STUDI LITERATUR REVIEW

Evaluasi Kinerja, Keamanan, dan Aplikasi Fungsi Hash Kriptografi Modern (SHA-256, SHA-3, SHA-512)

Disusun Oleh:

Nama : Eko Nurcahyo

Nim : 20230801169

Prodi : Teknik Informatika

UNIVERSITAS ESA UNGGUL

TANGERANG

2025

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang sangat pesat di era digital saat ini telah menghasilkan volume data yang masif dan kompleks. Data telah menjadi aset paling berharga dan krusial bagi individu maupun organisasi, mulai dari transaksi keuangan, pertukaran informasi pribadi, hingga penyimpanan data penting secara daring. Seiring dengan meningkatnya volume dan nilai data digital, tantangan terhadap keamanan data pun menjadi semakin kompleks dan tidak dapat diabaikan. Insiden keamanan seperti peretasan kata sandi, pencurian data, modifikasi dokumen, dan akses tidak sah telah menjadi ancaman serius yang dapat mengakibatkan kerugian finansial dan reputasi yang signifikan.

Untuk mengatasi tantangan keamanan ini, kriptografi menjadi teknologi inti dalam pengamanan data, menjamin keamanan dan privasi data yang mutlak. Salah satu metode kriptografi yang paling fundamental dan banyak digunakan adalah Fungsi Hash (Hash Function). Fungsi Hash berperan sentral sebagai "sidik jari digital" yang memastikan integritas data—bahwa data belum diubah—dan juga menjadi komponen krusial dalam otentikasi kata sandi. Tinjauan pustaka ini bertujuan untuk mengevaluasi secara kritis kinerja, keamanan, dan aplikasi Fungsi Hash modern (SHA-256, SHA-512, SHA-3, dan Blake2), berdasarkan penelitian terbaru untuk memberikan wawasan strategis mengenai trade-off dalam pemilihan algoritma hash yang optimal.

2. Konsep Dasar Kriptografi

Konsep ini memberikan landasan teori yang kokoh, dengan fokus utama pada Fungsi Hash sebagai komponen kunci dalam keamanan integritas data.

Definisi Kriptografi

Kriptografi adalah ilmu dan seni dalam mengamankan pesan dengan melakukan enkripsi (penyandian) dan dekripsi (pembukaan sandi). Secara umum, kriptografi modern adalah studi fundamental dalam keamanan data yang menerapkan prinsip-prinsip matematika yang kompleks untuk melindungi informasi. Perkembangannya dari metode klasik berbasis substitusi sederhana telah berevolusi menjadi algoritma yang sangat canggih yang menjadi tulang punggung keamanan digital global.

Tujuan Utama Kriptografi

Kriptografi memiliki beberapa tujuan utama yang dikenal sebagai konsep CIA (*Confidentiality, Integrity, dan Authentication*):

- Kerahasiaan (*Confidentiality*): Memastikan bahwa isi data hanya dapat diakses atau dipahami oleh pihak yang memiliki kunci atau otorisasi yang sah. Ini dicapai melalui algoritma enkripsi.
- Integritas (*Integrity*): Memastikan bahwa data belum diubah, dirusak, atau dimodifikasi selama proses transmisi atau penyimpanan. Fungsi *Hash* secara khusus dirancang untuk tujuan ini dengan menghasilkan message digest yang unik.
- Autentikasi (*Authentication*): Memverifikasi identitas pengguna atau sumber data. Fungsi Hash sering digunakan untuk otentikasi kata sandi, di mana *hash* kata sandi yang dimasukkan dicocokkan dengan *hash* yang tersimpan di *database*.

- Non-Repudiasi (*Non-Repudiation*): Mencegah seseorang menyangkal telah mengirim atau menerima pesan, biasanya dicapai melalui Tanda Tangan Digital yang menggunakan kriptografi asimetris yang dikombinasikan dengan *hashing*.

Jenis Kriptografi (Fokus: Hash Function)

Hash Function adalah algoritma matematis satu arah (*one-way function*) yang mengambil *input* data dengan panjang arbitrer dan menghasilkan *output* nilai *hash* dengan **panjang tetap**, yang disebut *message digest*. Sifat *one-way* ini menjadikannya mustahil untuk meregenerasi data asli hanya dari nilai *hash*-nya.

