



**PENERAPAN ALGORITMA AES DALAM OPTIMALISASI KONTROL
KEAMANAN DATA SESUAI STANDAR ISO 27001:2022: STUDI KASUS
PT XYZ**

SKRIPSI

NI AYU DIANDRA PUSPASARI

2110511120

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA
JAKARTA
2025**



**PENERAPAN ALGORITMA AES DALAM OPTIMALISASI KONTROL
KEAMANAN DATA SESUAI STANDAR ISO 27001:2022: STUDI KASUS
PT XYZ**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

**NI AYU DIANDRA PUSPASARI
2110511120**

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
JAKARTA
2025**

PERNYATAAN ORISINALITAS

Tugas skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Ni Ayu Diandra Puspasari
NIM : 2110511120
Tanggal : 06 Mei 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan persyaratan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 06 Mei 2025

Yang menyatakan,



Ni Ayu Diandra Puspasari

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Saya, civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, yang bertanda tangan di bawah ini:

Nama : Ni Ayu Diandra Puspasari
NIM : 2110511120
Fakultas : Fakultas Ilmu Komputer
Program Studi : SI Informatika

Demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti *Non-Eksklusif (Non-Exclusive Royalty-Free Right)* atas karya ilmiah saya yang berjudul:

Penerapan Algoritma AES Dalam Optimalisasi Kontrol Keamanan Data Sesuai Standar ISO 27001:2022: Studi Kasus PT XYZ

beserta perangkat yang ada (jika diperlukan). Dengan pemberian hak ini, Universitas Pembangunan Nasional Veteran Jakarta berhak untuk menyimpan, mengalih media/formalitas, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasi skripsi saya, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan pemegang Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Dibuat di : Jakarta
Pada Tanggal : 13 Juni 2025

Yang menyatakan,



Ni Ayu Diandra Puspasari

LEMBAR PENGESAHAN

Judul : Penerapan Algoritma AES Dalam Optimalisasi Kontrol Keamanan Data
Sesuai Standar ISO 27001:2022: Studi Kasus PT XYZ
Nama : Ni Ayu Diandra Puspasari
NIM : 2110511120
Program Studi : SI Informatika

Disetujui oleh:

Penguji 1:

Jayanta, S.Kom., M.Si.

Penguji 2:

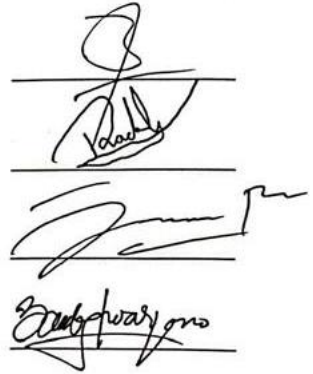
Radinal Setyadinsa, S.Pd., M.T.I.

Pembimbing 1:

Indra Permana Solihin, S.Kom, M.Kom.

Pembimbing 2:

Bambang Triwahyono, S.Kom., M.Si.



Diketahui oleh:

Koordinator Program Studi:

Dr. Widya Cholil, M.I.T

NIP. 221112080

Dekan Fakultas Ilmu Komputer:

Prof. Dr. Ir. Supriyanto, M.Sc., IPM.

NIP. 197605082003121002



Tanggal Ujian Tugas Akhir:

