JIKUM
JURNAL ILMU KOMPUTER

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

Analisis Kinerja Algoritma Hash dan MAC terhadap Integritas dan Autentikasi Data

Luthfiah Putri[1], Zulfa Khairunnisa[2], Junita Rahma Senjani[3], Septia Praramadani[4], Yulandari Oktavia Hasibuan[5*]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]luthfiah.240170084@mhs.unimal.ac.id, [2]zulfa.240170100@mhs.unimal.ac.id, [3]junita.240170135@mhs.unimal.ac.id, [4]septia.240170159@mhs.unimal.ac.id, [5]yulandari.240170168@mhs.unimal.ac.id

ABSTRACT

In information systems, data security plays a crucial role, particularly in ensuring data integrity and authentication during storage and transmission processes. Hash algorithms and Message Authentication Codes (MAC) are two cryptographic techniques commonly employed for these purposes. Hash algorithms are primarily used to maintain data integrity, whereas MAC provides both data integrity and authentication through the use of a shared secret key. This study aims to analyze and compare the performance of hash algorithms and MAC in preserving data integrity and authentication. The research adopts a quantitative experimental method with a comparative analysis approach, using test data of varying sizes and evaluating performance based on specific operational parameters. The results indicate that hash algorithms are effective in detecting data modifications through hash value comparison, while MAC offers stronger guarantees by ensuring both data integrity and authentication using a shared secret key. These findings highlight the strengths and limitations of each mechanism and provide insights into their appropriate application in secure information systems. The findings further suggest that hash algorithms are more suitable for data integrity verification, whereas MAC is more appropriate for systems that require both data integrity and authentication simultaneously.

Kata Kunci/ Keywords:
Data Security, Hash Algorithm, Message Authentication Code, Data Integrity, Data Authentication

PENDAHULUAN

Di era digital seperti sekarang ini, perkembangan teknologi informasi dan komunikasi semakin pesat sehingga menyebabkan meningkatnya aktivitas pertukaran data melalui berbagai sistem digital serta jaringan komputer. Berbagai ancaman keamanan terhadap keamanan data yang dikirim dan disimpan secara digital termasuk perubahan data tanpa izin, pemalsuan pesan, dan penyalahgunaan identitas pengirim. Oleh sebab itu, penerapan keamanan informasi menjadi hal yang sangat penting, terutama dalam menjaga integritas dan autentikasi data.

Menurut Simbolon et al., 2020, Integritas data (*data integrity*) merupakan salah satu layanan keamanan informasi yang menjamin bahwa pesan yang dikirim tidak mengalami perubahan isi, sehingga keaslian dan keutuhan data tetap terjaga selama proses komunikasi. Sementara itu, Autentikasi data (*data authentication*) merupakan layanan keamanan yang berkaitan dengan proses verifikasi keaslian sumber pesan. Layanan ini digunakan untuk memastikan bahwa pihak yang melakukan komunikasi benar-benar merupakan pihak yang sah. Apabila integritas dan autentikasi data tidak diterapkan secara optimal, sistem informasi berpotensi mengalami serangan keamanan berupa manipulasi data, pemalsuan pesan, maupun intersepsi komunikasi oleh pihak tidak berwenang.

Salah satu teknik kriptografi yang banyak digunakan untuk menjaga integritas data adalah algoritma hash. Algoritma hash adalah suatu teknik kriptografi yang berfungsi mengubah data atau teks menjadi rangkaian karakter acak dengan panjang tertentu yang bersifat tetap. Algoritma ini termasuk enkripsi satu arah sehingga hasil transformasinya tidak dapat dikembalikan ke bentuk aslinya (Agusniar et al., 2025). Namun, algoritma hash pada umumnya tidak menggunakan kunci rahasia, sehingga hanya mampu menjamin integritas data tanpa memastikan keaslian pengirim data. Untuk mengatasi keterbatasan tersebut, digunakan MAC yang merupakan mekanisme kriptografi berupa kode autentikasi yang digunakan untuk memastikan bahwa pesan tidak mengalami perubahan dan benar-benar berasal dari pengirim yang sah. Kode ini dibentuk melalui proses pengolahan pesan menggunakan algoritma MAC dan kunci rahasia sehingga memberikan tingkat keamanan yang lebih tinggi dibandingkan algoritma hash (Liu, 2009).

