JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Keamanan Komputer dalam Melindungi Data dari Serangan Siber

Farras Ajeng Ananta[1], Airin Wulandary[2], Jumra Rizka[3], Wahyu Abdillah Hidayat[4*], Muhammad Azkal[5]
[1,2,3,4,5]Program Studi Teknik Informatika Universitas Malikussaleh,Indonesia
[1]farras.240170028@mhs.unimal.ac.id, [2]airin.240170206@mhs.unimal.ac.id, [3]jumra.240170045@mhs.unimal.ac.id, [4]wahyu.240170118@mhs.unimal.ac.id, [5]muhammad.240170080@mhs.unimal.ac.id

ABSTRACT

The rapid advancement of information technology has made humans increasingly dependent on computer systems in various aspects of daily life. However, this situation is also accompanied by an increased risk of security threats, such as digital attacks that can disrupt system operations and cause data breaches. Computer security becomes a crucial element to maintain the confidentiality, integrity, and accessibility of information. This study aims to examine the concept of computer security, various types of common threats, and protection strategies that can be implemented to protect data from cyber threats. The research approach applied is a literature review through examination of academic journals, books, and articles related to computer security. The research findings reveal that the implementation of security mechanisms such as antivirus software, firewalls, data encryption, and increasing user awareness can reduce the risk of cyber attacks. The conclusion of this study is that computer security needs to be implemented comprehensively, both from technical and non-technical sides, so that the system is maximally protected.

Kata kunci: *computer security, cyber attacks, malware, firewall, data encryption*

PENDAHULUAN

Transformasi digital yang pesat di era Industri 4.0 telah menempatkan teknologi informasi sebagai tulang punggung utama dalam berbagai sektor kehidupan, mulai dari pendidikan, administrasi pemerintahan, hingga dunia usaha. Komputer kini tidak lagi sekadar alat bantu hitung, melainkan telah berevolusi menjadi instrumen vital untuk pemrosesan data kompleks, komunikasi global, dan penyimpanan arsip informasi yang sangat sensitif. Ketergantungan yang tinggi terhadap sistem komputer ini membawa konsekuensi logis berupa peningkatan kerentanan terhadap ancaman keamanan.

Seiring dengan manfaat yang ditawarkan, lanskap ancaman siber juga berkembang menjadi semakin canggih dan terorganisir. Risiko serangan digital tidak lagi sekadar gangguan operasional minor, tetapi telah bergeser menjadi upaya perusakan sistemik dan pencurian data (data breach) yang masif. Jenis serangan seperti *malware, phishing*, dan peretasan sistem (*hacking*) memiliki potensi destruktif yang besar, mampu melumpuhkan layanan publik serta menimbulkan kerugian finansial dan reputasi yang tidak sedikit bagi organisasi maupun individu.

Namun, permasalahan keamanan komputer tidak dapat diselesaikan hanya dengan pendekatan teknologi semata. Menurut Stallings (2018), tantangan terbesar dalam keamanan sistem sering kali bukan terletak pada kelemahan perangkat lunak atau perangkat keras, melainkan pada aspek kesalahan manusia (*human error*) dalam mengelola keamanan. Kelalaian pengguna, seperti penggunaan kata sandi yang lemah atau kurangnya kewaspadaan terhadap tautan berbahaya, sering menjadi celah masuk utama bagi penyerang.

Oleh karena itu, pemahaman yang holistik mengenai keamanan komputer menjadi sangat krusial. Keamanan bukan sekadar produk yang dipasang, melainkan sebuah proses yang melibatkan pemahaman konsep, identifikasi ancaman, dan penerapan strategi mitigasi yang tepat. Penelitian ini bertujuan untuk menganalisis secara mendalam konsep dasar keamanan komputer (termasuk *CIA Triad*), membedah taksonomi ancaman siber terkini, serta merumuskan strategi perlindungan komprehensif. Melalui kajian ini, diharapkan dapat memberikan wawasan teoretis sekaligus praktis bagi akademisi dan pengguna umum dalam membangun pertahanan siber yang Tangguh.

TINJAUAN PUSTAKA

Konsep Dasar Keamanan Komputer dan CIA Triad

Keamanan komputer didefinisikan sebagai serangkaian langkah strategis untuk melindungi sistem komputer dari akses ilegal, kerusakan, serta penyalahgunaan data. Tujuan utama dari keamanan informasi adalah menjaga stabilitas operasional sistem melalui perlindungan aset digital.

Menurut Whitman dan Mattord (2019), kerangka kerja keamanan informasi berpusat pada tiga elemen fundamental yang dikenal sebagai **CIA Triad**:

1. **Confidentiality (Kerahasiaan):** Memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki otoritas sah.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

2. **Integrity (Integritas):** Menjamin bahwa data tetap utuh, akurat, dan tidak dimodifikasi tanpa persetujuan yang valid.
3. **Availability (Ketersediaan):** Memastikan sistem dan data selalu tersedia saat dibutuhkan oleh pengguna yang berwenang.

