JIKUM
JURNAL ILMU KOMPUTER

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

Keamanan Informasi dalam Sistem Informasi Modern: Analisis Ancaman dan Upaya Pengamanan Berdasarkan Studi Literatur

Sucia Nurmadani[1], Nada Amal Ceria[2], Munawar Khalil[3*], Muhammad Fariz Riski[4], Muhammad Ramzy Rasyad[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]sucia.240170017@mhs.unimal.ac.id, [2]nada.240170018@mhs.unimal.ac.id, [3]munawar.240170132@mhs.unimal.ac.id, [4]muhammad.240170237@mhs.unimal.ac.id, [5]muhammad.240170142@mhs.unimal.ac.id

ABSTRACT

Information security is a critical aspect of modern information systems, as information assets are vulnerable to various cyber threats that may compromise confidentiality, integrity, and availability. Attacks such as phishing, malware, ransomware, data breaches, and network-based attacks continue to increase and pose serious risks to organizations and individuals. This study aims to examine the concepts, threats, and protection strategies in information security based on scientific literature. The research method used is a literature review by analyzing 20 references published between 2020 and 2025 related to information security, information system security, network security, cryptography, and risk management. The results indicate that effective information security requires an integrated approach involving technical controls, security policies, risk management, and user awareness.

Kata Kunci/ Keywords:
Information Security, Information System Security, Network Security, Cyber Threats, Cryptography

PENDAHULUAN

Perkembangan teknologi informasi mendorong pemanfaatan sistem digital secara masif dalam berbagai sektor, seperti pendidikan, pemerintahan, kesehatan, perbankan, dan industri bisnis (Alzahrani & Alomar, 2020; ISO/IEC, 2022). Sistem berbasis web, aplikasi mobile, serta layanan cloud computing telah menjadi bagian integral dalam pengelolaan data dan penyediaan layanan. Informasi yang dikelola melalui sistem tersebut memiliki nilai strategis karena mendukung proses pengambilan keputusan dan keberlangsungan operasional organisasi.

Seiring dengan meningkatnya pemanfaatan teknologi informasi, risiko terhadap keamanan informasi juga semakin tinggi. Ancaman siber berkembang tidak hanya dari sisi kuantitas, tetapi juga dari tingkat kompleksitas dan teknik serangan yang digunakan. Serangan seperti phishing, malware, ransomware, dan kebocoran data sering kali menargetkan kelemahan sistem serta kurangnya kesadaran pengguna (ENISA, 2023; Microsoft, 2024). Faktor manusia bahkan menjadi salah satu titik lemah utama dalam sistem keamanan informasi.

Keamanan dalam bidang informasi bertujuan untuk melindungi aset informasi agar tetap terjaga kerahasiaan, integritas, dan ketersediaannya. Penerapan keamanan informasi yang baik tidak hanya bergantung pada teknologi, tetapi juga melibatkan kebijakan, prosedur, serta manajemen risiko yang terstruktur. Oleh karena itu, kajian mengenai keamanan informasi menjadi sangat penting untuk memahami konsep, ancaman, dan solusi yang dapat diterapkan secara efektif.

Penelitian ini bertujuan untuk mengkaji konsep dasar keamanan informasi, jenis-jenis ancaman siber, serta strategi dan implementasi pengamanan informasi berdasarkan literatur ilmiah periode 2020–2025. Hasil kajian diharapkan dapat memberikan gambaran yang komprehensif mengenai pentingnya pendekatan keamanan informasi yang holistik dan berkelanjutan.

TINJAUAN PUSTAKA

Keamanan Informasi

Keamanan informasi merupakan serangkaian upaya yang dilakukan untuk melindungi informasi dari ancaman yang dapat menyebabkan kerugian, baik secara teknis maupun non-teknis. Tujuan utama keamanan informasi adalah menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi yang dikenal sebagai konsep CIA Triad (ISO/IEC, 2022; Rahardjo, 2020). Ketiga prinsip tersebut menjadi dasar dalam perancangan dan implementasi sistem keamanan informasi modern. Selain itu, keamanan informasi juga mencakup pengendalian akses agar hanya pihak yang berwenang yang dapat menggunakan informasi. Penerapan kebijakan dan prosedur keamanan menjadi faktor penting dalam memastikan perlindungan informasi berjalan secara konsisten. Teknologi seperti enkripsi, firewall, dan sistem deteksi intrusi digunakan untuk mencegah dan mendeteksi serangan siber. Manajemen risiko diperlukan untuk mengidentifikasi, menganalisis, dan mengurangi potensi ancaman terhadap aset informasi. Kesadaran dan perilaku pengguna juga berperan besar karena kesalahan manusia sering menjadi penyebab utama terjadinya insiden keamanan. Oleh karena itu, pelatihan dan edukasi keamanan informasi perlu dilakukan secara

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

berkelanjutan. Dengan pendekatan yang terpadu, organisasi dapat meningkatkan ketahanan sistem informasi terhadap berbagai ancaman siber.

