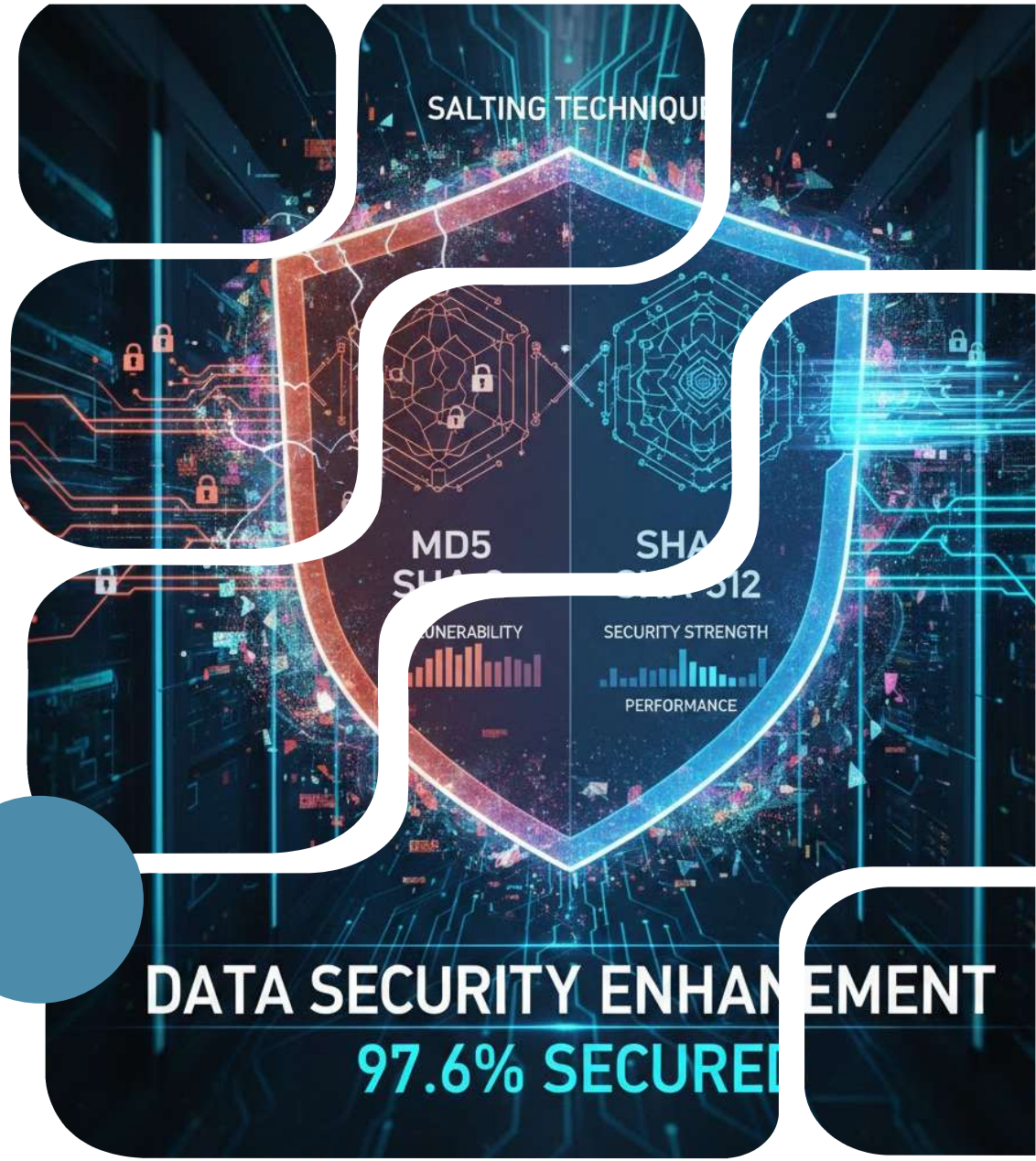
Analisis Komparasi Algoritma Hash (MD5, SHA-2, SHA-3, SHA-512) dan Teknik Salting untuk Peningkatan Keamanan Data.