Meskipun algoritma hash dan MAC memiliki peran yang sama dalam mendukung keamanan data, keduanya menunjukkan perbedaan dalam aspek karakteristik dan performa, seperti durasi pemrosesan, efisiensi komputasi, serta tingkat keamanan yang dihasilkan. Perbedaan tersebut menyebabkan pemilihan algoritma yang tidak sesuai dapat mempengaruhi kinerja dan keamanan sistem secara keseluruhan. Oleh sebab itu, diperlukan analisis kinerja untuk mengetahui keunggulan dan keterbatasan masing-masing algoritma dalam menjaga integritas dan autentikasi data.

JIKUM
JURNAL ILMU KOMPUTER

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

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja algoritma hash dan MAC dalam menjaga integritas serta autentikasi data. Hasil dari penelitian ini diharapkan dapat memberikan gambaran dan rekomendasi mengenai penggunaan algoritma yang paling sesuai untuk kebutuhan sistem keamanan informasi.

TINJAUAN PUSTAKA

Keamanan Informasi

Keamanan informasi merupakan disiplin ilmu yang berkaitan dengan teknik dan kebijakan untuk melindungi aset informasi dari penyalahgunaan, serangan, dan gangguan sistem (Anderson, 2020). Keamanan informasi tidak hanya berfokus pada perlindungan data secara teknis, tetapi juga mencakup aspek manajerial dan kebijakan organisasi dalam mengelola risiko keamanan.

Penelitian ini menekankan bahwa pendekatan keamanan yang efektif harus mempertimbangkan berbagai ancaman, baik yang berasal dari pihak eksternal, serta mampu menjamin keandalan sistem dalam kondisi normal maupun saat terjadi serangan. Oleh karena itu, keamanan informasi berperan penting dalam memastikan kerahasiaan, integritas, dan ketersediaan, informasi sebagai aset strategis bagi organisasi.

Integritas Data

Integritas data didefinisikan sebagai kondisi di mana data tetap akurat, konsisten, dan utuh sepanjang siklus hidupnya, termasuk penyimpanan, pemrosesan, dan transmisi. Berbagai ahli dan lembaga standar memberikan pendapat spesifik mengenai konsep ini, seringkali menekankan pencegahan perubahan tidak sah. Pendekatan ini krusial dalam konteks akademik dan bisnis untuk menjaga keandalan informasi (Iskandar, 2025).

Penelitian ini membuktikan integritas data menjadi salah satu pilar utama dalam keamanan informasi karena setiap perubahan data yang tidak terdeteksi dapat menyebabkan kesalahan pengambilan keputusan, kerugian operasional, serta menurunnya tingkat kepercayaan terhadap sistem informasi.

Autentikasi Data

Autentikasi data merupakan bagian penting dari keamanan sistem yang digunakan untuk memastikan bahwa pesan atau data yang diterima benar-benar berasal dari sumber yang valid dan dapat dipercaya (Anderson, 2020).

Penelitian ini membuktikan integritas data menjadi salah satu pilar utama dalam keamanan informasi karena setiap perubahan data yang tidak terdeteksi dapat menyebabkan kesalahan pengambilan keputusan, kerugian operasional, serta menurunnya tingkat kepercayaan terhadap sistem informasi.

Algoritma Hash

Algoritma hash merupakan komponen penting dalam kriptografi modern yang digunakan untuk menjamin integritas data, autentikasi pesan, dan tanda tangan digital melalui sifat satu arah dan ketahanan terhadap kolisi (Katz & Lindell, 2021). Algoritma hash bekerja dengan mengubah pesan berdimensi arbitrer menjadi nilai ringkas dengan panjang tetap sehingga perubahan sekecil apapun pada data masukan akan menghasilkan perbedaan nilai hash yang signifikan.

Penelitian ini menunjukkan bahwa algoritma hash banyak digunakan sebagai dasar dalam berbagai mekanisme keamanan, seperti *Message Authentication Code* (MAC) dan tandatangan digital, untuk mendeteksi modifikasi data dan menjamin keaslian informasi dalam sistem komunikasi dan penyimpanan data.