Keamanan Sistem Informasi

Keamanan sistem informasi mencakup perlindungan terhadap seluruh komponen sistem, termasuk perangkat keras, perangkat lunak, basis data, jaringan, serta pengguna. Sistem informasi yang aman harus mampu mencegah akses tidak sah, menjaga keakuratan data, dan memastikan layanan tetap tersedia saat dibutuhkan. Kelemahan pada salah satu komponen dapat berdampak pada keseluruhan sistem dan menimbulkan risiko kebocoran data maupun gangguan layanan. Oleh karena itu, diperlukan mekanisme autentikasi dan otorisasi yang kuat untuk mengendalikan akses pengguna. Penerapan pembaruan dan patch keamanan secara rutin juga penting untuk menutup celah kerentanan pada perangkat lunak. Selain itu, pencatatan dan pemantauan aktivitas sistem membantu dalam mendeteksi aktivitas mencurigakan sejak dini. Penggunaan backup dan sistem pemulihan bencana diperlukan untuk menjamin keberlangsungan operasional ketika terjadi kegagalan sistem. Standar keamanan seperti ISO/IEC 27001 dapat dijadikan acuan dalam pengelolaan keamanan sistem informasi (ISO/IEC, 2022; Nugroho, 2021). Manajemen risiko berperan dalam mengidentifikasi ancaman dan menentukan langkah mitigasi yang tepat. Dengan pengelolaan yang baik, keamanan sistem informasi dapat mendukung keandalan dan kepercayaan pengguna terhadap sistem.

Keamanan Jaringan

Keamanan jaringan berfokus pada perlindungan data dan sumber daya yang terhubung melalui jaringan komputer. Jaringan yang tidak aman rentan terhadap serangan seperti penyadapan data, serangan Distributed Denial of Service (DDoS), dan intrusi oleh pihak yang tidak berwenang (Cisco, 2023; Conti et al., 2021). Oleh karena itu, penerapan mekanisme pengamanan seperti firewall, intrusion detection system (IDS), intrusion prevention system (IPS), virtual private network (VPN), serta enkripsi data menjadi sangat penting dalam menjaga keamanan jaringan. Selain itu, segmentasi jaringan dapat membatasi penyebaran serangan dan mengisolasi sistem kritis dari ancaman. Pemantauan lalu lintas jaringan secara real-time membantu mendeteksi aktivitas mencurigakan sebelum menimbulkan kerugian. Pengelolaan kata sandi dan autentikasi multifaktor juga memperkuat perlindungan terhadap akses ilegal. Kebijakan keamanan jaringan yang jelas harus diterapkan agar seluruh pengguna memahami prosedur dan tanggung jawab mereka. Pembaruan perangkat keras dan perangkat lunak jaringan secara berkala penting untuk menutup celah keamanan. Pelatihan kesadaran keamanan bagi staf jaringan dapat mengurangi risiko kesalahan manusia yang sering menjadi pintu masuk serangan. Dengan penerapan strategi keamanan jaringan yang komprehensif, organisasi dapat menjaga kerahasiaan, integritas, dan ketersediaan data yang dikomunikasikan melalui jaringan.

