JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Analisis Keamanan Layanan, Sistem Operasi, Kriptografi, dan Steganografi dalam Pengelolaan Informasi Modern

Akhsanul Khairi Siregar [1*], M. Rifqy Pasha[2], Alif Asrovi [3], Fanni Rahmadayani[4], Muhammad Raihan Azhari[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]akhsanul.240170233@mhs.com, [2]rifqy.240170126@mhs.com, [3]alif.240170115@mhs.com,
[4]fanni.240170127@mhs.com, [5]muhammad.240170129@mhs.com

ABSTRACT

The rapid advancement of digital technology has significantly increased the need for stronger information security systems, particularly in digital services, operating systems, and data protection mechanisms such as cryptography and steganography. This study aims to analyze the role of service security, operating system security, cryptographic techniques, and steganographic methods in maintaining the confidentiality, integrity, and availability of information in the modern digital environment. The methodology used in this research is a literature review by examining scientific journals, reference books, and international security standards published between 2018 and 2024. The results indicate that service security protects communication processes and data exchange through authentication, authorization, and encryption. Operating system security supports access control management and minimizes exploitation risks through system hardening and regular security updates. Cryptography safeguards the confidentiality and integrity of data using symmetric and asymmetric algorithms, while steganography adds an extra layer of protection by concealing information within digital media. The study concludes that integrating these four security components can create a multilayered defense system that is more effective in mitigating cyber threats and ensuring comprehensive information protection.

Keywords: *Information Security, Operating System, Cryptography, Steganography, Digital Services.*

PENDAHULUAN

Latar Belakang

Perkembangan teknologi informasi yang semakin pesat telah mengubah berbagai aspek kehidupan, mulai dari komunikasi, pendidikan, industri, hingga pemerintahan. Transformasi digital ini mendorong peningkatan jumlah data yang disimpan, diproses, dan ditransmisikan melalui sistem berbasis komputer dan jaringan. Namun, pertumbuhan tersebut juga diiringi oleh meningkatnya ancaman keamanan seperti peretasan, pencurian data, ransomware, manipulasi sistem, dan serangan siber lainnya. Oleh karena itu, diperlukan mekanisme keamanan yang mampu melindungi informasi dari segala bentuk ancaman.

Keamanan layanan, sistem operasi, kriptografi, dan steganografi merupakan empat elemen penting yang memiliki peran berbeda namun saling melengkapi dalam menjaga keamanan informasi. Keamanan layanan berfungsi melindungi interaksi dan komunikasi antar pengguna dan sistem. Sistem operasi bertanggung jawab mengatur kontrol akses, manajemen proses, serta perlindungan terhadap perangkat keras dan perangkat lunak. Kriptografi digunakan untuk menyandikan informasi agar tidak dapat dibaca oleh pihak tidak berwenang, sementara steganografi menyembunyikan keberadaan pesan di dalam suatu media. Integrasi keempat aspek ini sangat penting dalam mewujudkan pengelolaan informasi yang aman dan terpercaya.

Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana keamanan layanan berperan dalam melindungi interaksi dan pertukaran data pada sistem digital modern?
2. Apa saja peran penting sistem operasi dalam meningkatkan keamanan informasi?
3. Bagaimana kriptografi digunakan untuk menjaga kerahasiaan dan integritas data?
4. Bagaimana steganografi berfungsi dalam menyembunyikan informasi dan menambah lapisan keamanan?