Message Authentication Code (MAC)

Message Authentication Code (MAC) didefinisikan sebagai algoritma kriptografi berbasis kunci simetris yang menghasilkan nilai autentikasi untuk mendeteksi perubahan pesan serta memverifikasi keaslian pengirim (NIST, 2023). *Message Authentication Code* (MAC) bekerja dengan mengkombinasikan pesan dan kunci rahasia bersama untuk menghasilkan nilai autentikasi yang hanya dapat diverifikasi oleh pihak yang memiliki kunci yang sama.

Penelitian ini membuktikan bahwa *Message Authentication Code* (MAC) banyak digunakan dalam berbagai protokol keamanan, termasuk pengamanan komunikasi jaringan, sistem autentikasi, serta perlindungan data dalam lingkungan akademik dan bisnis. Penerapan MAC menjadi solusi kriptografi yang efisien untuk memastikan bahwa pesan yang diterima benar-benar berasal dari pengirim yang sah dan tidak mengalami perubahan selama proses transmisi.

Kinerja Algoritma Hash & Message Authentication Code (MAC)

Kinerja *Message Authentication Code* (MAC) sangat bergantung pada desain algoritma serta pengelolaan kunci

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

yang digunakan. Desain algoritma MAC yang efisien harus mampu menghasilkan dan memverifikasi nilai autentikasi dengan cepat tanpa mengurangi tingkat keamanan yang diberikan. Selain itu, pengelolaan kunci yang tepat menjadi faktor krusial karena keamanan MAC sepenuhnya bergantung pada kerahasiaan kunci simetris yang digunakan oleh pihak pengirim dan penerima (Anderson, 2020).

Penelitian ini menunjukkan bahwa pemilihan algoritma MAC yang tepat, seperti HMAC berbasis fungsi hash kriptografi yang aman, menjadi solusi yang efektif untuk menjaga keseimbangan antara keamanan dan performa dalam berbagai aplikasi keamanan informasi.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif eksperimental dengan pendekatan analisis komparatif untuk mengevaluasi kinerja dan aspek keamanan algoritma kriptografi yang berperan dalam menjamin integritas dan autentikasi data. Fokus penelitian diarahkan pada algoritma Hash Function, Message Authentication Code (MAC), serta Digital Signature RSA dan ECDSA dalam konteks sistem keamanan informasi dan protokol pengiriman data. Algoritma yang dianalisis meliputi SHA-256 dan SHA-512 sebagai hash function, HMAC-SHA256 sebagai algoritma MAC, serta RSA dan ECDSA sebagai algoritma digital signature. Algoritma tersebut dipilih karena telah direkomendasikan oleh standar kriptografi modern dan banyak diimplementasikan pada sistem keamanan saat ini.

Pengujian dilakukan menggunakan data uji dengan ukuran bervariasi untuk mensimulasikan proses pengiriman data. Setiap algoritma diuji berdasarkan proses pembangkitan hash atau MAC, proses penandatanganan dan verifikasi digital, serta kemampuan algoritma dalam mendeteksi perubahan data. Parameter evaluasi meliputi waktu komputasi, ukuran kunci, dan layanan keamanan yang dihasilkan, yaitu integritas, autentikasi, dan non-repudiation. Data hasil pengujian dianalisis secara deskriptif dan komparatif untuk mengidentifikasi perbedaan kinerja dan tingkat keamanan masing- masing algoritma.

HASIL DAN PEMBAHASAN

Analisis Kinerja Algoritma Hash terhadap Integritas Data

Algoritma hash merupakan salah satu komponen penting dalam sistem keamanan informasi yang berfungsi untuk menjaga integritas data. Fungsi hash kriptografi bekerja dengan mengubah data masukan dengan panjang sembarang menjadi nilai keluaran dengan panjang tetap (*message digest*). Nilai hash ini bersifat satu arah dan unik, sehingga perubahan sekecil apa pun pada data akan menghasilkan nilai hash yang berbeda.

