Gudang Jurnal Multidisiplin Ilmu
Volume 3 ; Nomor 10 ; Oktober 2025 ; Page 26-31
Doi : https://doi.org/10.59435/gjmi.v3i10.1761
Website : https://gudangjurnal.com/index.php/gjmi

E-ISSN : 2988-5760

Keamanan Sistem Informasi Dalam Mengatasi Ancaman, Kerentanan, Dan Penanggulangan Di Dalam Penggunaan Perangkat Komputer

Gadis Fitria Aulia Dhini[1], Ayuhana Vanesya Purba[2], Dea Cindiasyahwa[3], Indra Gunawan[4]

[1]Mahasiswa Program Studi Sistem Informasi, STIKOM Tunas Bangsa Pematangsiantar
[2]Mahasiswa Program Studi Sistem Informasi, STIKOM Tunas Bangsa Pematangsiantar
[3]Mahasiswa Program Studi Sistem Informasi, STIKOM Tunas Bangsa Pematangsiantar
[4]Dosen Program Studi Sistem Informasi, STIKOM Tunas Bangsa Pematangsiantar

[1]gadisfitri46@gmail.com, [2]syavanes5@gmail.com, [3]deacindiya@gmail.com, [4]indra@amiktunasbangsa.ac.id

Abstrak

Perkembangan teknologi informasi telah memberikan kontribusi besar terhadap efisiensi dan efektivitas kerja manusia, namun juga membawa tantangan serius terhadap keamanan sistem informasi. Ancaman seperti phishing, malware, data breach, dan eksploitasi kerentanan pada jaringan komputer kini menjadi permasalahan global yang terus meningkat [1]. Penelitian ini bertujuan untuk menganalisis ancaman, kerentanan, dan strategi penanggulangan dalam keamanan sistem informasi khususnya pada penggunaan perangkat komputer dan aplikasi berbasis internet. Metode penelitian menggunakan pendekatan deskriptif kualitatif dengan studi literatur dari berbagai sumber primer dan sekunder, termasuk jurnal ilmiah nasional dan artikel daring yang relevan [1]–[2]. Hasil penelitian menunjukkan bahwa keamanan sistem informasi dipengaruhi oleh tiga komponen utama, yaitu manusia, teknologi, dan kebijakan organisasi [3]. Penerapan prinsip Confidentiality, Integrity, Availability (CIA), pemanfaatan kerangka kerja OWASP, serta audit keamanan dan peningkatan literasi digital terbukti efektif dalam mengurangi risiko serangan siber [4][5][1]. Penelitian ini diharapkan dapat memberikan kontribusi dalam memperkuat strategi keamanan sistem informasi di Indonesia dan menjadi acuan bagi organisasi dalam menjaga keutuhan aset digitalnya.

Kata Kunci : Keamanan Sistem Informasi, Ancaman Siber, Kerentanan, OWASP, CIA Triad.

Abstract

The development of information technology has made a significant contribution to the efficiency and effectiveness of human work, but it also brings serious challenges to information system security. Threats such as phishing, malware, data breaches, and exploitation of vulnerabilities in computer networks have now become global issues that continue to increase [1]. This study aims to analyze threats, vulnerabilities, and mitigation strategies in information system security, particularly in the use of computers and internet-based applications. The research method employs a qualitative descriptive approach with a literature review from various primary and secondary sources, including national scientific journals and relevant online articles [1]–[2]. Research results indicate that information system security is influenced by three main components: humans, technology, and organizational policies [3]. The implementation of the Confidentiality, Integrity, Availability (CIA) principles, utilization of the OWASP framework, as well as security audits and improvement of digital literacy have been proven effective in reducing the risk of cyberattacks [4][5][1]. This study is expected to contribute to strengthening information system security strategies in Indonesia and serve as a reference for organizations in safeguarding the integrity of their digital assets.