27 Mei 2025

PENERAPAN ALGORITMA AES DALAM OPTIMALISASI KONTROL KEAMANAN DATA SESUAI STANDAR ISO 27001:2022: STUDI KASUS PT XYZ

Ni Ayu Diandra Puspasari

ABSTRAK

Penerapan algoritma *Advanced Encryption Standard* (AES-256) menjadi salah satu upaya strategis dalam mengoptimalkan kontrol keamanan data di PT XYZ, sejalan dengan standar ISO 27001:2022. Meningkatnya serangan siber dan kompleksitas ancaman keamanan informasi menuntut perusahaan untuk memiliki sistem manajemen keamanan data yang kuat dan adaptif. Studi ini berfokus pada analisis efektivitas kontrol akses (*Annex A.9*) dan keamanan komunikasi (*Annex A.13*) pada modul pengajuan klaim asuransi, yang selama ini menunjukkan efektivitas yang beragam. Penelitian dilakukan dengan pendekatan kuantitatif melalui kuesioner kepada personel *Digital Marketing* dan *IT Governance*, serta didukung oleh analisis teknis terhadap implementasi enkripsi AES-256 di sisi *backend*. Hasil menunjukkan bahwa meskipun pengendalian akses telah berjalan cukup efektif, masih terdapat celah pada aspek keamanan komunikasi yang berpotensi menimbulkan risiko kebocoran data. Sebagai solusi, diusulkan implementasi AES-256 dalam proses enkripsi dan dekripsi data klaim melalui pengembangan API berbasis JavaScript dan PostgreSQL. Pengujian membuktikan bahwa solusi ini mampu meningkatkan perlindungan data secara signifikan sekaligus mendukung kepatuhan terhadap ISO 27001:2022. Temuan ini diharapkan dapat menjadi acuan dalam penguatan sistem keamanan informasi di sektor asuransi melalui penerapan teknologi enkripsi yang lebih optimal.

Kata kunci: AES-256, ISO 27001:2022, Kontrol Akses, Enkripsi Data, Klaim Asuransi

**PENERAPAN ALGORITMA AES DALAM OPTIMALISASI KONTROL
KEAMANAN DATA SESUAI STANDAR ISO 27001:2022: STUDI KASUS
PT XYZ**

Ni Ayu Diandra Puspasari

ABSTRACT

The implementation of the Advanced Encryption Standard (AES-256) algorithm serves as a strategic initiative to optimize data security controls at PT XYZ, in alignment with the ISO 27001:2022 standard. The rising frequency of cyberattacks and the growing complexity of information security threats underscore the need for a robust and adaptive data security management system. This study focuses on evaluating the effectiveness of access control (Annex A.9) and communication security (Annex A.13) within the insurance claim submission module, which has demonstrated varying levels of effectiveness. A quantitative approach was employed through questionnaires distributed to Digital Marketing and IT Governance personnel, supported by technical analysis of AES-256 encryption implementation on the backend. The results indicate that while access control has been effectively implemented, notable gaps remain in communication security that may increase the risk of data leakage. To address this issue, the implementation of AES-256 is proposed for encrypting and decrypting claim data through API development using JavaScript and PostgreSQL. Testing results show that this encryption solution significantly enhances data protection and supports compliance with ISO 27001:2022. These findings are expected to serve as a reference for strengthening information security systems in the insurance sector through the optimal application of encryption technologies.

Keywords: AES-256, ISO 27001:2022, Access Control, Data Encryption, Insurance Claims

KATA PENGANTAR

Puji dan Syukur penulis panjatkan atas kehadiran Tuhan Yang Maha Esa, karena berkat rahmat, karunia, dan hidayah-Nya, penulis dapat menyelesaikan skripsi yang berjudul “Penerapan Algoritma AES Dalam Optimalisasi Kontrol Keamanan Data Sesuai Standar ISO 27001:2022: Studi Kasus PT XYZ”. Skripsi ini merupakan hasil penelitian yang penulis lakukan sebagai salah satu syarat untuk menyelesaikan studi di Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Dalam proses penyusunan skripsi ini tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Tuhan Yang Maha Esa, atas segala karunia, rahmat, dan hidayah-Nya selama penulis menjalani proses penelitian dan penulisan skripsi ini.
2. Papa dan Mama, orang tua penulis yang selalu menjadi cahaya saat penulis kehilangan arah dan tempat berpulang yang penuh kasih.
3. Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM, selaku Dekan Fakultas Ilmu Komputer.
4. Ibu Dr. Widya Cholil, S.Kom., M.I.T. selaku Ketua Program Studi Sarjana Jurusan Informatika.
5. Bapak Indra Permana Solihin, S.Kom., M.Kom. selaku Dosen Pembimbing 1, atas segala waktu, ilmu, dan arahannya yang begitu berharga dalam proses penyusunan penelitian ini.
6. Bapak Bambang Triwahyono, S.Kom., M.Si. selaku Dosen Pembimbing 2, yang dengan sabar memberikan masukan dan panduan yang sangat membantu dalam menyempurnakan penelitian ini.
7. Bapak Henki Bayu Seta, S.Kom., MTI. selaku Dosen Pembimbing Akademik Program Studi Sarjana Jurusan Informatika.
8. Adik Bayu, saudara penulis, yang menjadi saksi perjuangan penulis, baik dalam tawa maupun air mata.
9. Teman-teman tercinta, Kak M. Alfaiz Surya, Amalia Balqis, Rifky Halsandrian, dan Abimanyu Damarjati, yang selalu kebersamaan penulis

dalam suka maupun duka selama menjalani perkuliahan di FIK UPN Veteran Jakarta.