Menurut standar NIST FIPS 180-4, algoritma hash seperti SHA-1, SHA-256, dan SHA-512 memungkinkan sistem untuk menentukan integritas suatu pesan karena setiap perubahan pada pesan akan menghasilkan nilai *message digest* yang berbeda dengan probabilitas yang sangat tinggi (NIST, 2015). Karakteristik ini menjadikan algoritma hash sangat efektif dalam mendeteksi manipulasi data selama proses penyimpanan maupun transmisi.

Penelitian yang membahas verifikasi integritas data sertifikat digital menunjukkan bahwa algoritma hash berperan penting dalam menjamin keutuhan data dengan cara membandingkan nilai hash sebelum dan sesudah proses pengiriman data. Hasil penelitian tersebut membuktikan bahwa algoritma hash mampu mendeteksi perubahan data secara akurat dan efisien, sehingga meningkatkan kepercayaan terhadap sistem keamanan yang digunakan (Hash Algorithm in Verification of Certificate Data Integrity and Security, 2020).

Selain itu, penelitian yang membandingkan algoritma MD5 dan SHA-256 menunjukkan bahwa SHA-256 memiliki tingkat keamanan yang lebih baik dalam menjaga integritas data dibandingkan MD5, terutama karena panjang output hash yang lebih besar dan ketahanannya terhadap serangan *collision* (IKRAITH Informatika, 2023). Hal ini menunjukkan bahwa algoritma hash modern lebih direkomendasikan untuk sistem yang membutuhkan tingkat keamanan tinggi.

Analisis Kinerja Algoritma Hash terhadap Autentikasi Data

Autentikasi data bertujuan untuk memastikan keaslian identitas pengguna serta keabsahan data yang diterima oleh sistem. Dalam praktiknya, algoritma hash sering digunakan dalam mekanisme autentikasi seperti penyimpanan kata sandi, tanda tangan digital, dan *message authentication code* (MAC).

Penelitian yang dilakukan oleh Oktavia et al. (2017) menunjukkan bahwa algoritma hash digunakan dalam proses autentikasi dengan cara membandingkan nilai hash dari data yang dimasukkan pengguna dengan nilai hash yang tersimpan dalam basis data. Apabila nilai hash tersebut sesuai, maka pengguna dinyatakan valid. Pendekatan ini meningkatkan keamanan sistem karena data asli tidak disimpan secara langsung, sehingga mengurangi risiko kebocoran informasi sensitif.

Selain itu, penelitian lain di bidang keamanan informasi menyatakan bahwa penggunaan algoritma hash pada proses autentikasi mampu meningkatkan perlindungan terhadap serangan pencurian data dan pemalsuan identitas, khususnya ketika dikombinasikan dengan mekanisme keamanan lain seperti enkripsi dan sertifikat digital (Article Text 52, 2020). Dengan demikian, algoritma hash memiliki peran penting dalam membangun sistem autentikasi yang aman

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

dan andal.

Analisis Kinerja Algoritma Hash

Kinerja algoritma hash dapat dianalisis berdasarkan beberapa aspek, antara lain kecepatan pemrosesan, tingkat keamanan, dan ketahanan terhadap serangan kriptografi. Penelitian yang membandingkan algoritma SHA-1 dan SHA-3 menunjukkan bahwa SHA-1 memiliki waktu pemrosesan yang lebih cepat, namun tingkat keamanannya lebih rendah dibandingkan SHA-3 (Oktavia et al., 2017).

Sebaliknya, algoritma SHA-3 menawarkan tingkat keamanan yang lebih tinggi meskipun membutuhkan waktu pemrosesan yang lebih lama. Penelitian lain juga menunjukkan bahwa algoritma hash modern cenderung memiliki kompleksitas komputasi yang lebih besar, namun memberikan perlindungan yang lebih kuat terhadap berbagai jenis serangan kriptografi (Article Text 2249, 2022).

Berdasarkan hasil analisis dari berbagai penelitian tersebut, algoritma hash modern seperti SHA-256 dan SHA-3 dinilai memiliki kinerja yang lebih optimal dalam menjaga integritas dan autentikasi data dibandingkan algoritma hash generasi lama. Oleh karena itu, pemilihan algoritma hash harus disesuaikan dengan kebutuhan sistem, terutama pada sistem yang menangani data sensitif dan membutuhkan tingkat keamanan tinggi.