Keyword : *Information System Security, Cyber Threats, Vulnerabilities, OWASP, CIA Triad.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak besar bagi transformasi digital di berbagai sektor kehidupan, termasuk dunia pendidikan, pemerintahan, dan bisnis. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman terhadap keamanan sistem informasi, seperti pencurian data, serangan malware, dan eksploitasi kerentanan perangkat lunak [6].

Di Indonesia, serangan siber terus meningkat setiap tahun. Berdasarkan penelitian Zainuddin [6], kasus pelanggaran keamanan digital masih tinggi karena lemahnya kesadaran masyarakat serta belum optimalnya kebijakan

hukum dalam menanggulangi cybercrime. Sementara itu, Raharjo [7] menegaskan bahwa perlindungan terhadap sistem informasi harus berlandaskan tiga prinsip utama, yaitu Confidentiality, Integrity, dan Availability (CIA).

Yel dan Nasution [4] menambahkan bahwa keamanan informasi tidak hanya sebatas perlindungan teknis, tetapi juga menyangkut privasi pengguna serta tanggung jawab individu dalam menjaga data pribadi di media digital. Kerahasiaan (confidentiality) memastikan informasi tidak diakses pihak yang tidak berwenang, integritas (integrity) menjamin keaslian data, dan ketersediaan (availability) memastikan sistem tetap dapat diakses pengguna yang sah.

Buku Keamanan Sistem Informasi oleh Raharjo [7] juga menjelaskan bahwa aspek keamanan mencakup perlindungan terhadap perangkat keras, perangkat lunak, jaringan, dan pengguna. Dengan meningkatnya integrasi sistem berbasis cloud dan Internet of Things (IoT), risiko kebocoran data menjadi semakin tinggi. Wulan et al. [5] menemukan bahwa penggunaan layanan cloud computing tanpa pengamanan yang memadai dapat menyebabkan peningkatan potensi serangan terhadap sistem informasi.

Selain ancaman eksternal, kerentanan internal juga berperan besar dalam melemahkan sistem keamanan. Mukhlis dan Alfila [8] menjelaskan bahwa kesalahan pengguna, lemahnya konfigurasi sistem, dan kurangnya audit berkala dapat memicu kebocoran informasi. Penelitian lain oleh Shinta et al. [3] menunjukkan bahwa perilaku pengguna yang tidak berhati-hati seperti penggunaan kata sandi lemah atau membagikan kredensial login berkontribusi terhadap tingginya risiko keamanan.

Derry et al. [9] menjelaskan bahwa meningkatkan keamanan siber secara efektif membutuhkan gabungan beberapa strategi yang saling terkait, seperti penggunaan teknologi terbaru, penerapan kebijakan yang tegas, serta pelatihan dan kesadaran bagi para pekerja. Dalam hal ini, regulasi yang sudah ada, seperti Undang-Undang ITE dan Peraturan Pemerintah 82/2012, serta kerja sama antarinstansi pemerintah, menjadi fondasi kuat untuk memperkuat keamanan siber di Indonesia. Penelitian Achmad Syafaat [10] pada website Fakultas Ilmu Komputer Universitas Subang menemukan adanya beberapa kerentanan yang termasuk dalam kategori OWASP Top 10, seperti SQL Injection dan Cross-Site Scripting (XSS). Hal ini membuktikan bahwa ancaman siber juga mengincar lembaga akademik yang mengelola data sensitif mahasiswa dan dosen.

Munawar [11] menambahkan bahwa peningkatan volume data dan konektivitas jaringan menyebabkan risiko keamanan yang lebih tinggi terhadap infrastuktur digital organisasi. Ancaman tersebut dapat muncul dari kesalahan informasi sistem, serangan malware, serta rendahnya kesadaran oleh pengguna. Oleh karena itu, organisasi perlu mengintegrasikan teknologi perlindungan, kebijakan keamanan, serta pembinaan budaya kesadaran keamanan siber.