Tujuan

Tujuan dari penelitian ini adalah:

1. Menganalisis mekanisme keamanan layanan dalam melindungi proses pertukaran data.
2. Mengkaji peran dan fungsi keamanan pada sistem operasi modern.
3. Menjelaskan konsep, jenis, dan penerapan algoritma kriptografi dalam keamanan informasi.
4. Mendeskripsikan teknik steganografi dan bagaimana metode tersebut meningkatkan keamanan data.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, Number 01, Mei 2026

Manfaat Penelitian

Penelitian ini diharapkan memberikan beberapa manfaat sebagai berikut:

1. Memberikan pemahaman menyeluruh tentang berbagai mekanisme keamanan informasi.
2. Menjadi referensi bagi mahasiswa, peneliti, atau praktisi yang mempelajari keamanan digital.
3. Menambah wawasan mengenai integrasi keamanan layanan, sistem operasi, kriptografi, dan steganografi.
4. Memberikan gambaran strategi keamanan berlapis yang dapat digunakan organisasi untuk menghadapi ancaman siber

TINJAUAN PUSTAKA

Teori Keamanan Informasi (CIA Triad)

Menurut teori *Confidentiality, Integrity, Availability (CIA)*, keamanan informasi harus menjamin bahwa:

- **Confidentiality:** data hanya diakses oleh pihak berwenang.
- **Integrity:** data tidak boleh dimodifikasi tanpa izin.
- **Availability:** data harus tersedia ketika dibutuhkan.

Teori ini menjadi fondasi utama dalam memahami keamanan layanan, OS, kriptografi, dan steganografi.

Teori Keamanan Layanan Digital

Keamanan layanan digital fokus pada mekanisme perlindungan yang memastikan interaksi antara pengguna dan sistem berjalan aman. Menurut OWASP, aspek terpenting mencakup:

- autentikasi (authentication),
- otorisasi (authorization),
- manajemen sesi (session management),
- proteksi data transmisi (encryption),
- validasi input dan output.

Layanan dianggap aman apabila proses komunikasi terlindungi dari serangan seperti *phishing, SQL injection, session hijacking,* dan *MITM attack*.

Teori Keamanan Sistem Operasi

Teori keamanan OS berfokus pada bagaimana sistem operasi melindungi sumber daya komputer. Menurut NIST SP 800-123, OS harus menyediakan:

- kontrol akses,
- proteksi kernel,
- isolasi proses,
- manajemen memori aman,
- pembaruan dan patching reguler.

Keamanan OS sangat berpengaruh pada keamanan seluruh aplikasi yang berjalan di atasnya.

Teori Kriptografi

Kriptografi adalah ilmu yang mempelajari metode pengamanan data dengan menggunakan algoritma matematis. Elemen utama kriptografi meliputi:

- Enkripsi dan dekripsi
- Kriptografi simetris (AES)
- Kriptografi asimetris (RSA, ECC)
- Hashing (SHA-256)
- Digital signature

Tujuannya untuk memastikan confidentiality, integrity, authenticity, dan non-repudiation.

Penelitian Terdahulu

Penelitian tentang Keamanan Layanan Digital

Penelitian oleh Rahman (2021) menunjukkan bahwa serangan pada layanan web umumnya terjadi akibat lemahnya autentikasi dan tidak adanya enkripsi pada transmisi data. Penggunaan TLS, firewall, dan MFA terbukti efektif mengurangi risiko serangan.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Penelitian tentang Keamanan Sistem Operasi

Studi oleh Nasution & Kurniawan (2020) menemukan bahwa sebagian besar serangan malware terjadi melalui celah OS yang tidak diperbarui. Penelitian lain menegaskan bahwa fitur seperti *secure boot* dan *sandboxing* sangat berpengaruh dalam mencegah exploit tingkat kernel.

Penelitian tentang Kriptografi

Penelitian oleh Susanto (2022) membuktikan bahwa algoritma AES dan RSA masih menjadi standar teraman untuk perlindungan data modern. Penggunaan digital signature juga terbukti meningkatkan integritas dan validitas informasi.

Penelitian tentang Steganografi

Studi oleh Lestari (2023) menunjukkan bahwa metode LSB merupakan teknik steganografi yang paling banyak digunakan untuk penyembunyian pesan berbasis citra. Penelitian lain menegaskan bahwa penggunaan steganografi yang digabungkan dengan kriptografi mampu meningkatkan keamanan pesan secara signifikan.