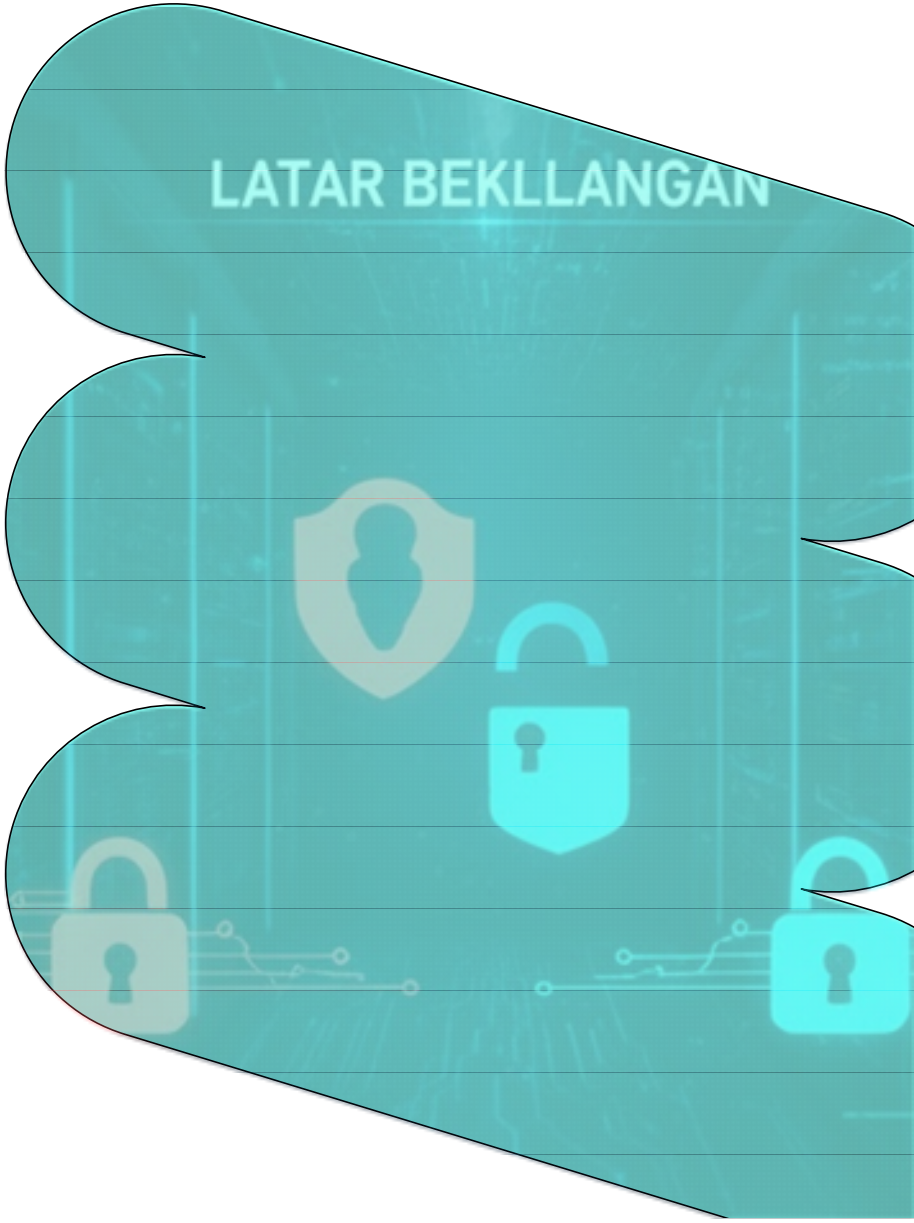
Dini Febryana Sari, Athirah Media Sari, Inayatul Janah,



Latar Belakang

Keamanan data pada sistem digital kini menghadapi tantangan yang semakin kompleks seiring pesatnya transformasi digital, sebagaimana diungkapkan oleh **Agusniar et al. (2025)** Risiko ini diperparah dengan seringnya insiden siber yang terjadi akibat lemahnya pengelolaan kredensial kata sandi, seperti yang ditemukan dalam studi **Natho et al. (2024).**

Sayangnya, di tengah ancaman ini, masih banyak sistem yang mempertahankan algoritma lawas seperti MD5 dan SHA-1. Padahal, **Rahim et al. (2023)** telah membuktikan bahwa algoritma tersebut memiliki kerentanan tinggi terhadap serangan kriptografi modern. Oleh karena itu, penelitian ini berfokus mengevaluasi algoritma hash modern dan efektivitas teknik salting sebagai solusi keamanan yang lebih handal.



Metodologi Penelitian

Pendekatan
Eksperimental melalui simulasi komputasi untuk mengukur performa waktu eksekusi (execution time).

Alat & Lingkungan
Bahasa pemrograman Python (pustaka hashlib) yang dijalankan pada sistem operasi Linux (Ubuntu).

Skenario Pengujian
Melakukan proses enkripsi (hashing) berulang sebanyak 100.000 iterasi untuk setiap algoritma.

Mekanisme Salting
Menerapkan model keamanan hibrida menggunakan SHA-512 yang dikombinasikan dengan Teknik Salting, merujuk pada model yang disarankan oleh **Aranuwa et al. (2022)** untuk meningkatkan kompleksitas serangan.

Hasil Analisis & Pembahasan

1. Perbandingan Kecepatan Eksekusi (100.000 Data)

Algoritma	Total Waktu (detik)	Rata-rata (ms)	Tingkat Keamanan
MD5	0.1343	0.00134	rendah
SHA-256	0.1359	0.00136	tinggi
SHA-512	0.1990	0.00199	sangat tinggi
SHA-3 (256 bit)	0.2764	0.00276	sangat tinggi
SHA-512 + salt	0.4700	0.00470	maksimal

Kecepatan Eksekusi (100.000 data):

- **MD5: Tercepat (0.1343 detik), namun berisiko tinggi terhadap serangan Brute Force.**
- **SHA-512 + Salt: Paling lambat (0.4700 detik), justru memberikan keamanan lebih karena mempersulit komputasi peretas**

Tingkat Keamanan:

- MD5: Sangat rentan (Serangan sukses 35%).
- SHA-3: Paling aman (Serangan sukses hanya 20%).

Performa: SHA-512 (512,8 ms) adalah yang paling seimbang untuk sistem seperti JWT **(Rasyada, 2022).**

Kesimpulan & Rekomendasi

Kesimpulan

- Algoritma lawas (MD5 dan SHA-1) tidak lagi direkomendasikan untuk sistem keamanan modern karena kerentanannya yang tinggi.
- SHA-3 adalah pilihan terbaik untuk prioritas keamanan maksimum, sedangkan SHA-512 memberikan keseimbangan performa terbaik.

Rekomendasi

- Implementasi algoritma hash modern (seperti SHA-512 atau SHA-3) yang dikombinasikan dengan Teknik Salting terbukti mampu meningkatkan ketahanan sistem secara signifikan hingga mencapai 97,6%.