- SHA-2 (SHA-256 & SHA-512): Merupakan keluarga algoritma yang dikembangkan oleh NSA dan distandardisasi oleh NIST. Algoritma ini dianggap aman hingga saat ini. SHA-256 menghasilkan *hash* 256-bit dan menjadi standar *de facto* dalam banyak protokol keamanan, sementara SHA-512 menghasilkan *hash* 512-bit, menawarkan keamanan *output* yang lebih besar, namun membutuhkan daya komputasi yang sedikit lebih besar.
- SHA-3: Standar terbaru dari NIST, didasarkan pada algoritma Keccak dan menggunakan arsitektur Sponge Construction yang sangat berbeda dari SHA-2. Arsitektur ini dirancang untuk lebih unggul dalam ketahanan kolisi (*collision resistance*) dan *pre-image resistance*.
- Blake2: Algoritma alternatif yang dikembangkan untuk menjadi lebih cepat daripada SHA-256 sambil tetap mempertahankan tingkat keamanan yang tinggi, menjadikannya pilihan populer untuk aplikasi yang sensitif terhadap kinerja.

Kategori Algoritma	**Kunci Digunakan**	**Kecepatan**	**Fungsi Utama**	**Fokus SHA-2 & SHA-3**
Simetris (AES)	Kunci Tunggal Rahasia	Sangat Cepat	Kerahasiaan Data Massal	Dikombinasikan untuk Integritas
Asimetris (RSA/ECC)	Pasangan Kunci Publik/Privat	Lambat	Pertukaran Kunci, Non-Repudiasi	Tidak Relevan
Hash Function	Tidak Ada (Publik)	Variatif	**Integritas Data** & Otentikasi	**Verifikasi dan Keutuhan Data**

3. Tinjauan Penelitian Terdahulu

Bagian inti ini membahas hasil riset spesifik yang menguji kinerja dan aplikasi algoritma *Hash* modern, dengan detail temuan dari ketiga jurnal yang ditinjau.

Peneliti & Tahun	Metode / Algoritma	Tujuan Penelitian	Hasil & Temuan Kunci	Kelemahan / Keterbatasan
Sitorus et al. (2024)	**SHA-256, SHA-3, & Blake2**	Menganalisis kinerja dan keamanan (ketahanan *brute force*, *avalanche effect*, waktu pemrosesan).	**Keamanan:** SHA-3 unggul dalam **konsistensi *avalanche effect*** (>50%). **Kecepatan: Blake2** paling cepat, SHA-3 paling lambat.	Tidak mencakup teknik **salting** atau **SHA-512** dalam perbandingan langsung.
Batubara & Aritonang (2025)	**SHA-256 & SHA-512**	Membandingkan kinerja (waktu *decrypt* simulasi) dan keamanan kedua algoritma untuk **keamanan sandi** dengan *input* karakter berbeda.	**Perbandingan:** Karakter *abjad* dan *campuran* lebih lama di *decrypt* di SHA-512. **Keunikan:** Karakter *angka* pada **SHA-256** lebih aman (*decrypt* lebih lama) dibandingkan SHA-512.	Fokus pada simulasi *decrypt* berdasarkan jenis karakter *input*, bukan kriptanalisis teoritis.
Nurjaman & Turnip (2024)	AES-256 dan **SHA3-512**	Mengevaluasi efektivitas kombinasi AES-256 dengan SHA3-512 dalam melindungi **dokumen digital (.pdf)**.	Kombinasi **AES-256 dan SHA3-512** terbukti **stabil dan efisien** dalam hal waktu pemrosesan, menjamin integritas dan kerahasiaan dokumen secara efektif.	Penelitian hanya menguji **kombinasi SHA3-512** dan tidak membandingkannya dengan kombinasi *hash* lain (misalnya SHA-256).

4. Analisis dan Sintesis

Analisis ini menyatukan temuan dari penelitian yang ditinjau untuk mengidentifikasi pola, tren, dan celah penelitian (*research gap*) dalam penggunaan Fungsi Hash:

- Tren Evolusi Algoritma Hash: Penelitian menunjukkan bahwa standar *hash* terus berevolusi. Terdapat pengakuan luas akan keunggulan arsitektur baru SHA-3 dibandingkan SHA-2, terutama dalam hal ketahanan terhadap serangan kolisi di masa depan (Sitorus et al., 2024). Meskipun demikian, SHA-256 masih sangat relevan karena menawarkan keseimbangan yang memadai antara kecepatan dan keamanan yang teruji.
- Perbandingan Performa (*Trade-off*): Hasil penelitian menggarisbawahi adanya *trade-off* yang harus dipertimbangkan.
    - Kecepatan vs. Keamanan Mutlak: Algoritma Blake2 terbukti paling efisien dalam hal waktu pemrosesan (*hashing*), menjadikannya pilihan cepat untuk lingkungan sensitif waktu. Sebaliknya, SHA-3 menunjukkan kinerja yang lebih