Konsep atau Model yang Digunakan

Model Keamanan Berlapis (Defense in Depth)

Model ini menjelaskan bahwa keamanan ideal harus menggunakan beberapa lapisan perlindungan, bukan satu metode saja. Empat aspek—layanan digital, OS, kriptografi, dan steganografi—mewakili empat lapisan berbeda yang saling melengkapi.

Model OSI dalam Komunikasi Data

Model OSI digunakan untuk memahami bagaimana data bergerak dari satu perangkat ke perangkat lain. Keamanan diimplementasikan di berbagai layer:

- Layer 4 (transport): TLS
- Layer 7 (aplikasi): autentikasi dan enkripsi data

Konsep ini membantu menganalisis posisi keamanan layanan digital dalam arsitektur jaringan.

Model Enkripsi Kriptografi Modern

Model ini menunjukkan bagaimana data diproses melalui:

- plaintext → enkripsi → ciphertext → dekripsi → plaintext
  Model ini digunakan dalam analisis peran AES, RSA, hash, dan digital signature dalam menjaga keamanan data.

Model Steganografi Multimedia

Model steganografi menjelaskan alur:

- Penyisipan (embedding)
- Pengiriman (transmission)
- Ekstraksi (extraction)

Model ini digunakan untuk menunjukkan bagaimana pesan tersembunyi dapat dikirim secara aman tanpa terdeteksi.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan **pendekatan deskriptif kualitatif-kuantitatif (mixed method)**.

- Deskriptif digunakan untuk menjelaskan konsep keamanan layanan, sistem operasi, kriptografi, dan steganografi secara teoritis.
- Kualitatif digunakan untuk menganalisis literatur, standar keamanan, dan model-model teori keamanan informasi.
- Kuantitatif digunakan untuk menganalisis data survei mengenai tingkat pemahaman dan persepsi pengguna terhadap keamanan layanan dan teknologi pengelolaan informasi modern.

Pendekatan ini dipilih untuk memberikan gambaran menyeluruh baik dari sisi teknis maupun persepsi pengguna.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, Number 01, Mei 2026

Subjek dan Objek Penelitian

Subjek Penelitian

Subjek dalam penelitian ini adalah:

- Mahasiswa bidang teknologi informasi.
- Pengguna umum layanan digital (media sosial, aplikasi perbankan, cloud storage).

Mereka dipilih karena merupakan kelompok yang aktif berinteraksi dengan sistem informasi modern dan rentan terhadap isu keamanan data.

Objek Penelitian

Objek penelitian meliputi empat aspek utama:

1. **Keamanan layanan digital** (misalnya autentikasi, enkripsi, firewall).
2. **Keamanan sistem operasi** (akses kontrol, proteksi kernel, manajemen patch).
3. **Penerapan kriptografi** (AES, RSA, hash, digital signature).
4. **Teknik steganografi** (LSB, transform-domain).

Objek ini dipilih karena menjadi pilar utama dalam menjaga keamanan pengelolaan informasi modern.

Teknik Pengumpulan Data

Penelitian ini menggunakan dua jenis sumber data yaitu data primer dan sekunder:

1. Data Primer diperoleh secara langsung melalui:
   - **Survei/kuisioner online** yang diberikan kepada mahasiswa dan masyarakat umum. Pertanyaan mencakup pemahaman mengenai keamanan layanan, OS, kriptografi, dan steganografi.
2. Data Sekunder diperoleh dari:
   - Buku dan jurnal ilmiah tentang keamanan informasi, sistem operasi, kriptografi, steganografi, dan model keamanan.
   - Standar keamanan seperti ISO 27001, NIST CSF, RFC kriptografi.
   - Laporan keamanan siber dari lembaga resmi (Cybersecurity Ventures, OWASP).

Metode ini dipilih untuk memperoleh referensi komprehensif dan mendalam.

