JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Analisis Penggunaan Hash Function dan Digital Signature pada Sistem Keamanan Informasi

Arya Bagas Saika[1*], Muhammad Fauzul[2], Alif Akbar Rafsanjani [3,] Rizky Hajriani Nasution[4], Marsha Ramadhani[5]
[1,2,3,4,5] Universitas Malikussaleh, Indonesia
[1]arya.240170125@mhs.unimal.ac.id, [2]muhammad.240170211@mhs.unimal.ac.id,
[3]alif.240170106@mhs.unimal.ac.id, [4]rizky.240170230@mhs.unimal.ac.id, [5]marsha.240170089@mhs.unimal.ac.id

ABSTRACT

Information security is a critical issue in the development of modern information systems due to increasing threats such as data manipulation, forgery, and unauthorized access. This study aims to analyze the use of hash functions and digital signatures as cryptographic mechanisms to ensure data integrity, authentication, and non-repudiation in information security systems. The research method used is a literature review by analyzing scientific journals related to the implementation of hash functions and digital signature algorithms in various information systems. The results show that hash functions play an important role in maintaining data integrity, while digital signatures provide assurance of authenticity and accountability of data transmission. The combination of hash functions and digital signatures is proven to significantly enhance the security of information systems and reduce the risk of data tampering and security breaches.

Keywords : *Hash function, Digital signature, Information security, Data integrity, Cryptography.*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong meningkatnya pertukaran data digital dalam berbagai bidang, seperti sistem akademik, transaksi elektronik, layanan berbasis web, dan komunikasi digital. Namun, kemajuan tersebut juga diiringi dengan meningkatnya ancaman terhadap keamanan informasi, seperti pemalsuan data, penyadapan, perubahan isi informasi, dan akses tidak sah oleh pihak yang tidak berwenang. Kondisi ini menuntut adanya mekanisme keamanan yang mampu menjaga keutuhan, keaslian, dan keandalan data.

Sistem keamanan informasi memerlukan penerapan teknik kriptografi yang efektif untuk melindungi data dari berbagai serangan. Dua mekanisme kriptografi yang umum digunakan adalah fungsi hash dan tanda tangan digital. Fungsi hash digunakan untuk memastikan integritas data dengan menghasilkan nilai hash unik dari suatu pesan, sehingga setiap perubahan kecil pada data dapat terdeteksi. Sementara itu, tanda tangan digital berperan dalam proses autentikasi dan non-repudiation, yaitu menjamin keaslian pengirim dan mencegah penyangkalan terhadap data yang telah dikirimkan.

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan fungsi hash dan tanda tangan digital dapat meningkatkan tingkat keamanan sistem informasi secara signifikan. Namun, pemilihan algoritma hash dan metode tanda tangan digital yang kurang tepat dapat menimbulkan celah keamanan, terutama jika algoritma yang digunakan sudah tidak lagi aman.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis penggunaan fungsi hash dan tanda tangan digital dalam sistem keamanan informasi serta mengkaji peran dan kontribusinya dalam menjaga integritas dan keaslian data. Diharapkan hasil penelitian ini dapat memberikan gambaran mengenai pentingnya penerapan kedua mekanisme tersebut dalam meningkatkan keamanan sistem informasi.

Selain penerapan kriptografi seperti fungsi hash dan tanda tangan digital, aspek keamanan informasi juga perlu dievaluasi secara menyeluruh melalui pengukuran tingkat kesiapan dan pengelolaan risiko keamanan sistem informasi, seperti yang dilakukan menggunakan Indeks Keamanan Informasi (Indeks KAMI) dan standar manajemen keamanan informasi ISO 27001 (Jenny, 2024; Susanto & Legowo, 2023).

KAJIAN LITERATUR

Keamanan informasi merupakan upaya untuk melindungi data dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Dalam sistem informasi modern, penerapan teknik kriptografi menjadi salah satu solusi utama untuk menjaga keamanan data, khususnya dalam proses penyimpanan dan transmisi informasi (Susanto & Legowo, 2023).

