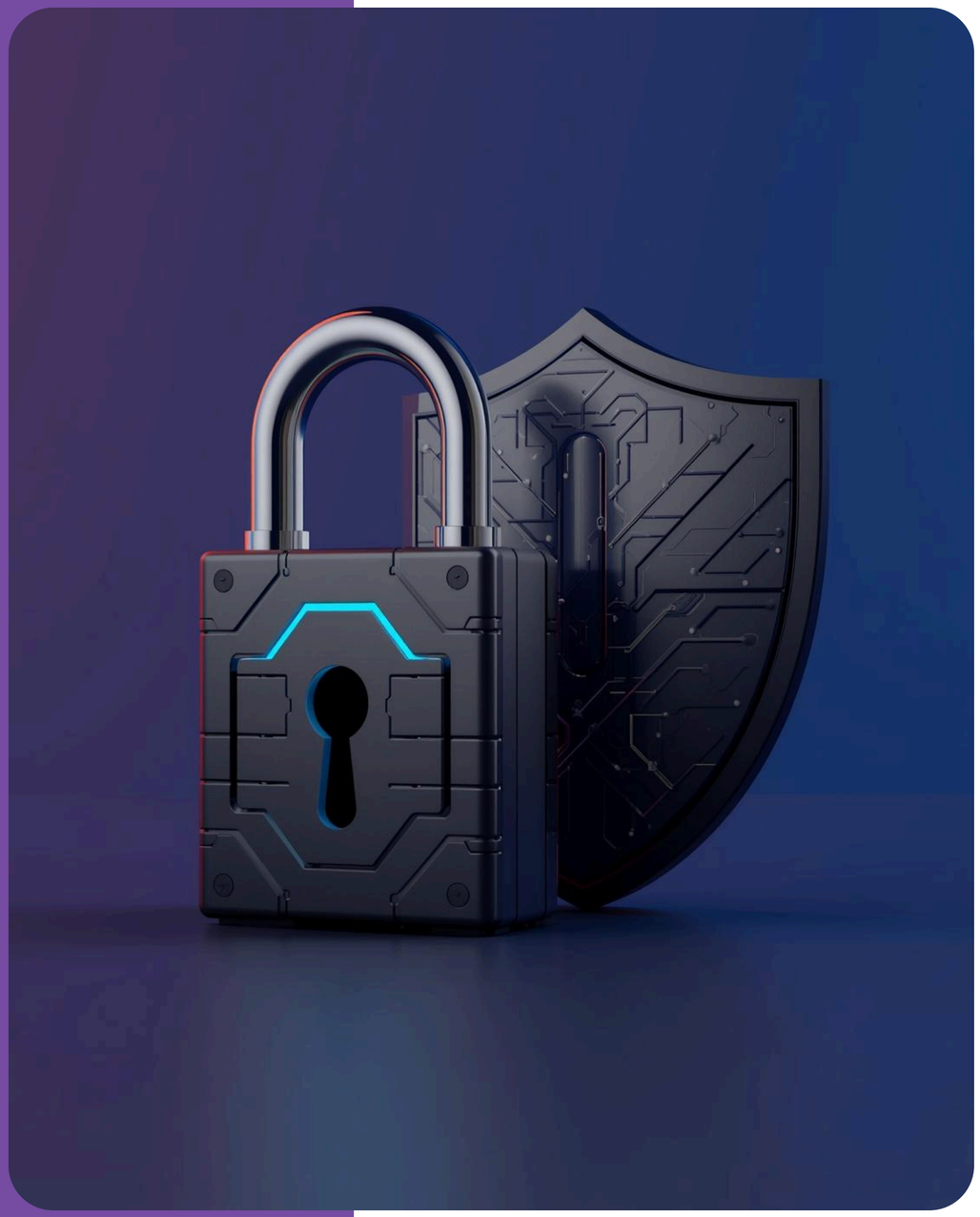

Cybersecurity Presentation

Implementation of AES Algorithm and Blockchain Technology

Satria Adi Wijaya & Abyan Zaky Danur Saputra

Latar Belakang

Ancaman kebocoran data dan serangan siber meningkat 40% pada tahun 2024 (BSSN). Sistem proteksi data konvensional memiliki kelemahan kritis dalam keamanan, transparansi, dan ketahanan terhadap serangan.

Tujuan & Metode Penelitian

Tujuan Penelitian

- Mengimplementasikan kombinasi AES-256 dan Blockchain untuk sistem proteksi data karyawan
- Menciptakan sistem yang aman, terintegrasi, dan terdesentralisasi
- Evaluasi performa dan keamanan sistem terintegrasi

Metode Penelitian

- Pendekatan: Eksperimental dengan Research & Development
- Enkripsi: AES-256 dengan mode CBC (Cipher Block Chaining)
- Blockchain: Hyperledger Fabric untuk private blockchain
- Hash: SHA-256 untuk integritas data

Hasil Implementasi

0.45s Waktu Enkripsi per Record (2KB)	**100%** Tingkat Keberhasilan Enkripsi-Dekripsi
2,200 Transaksi per Menit (Throughput)	**100%** Deteksi Upaya Manipulasi Data

Arsitektur Sistem

Pipeline Terintegrasi: Validasi Input → Enkripsi AES-256 → Bundle Metadata → Digital Signature → Broadcast ke Blockchain → Consensus → Blok Baru → Konfirmasi

Evaluasi Keamanan & Performa

🛡️ Uji Ketahanan Keamanan

- Brute Force Attack: Memerlukan >10^{68} tahun untuk memecahkan AES-256
- Man-in-the-Middle: 100% deteksi melalui digital signature
- Replay Attack: 100% pencegahan dengan timestamp & nonce
- Data Tampering: 100% deteksi melalui immutable blockchain

Evaluasi Keamanan & Performa

⚡ Analisis Performa Sistem

- 10 Concurrent Users: 2,200 trans/menit, 0.52s response time
- 100 Concurrent Users: 1,950 trans/menit, 0.89s response time
- Resource Usage: Enkripsi 30%, Blockchain 40%, Database & Network 30%
- Trade-off: Overhead 15–20% lebih lambat dari sistem konvensional, namun keamanan jauh lebih tinggi

Kesimpulan & Kontribusi

✅ Kesimpulan Utama

- Sistem berhasil mengintegrasikan AES-256 dan Blockchain dengan performa optimal
- Keamanan berlapis terbukti efektif menahan berbagai jenis serangan siber
- Throughput 2,200 transaksi/menit dengan tingkat keberhasilan 100%
- Sistem tahan terhadap brute force, MITM, replay attack, dan data tampering

Kesimpulan & Kontribusi

🌟 Keunggulan Sistem

- Keamanan Berlapis: Kombinasi enkripsi AES-256 + immutability blockchain
- Transparansi Penuh: Audit trail lengkap untuk semua aktivitas
- Desentralisasi: Mengurangi risiko single point of failure
- Compliance: Sesuai GDPR dan UU PDP Indonesia

Implikasi Praktis: Solusi ideal untuk institusi finansial, healthcare, dan sektor pemerintahan yang memerlukan tingkat keamanan data tinggi