Kriptografi

Kriptografi merupakan teknik pengamanan informasi dengan cara mengubah data asli menjadi bentuk tersandi sehingga tidak dapat dibaca oleh pihak yang tidak berwenang. Kriptografi berperan penting dalam menjaga kerahasiaan dan integritas data, terutama pada komunikasi digital dan transaksi elektronik (Kumar & Somani, 2020; Behl & Behl, 2022). Algoritma kriptografi modern digunakan secara luas dalam sistem keamanan jaringan, aplikasi web, dan penyimpanan data. Selain itu, kriptografi juga digunakan untuk autentikasi, memastikan identitas pengirim dan penerima data dapat diverifikasi dengan benar. Teknik tanda tangan digital dan sertifikat elektronik memanfaatkan kriptografi untuk menjamin keaslian dan integritas informasi. Kriptografi kunci simetris dan kunci publik merupakan dua metode utama yang digunakan dalam enkripsi data. Penggunaan kriptografi yang tepat dapat mencegah serangan seperti penyadapan, pemalsuan data, dan manipulasi informasi. Manajemen kunci yang baik sangat penting untuk menjaga keamanan sistem kriptografi. Kriptografi juga mendukung keamanan dalam penyimpanan data di cloud dan transaksi perbankan online. Seiring berkembangnya teknologi, algoritma kriptografi terus diperbarui untuk menghadapi ancaman baru dari serangan siber yang semakin canggih.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif dengan pendekatan studi pustaka. Metode ini dipilih karena bertujuan untuk mengkaji dan menganalisis konsep serta temuan penelitian terdahulu yang relevan dengan keamanan informasi (Sarker, 2021). Data diperoleh dari 20 referensi ilmiah yang terdiri atas jurnal nasional, jurnal internasional, buku akademik, dan laporan resmi yang diterbitkan pada periode 2020–2025. Literatur yang dikaji dipilih berdasarkan relevansi dengan topik keamanan informasi, keamanan sistem informasi, keamanan jaringan, kriptografi, dan manajemen risiko keamanan. Analisis data dilakukan secara kualitatif dengan mengelompokkan konsep, jenis ancaman, serta solusi keamanan informasi yang dibahas dalam masing-masing referensi. Hasil analisis digunakan sebagai dasar dalam menyusun pembahasan dan kesimpulan penelitian.

Proses studi pustaka ini dimulai dengan identifikasi topik utama dan kata kunci yang relevan. Selanjutnya, setiap referensi dievaluasi dari segi kredibilitas, tahun publikasi, dan kontribusinya terhadap pengembangan keamanan

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

informasi. Setelah literatur terkumpul, informasi yang relevan disusun secara sistematis untuk memudahkan analisis dan interpretasi. Pengelompokan data dilakukan berdasarkan kategori seperti jenis ancaman, teknologi keamanan, dan kebijakan atau prosedur yang diterapkan. Analisis kualitatif memungkinkan peneliti memahami tren, kesenjangan penelitian, serta praktik terbaik dalam bidang keamanan informasi. Metode ini juga membantu mengidentifikasi hubungan antara komponen teknis dan non-teknis dalam pengamanan sistem informasi.

Selain itu, studi pustaka memberikan dasar teoritis yang kuat untuk menyusun rekomendasi praktis bagi organisasi dan pengguna. Setiap temuan dibandingkan dengan penelitian sebelumnya untuk menilai konsistensi dan relevansinya dalam konteks keamanan informasi modern. Penelitian ini juga menyoroti pentingnya integrasi antara teknologi, kebijakan, dan kesadaran pengguna dalam menjaga keamanan informasi. Dengan pendekatan ini, penelitian mampu memberikan gambaran komprehensif tentang konsep, ancaman, dan strategi perlindungan dalam keamanan informasi.

HASIL DAN PEMBAHASAN

Berdasarkan kajian terhadap 20 literatur ilmiah periode 2020–2025, ditemukan bahwa ancaman keamanan informasi terus meningkat baik dari segi jumlah maupun kompleksitas. Ancaman yang paling dominan meliputi *phishing*, *malware*, *ransomware*, kebocoran data, dan serangan jaringan. Temuan ini menunjukkan bahwa keamanan informasi tidak hanya menghadapi risiko teknis, tetapi juga sangat dipengaruhi oleh faktor manusia melalui teknik *social engineering* (Alasmary et al., 2021; ENISA, 2023).

Hasil kajian menunjukkan bahwa penerapan teknologi pengamanan seperti kriptografi, firewall, serta intrusion *detection and prevention system* (IDS/IPS) berperan penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Selain itu, standar keamanan informasi seperti ISO/IEC 27001 memberikan kerangka kerja sistematis dalam pengelolaan risiko keamanan informasi.

Namun demikian, literatur menegaskan bahwa teknologi pengamanan saja belum cukup untuk menjamin keamanan informasi secara menyeluruh. Tanpa kebijakan keamanan yang jelas, prosedur operasional yang konsisten, serta manajemen risiko yang berkelanjutan, sistem informasi tetap rentan terhadap serangan. Hal ini sejalan dengan temuan Microsoft (2024) dan IBM Security (2022) yang menekankan pentingnya pendekatan manajerial dan organisasi.