Fungsi hash adalah algoritma kriptografi yang mengubah data dengan panjang variabel menjadi nilai hash dengan panjang tetap. Algoritma hash seperti SHA-1, SHA-256, dan SHA-512 banyak digunakan untuk menjamin integritas data, karena perubahan sekecil apa pun pada data akan menghasilkan nilai hash yang berbeda secara

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

signifikan (Ipdal, 2021). Penelitian oleh Taqiyyah dan Adriansyah (2020) menunjukkan bahwa fungsi hash efektif digunakan dalam proses otentikasi file digital dan menjadi komponen penting dalam sistem tanda tangan digital.

Tanda tangan digital merupakan mekanisme keamanan yang menggunakan kriptografi kunci publik untuk memastikan keaslian dan integritas pesan. Proses tanda tangan digital melibatkan pembuatan nilai hash dari pesan yang kemudian dienkripsi menggunakan kunci privat pengirim. Penelitian oleh Aminuddin dan Arifianto (2021) membuktikan bahwa penerapan algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) dengan fungsi hash tertentu mampu meningkatkan efisiensi dan keamanan tanda tangan digital.

Beberapa penelitian lain juga menunjukkan bahwa penerapan tanda tangan digital pada berbagai sistem, seperti sistem penggajian dan sistem berbasis web, mampu mencegah pemalsuan data dan meningkatkan kepercayaan pengguna terhadap sistem informasi (Eritza et al., 2022; Gafrun & Supit, 2024). Berdasarkan kajian literatur tersebut, dapat disimpulkan bahwa fungsi hash dan tanda tangan digital memiliki peran yang sangat penting dalam menjaga keamanan sistem informasi, baik dari sisi integritas maupun autentikasi data.

Beberapa penelitian juga menyoroti pentingnya pengujian keamanan sistem untuk mengidentifikasi celah kerentanan yang dapat dimanfaatkan oleh pihak tidak berwenang. Salah satu pendekatan yang umum digunakan adalah penetration testing dengan mengacu pada standar OWASP Top 10 sebagai kerangka evaluasi keamanan aplikasi dan sistem informasi (Mustofa et al., 2024).

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan pendekatan kualitatif deskriptif. Metode ini dipilih untuk menganalisis konsep, penerapan, serta peran fungsi hash dan tanda tangan digital dalam sistem keamanan informasi berdasarkan penelitian-penelitian sebelumnya yang relevan.

Ruang lingkup penelitian difokuskan pada pembahasan algoritma fungsi hash dan tanda tangan digital yang umum digunakan dalam sistem keamanan informasi, seperti SHA dan algoritma tanda tangan digital. Objek penelitian berupa jurnal ilmiah, artikel penelitian, dan publikasi akademik yang membahas penerapan fungsi hash dan tanda tangan digital pada berbagai sistem informasi.

Teknik pengumpulan data dilakukan dengan cara mengumpulkan referensi dari jurnal nasional dan internasional yang relevan dengan topik penelitian. Data yang diperoleh kemudian diseleksi berdasarkan kesesuaian topik dan tahun publikasi untuk memastikan relevansi dan kebaruan informasi.

Teknik analisis data dilakukan secara deskriptif dengan membandingkan hasil penelitian sebelumnya, mengidentifikasi kelebihan dan kekurangan dari setiap metode yang digunakan, serta menarik kesimpulan mengenai efektivitas penggunaan fungsi hash dan tanda tangan digital dalam meningkatkan keamanan sistem informasi.

HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis terhadap berbagai penelitian yang telah dikaji, diketahui bahwa fungsi hash dan tanda tangan digital memiliki peran yang sangat penting dalam menjaga keamanan sistem informasi. Fungsi hash digunakan untuk memastikan integritas data dengan cara menghasilkan nilai hash yang unik dari setiap data atau pesan yang diproses. Hasil kajian menunjukkan bahwa algoritma hash seperti SHA-256 dan SHA-512 lebih direkomendasikan dibandingkan SHA-1 karena memiliki tingkat keamanan yang lebih tinggi dan lebih tahan terhadap serangan collision (Ipdal, 2021).

