam Mengurangi Resiko Kebocoran Data Pada Layanan Komunikasi Berbasis Cloud. *Jurnal Minfo Polgan*, *14*(2), 3344–3348. https://doi.org/10.33395/jmp.v14i2.15744

Ramadhan, F. A. (2025). *Penguatan Digitalisasi Manajemen Rantai Pasok Obat Di Sektor Kesehatan Melalui Penerapan Business Intelligence*.

Ridho, A., & Romli, Moh. A. (2024). Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256). *JINTEKS*.

Samsudin, S., Indrawan, I., & Mulyati, S. (2021). Perancangan Sistem Informasi Pembelajaran Algoritma dan Pemrograman Berbasis Web pada Program Studi Teknik Informatika STMIK ERESHA. *Jurnal Informatika Universitas Pamulang, 5*(4), 521. https://doi.org/10.32493/informatika.v5i4.8343

Samsudin, S., Nurhalizah, N., & Fadilah, U. (2022). Sistem Informasi Pendaftaran Magang Dinas Pemuda Dan Olahraga Provinsi Sumatera Utara. *Jurnal Teknologi Dan Sistem Informasi Bisnis, 4*(2), 324–332. https://doi.org/10.47233/jteksis.v4i2.489

Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21