10. Chinos, kucing penulis, yang setia menagih makan di siang dan sore hari. Adik berbulu ini telah menjadi penyemangat hidup di tengah proses panjang penelitian ini.
11. Semua keluarga, sahabat, dan pihak-pihak lainnya yang tidak dapat penulis sebutkan satu per satu, namun telah memberikan dukungan secara langsung maupun tidak langsung.

Skripsi ini diketik dan disusun dengan banyak kebahagiaan dan tangisan, sehingga penulis sangat-sangat berterima kasih kepada semua pihak yang membantu penulis dari awal hingga akhir. Serta tidak lupa penulis ucapkan rasa bersyukur yang mendalam kepada Tuhan YME karena masih mengizinkan penulis menyelesaikan tugas akhir ini. Penulis menyadari skripsi ini masih belum sempurna, baik dari materi, penelitian, maupun dari segi penyajian karena keterbatasan pengetahuan dan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan saran dan kritik untuk kesempurnaan skripsi ini.

Jakarta, 16 Oktober 2024



Penulis,
Ni Ayu Diandra Puspasari

DAFTAR ISI

LEMBAR JUDUL	ii
PERNYATAAN ORISINALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iv
LEMBAR PENGESAHAN	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah	3
1.4. Tujuan dan Manfaat Penelitian.....	3
1.4.1. Tujuan Penelitian	3
1.4.2. Manfaat Penelitian	4
1.5. Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	7
2.1. Kajian Teori.....	7
2.1.1. Sistem Manajemen Keamanan Informasi (SMKI)	7
2.1.2. ISO 27001:2022	8
2.1.3. <i>Annex A</i>	10
2.1.4. <i>Access Control</i>	10
2.1.5. <i>Communications Security</i>	11
2.1.6. <i>Advanced Encryption Standard (AES)</i>	12
2.1.7. <i>Application Programming Interface (API)</i>	14
2.1.8. JavaScript.....	15
2.1.9. Express.js	16

2.1.10. Database PostgreSQL.....	16
2.2. Parameter Kontrol	17
2.3. Penelitian Terdahulu.....	19
BAB III METODOLOGI PENELITIAN.....	24
3.1. Alur Penelitian.....	24
3.1.1. Identifikasi Masalah.....	25
3.1.2. Studi Literatur	25
3.1.3. Perancangan Penelitian	25
3.2. Rancangan dan Instrumen Penelitian	25
3.2.1. Fokus Penelitian pada <i>Annex A ISO 27001:2022</i>	26
3.2.2. Struktur Kuesioner.....	26
3.2.3. Penentuan Populasi dan Sampel	27
3.2.4. Penentuan Instrumen Penelitian.....	28
3.2.5. Teknik Analisis Data	35
3.2.6. Identifikasi Celah Keamanan.....	36
3.2.7. Rekomendasi Solusi.....	36
3.3. Perangkat Penelitian	37
3.4. Jadwal Penelitian	38
BAB IV HASIL DAN PEMBAHASAN	39
4.1. Profil Perusahaan.....	39
4.2. Hasil Analisis Kuesioner	40
4.2.1. Deskripsi Responden	40
4.2.2. Analisis Data Kuesioner	40
4.3. Hasil dan Rekomendasi	41
4.3.1. Identifikasi Masalah Utama	41
4.3.2. Strategi dan Rekomendasi Solusi	42
4.3.3. Pemilihan Bahasa.....	43
4.3.4. Analisis Tahapan Manual Enkripsi AES-256-CBC pada Data JSON. 44	
4.3.5. Analisis Tahapan Manual Dekripsi AES-256-CBC pada Data JSON. 46	
4.3.6. Proses Generasi Kunci dan IV (<i>Initialization Vector</i>).....	47
4.3.7. Implementasi Enkripsi Data dengan AES-256	49
4.3.8. Implementasi Dekripsi Data dengan AES-256.....	51

4.3.9. Integrasi Enkripsi dan Dekripsi AES-256 ke Dalam Sistem <i>Backend</i> Pengajuan Klaim Asuransi PT XYZ.....	54
4.3.10. Pengujian Enkripsi dan Dekripsi	63
BAB V PENUTUP.....	73
5.1. Kesimpulan	73
5.2. Saran	73
DAFTAR PUSTAKA	75
DAFTAR LAMPIRAN.....	78