Penerapan tanda tangan digital pada sistem informasi terbukti mampu meningkatkan aspek autentikasi dan non-repudiation. Dengan menggunakan kriptografi kunci publik, tanda tangan digital memungkinkan penerima pesan untuk memverifikasi keaslian pengirim serta memastikan bahwa data tidak mengalami perubahan selama proses transmisi. Penelitian oleh Aminuddin dan Arifianto (2021) menunjukkan bahwa penggunaan algoritma ECDSA dengan fungsi hash tertentu memberikan efisiensi yang lebih baik dibandingkan metode konvensional, terutama dari sisi kecepatan dan ukuran kunci.

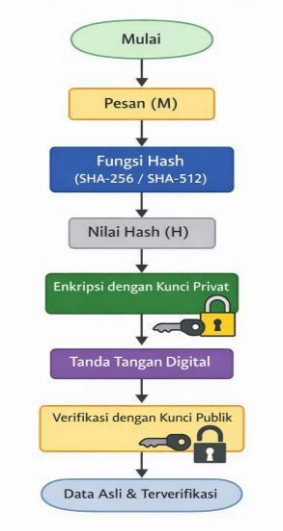
Selain itu, beberapa penelitian juga menunjukkan bahwa kombinasi fungsi hash dan tanda tangan digital dapat diterapkan secara efektif pada berbagai sistem, seperti sistem penggajian, sistem akademik, dan aplikasi berbasis web, untuk mencegah pemalsuan data dan meningkatkan kepercayaan pengguna (Eritza et al., 2022; Gafrun & Supit, 2024). Namun demikian, hasil kajian juga mengungkapkan bahwa penggunaan algoritma yang sudah tidak direkomendasikan dapat menimbulkan celah keamanan dan berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dengan demikian, hasil dan pembahasan ini menunjukkan bahwa pemilihan algoritma yang tepat serta penerapan fungsi hash dan tanda tangan digital secara benar sangat berpengaruh terhadap tingkat keamanan sistem informasi. Integrasi kedua mekanisme ini dapat menjadi solusi yang efektif dalam menghadapi ancaman keamanan informasi yang terus berkembang, sebagaimana ditunjukkan pada Gambar 1.

Integrasi mekanisme autentikasi dan otorisasi yang aman juga menjadi faktor penting dalam mendukung penerapan tanda tangan digital pada sistem informasi. Penggunaan JSON Web Token (JWT) sebagai mekanisme pengelolaan hak akses terintegrasi dapat meningkatkan keamanan sistem apabila dikonfigurasikan dengan benar (JWT,

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

2023).



Gambar 1. Alur penerapan fungsi hash dan tanda tangan digital dalam sistem keamanan informasi

Gambar 1 menunjukkan alur penerapan fungsi hash dan tanda tangan digital dalam sistem keamanan informasi. Proses dimulai dari pesan atau data awal (M) yang diproses menggunakan fungsi hash, seperti SHA- 256 atau SHA-512, untuk menghasilkan nilai hash (H). Nilai hash tersebut kemudian dienkripsi menggunakan kunci privat pengirim sehingga membentuk tanda tangan digital. Pada sisi penerima, proses verifikasi dilakukan menggunakan kunci publik untuk memastikan keaslian tanda tangan digital serta kesesuaian nilai hash. Apabila proses verifikasi berhasil, maka data dinyatakan asli dan terjaga integritasnya.

Tabel 1.

No	Mekanisme Keamanan	Algoritma	Fungsi Utama	Kelebihan	Kekurangan
1	Fungsi Hash	SHA-1	Menjaga integritas data	Proses cepat	Rentan terhadap collision
2	Fungsi Hash	SHA-256	Menjaga integritas data	Tingkat keamanan tinggi	Komputasi lebih berat
3	Fungsi Hash	SHA-512	Integritas data tingkat tinggi	Sangat aman	Konsumsi sumber daya besar
4	Tanda Tangan Digital	RSA	Autentikasi dan non-repudiation	Implementasi luas	Ukuran kunci besar
5	Tanda Tangan Digital	ECDSA	Autentikasi dan integritas	Efisien, ukuran kunci kecil	Implementasi lebih kompleks

KESIMPULAN

Berdasarkan hasil studi literatur yang telah dilakukan, dapat disimpulkan bahwa fungsi hash dan tanda tangan digital memiliki peran penting dalam menjaga keamanan sistem informasi. Fungsi hash berfungsi untuk memastikan integritas data dengan mendeteksi perubahan informasi, sebagaimana ditunjukkan oleh Taqiyyah dan Adriansyah (2020) serta Ipdal (2021).