lambat, namun karakteristik ini dikompensasi dengan tingkat keamanan yang paling superior, khususnya dalam konsistensi *avalanche effect* (Jurnal Sitorus).
    - Varian SHA-2: Perbandingan antara SHA-256 dan SHA-512 (Batubara & Aritonang, 2025) menunjukkan bahwa SHA-512 umumnya lebih direkomendasikan karena *output* 512-bit yang lebih besar. Namun, temuan unik menunjukkan bahwa *input* berbasis angka memiliki waktu *decrypt* yang lebih lama pada SHA-256, menyarankan bahwa kinerja keamanan dapat bergantung pada jenis *input* data sandi.
- Penggunaan Kriptografi di Bidang Tertentu: Fungsi *Hash* tidak hanya berdiri sendiri. Penerapannya sering kali bersifat hibrida, di mana SHA3-512 digunakan bersama enkripsi simetris AES-256 (Nurjaman & Turnip, 2024). Dalam skema ini, SHA3-512 menjamin integritas dokumen (.pdf) yang telah dienkripsi, membuktikan perannya yang vital dalam memastikan bahwa data rahasia tidak dirusak selama proses transmisi dan penyimpanan.
- Tantangan dan Masalah yang Belum Terselesaikan (Research Gap): Meskipun algoritma ini terbukti aman dalam lingkungan komputasi standar, penelitian yang ditinjau belum secara komprehensif membahas kinerja SHA-3/SHA-512 dalam konteks perangkat *Internet of Things* (IoT) atau *mobile*, di mana sumber daya (daya baterai, memori) sangat terbatas. Selain itu, ada celah besar dalam studi perbandingan kinerja yang secara langsung menguji efektivitas algoritma *hash* yang dikombinasikan dengan teknik Salting, yang merupakan praktik terbaik untuk keamanan *password*.

5. Arah dan Peluang Penelitian

Berdasarkan analisis celah yang teridentifikasi dari tinjauan pustaka, berikut adalah peluang penelitian yang dapat dilanjutkan:

1. Pengembangan Algoritma Kriptografi Ringan (*Lightweight Cryptography*): Penelitian mendalam diperlukan untuk mengoptimalkan implementasi SHA-3 dan Blake2 agar efisien untuk perangkat IoT dan sistem *mobile*. Studi harus berfokus pada pengurangan konsumsi daya dan jejak memori, yang merupakan faktor kunci dalam perangkat *resource-constrained*.
2. Model Hibrida Kinerja Tinggi dan *Salting*: Perlu dilakukan perbandingan kinerja yang komprehensif antara model *hashing* yang mengintegrasikan teknik Salting dengan algoritma cepat (Blake2) melawan algoritma aman (SHA-3). Penelitian ini penting untuk menentukan model *password hashing* yang paling efisien dan tangguh bagi *database* modern, yang dapat melawan serangan *rainbow table* dan *brute force* yang semakin canggih.
3. Optimalisasi *Hash* untuk Dokumen Bervariasi: Melanjutkan studi hibrida (Nurjaman & Turnip, 2024) dengan menguji efektivitas kombinasi *hash* (SHA-512) dan *cipher* simetris pada berbagai ekstensi dokumen (selain PDF), untuk memastikan validitas dan efisiensi skema perlindungan data di berbagai *platform* dan format data.

6. Kesimpulan

Tinjauan literatur ini menyimpulkan bahwa algoritma *Hash* modern (SHA-256, SHA-512, SHA-3, dan Blake2) menawarkan ketahanan yang sangat baik dan menjadi fondasi keamanan data saat ini. SHA-3 menawarkan keamanan teoritis terkuat (terutama *avalanche effect*), Blake2 unggul dalam efisiensi waktu pemrosesan, dan SHA-512 memberikan keseimbangan yang baik untuk otentikasi. Implementasi SHA3-512 yang dikombinasikan dengan AES-256 terbukti efektif menjamin integritas dan kerahasiaan dokumen digital. Meskipun kemajuan ini signifikan, tantangan utama ke depan adalah optimalisasi *lightweight hash* untuk lingkungan IoT dan kebutuhan untuk menguji model *hashing* yang komprehensif yang menyertakan praktik *salting* untuk meningkatkan keamanan *password*.

7. Daftar Pustaka

Algoritma, K., Dan, K. A.-, Meningkatkan, S.-U., & Dokumen, K. (2024). *Kombinasi algoritma kriptografi aes-256 dan sha3-512 untuk meningkatkan keamanan dokumen pdf*. *11*(1),4654. https://journal.widyatama.ac.id/index.php/jitter/article/download/2346/1153/8496

Sandi, U. K., Batubara, T. P., Adi, M., & Aritonang, S. (2025). *Perbandingan Algoritma Kriptografi Hash Sha 256 dan Sha 512*. *3*(1), 6–10. https://journal.iteba.ac.id/index.php/jurnal_quancom/article/download/627/278/3193

Sha-, A., Sitorus, N., Sharon, J., Sinaga, G., & Samosir, S. L. (2024). *Analisis Kinerja Algoritma Hash pada Keamanan Data : Perbandingan*. *2*(2). https://doi.org/10.62375/jqc.v2i2.432