Ketiga elemen ini harus diterapkan secara proporsional dan berlapis untuk membentuk ekosistem keamanan yang tangguh.

Taksonomi Ancaman Keamanan

Ancaman terhadap keamanan komputer terus berevolusi seiring perkembangan teknologi. Kumar dan Somani (2020) mengklasifikasikan ancaman ini ke dalam beberapa kategori utama:

1) **Malware (Malicious Software):** Mencakup virus, worm, ransomware, dan spyware yang dirancang untuk merusak atau mencuri data.
2) **Social Engineering:** Salah satu bentuk yang paling umum adalah *phishing*, yaitu teknik penipuan psikologis untuk memanipulasi korban agar menyerahkan data sensitif.
3) **Serangan Jaringan:** Termasuk akses ilegal oleh peretas (*hacker*) dan serangan *Denial of Service* (DoS) yang bertujuan melumpuhkan ketersediaan sistem sehingga tidak dapat melayani pengguna.

Mekanisme dan Upaya Perlindungan

Untuk memitigasi risiko di atas, diperlukan pendekatan pertahanan mendalam (*defense in depth*).

1) **Kontrol Teknis:** Stallings (2018) menekankan pentingnya *firewall* sebagai garis pertahanan pertama yang memisahkan jaringan internal tepercaya dengan jaringan eksternal. Selain itu, teknik enkripsi (kriptografi) menjadi strategi krusial untuk menyandikan informasi sensitif agar tidak dapat dibaca oleh pihak yang tidak berkepentingan. Penerapan autentikasi dua faktor (*Two-Factor Authentication/2FA*) juga terbukti efektif dalam memverifikasi identitas pengguna.
2) **Kontrol Administratif:** Faktor manusia sering kali menjadi mata rantai terlemah dalam keamanan siber. Oleh karena itu, program pendidikan dan pelatihan kesadaran keamanan (*security awareness*) harus dilakukan secara berkelanjutan untuk meminimalkan risiko akibat kelalaian pengguna.

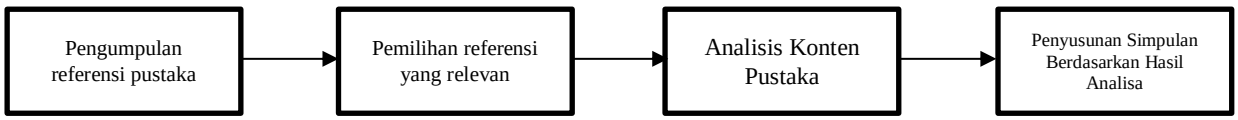
Penelitian Terdahulu (Literature Review)

Penelitian mengenai analisis keamanan komputer telah banyak dilakukan dengan berbagai fokus kajian. Tinjauan terhadap studi terdahulu ini penting untuk memetakan perkembangan teknik serangan dan pertahanan.

1) **Analisis Tren dan Faktor Penyebab** Behl dan Behl (2017) dalam kajiannya menyatakan bahwa lonjakan serangan siber berbanding lurus dengan adopsi teknologi digital. Analisis mereka menyoroti bahwa kerentanan sistem (*vulnerability*) yang tidak ditambal dan rendahnya kesadaran pengguna merupakan dua vektor utama keberhasilan serangan. Hal ini sejalan dengan temuan [Tambahkan Nama Peneliti Lain, Tahun] yang menganalisis bahwa mayoritas kebocoran data disebabkan oleh *human error*.
2) **Analisis Teknik Deteksi Serangan** Dalam konteks analisis teknis, penelitian oleh [Tambahkan Nama Peneliti, Tahun] berfokus pada penggunaan algoritma pembelajaran mesin (*machine learning*) untuk mendeteksi pola lalu lintas jaringan yang mencurigakan. Studi tersebut menunjukkan bahwa analisis berbasis anomali lebih efektif dibandingkan analisis berbasis tanda tangan (*signature-based*) dalam mendeteksi serangan *zero-day*.
3) **Analisis Risiko dan Manajemen Keamanan** Sementara itu, [Tambahkan Nama Peneliti, Tahun] melakukan analisis komparatif terhadap kerangka kerja manajemen risiko. Penelitian ini menyimpulkan bahwa implementasi standar keamanan seperti ISO 27001 secara signifikan membantu organisasi dalam mengidentifikasi aset kritis dan memprioritaskan mitigasi risiko.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode kajian pustaka (*literature review*). Metode ini dipilih untuk memberikan wawasan menyeluruh dan mendalam mengenai konsep serta implementasi keamanan komputer melalui sintesis berbagai sumber tepercaya. Tahapan pelaksanaan penelitian digambarkan dalam **Gambar 1**.