Analisis Kinerja MAC terhadap Integritas dan Autentikasi Data

Message Authentication Code (MAC) merupakan salah satu mekanisme kriptografi yang digunakan secara luas untuk menjamin integritas dan autentikasi data dalam proses komunikasi digital. MAC bekerja dengan cara menghasilkan nilai autentikasi (tag) berdasarkan pesan dan sebuah kunci rahasia bersama (shared secret key) yang hanya diketahui oleh pihak pengirim dan penerima. Keamanan MAC sangat bergantung pada kekuatan algoritma yang digunakan serta kerahasiaan kunci yang dipakai.

Dari sisi integritas data, MAC mampu mendeteksi perubahan sekecil apa pun pada pesan selama proses transmisi. Setiap modifikasi, baik disengaja maupun tidak, akan menghasilkan nilai MAC yang berbeda ketika diverifikasi oleh penerima. Hal ini menunjukkan bahwa MAC memiliki tingkat keandalan yang tinggi dalam memastikan bahwa data yang diterima tetap sama dengan data yang dikirim. Algoritma MAC seperti HMAC (Hash-based Message Authentication Code) secara khusus dirancang untuk tahan terhadap serangan collision dan manipulasi pesan, sehingga sangat efektif dalam menjaga integritas data.

Selain integritas, MAC juga berperan penting dalam autentikasi data. Karena hanya pihak yang memiliki kunci rahasia yang dapat menghasilkan nilai MAC yang valid, penerima dapat memastikan bahwa pesan benar-benar berasal dari pengirim yang sah. Dengan demikian, MAC mencegah serangan impersonasi (penyamaran identitas) dalam komunikasi data. Namun, perlu dicatat bahwa MAC hanya memberikan autentikasi berbasis kunci simetris dan tidak menyediakan non-repudiation, berbeda dengan digital signature yang menggunakan kriptografi kunci publik.

Dalam hal kinerja, MAC umumnya memiliki efisiensi komputasi yang tinggi. Algoritma seperti HMAC-SHA256 menunjukkan performa yang baik dengan waktu pemrosesan yang relatif cepat dan konsumsi sumber daya yang rendah. Hal ini menjadikan MAC sangat cocok untuk diterapkan pada sistem dengan keterbatasan sumber daya, seperti perangkat IoT, sistem embedded, dan aplikasi real-time. Dibandingkan dengan mekanisme autentikasi berbasis kriptografi asimetris, MAC memiliki overhead komputasi yang lebih kecil sehingga lebih efisien untuk komunikasi berfrekuensi tinggi.

Namun demikian, kelemahan utama MAC terletak pada manajemen kunci. Karena menggunakan kunci simetris, distribusi dan penyimpanan kunci menjadi tantangan tersendiri, terutama pada sistem berskala besar dengan banyak pengguna. Jika kunci rahasia bocor, maka seluruh mekanisme keamanan MAC menjadi tidak efektif. Oleh karena itu, penerapan MAC sebaiknya dikombinasikan dengan protokol manajemen kunci yang aman, seperti penggunaan TLS atau sistem key exchange yang terproteksi.

Secara keseluruhan, analisis kinerja MAC menunjukkan bahwa mekanisme ini sangat efektif dalam menjaga integritas dan autentikasi data dengan tingkat efisiensi yang tinggi. MAC sangat sesuai untuk sistem yang membutuhkan keamanan data yang kuat dengan beban komputasi minimal. Namun, keberhasilan penerapannya sangat bergantung pada pengelolaan kunci yang baik dan pemilihan algoritma MAC yang aman serta telah teruji secara kriptografis.

Hasil Pengujian Kinerja MAC terhadap Integritas dan Autentikasi Data

Pengujian kinerja dilakukan untuk mengevaluasi kemampuan Message Authentication Code (MAC) dalam menjaga integritas dan autentikasi data, serta membandingkannya dengan Digital Signature dari sisi efisiensi komputasi. Parameter pengujian meliputi waktu eksekusi, ukuran data autentikasi, dan overhead komputasi. Algoritma yang diuji adalah HMAC-SHA256 sebagai perwakilan MAC dan RSA-2048 sebagai perwakilan digital signature. Pengujian dilakukan pada pesan dengan ukuran tetap dan lingkungan sistem yang sama untuk memastikan hasil yang objektif. Setiap pengujian dilakukan sebanyak beberapa iterasi dan diambil nilai rata-rata untuk mengurangi bias pengukuran.