Teknik Analisis Data

Analisis Kualitatif

Data kualitatif dari literatur dan dokumen dianalisis melalui:

- Analisis isi (content analysis) untuk mengidentifikasi teori, konsep, dan pola yang relevan.
- Reduksi data untuk memilah informasi yang sesuai dengan tujuan penelitian.
- Interpretasi tematik untuk menarik hubungan antara keamanan layanan, OS, kriptografi, dan steganografi.

Analisis Kuantitatif

Data survei dianalisis menggunakan:

- Statistik deskriptif (persentase, diagram, tabel) untuk menggambarkan tingkat pengetahuan dan persepsi responden.
- Uji validitas sederhana terhadap hasil survei jika diperlukan.

Analisis Komparatif

Dilakukan untuk membandingkan:

- Tingkat keamanan antar komponen (layanan, OS, kriptografi, steganografi).
- Relevansi masing-masing aspek dalam pengelolaan informasi modern.

Analisis ini menghasilkan pemahaman komprehensif mengenai peran setiap elemen dalam keamanan informasi

HASIL DAN PEMBAHASAN

Hasil Penelitian

Hasil penelitian diperoleh melalui analisis literatur, jurnal ilmiah, standar keamanan internasional, serta kajian teoritis mengenai empat aspek utama: **keamanan layanan**, **keamanan sistem operasi**, **kriptografi**, dan **steganografi**. Temuan penelitian dipaparkan sebagai berikut.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Keamanan Layanan Digital

Analisis literatur menunjukkan bahwa layanan digital modern, seperti layanan perbankan, cloud, dan aplikasi online, mengandalkan mekanisme keamanan seperti:

- Autentikasi (single-factor, MFA)
- Proteksi koneksi melalui TLS/SSL
- Firewall dan intrusion detection system (IDS)
- Manajemen sesi dan token keamanan

Temuan ini menunjukkan bahwa keamanan layanan ditujukan untuk menjaga proses komunikasi agar tetap aman, mencegah pencurian kredensial, serta memastikan identitas pengguna valid.

Keamanan Sistem Operasi

Sistem operasi modern telah menerapkan berbagai fitur keamanan, seperti:

- Access Control List (ACL)
- Secure Boot dan kernel protection
- Sandboxing
- Patching dan update rutin
- Proteksi memori dan isolasi proses

OS berperan sebagai lapisan dasar yang menentukan apakah aplikasi dan layanan berjalan dalam lingkungan yang aman.

Penerapan Kriptografi

Literatur menunjukkan bahwa kriptografi merupakan fondasi utama keamanan data. Elemen kriptografi modern meliputi:

- Enkripsi simetris (AES)
- Enkripsi asimetris (RSA, ECC)
- Fungsi hash (SHA-256)
- Digital signature
- Integrity checks

Temuan ini menguatkan bahwa kriptografi menjaga *kerahasiaan, integritas, dan keaslian* data.

Teknik Steganografi

Studi literatur menunjukkan bahwa steganografi digunakan untuk menyembunyikan informasi di dalam media digital seperti gambar, audio, atau video. Metode umum yang digunakan adalah:

- Least Significant Bit (LSB)
- Transform domain (DCT, DWT)
- Adaptive steganography

Teknik ini menjadi pelengkap kriptografi karena mampu menyembunyikan keberadaan data itu sendiri.

Pembahasan

Pembahasan Keamanan Layanan Digital

Hasil penelitian menunjukkan bahwa layanan digital sangat bergantung pada autentikasi dan enkripsi untuk melindungi proses komunikasi. Jika autentikasi lemah, maka potensi ancaman seperti phishing, session hijacking, dan MITM (Man in the Middle) meningkat.

Temuan ini sejalan dengan teori pada OWASP Top 10 yang menjelaskan bahwa kontrol identitas dan manajemen sesi adalah komponen paling krusial dalam keamanan layanan.

Interpretasinya:

Tanpa perlindungan pada level layanan, keamanan data tidak dapat dijamin meskipun OS dan kriptografi sudah kuat.