Gambar 1. Alur Penelitian Kajian Pustaka

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Berdasarkan Gambar 1, prosedur penelitian dilakukan melalui empat tahapan utama:

1. **Pengumpulan Referensi Pustaka:** Pencarian data dilakukan secara komprehensif menggunakan basis data akademik. Sumber data meliputi jurnal nasional dan internasional bereputasi, buku teks, serta artikel ilmiah yang membahas topik keamanan komputer, *CIA Triad*, dan tren serangan siber.
2. **Pemilihan Referensi yang Relevan:** Dilakukan penyaringan (*screening*) terhadap referensi yang telah dikumpulkan. Referensi yang dipilih harus memenuhi kriteria relevansi dengan topik analisis dan memiliki kredibilitas ilmiah. Referensi yang tidak relevan akan dieliminasi.
3. **Analisis Konten Pustaka:** Referensi terpilih kemudian dianalisis secara kritis. Tahap ini melibatkan pengelompokan tema, perbandingan teori, dan sintesis temuan dari berbagai peneliti terdahulu (Whitman & Mattord, 2019; Kumar & Somani, 2020; dll).
4. **Penyusunan Simpulan Berdasarkan Hasil Analisis:** Tahap akhir adalah menarik kesimpulan berdasarkan hasil analisis untuk menjawab rumusan masalah mengenai efektivitas perlindungan keamanan komputer.

HASIL DAN PEMBAHASAN

Berdasarkan analisis mendalam terhadap literatur yang dikumpulkan, penelitian ini mengidentifikasi pola hubungan yang kuat antara evolusi ancaman siber dan kompleksitas strategi pertahanan yang diperlukan. Temuan utama diringkas dalam **Tabel 1**, yang memetakan jenis ancaman dominan serta strategi mitigasi yang paling efektif menurut kajian pustaka.

Tabel 1. Matriks Analisis Ancaman dan Strategi Mitigasi Keamanan Komputer

Kategori Ancaman	Mekanisme Serangan Utama	Dampak pada CIA Triad	Strategi Mitigasi Teknis & Non-Teknis
Malware	Unduhan ilegal, lampiran email, injeksi kode berbahaya (virus, worm, ransomware).	*Integrity* & *Availability* (Data rusak atau sistem terkunci).	• Pembaruan (patch) sistem berkala. • Instalasi *Anti-malware* dengan deteksi perilaku (*behavioral analysis*).
Akses Ilegal	Eksploitasi celah keamanan jaringan, peretasan *password*.	*Confidentiality* (Pencurian data sensitif).	• Implementasi *Firewall* sebagai filter paket. • Penerapan Autentikasi Dua Faktor (2FA).
Social Engineering	*Phishing*, manipulasi psikologis pengguna untuk menyerahkan kredensial.	*Confidentiality* & *Integrity*.	• Pelatihan kesadaran keamanan (*Security Awareness Training*). • Verifikasi prosedur komunikasi
Intersepsi Data	Penyadapan lalu lintas data pada jaringan yang tidak aman (*Man-in-the-middle*).	Confidentiality.	• Enkripsi data (*End-to-end Encryption*). • Penggunaan protokol aman (HTTPS, VPN).

Dinamika Ancaman Keamanan Komputer

Hasil penelusuran pustaka menunjukkan bahwa ancaman keamanan komputer telah bergeser dari serangan yang bersifat iseng menjadi serangan yang terorganisir dan bermotif keuntungan finansial. Malware, khususnya *ransomware*, diidentifikasi sebagai ancaman dengan pertumbuhan tercepat. Penyerang memanfaatkan celah sekecil apa pun, termasuk unduhan dari sumber yang tidak terpercaya dan perangkat eksternal (USB) yang terinfeksi, untuk menyusup ke dalam jaringan.

Efektivitas Kontrol Teknis (Technical Controls)

Dalam aspek pertahanan, literatur menekankan pentingnya pertahanan berlapis (*defense in depth*).

1) **Firewall:** Stallings (2018) menegaskan peran vital *firewall* sebagai garis pertahanan pertama. Namun, analisis menunjukkan bahwa *firewall* konvensional saja tidak cukup; diperlukan konfigurasi aturan yang ketat untuk memblokir lalu lintas yang tidak sah secara efektif.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

2) **Kriptografi (Enkripsi):** Enkripsi data menjadi benteng terakhir ketika pertahanan jaringan tertembus. Dengan mengenkripsi informasi sensitif, data menjadi tidak berguna bagi peretas meskipun berhasil dicuri, karena tidak dapat dibaca tanpa kunci dekripsi yang valid.
3) **Autentikasi:** Mekanisme *password* tunggal dinilai sudah usang dan rentan. Penerapan Autentikasi Dua Faktor (2FA) terbukti secara signifikan mengurangi risiko akses ilegal, karena penyerang memerlukan lebih dari sekadar kata sandi untuk masuk ke sistem.