DAFTAR TABEL

Tabel 2.1. Poin Utama ISO 27001:2022	8
Tabel 2.2. Ukuran Kunci AES dan Jumlah Putarannya	12
Tabel 2.3. Parameter Kontrol	17
Tabel 2.4. Review Jurnal.....	19
Tabel 3.1. Contoh Pertanyaan Kuesioner.....	26
Tabel 3.2. Daftar Pertanyaan Kuesioner	28
Tabel 3.3. Jadwal Penelitian.....	38
Tabel 4.1. Tahapan Manual Enkripsi AES-256-CBC terhadap Data JSON	45
Tabel 4.2. Tahapan Manual Dekripsi AES-256-CBC terhadap Data JSON.....	46

DAFTAR GAMBAR

Gambar 2.1. Siklus PDCA	7
Gambar 2.2. Proses Enkripsi dan Dekripsi AES.....	13
Gambar 2.3. Skala Tingkat Kesadaran Keamanan Informasi	19
Gambar 4. 1. Kode untuk Generasi.....	48
Gambar 4.2. Kode untuk Generasi IV.....	48
Gambar 4.3. Diagram Alur Proses Enkripsi Data dengan AES-256.....	49
Gambar 4.4. Kode untuk Persiapan Data Enkripsi	49
Gambar 4.5. Kode untuk Inisialisasi Cipher Enkripsi	50
Gambar 4.6. Kode untuk Enkripsi Data	50
Gambar 4.7. Kode untuk Pengembalian Hasil Enkripsi	51
Gambar 4.8. Diagram Alur Proses Dekripsi Data dengan AES-256	52
Gambar 4.9. Kode untuk Persiapan Data Dekripsi	52
Gambar 4.10. Kode untuk Inisialisasi Decipher Dekripsi.....	52
Gambar 4.11. Kode untuk Dekripsi Data.....	53
Gambar 4.12. Kode untuk Pengembalian Hasil Dekripsi	53
Gambar 4.13. Kode Implementasi create pada PengajuanKlaimRepository.js	55
Gambar 4.14. Kode Implementasi getAllClaims pada PengajuanKlaimRepository.js	55
Gambar 4.15. Kode Implementasi getPendingClaims pada PengajuanKlaimRepository.js	56
Gambar 4.16. Kode Implementasi getClaimById pada PengajuanKlaimRepository.js	56
Gambar 4.17. Kode Implementasi updateClaimStatus pada PengajuanKlaimRepository.js	57
Gambar 4.18. Kode Implementasi Kelas PengajuanKlaimUseCase.js	58
Gambar 4.19. Kode Implementasi Endpoint POST /claims	59
Gambar 4.20. Kode Implementasi Endpoint GET /claims	60
Gambar 4.21. Kode Implementasi Endpoint GET /claims/pending	60
Gambar 4.22. Kode Implementasi GET /claims/:klaimId	60

Gambar 4.23. Kode Implementasi Endpoint PATCH /claims/:klaimId/status	61
Gambar 4.24. Implementasi Kode App.js.....	62
Gambar 4.25. Inisialisasi Repository dan Pengaturan Rute API	62
Gambar 4.26. Konfigurasi Port dan Menjalankan Server	63
Gambar 4.27. Tampilan Request Body pada Endpoint POST /api/claims	64
Gambar 4.28. Tampilan Hasil Enkripsi pada DBMS DBeaver (Tabel pengajuan_klaim_asuransi).....	68
Gambar 4.29. Tampilan Hasil Response Body pada Endpoint GET /api/claims...	68
Gambar 4.30. Tampilan Hasil Response Body pada Endpoint GET /api/claims/:klaimId.....	69
Gambar 4.31. Tampilan Hasil Response Body pada Endpoint GET /api/claims/pending	70
Gambar 4.32. Tampilan Request Body pada Endpoint PATCH /api/claims/:klaimId/status	70
Gambar 4.33. Tampilan Hasil Response Body pada Endpoint PATCH /api/claims/:klaimId/status	71
Gambar 4.34. Tampilan Hasil Pengubahan Status di DBMS DBeaver (Tabel pengajuan_klaim_asuransi).....	71