Penelitian Wahyu Hidayat et al. [1] memperkuat fakta tersebut dengan menunjukkan bahwa banyak pengguna masih mengabaikan keamanan email, padahal email merupakan pintu utama penyebaran malware dan upaya pencurian data pribadi. Di sisi lain, situs UNSIA [12] dan Integrasolusi [2] menekankan bahwa mitigasi ancaman siber harus dilakukan secara menyeluruh melalui penguatan kebijakan organisasi, audit berkala, serta edukasi keamanan bagi seluruh pengguna.

Berdasarkan uraian di atas, dapat disimpulkan adanya research gap antara kemajuan teknologi dan kesiapan keamanan informasi di Indonesia. Oleh karena itu, penelitian ini bertujuan untuk menganalisis strategi keamanan sistem informasi dalam mengatasi ancaman, kerentanan, dan penanggulangan terhadap penggunaan perangkat komputer secara komprehensif melalui pendekatan teknologi, kebijakan, dan kesadaran pengguna.

2. METODOLOGI PENELITIAN

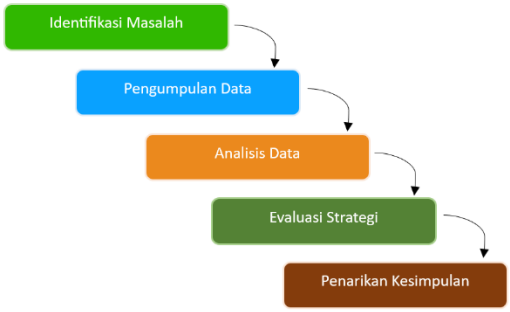
Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi literatur. Metode ini digunakan untuk menganalisis berbagai referensi primer, seperti jurnal ilmiah, buku, dan sumber daring yang relevan dengan topik keamanan sistem informasi. Fokus utama penelitian adalah meninjau ancaman, kerentanan, dan strategi penanggulangan pada sistem informasi berbasis komputer.

2.1 Tahapan Penelitian

Tahapan penelitian dijelaskan sebagai berikut:

1. Identifikasi Masalah: Menganalisis permasalahan utama yaitu meningkatnya ancaman terhadap keamanan sistem informasi di berbagai institusi [6][5].
2. Pencarian Data: Mengumpulkan sumber-sumber ilmiah dari 12 referensi, terdiri dari jurnal nasional, buku akademik, dan situs web terpercaya seperti UNSIA [12] dan Integrasolusi [2].
3. Analisis Data: Menelaah setiap literatur untuk mengidentifikasi faktor penyebab ancaman dan kerentanan, serta menilai efektivitas metode pengamanan yang diterapkan [8].
4. Evaluasi Strategi: Mengevaluasi pendekatan keamanan berdasarkan prinsip Confidentiality, Integrity, Availability (CIA) dan kerangka OWASP Top 10 [4][10].
5. Penarikan Kesimpulan: Merumuskan hasil penelitian berupa rekomendasi strategi keamanan sistem informasi yang dapat diterapkan secara komprehensif.

Gambar 1. Tahapan Penelitian Keamanan Sistem Informasi



2.2 Metode Penyelesaian Masalah

Metode penyelesaian masalah dilakukan dengan mengidentifikasi tiga komponen utama: ancaman (threats), kerentanan (vulnerabilities), dan pengendalian (controls) [8].

Langkah-langkahnya adalah:

1. Analisis Ancaman: Meninjau berbagai bentuk serangan seperti phishing, SQL Injection, malware, dan ransomware yang dapat merusak integritas sistem [1][10].
2. Identitfikasi kerentanan: Menilai kelemahan dari aspek teknis, manusia, dan kebijakan organisasi yang dapat menjadi pintu masuk serangan [4][3].

