Business Requirements Document (BRD)

Proyek: Sistem Proteksi Data Karyawan Terintegrasi (AES & Blockchain)

Sumber Referensi: Studi Literatur Review: Implementasi Integrasi Algoritma AES dan Teknologi Blockchain

1. Ringkasan Eksekutif

Dokumen ini menguraikan kebutuhan bisnis untuk pengembangan sistem keamanan data karyawan yang menggabungkan algoritma *Advanced Encryption Standard* (AES) dan teknologi Blockchain. Tujuannya adalah menciptakan solusi keamanan yang komprehensif, tangguh (*robust*), dan transparan untuk melindungi aset digital perusahaan yang berharga.

2. Latar Belakang Masalah

- **Aset Bernilai Tinggi:** Data karyawan mencakup informasi sensitif seperti identitas pribadi, riwayat kesehatan, dan data finansial yang membutuhkan perlindungan ekstra ketat.
- **Peningkatan Ancaman:** Terdapat lonjakan insiden keamanan data sebesar 40% pada tahun 2024 berdasarkan laporan BSSN.
- **Kelemahan Sistem Konvensional:** Sistem keamanan saat ini yang mengandalkan database terpusat memiliki kerentanan terhadap *single point of failure* (titik kegagalan tunggal) dan kurangnya transparansi dalam *audit trail* (jejak audit).

3. Tujuan Proyek

Mengimplementasikan sistem keamanan berlapis (*layered security*) yang mengintegrasikan:

1. **AES-256** untuk menjamin kerahasiaan (*confidentiality*) data.
2. **Blockchain** untuk menjamin integritas, desentralisasi, dan *immutability* (ketidakbisaan diubah) data.

4. Kebutuhan Fungsional (Functional Requirements)

4.1. Manajemen Enkripsi Data

- **FR-01:** Sistem harus menggunakan algoritma AES-256 untuk mengenkripsi data karyawan.
- **FR-02:** Sistem harus memastikan data tidak dapat dibaca oleh pihak yang tidak berwenang melalui mekanisme kerahasiaan AES.

4.2. Manajemen Integritas & Transaksi (Blockchain)

- **FR-03:** Sistem harus mencatat data dalam blok-blok yang saling terhubung melalui *hash* kriptografis menggunakan teknologi *distributed ledger*.
- **FR-04:** Sistem harus menjamin sifat *immutability*, di mana data yang sudah dicatat tidak dapat diubah tanpa merusak validitas seluruh rantai blok.
- **FR-05:** Sistem harus menyediakan jejak audit (*audit trail*) yang transparan di mana setiap transaksi dapat diverifikasi.

- **FR-06:** Sistem harus mampu mendeteksi upaya manipulasi data (*data tampering*) secara otomatis karena perubahan *hash* akan terdeteksi oleh jaringan.

4.3. Arsitektur Sistem

- **FR-07:** Sistem harus beroperasi secara terdesentralisasi untuk menghilangkan risiko kegagalan terpusat (*single point of failure*).

5. Kebutuhan Non-Fungsional (Non-Functional Requirements)

5.1. Performa (Performance)

- **NFR-01 (Throughput):** Sistem harus mampu menangani beban transaksi hingga 2.200 transaksi per menit.
- **NFR-02 (Latency):** Waktu rata-rata proses enkripsi per *record* data tidak boleh melebihi 0.45 detik.
- **NFR-03 (Tolerance):** Penurunan performa sistem diperbolehkan berada di kisaran 15-20% dibandingkan database konvensional, yang dianggap batas wajar untuk aplikasi *enterprise*.

5.2. Keamanan (Security)

- **NFR-04:** Sistem harus tahan terhadap serangan *brute force* dengan memanfaatkan ruang kunci 256-bit yang secara komputasional mustahil ditembus teknologi saat ini.
- **NFR-05:** Sistem harus tahan terhadap serangan *Man-in-the-Middle* dan manipulasi data (*data tampering*).

5.3. Infrastruktur (Resource Usage)

- **NFR-06:** Infrastruktur harus disiapkan untuk menangani konsumsi sumber daya komputasi dengan estimasi alokasi: 30% untuk proses enkripsi dan 40% untuk operasi blockchain.

6. Risiko dan Batasan

- **Overhead Performa:** Terdapat *trade-off* di mana proses konsensus dan *hashing* akan menambah beban (*overhead*) pada sistem, membuatnya lebih lambat dibandingkan database SQL biasa.
- **Kompleksitas Manajemen:** Tantangan implementasi meliputi manajemen kunci enkripsi yang aman serta proses sinkronisasi data antar *node* dalam jaringan blockchain.

7. Kesimpulan Solusi

Solusi ini direkomendasikan karena AES menutupi kelemahan privasi pada blockchain, sementara blockchain menutupi kelemahan integritas dan sentralisasi pada sistem enkripsi tradisional. Hal ini memberikan nilai lebih dalam perlindungan data sensitif dan kepatuhan terhadap regulasi.