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*