Tabel 1. Jenis-Jenis Ancaman dan Strategi Penanggulangan

Jenis Ancaman	Dampak Terhadap Sistem	Strategi Penanggulangan
Phishing dan Email-Fraud	Kebocoran data pribadi	Edukasi pengguna, filter spam, enkripsi komunikasi
Malware dan Ransomware	Kerusakan file dan sistem	Antivirus, patching rutin, backup data
SQL Injection	Manipulasi basis data	Validasi input, parameterized query
DDoS Attack	Gangguan layanan sistem	Firewall dan load balancing
Human Error	Akses tidak sah	Pelatihan keamanan dan audit berkala

3. HASIL DAN PEMBAHASAN

3.1 Analisis Hasil Penelitian

Berdasarkan hasil telaah literatur dan analisis terhadap berbagai sumber primer, ditemukan bahwa keamanan sistem informasi menghadapi tiga jenis ancaman utama yang saling berhubungan, yaitu ancaman teknis, manusia, dan kebijakan organisasi.

a. Ancaman Teknis

Ancaman teknis merupakan gangguan yang bersumber dari aspek teknologi dan sistem perangkat lunak.

1. Phishing – metode penipuan untuk mencuri data pribadi pengguna melalui email atau situs tiruan [9].
2. SQL Injection – serangan yang mengeksploitasi celah validasi input pada aplikasi web untuk memanipulasi basis data [10].
3. Malware – perangkat lunak berbahaya yang dapat merusak atau mencuri data sistem komputer [6].

b. Ancaman Manusia (Human Error)

Faktor manusia berperan besar dalam keamanan sistem informasi.

1. Kurangnya kesadaran keamanan (security awareness) menyebabkan pengguna mudah menjadi korban rekayasa sosial (social engineering) [3][1].
2. Penggunaan kata sandi yang lemah dan berulang di berbagai akun meningkatkan risiko kebocoran data pribadi [4].

c. Ancaman Kebijakan dan Regulasi

Kurangnya penerapan regulasi keamanan dan pengawasan menjadi salah satu penyebab utama lemahnya sistem keamanan.

1. Zainuddin [1] menegaskan bahwa kebijakan hukum di Indonesia belum adaptif terhadap dinamika ancaman digital.
2. Keberhasilan dalam meningkatkan keamanan siber memerlukan regulasi yang ada, seperti UU ITE dan PP 82/2012, serta koordinasi antar lembaga pemerintah, memberikan dasar yang kuat bagi upaya penguatan keamanan siber di Indonesia [9].
3. Tidak adanya audit keamanan rutin menyebabkan celah sistem tetap terbuka dalam jangka panjang [7].

3.1.1 Kerentanan Sistem Informasi

Berdasarkan hasil analisis, kerentanan (vulnerability) sistem informasi dapat dikelompokkan menjadi tiga kategori utama:

1. Kerentanan Teknis, yaitu kelemahan pada perangkat lunak, basis data, atau jaringan seperti celah SQL Injection, Cross-Site Scripting (XSS), dan kegagalan enkripsi data [10].
2. Kerentanan Manusia, yang muncul karena kesalahan pengguna, seperti menggunakan kata sandi lemah, tidak memperbarui sistem, atau menjadi korban phishing [4][3][1].
3. Kerentanan Kebijakan, yang berasal dari kelemahan manajerial, seperti tidak adanya security policy, audit keamanan, atau standar Information Security Management System (ISMS) [6].

Ketiga jenis kerentanan tersebut saling terkait dan dapat dimanfaatkan oleh pelaku kejahatan digital untuk menembus sistem informasi. Oleh karena itu, identifikasi dan mitigasi terhadap kerentanan harus menjadi prioritas utama dalam penerapan kebijakan keamanan organisasi.