Tanda tangan digital berperan dalam menjamin keaslian pengirim dan mencegah penyangkalan terhadap data yang dikirimkan. Penelitian Aminuddin dan Arifianto (2021) serta Eritza et al. (2022) menunjukkan bahwa penerapan tanda tangan digital mampu meningkatkan keandalan dan kepercayaan terhadap sistem informasi.

Integrasi fungsi hash dan tanda tangan digital terbukti efektif dalam meningkatkan keamanan data pada berbagai sistem informasi. Namun, pemilihan algoritma yang tepat dan penerapan sesuai standar keamanan tetap diperlukan agar sistem tidak rentan terhadap ancaman. Penelitian selanjutnya disarankan untuk mengimplementasikan mekanisme ini secara langsung pada sistem nyata guna mengevaluasi performa dan tingkat keamanannya secara empiris.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pengampu mata kuliah Keamanan Sistem Komputer Program Studi Teknik Informatika atas bimbingan dan materi yang telah diberikan selama perkuliahan. Penulis juga

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

menyampaikan apresiasi kepada berbagai sumber referensi yang digunakan dalam penyusunan tugas ini. Semoga laporan ini dapat menambah pemahaman mengenai penerapan fungsi hash dan tanda tangan digital dalam sistem keamanan informasi.

REFERENSI

Aminuddin, A., & Arifianto, S. (2021). Perbandingan kinerja algoritma elliptic curve digital signature algorithm (ECDSA) menggunakan fungsi hash secure hash algorithm (SHA-1) dan Keccak pada tanda tangan digital. *Jurnal Repositor, 3*(3).

Eritza, A., Ramadhan, M., & Hafizah, H. (2022). Penerapan digital signature metode SHA dan DSA pada slip gaji pegawai. *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD), 1*(6), 906–914.

Gafrun, G., & Supit, Y. (2024). Algoritma tanda tangan digital untuk meningkatkan keamanan pesan. *Simtek: Jurnal Sistem Informasi dan Teknik Komputer, 9*(2), 198–204.

Ipdal, M. (2021). Analisa metode SHA-512 untuk tanda tangan digital pada file video. *Journal of Informatics Management and Information Technology, 1*(1), 23–29.

Jenny, M. S. (2024). Analisis tingkat kesiapan keamanan informasi menggunakan indeks keamanan informasi (Indeks KAMI) versi 4.2 pada sistem informasi akademik (SIMAK) Universitas Siliwangi. *Jurnal SITECH: Sistem Informasi dan Teknologi, 7*(1), 73–80.

JWT, P. (2023). Evaluasi keamanan privilege terintegrasi JSON web token pada sistem informasi akademik.
Jurnal Informasi dan Teknologi, 5(2), 120–128.

Mustofa, P. Z., Sumaryana, Y., & Ruuhwan, R. (2024). Penetration testing pada domain xyz.ac.id menggunakan OWASP 10. *e-Jurnal JUSITI (Jurnal Sistem Informasi dan Teknologi Informasi), 13*(2), 175–182.

Setiaji, K., & Aminulloh, M. (2025). Analisis yuridis keabsahan penggunaan digital signature pada naskah dinas untuk kegiatan operasional Polres Bogor. *Karimah Tauhid, 4*(3), 1666–1677.

Susanto, E., & Legowo, N. (2023). Hasil penilaian risiko keamanan informasi pada laboratorium klinik berdasarkan kriteria kendali dalam penerapan ISO 27001. *Jurnal Rekayasa Sistem Industri, 12*(2), 155– 164.

Taqiyyah, R., & Adriansyah, A. R. (2020). Implementasi fungsi hash untuk otentikasi file digital (digital signature). *Jurnal Informatika Terpadu, 6*(1), 7–13.