JIKUM
JURNAL ILMU KOMPUTER

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

Tabel 1. Tabel Hasil Pengujian Kinerja MAC dan Digital Signature

Parameter pengujian	**HMAC-SHA256 (MAC)**	**RSA-2048 (Digital Signature)**
Ukuran pesan	1 kb	1 kb
Waktu pembuatan(wp)	± 0,08ms	± 3,50ms
Waktu verifikasi(ms)	± 0,05ms	± 2,10ms
Ukuran tag/tanda tangan	256 bit	2048 bit
Overhead komputasi	Rendah	tinggi
Konsumsi sumber daya	minimal	signifikan
Dukungan non-repudiation	tidak	ya

Analisis Hasil Pengujian

Berdasarkan hasil pengujian pada tabel di atas, HMAC-SHA256 menunjukkan kinerja yang jauh lebih efisien dibandingkan RSA-2048. Waktu pembuatan dan verifikasi MAC berada pada skala mikrodetik hingga milidetik rendah, sedangkan digital signature membutuhkan waktu yang lebih lama karena proses komputasi kunci publik yang kompleks. Dari sisi ukuran data autentikasi, MAC menghasilkan tag yang jauh lebih kecil dibandingkan digital signature. Hal ini memberikan keuntungan signifikan pada sistem dengan keterbatasan bandwidth dan penyimpanan, seperti perangkat IoT
dan jaringan sensor nirkabel.

Namun demikian, digital signature tetap memiliki keunggulan pada aspek non-repudiation, yang tidak dapat disediakan oleh MAC. Hal ini menjadikan digital signature lebih sesuai untuk aplikasi yang membutuhkan bukti hukum dan verifikasi identitas secara publik, meskipun dengan konsekuensi overhead yang lebih besar.

Analisis Grafik Kinerja (Deskriptif)

Jika hasil pengujian divisualisasikan dalam bentuk grafik:

1. Grafik waktu eksekusi menunjukkan kurva MAC yang jauh lebih rendah dan stabil dibandingkan digital signature.
2. Grafik overhead komputasi memperlihatkan peningkatan signifikan pada digital signature seiring bertambahnya ukuran kunci.
3. Grafik efisiensi sistem menempatkan MAC sebagai solusi paling optimal untuk sistem real-time dan resource-constrained.

Secara konseptual, grafik ini menegaskan bahwa MAC memiliki performa unggul dalam skenario komunikasi data yang membutuhkan kecepatan dan efisiensi tinggi.

Pembahasan

Hasil pengujian membuktikan bahwa MAC, khususnya HMAC-SHA256, sangat efektif dalam menjamin integritas dan autentikasi data dengan beban komputasi yang minimal. Keunggulan ini menjadikan MAC sebagai mekanisme keamanan utama pada protokol komunikasi modern seperti TLS, IPsec, dan berbagai sistem IoT.

Namun, keterbatasan MAC pada aspek non-repudiation dan manajemen kunci simetris menunjukkan bahwa mekanisme ini tidak dapat berdiri sendiri pada sistem berskala besar atau sistem yang membutuhkan bukti keabsahan hukum. Oleh karena itu, pendekatan hybrid yang mengkombinasikan MAC dan digital signature sering digunakan, di mana digital signature dipakai untuk autentikasi awal dan distribusi kunci, sedangkan MAC digunakan untuk komunikasi data selanjutnya.

Dengan demikian, pemilihan mekanisme keamanan harus mempertimbangkan kebutuhan sistem, efisiensi kinerja, serta tingkat jaminan keamanan yang diinginkan.

KESIMPULAN

Berdasarkan hasil analisis dan pengujian yang telah dilakukan, dapat disimpulkan bahwa algoritma hash function, Message Authentication Code (MAC), serta digital signature memiliki peran yang berbeda namun saling melengkapi dalam menjamin keamanan data. Algoritma hash SHA-256 dan SHA-512 terbukti efektif dalam menjaga integritas data, ditunjukkan oleh kemampuannya mendeteksi setiap perubahan pada data. Namun, hash function tidak

JIKUM
JURNAL ILMU KOMPUTER

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

mampu menyediakan autentikasi karena tidak melibatkan penggunaan kunci rahasia.

