BUSINESS REQUIREMENTS DOCUMENT (BRD)

Sistem Keamanan Data Digital Menggunakan Algoritma Advanced Encryption Standard (AES)

1. Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi mendorong meningkatnya pertukaran data digital dalam berbagai sektor, seperti sistem informasi akademik, aplikasi web, layanan cloud, dan sistem mobile. Kondisi ini secara langsung meningkatkan risiko kebocoran data, manipulasi informasi, serta serangan siber. Oleh karena itu, penerapan mekanisme keamanan data yang kuat dan efisien menjadi kebutuhan utama.

Berdasarkan hasil studi literatur dan analisis jurnal, algoritma Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang telah menjadi standar global dalam pengamanan data. AES tersedia dalam tiga varian panjang kunci, yaitu AES-128, AES-192, dan AES-256, yang masing-masing memiliki perbedaan dari sisi tingkat keamanan, performa, dan kebutuhan sumber daya.

Namun, dalam praktik implementasi sistem, masih ditemukan ketidaktepatan dalam pemilihan varian AES karena kurangnya pemahaman terhadap trade-off antara efisiensi komputasi dan kekuatan enkripsi. Oleh sebab itu, diperlukan dokumen kebutuhan bisnis yang mampu menjabarkan kebutuhan sistem secara jelas dan terstruktur sebagai dasar pengembangan sistem keamanan data berbasis AES.

1.2 Tujuan Dokumen

Tujuan penyusunan Business Requirements Document (BRD) ini adalah:

- Mendefinisikan kebutuhan bisnis sistem keamanan data digital.
- Menjabarkan kebutuhan fungsional dan non-fungsional sistem enkripsi berbasis AES.
- Menjadi acuan pemilihan varian AES yang sesuai dengan konteks sistem.
- Menjembatani kebutuhan bisnis dengan proses perancangan dan pengembangan sistem.

1.3 Ruang Lingkup Dokumen

Dokumen ini membahas:

- Penerapan algoritma AES-128, AES-192, dan AES-256.
- Pengamanan data digital dalam penyimpanan dan transmisi.
- Kebutuhan bisnis, fungsional, dan non-fungsional sistem enkripsi.
- Analisis risiko dan mitigasi dalam implementasi AES.

2 Deskripsi Umum Sistem

2.1 Gambaran Sistem

Sistem yang dikembangkan merupakan sistem keamanan data digital yang menggunakan algoritma AES sebagai mekanisme utama enkripsi dan dekripsi. Sistem ini dirancang agar fleksibel dalam memilih varian AES sesuai dengan tingkat keamanan dan performa yang dibutuhkan.

Sistem dapat diterapkan pada:

- Aplikasi web
- Aplikasi mobile
- Sistem penyimpanan data (database dan file)
- Sistem cloud dan server

2.2 Tujuan Bisnis Sistem

- Menjaga kerahasiaan data digital.
- Menjamin integritas data selama penyimpanan dan transmisi.
- Menyediakan sistem keamanan yang efisien dan adaptif.
- Mengurangi risiko kebocoran dan penyalahgunaan data.

3 Stakeholder

3.1 Identifikasi Stakeholder

- **Pengguna Akhir**: Pihak yang menyimpan dan mengakses data.
- **Administrator Sistem**: Pihak yang mengelola konfigurasi keamanan dan kunci enkripsi.
- **Pengembang Sistem**: Tim teknis yang mengimplementasikan algoritma AES.
- **Manajemen/Owner Sistem**: Pihak pengambil keputusan terkait tingkat keamanan dan investasi sistem.

4 Permasalahan Bisnis

Permasalahan yang diidentifikasi berdasarkan studi literatur:

- Tingginya kebutuhan keamanan sering menurunkan performa sistem.
- Tidak semua data memerlukan tingkat keamanan AES-256.
- Beban komputasi meningkat seiring panjang kunci AES.
- Belum adanya standar pemilihan varian AES berbasis kebutuhan bisnis.

5 Kebutuhan Bisnis (Business Requirements)

5.1 Kebutuhan Utama

- Sistem harus mampu melindungi data dari akses tidak sah.
- Sistem harus mendukung lebih dari satu varian AES.
- Sistem harus fleksibel terhadap kebutuhan keamanan yang berbeda.

5.2 Kebutuhan Pendukung

- Sistem harus efisien dalam penggunaan CPU dan memori.
- Sistem harus dapat digunakan pada berbagai platform.
- Sistem harus mampu menangani data berukuran kecil hingga besar.

6 Kebutuhan Fungsional

1. Sistem harus dapat melakukan enkripsi data menggunakan AES-128.
2. Sistem harus dapat melakukan enkripsi data menggunakan AES-192.
3. Sistem harus dapat melakukan enkripsi data menggunakan AES-256.
4. Sistem harus dapat melakukan dekripsi data sesuai kunci enkripsi.
5. Sistem harus menjamin data hasil dekripsi identik dengan data asli.
6. Sistem harus memungkinkan pemilihan varian AES berdasarkan kebutuhan pengguna atau sistem.

7 Kebutuhan Non-Fungsional

7.1 Keamanan

- Sistem harus tahan terhadap brute-force attack.
- Kunci enkripsi harus disimpan secara aman.
- Sistem harus mencegah kebocoran kunci enkripsi.

7.2 Performa

- AES-128 digunakan untuk sistem real-time dan mobile.
- AES-256 digunakan untuk data sensitif dan sistem keamanan tinggi.
- Waktu enkripsi dan dekripsi harus berada dalam batas toleransi sistem.

7.3 Skalabilitas

- Sistem harus mampu menangani peningkatan volume data.
- Sistem harus dapat berjalan stabil pada beban tinggi.

7.4 Reliabilitas

- Sistem harus memastikan data tidak rusak selama proses enkripsi dan dekripsi.

8 Analisis Varian AES Berdasarkan Kebutuhan Bisnis

Varian AES	Karakteristik Utama	Kesesuaian Kebutuhan
AES-128	Cepat, ringan	Mobile, real-time system
AES-192	Seimbang	Sistem keamanan menengah
AES-256	Sangat aman	Data sensitif, cloud, finansial

9 Risiko dan Mitigasi

9.1 Risiko

- Penurunan performa sistem.
- Beban server meningkat.
- Kesalahan manajemen kunci.

9.2 Mitigasi

- Pemilihan varian AES sesuai konteks sistem.
- Optimalisasi performa dan hardware.
- Penerapan kebijakan manajemen kunci yang ketat.

10 Asumsi dan Ketergantungan

10.1 Asumsi

- Sistem memiliki sumber daya yang memadai.
- Pengguna memahami tingkat keamanan yang dipilih.

10.2 Ketergantungan

- Spesifikasi perangkat keras.
- Jenis dan ukuran data.
- Lingkungan implementasi sistem.

11 Kesimpulan

BRD ini menyimpulkan bahwa implementasi algoritma AES harus disesuaikan dengan kebutuhan bisnis dan karakteristik sistem. AES-128 unggul dalam efisiensi, AES-192 menawarkan keseimbangan, dan AES-256 memberikan keamanan tertinggi. Dokumen ini

dapat dijadikan dasar perancangan sistem keamanan data digital yang efektif, efisien, dan adaptif.