Pembahasan Keamanan Sistem Operasi

Analisis menunjukkan bahwa keamanan OS adalah fondasi dari seluruh sistem komputer. OS menyediakan mekanisme isolasi, proteksi kernel, dan kontrol akses yang mencegah aplikasi berbahaya mengakses data secara ilegal.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Teori dari NIST menyatakan bahwa keamanan OS ditentukan oleh *hardening*, konfigurasi, dan pembaruan reguler.
Interpretasi:

Jika sistem operasi tidak aman, maka layanan digital dan mekanisme kriptografi dapat dibypass oleh malware, rootkit, atau exploit tingkat kernel.

Pembahasan Kriptografi

Berdasarkan hasil literatur, kriptografi menjamin keamanan data pada saat disimpan maupun dikirimkan. Tanpa kriptografi, data raw rentan diintersepsi dan dimodifikasi.

Teori dari ISO/IEC 27001 memperkuat bahwa kriptografi merupakan kontrol wajib untuk kerahasiaan dan integritas.
Interpretasi:

Kriptografi memberikan perlindungan matematis berbasis algoritma sehingga mampu melindungi data bahkan ketika layanan dan jaringan tidak sepenuhnya aman.

Pembahasan Steganografi

Steganografi bukan hanya menyembunyikan pesan, tetapi juga mengaburkan keberadaan data. Teknik ini dapat digunakan sebagai lapisan tambahan (defense in depth) untuk mencegah deteksi oleh pihak yang tidak bertanggung jawab.

Teori mendukung bahwa steganografi kurang efektif sebagai satu-satunya mekanisme keamanan, tetapi sangat kuat bila dikombinasikan dengan kriptografi.
Interpretasi:

Steganografi memberikan keamanan berbasis penyamaran, bukan berbasis algoritma matematis seperti kriptografi.

Perbandingan dengan Teori

Tabel 1. Perbandingan dengan Teori

Aspek	Temuan Penelitian	Kesesuain dengan Teori
Keamanan Layanan	Layanan digital bergantung pada autentikasi, enkripsi, dan manajemen sesi.	Sesuai OWASP dan RFC TLS.
Sistem Operasi	OS modern memakai ACL, secure boot, dan patching.	Sesuai NIST SP 800-123 (Operating System Security).
Kriptografi	Digunakan untuk confidentiality, integrity, authenticity.	Sesuai ISO/IEC 27001 dan teori Schneier.
Steganografi	Menyembunyikan informasi dalam media digital.	Sesuai teori Johnson & Jajodia tentang steganografi modern.

Interpretasi Keseluruhan

Penelitian ini menginterpretasikan bahwa:

- Keamanan layanan berfungsi menjaga komunikasi aman.
- Keamanan sistem operasi memberi perlindungan dasar dari serangan lokal maupun jaringan.
- Kriptografi melindungi isi data.
- Steganografi menyembunyikan data dan menambah lapisan perlindungan.

Keempat elemen ini saling melengkapi dan membentuk sistem keamanan informasi modern yang bersifat **berlapis (layered security)**.

KESIMPULAN

Berdasarkan hasil analisis terhadap keamanan layanan, sistem operasi, kriptografi, dan steganografi, dapat disimpulkan bahwa:

1. **Keamanan layanan digital** merupakan lapisan terdepan dalam melindungi proses komunikasi antara pengguna dan sistem. Mekanisme autentikasi, enkripsi koneksi, dan manajemen sesi menjadi komponen penting untuk mencegah penyalahgunaan identitas dan penyadapan data.
2. **Keamanan sistem operasi** berfungsi sebagai fondasi utama yang menentukan tingkat keamanan keseluruhan sistem. Proteksi kernel, access control, sandboxing, serta update rutin sangat berpengaruh dalam mencegah eksploitasi dan serangan malware.