3.1.2 Pembahasan Strategi Penanggulangan

Dari hasil identifikasi ancaman dan kerentanan tersebut, dirumuskan strategi penanggulangan yang terdiri dari tiga pendekatan utama: teknis, manusia, dan kebijakan organisasi.

a. Pendekatan Teknis
   1. Penerapan firewall, Intrusion Detection System (IDS), dan Security Information and Event Management (SIEM) untuk mencegah akses tidak sah [8].
   2. Penggunaan enkripsi end-to-end dalam proses transmisi data guna menjaga kerahasiaan informasi [4][7].
   3. Penerapan OWASP Top 10 sebagai standar evaluasi keamanan aplikasi web, seperti input validation dan parameterized query [10].

b. Pendekatan Manusia
   1. Pelatihan keamanan informasi (security awareness training) secara berkala bagi pengguna sistem [12].
   2. Simulasi serangan phishing internal untuk meningkatkan kesiapsiagaan karyawan atau mahasiswa [1].
   3. Pembentukan budaya keamanan digital (cyber hygiene) di lingkungan organisasi [3].

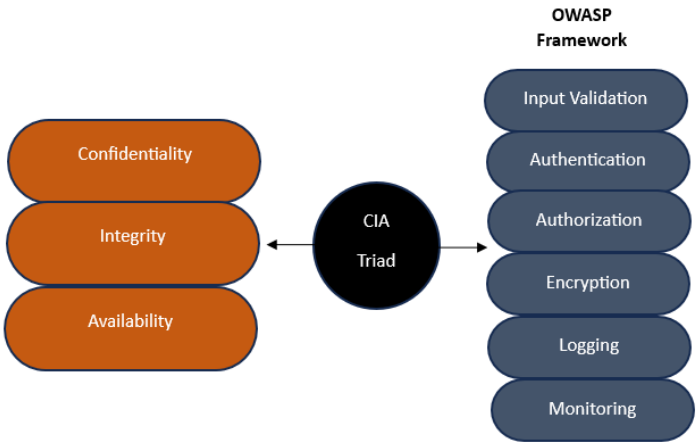
c. Pendekatan Kebijakan Organisasi
   1. Penerapan kebijakan kontrol akses (access control policy) dan manajemen kata sandi [7].
   2. Audit sistem berkala untuk memastikan kepatuhan terhadap standar keamanan [11].
   3. Pengembangan incident response plan agar organisasi dapat merespons serangan secara cepat dan efektif [2].

3.2 Implementasi

Implementasi dari hasil kajian ini dapat diterapkan melalui model integrasi antara CIA Triad dan OWASP Framework sebagai acuan strategis dalam pengembangan keamanan sistem informasi.

Model ini menempatkan Confidentiality sebagai lapisan pertama yang fokus pada privasi data pengguna, Integrity sebagai lapisan kedua yang menjaga keaslian data, dan Availability sebagai lapisan ketiga yang memastikan sistem tetap dapat diakses oleh pengguna sah.

Gambar 2. Model Integrasi CIA Triad dan OWASP Framework dalam Pengamanan Sistem Informasi



4. KESIMPULAN

Penelitian ini menegaskan bahwa keamanan sistem informasi merupakan aspek fundamental dalam menjaga kerahasiaan, integritas, dan ketersediaan data di era digital. Berdasarkan hasil analisis, ditemukan bahwa ancaman terbesar terhadap sistem informasi berasal dari tiga faktor utama, yaitu faktor teknis, manusia, dan kebijakan organisasi.

Pendekatan yang paling efektif dalam mengatasi ancaman dan kerentanan adalah kombinasi strategi teknis dan non-teknis. Dari sisi teknis, penerapan firewall, enkripsi, dan audit keamanan berbasis OWASP Framework terbukti mampu memperkuat pertahanan sistem. Dari sisi manusia, kesadaran dan pelatihan keamanan siber secara berkala terbukti meningkatkan kesiapsiagaan pengguna terhadap serangan phishing dan malware. Dari sisi kebijakan, penerapan security policy, audit rutin, serta penegakan regulasi hukum menjadi komponen penting dalam menjaga keberlanjutan keamanan informasi.