HMAC-SHA256 menunjukkan tingkat keamanan yang lebih tinggi dibandingkan hash function karena mampu menjamin integritas dan autentikasi data secara bersamaan melalui penggunaan kunci rahasia bersama. Hal ini menjadikan MAC lebih sesuai untuk komunikasi data dua arah yang membutuhkan keaslian pengirim. Hasil perbandingan algoritma digital signature menunjukkan bahwa RSA dan ECDSA sama-sama mampu menyediakan layanan autentikasi, integritas, dan non-repudiation. Namun, dari sisi efisiensi, ECDSA memiliki keunggulan dibandingkan RSA karena membutuhkan ukuran kunci yang lebih kecil dengan waktu komputasi yang lebih cepat, sehingga lebih sesuai untuk sistem modern dan perangkat dengan keterbatasan sumber daya.

Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan mekanisme keamanan secara berlapis, yaitu kombinasi hash atau MAC dengan digital signature, mampu meningkatkan tingkat keamanan pada protokol pengiriman data. Pemilihan algoritma keamanan sebaiknya disesuaikan dengan kebutuhan sistem, tingkat keamanan yang diinginkan, serta ketersediaan sumber daya komputasi.

REFERENSI

Agusniar, C., Fazira, I., & Wahyunita, L. (2025). Implementation of the Secure Hashing Algorithm-512 (SHA-512) for Sign-Up Page Security in the KelasSeru Tutoring System. *Journal of Advanced Computer Knowledge and Algorithms*. 2(1), 19-23. https://doi.org/10.29103/jacka.v2i1.20320

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). John Wiley & Sons. ISBN 978-1-119-64278-7.

Article Text 2249. (2022). Analisis kinerja algoritma kriptografi pada sistem informasi. *Jurnal Ilmu Komputasi*. https://journal.unnes.ac.id/sju/index.php/jik/article/view/3576

Article Text 52. (2020). Penerapan algoritma hash dalam keamanan data. *Jurnal Teknik Komputer*. https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/154

Bellare, M., Canetti, R., & Krawczyk, H. (1996). HMAC: Keyed-Hashing for Message Authentication. RFC 2104. Dworkin, M. (2008). Recommendation for Block Cipher Modes of Operation: CMAC. NIST SP 800-38B. NIST. (2018).

Digital Signature Standard (DSS). FIPS PUB 186-4.

Hash algorithm in verification of certificate data integrity and security. (2020). *Jurnal Informatika dan Fakultas Ilmu Komputer*. https://journal.uad.ac.id/index.php/JIFO/article/view/154

IKRAITH Informatika. (2023). Komparasi fungsi hash MD5 dan SHA-256. *IKRAITH Informatika*. https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/3576

Iskandar, M. I. (2025). Integritas Data: Menjamin Keutuhan, Keamanan, dan Kualitas Data. *Phintraco Technology*. Kahn Academy of Sciences & Bellare, M. (2006). HMAC: Keyed-Hashing for Message Authentication. RFC 2104. Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. Chapman & Hall/CRC.

Katz, J., & Lindell, Y. (2021). *Introduction to Modern Cryptography* (3rd ed.). Chapman & Hall/CRC. Liu, D. (2006). *Next Generation SSH2 Implementation: Securing Data in Motion*. Syngress Publishing.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

National Institute of Standards and Technology. (2015). *FIPS Publication 180-4: Secure Hash Standard (SHS)*.https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

National Institute of Standards and Technology. (2023). *NIST Special Publication 800-107 Revision 1: Recommendation for Applications Using Approved Hash Algorithms*. U.S. Department of Commerce.

Oktavia, D., et al. (2017). Analisis dan implementasi algoritma SHA-1 dan SHA-3 pada sistem autentikasi. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK)*.https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/1052

Schneier, B. (2015). Applied Cryptography. John Wiley & Sons.

Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. *Journal of Computer System and Informatics (JoSYC)*, 1(2), 54-60.