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

3. **Kriptografi** adalah aspek yang paling penting dalam menjaga kerahasiaan, integritas, dan keaslian data. Algoritma seperti AES, RSA, dan SHA berkontribusi besar dalam mengamankan informasi baik saat disimpan maupun ditransmisikan.
4. **Steganografi** berperan sebagai lapisan tambahan dalam keamanan informasi. Teknik penyembunyian data dalam media digital memperkuat sistem dengan membuat pesan lebih sulit diidentifikasi oleh pihak yang tidak berwenang.
5. Integrasi antara keamanan layanan, keamanan OS, kriptografi, dan steganografi menciptakan pendekatan **defense in depth** yang efektif dalam melindungi informasi di lingkungan digital modern.

Dengan demikian, pengelolaan informasi yang aman memerlukan pendekatan berlapis, tidak hanya mengandalkan satu aspek, melainkan memadukan berbagai teknik dan teknologi keamanan secara menyeluruh.

.

REFERENSI

ADDIN Mendeley Bibliography CSL_BIBLIOGRAPHY Adebayo, O. S., Olusegun Ganiyu, S., Bukie Osang, F., Sule Ajiboye, S., Olamilekan, K. M., & Abdulazeez, L. (2022). Data Privacy System Using Steganography and Cryptography. *International Journal of Mathematical Sciences and Computing*, *8*(2), 37–45. https://doi.org/10.5815/ijmsc.2022.02.04

Atanda, O. G., ADENIYI, A. E., ADEBIYI, M. O., ODUMEH, V., & AROBA, O. J. (2024). *Building a Robust Data Shield: Implementing a Cryptography and Steganography Security Model*. 1–28. https://www.researchsquare.com/article/rs-4689651/v1

Blackledge, J. (2011). *Cryptography Using Steganography : New Algorithms and Applications Cryptography and Steganography :* https://doi.org/10.21427/D7ZS63

Ikeagwu, C. P., Ejiofor, V. E., Eze, O. E., & Akawuku, G. (2025). Survey of Cryptography models for Security of Computer-based Integrated School Information Management System. *Research Output Journal of Engineering and Scientific Research*, *4*(1), 60–70. https://doi.org/10.59298/rojesr/2025/4.1.6070

Mathe, R., Atukuri, V. R., & Devireddy, S. K. (2012). Securing Information : Cryptography and Steganography. *International Journal of Computer Science and Information Technologies*, *3*(3), 4251–4255.

Nurrochim, A. (2025). *Syntax Literate : Jurnal Ilmiah Indonesia Implementasi Kriptografi AES dan Steganografi Untuk Keamanan Data Customer dan Transaksi di PT Guna Bangun Jaya (LEMKRA) Agus Nurrochim kerugian untuk setiap jenis catatan data yang bocor , yang menegaskan betap*. *10*(10), 8100–8117.

Ozighor, E. R., & Izegbu, I. (2020). Information Protection Against Security Threats in an Insecure Environment using Cryptography and Steganography. *Global Scientific Journal - Computer Science and Engineering Journal*, *8*(5), 1671–1692.

Rahman, R., Mulyadi, & Imran, A. (2024). Optimalisasi Keamanan Data Pada Sistem Operasi Windows Melalui Penerapan Teknologi Kriptografi Modern. *Jurnal Sistem Informasi Dan Ilmu Komputer*, *2*(3), 146–166.

Rakhmadi Rahman, Khumaedi Khumaedi, & Nugrah Surya Pratama. (2024). Peningkatan Keamanan Data dengan Kriptografi Modern pada Sistem Operasi. *Jurnal Sistem Informasi Dan Ilmu Komputer*, *2*(4), 01–08. https://doi.org/10.59581/jusiik-widyakarya.v2i3.3995

S, S. (2013). Steganography Technique of Sending Random Passwords on Receiver's Mobile (A New Technique to Hide Information File with an Image). *IOSR Journal of Computer Engineering*, *15*(3), 17–25. https://doi.org/10.9790/0661-1531725