Dengan demikian, keamanan sistem informasi harus dipandang sebagai tanggung jawab bersama antara teknologi, kebijakan organisasi, dan perilaku manusia. Implementasi model integrasi CIA Triad dan OWASP diharapkan dapat menjadi solusi komprehensif untuk meningkatkan keamanan data di lembaga pendidikan, pemerintahan, maupun sektor industri.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu terlaksananya penelitian ini, terutama kepada rekan-rekan akademisi yang memberikan kontribusi berupa literatur dan masukan ilmiah dalam proses penyusunan jurnal ini. Penghargaan juga disampaikan kepada dosen pembimbing yang telah mendukung dalam menyediakan sumber referensi dan fasilitas penelitian. Ucapan terima kasih juga disampaikan kepada para penulis jurnal yang karyanya menjadi sumber referensi dalam penelitian ini. Kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] W. Hidayat, N. Musdira, N. Rasyid, M. Khairi, and M. Juharman, "Analisis Ancaman Terhadap Keamanan Data Pribadi pada Email," *J. Pendidik. Terap.*, vol. 01, pp. 7–12, 2023, [Online]. Available: https://journal.diginus.id/index.php/JUPITER/index

[2] INTEGRASOLUSI, "Melawan Ancaman Digital: Menghadapi Isu Keamanan Informasi Terkini," INTEGRASOLUSI (Integra Teknologi Solusi). [Online]. Available: https://integrasolusi.com/keamanan/audit-keamanan-informasi/melawan-ancaman-digital-menghadapi-isu-keamanan-informasi-terkini/

[3] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.

[4] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data PribaYel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. Jurnal Informatika Kaputama (JIK), 6(1), 92–101. https://doi.org/10.59697/jik.v6i1.144di Pada Media Sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022.

[5] W. Wulan *et al.*, "Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud

Computing dalam Penggunaan E-Commerce dan Rencana Strategis," *J. Kewirausahaan dan Multi Talent.*, vol. 2, no. 2, pp. 126–137, 2024, doi: 10.38035/jkmt.v2i2.164.

[6] Zainuddin Kasim, "Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia," *Indragiri Law Rev.* , vol. 2, no. 1, pp. 18–24, 2024, [Online]. Available: https://ejournalpasca.unisi.ac.id/index.php/ilr/article/view/22/23

[7] B. Raharjo, *P Y YAYASAN PRIMA AGUS TEKNIK YAYASAN PRIMA AGUS TEKNIK YAYASAN PRIMA AGUS TEKNIK Keamanan SISTEM INFORMASI*. 2021.

[8] B. Laila Alfila, A. Mukhlis, and A. Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 143–152, 2023, [Online]. Available: https://doi.org/10.55606/juisik.v3i2.496

[9] Derri Anjuju, S. Suryayusra, Maria Ulfa, and Dedi Irawan, "Analisis Keamanan Infrastruktur Teknologi Informasi Dalam Menghadapi Ancaman Cybersecurity," *J. Data Anal. Information, Comput. Sci.*, vol. 2, no. 1, pp. 75–80, 2025, doi: 10.70248/jdaics.v2i1.1792.

[10] A. Syafaat, "Menggunakan Metodologi Owasp," *Global*, vol. 11, no. 1, pp. 84–99, 2024, [Online]. Available: http://ejournal.unsub.ac.id/index.php/Fasilkom

[11] Z. Munawar, M. Kom, and N. I. Putri, "KeamMunawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. Jurnal Sistem Informasi-J-SIKA, 02, 14–20.anan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 14–20, 2020.

[12] UNSIA, "Mengamankan Sistem Informasi dalam Era Digital: Tantangan dan Strategi," UNSIA (Universitas Siber Asia). [Online]. Available: https://unsia.ac.id/mengamankan-sistem-informasi-dalam-era-digital-tantangan-dan-strategi/