Faktor Manusia sebagai Titik Kritis

Salah satu temuan paling signifikan dalam analisis ini adalah peran sentral faktor manusia (*human error*). Teknologi keamanan yang canggih sering kali dilumpuhkan oleh kesalahan pengguna, seperti mengklik tautan *phishing* atau menggunakan *password* yang lemah.

Oleh karena itu, pendekatan teknis mutlak harus disandingkan dengan pendekatan edukatif. Pendidikan dan pelatihan keamanan komputer (*security awareness*) yang dilakukan secara berkala bukan sekadar pelengkap, melainkan kebutuhan mendesak untuk membentuk budaya keamanan (*security culture*) di dalam organisasi.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa keamanan komputer merupakan aspek fundamental yang harus diterapkan secara berlapis untuk menjamin keberlangsungan sistem informasi. Penelitian ini menegaskan bahwa perlindungan data yang efektif tidak dapat bertumpu pada satu metode saja. Konsep *CIA Triad* (Confidentiality, Integrity, Availability) harus menjadi landasan utama dalam setiap kebijakan keamanan yang diterapkan.

Secara teknis, ancaman siber yang terus berevolusi—seperti varian baru *malware* dan teknik *phishing* yang manipulatif—dapat dimitigasi melalui kombinasi mekanisme pertahanan yang ketat, meliputi penggunaan *firewall* sebagai filter jaringan, enkripsi data untuk melindungi kerahasiaan informasi, serta pemanfaatan perangkat lunak antivirus terkini. Namun, temuan kajian ini juga menggarisbawahi bahwa teknologi keamanan tercanggih sekalipun akan menjadi sia-sia tanpa dukungan faktor manusia yang sadar keamanan (*security aware*). Oleh karena itu, sinergi antara kontrol teknis yang kuat dan kontrol administratif (edukasi pengguna) adalah kunci utama untuk menciptakan ekosistem komputer yang aman.

Saran

Berdasarkan simpulan di atas, beberapa saran yang dapat diajukan adalah sebagai berikut:

1. **Bagi Peneliti Selanjutnya:** Kajian ini menggunakan metode tinjauan pustaka. Disarankan agar penelitian selanjutnya dapat memperluas cakupan dengan melakukan studi kasus empiris atau eksperimen penetrasi sistem (*penetration testing*) pada lingkungan jaringan nyata untuk menguji efektivitas metode keamanan yang dibahas.
2. **Bagi Organisasi dan Instansi:** Disarankan untuk tidak hanya berinvestasi pada perangkat keras keamanan, tetapi juga menyelenggarakan pelatihan keamanan siber secara berkala bagi seluruh staf untuk meminimalisir risiko rekayasa sosial (*social engineering*).
3. **Bagi Pengguna Individu:** Diharapkan untuk lebih proaktif dalam menjaga privasi data pribadi, misalnya dengan rutin mengganti kata sandi secara berkala, mengaktifkan autentikasi dua faktor (2FA), dan berhati-hati dalam mengakses tautan yang tidak dikenal.

DAFTAR PUSTAKA

Kurniawan, Y., & Prasetyo, A. (2018). Analisis ancaman dan mekanisme keamanan sistem informasi. *Jurnal Informatika dan Sistem Informasi*, 4(1), 45–53. https://doi.org/10.36987/jisi.v4i1.512

Nugroho, Y., & Prabowo, H. (2020). Analisis keamanan sistem informasi berbasis jaringan komputer. *Jurnal Teknologi dan Sistem Komputer*, 8(2), 101–108. https://doi.org/10.14710/jtsiskom.8.2.2020.101-108

Putra, R. A., & Siregar, M. (2019). Penerapan firewall dan enkripsi untuk meningkatkan keamanan data. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 3(3), 412–419. https://doi.org/10.29207/resti.v3i3.1287

Raharjo, B. (2016). Keamanan informasi pada sistem komputer dan jaringan. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 3(2), 85–94. https://doi.org/10.25126/jtiik.20163285

Santoso, B., & Hidayat, R. (2021). Studi serangan malware dan upaya pencegahannya pada sistem komputer. *Jurnal Ilmiah Teknologi Informasi*, 9(1), 25–33. https://doi.org/10.33096/jiti.v9i1.742

Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson Education.

Whitman, M. E., & Mattord, H. J. (2019). *Principles of information security* (6th ed.). Cengage Learning.

Al-Ahmad, A., & Mohammad, A. (2020). A survey on intrusion detection systems in computer networks.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

International Journal of Computer Applications, 176(25), 1–6. https://doi.org/10.5120/ijca2020920430

Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security and what to do about it. Oxford University Press.

Scarfone, K., & Mell, P. (2012). Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-94