Business Requirement Document (BRD)

Proyek: Peningkatan Standar Keamanan Penyimpanan Password (Implementasi Hashing Adaptif) **Sumber Referensi**: Analisis Komparatif Algoritma Password Hashing

1. Ringkasan Eksekutif

Organisasi saat ini menghadapi risiko keamanan siber yang tinggi akibat evolusi kemampuan perangkat keras peretas. Penggunaan algoritma hashing lama (MD5/SHA-1) yang berfokus pada kecepatan kini dianggap sebagai kerentanan kritis. Dokumen ini menjabarkan kebutuhan bisnis untuk beralih ke algoritma password hashing modern yang "sengaja lambat" (Bcrypt atau Argon2) untuk memitigasi serangan Brute-Force dan Rainbow Table.

2. Pernyataan Masalah & Latar Belakang

- **Masalah Utama:** Algoritma lawas seperti MD5 dan SHA-1 dirancang untuk kecepatan dan integritas data, bukan keamanan password. Kecepatan ini memungkinkan peretas menggunakan GPU modern untuk mencoba miliaran tebakan password per detik.
- **Risiko:**
    - **Serangan Rainbow Table:** Karena algoritma lama bersifat deterministik dan sering tidak menggunakan salt, peretas dapat menggunakan kamus hash yang sudah dihitung sebelumnya untuk membobol password secara instan.
    - **Serangan Brute-Force GPU:** GPU modern dapat mengeksploitasi efisiensi MD5/SHA-1 untuk memecahkan password kompleks dalam hitungan menit.

3. Tujuan Proyek

1) Mengganti mekanisme penyimpanan password yang tidak aman dengan standar kriptografi modern.
2) Meningkatkan resistensi sistem terhadap serangan hardware paralel (GPU/ASIC).
3) Memastikan integritas dan kerahasiaan kredensial pengguna sesuai standar OWASP.

4. Kebutuhan Fungsional (Functional Requirements)

Berikut adalah kebutuhan teknis yang wajib dipenuhi oleh sistem autentikasi baru, berdasarkan analisis komparatif dalam studi literatur:

4.1.Mekanisme Salting Otomatis

- **Kebutuhan:** Sistem wajib menghasilkan salt (data acak unik) secara otomatis untuk setiap user sebelum proses hashing dilakukan.
- **Dasar Teori:** Penggunaan salt memastikan bahwa dua password yang sama akan menghasilkan hash yang berbeda, yang secara efektif mematikan ancaman serangan Rainbow Table.

4.2.Penerapan "Cost Factor" (Faktor Biaya)

- **Kebutuhan:** Algoritma yang dipilih harus memiliki parameter Work Factor atau Cost Factor yang dapat dikonfigurasi (disetel).

- **Dasar Teori:** Algoritma harus "sengaja lambat". Kelambatan ini membuat serangan brute-force menjadi sangat mahal secara komputasi bagi peretas, namun tetap dapat ditoleransi oleh pengguna saat login (misal: durasi ~300ms).

4.3.Pemilihan Algoritma Hashing

Berdasarkan "Analisis Sintesis", tim pengembang harus memilih salah satu dari dua opsi berikut sesuai infrastruktur server:

- Opsi A: Bcrypt (Rekomendasi Standar/Legacy)
  - Karakteristik: CPU-Hard (bergantung pada prosesor).
  - Kelebihan: Sangat matang, mudah diimplementasikan (hanya 1 parameter cost), dan didukung universal.
  - Keterbatasan: Secara teoretis masih rentan terhadap serangan GPU/ASIC canggih karena tidak memakan banyak memori.
  - Target Penggunaan: Sistem standar yang membutuhkan kemudahan implementasi.
- Opsi B: Argon2 (Rekomendasi Keamanan Tinggi/Modern)
  - Karakteristik: Memory-Hard (wajib memakan RAM besar).
  - Kelebihan: Dirancang khusus untuk menahan serangan GPU/ASIC karena GPU memiliki memori terbatas per unit pemrosesan.
  - Keterbatasan: Implementasi lebih kompleks (memerlukan penyetelan 3 parameter: Time, Memory, Parallelism).
  - Target Penggunaan: Sistem baru atau sistem dengan data sensitif tinggi (Keuangan/Kesehatan).

5. Kebutuhan Non-Fungsional (Performance & Constraints)

5.1.Kinerja (Latency)

- Proses verifikasi password tidak boleh instan (seperti MD5: 0.00002 detik) karena tidak aman.
- Target latensi verifikasi harus diatur agar cukup lambat bagi mesin tetapi wajar bagi manusia (disarankan sekitar 200ms - 300ms per percobaan login).

5.2.Kebutuhan Sumber Daya (Resource)

- Jika menggunakan Argon2: Server harus memiliki kapasitas RAM yang memadai untuk dialokasikan pada setiap thread proses login guna mengaktifkan fitur memory-hard.
- Jika menggunakan Bcrypt: Server harus memiliki kemampuan CPU yang cukup untuk menangani beban cost factor yang tinggi saat traffic login padat.

6. Analisis Komparatif & Matriks Keputusan

Tabel berikut digunakan sebagai acuan pengambilan keputusan teknis :

Fitur	MD5/SHA-1(Dilarang)	BCRYPT(Opsi A)	Argon2(Opsi B – Prioritas)
Tujuan Desain	Kecepatan / Integritas File	Keamanan Password	Keamanan Password Modern
Ketahanan Brute-Force	Sangat Buruk (Rentan GPU)	Baik (CPU-Hard)	Sangat Baik (Memory-Hard)

Ketahanan Rainbow Table	Buruk (Deterministik)	Aman (Auto-Salt)	Aman (Auto-Salt)
Resistensi GPU/ASIC	Tidak ada	Rendah - Menengah	Tinggi
Kompleksitas Config	Tidak ada	Rendah (1 Parameter)	Tinggi (3 Parameter)

7. Rekomendasi Langkah Selanjutnya

Berdasarkan kesimpulan studi literatur :

1) Audit Sistem Saat Ini: Periksa apakah sistem masih menggunakan MD5/SHA-1. Jika ya, migrasi adalah prioritas kritis.
2) Pilih Argon2id: Jika membangun sistem baru, gunakan Argon2id sebagai standar modern karena keunggulan teoretisnya melawan perangkat keras modern.
3) Benchmark: Lakukan pengujian beban (load testing) pada server produksi untuk menentukan parameter cost (Bcrypt) atau memory/time cost (Argon2) yang optimal agar tidak membebani server secara berlebihan.