Kesadaran pengguna juga menjadi faktor krusial dalam efektivitas keamanan informasi. Banyak insiden keamanan terjadi akibat kesalahan manusia, seperti penggunaan kata sandi yang lemah dan kurangnya kewaspadaan terhadap serangan *phishing*. Oleh karena itu, edukasi dan pelatihan keamanan informasi secara berkala diperlukan untuk meminimalkan risiko tersebut.

Selain itu, pemanfaatan teknologi kecerdasan buatan dan *machine learning* terbukti mampu meningkatkan kemampuan deteksi ancaman serta mempercepat respons terhadap insiden keamanan secara proaktif (Nguyen et al., 2023; Rahman et al., 2024). Integrasi antara teknologi, kebijakan, manajemen risiko, dan kesadaran pengguna menjadi kunci penerapan keamanan informasi yang efektif dan berkelanjutan.

Figure

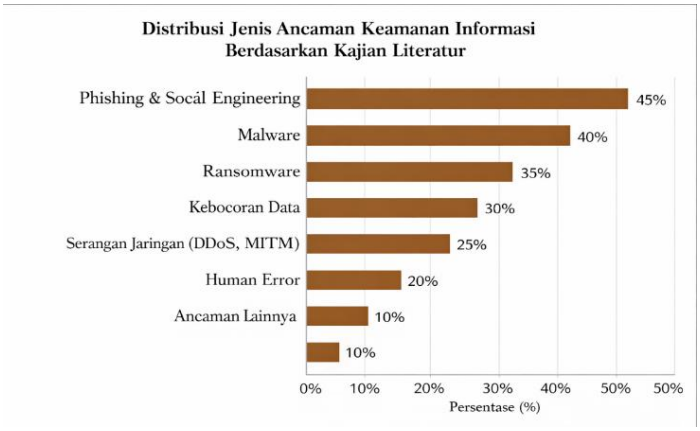

Fig. 1 Distribusi Jenis Ancaman Keamanan Informasi Berdasarkan Kajian Literatur

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Table

Table 1. Ringkasan Hasil Kajian Keamanan Informasi

Aspek Keamanan	Ancaman Utama	Dampak	Strategi Pengamanan
Keamanan Informasi	Phishing,Malware	Kebocoran data	Edukasi pengguna firewall
Keamanan Sistem	Akses tidak sah	Hilangnya integritas	Autentikasi, patch sistem
Keamanan Jaringan	DDos, MITM	Gangguan layanan	IDS/IPS, VPN
Kriptografi	Penyadap-an data	Pelanggaran kerahasiaan	Enkripsi, manajemen kunci
Faktor Manusia	Human error	Insiden keamanan	Pelatihan keamanan

Equations

Persamaan berikut merepresentasikan hubungan konseptual faktor utama dalam keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

$$KI = C + I + A \qquad (1)$$

Keterangan:
KI = Keamanan Informasi;
C = Kerahasiaan;
I = Integritas;
A = Ketersediaan.

Persamaan (1) menunjukkan bahwa keamanan informasi dibentuk oleh kombinasi ketiga prinsip utama tersebut.Untuk menggambarkan pengaruh faktor pendukung, keamanan informasi juga dipengaruhi oleh teknologi, kebijakan, dan kesadaran pengguna, yang dirumuskan sebagai berikut:

$$KI = (C + I + A) \times (T + K + U) \qquad (2)$$

Keterangan:
T = Teknologi Keamanan;
K = Kebijakan dan Manajemen Risiko;
U = Kesadaran Pengguna.

Persamaan (2) menegaskan bahwa keamanan informasi tidak hanya bergantung pada aspek teknis, tetapi juga pada faktor manajerial dan perilaku pengguna.

Implementasi keamanan informasi dapat dilakukan melalui beberapa langkah berikut:

1. Penerapan kebijakan dan standar keamanan informasi untuk memberikan pedoman dan kerangka kerja yang jelas dalam pengelolaan keamanan.
2. Pengamanan sistem dan jaringan komputer melalui firewall, sistem deteksi intrusi (IDS), sistem pencegahan intrusi (IPS), dan pengaturan akses yang tepat.
3. Penggunaan kriptografi untuk perlindungan data, baik saat penyimpanan maupun saat transmisi, guna menjaga kerahasiaan dan integritas informasi.
4. Manajemen risiko keamanan informasi dengan mengidentifikasi ancaman, menganalisis dampaknya, dan menentukan langkah mitigasi yang tepat.
5. Monitoring dan evaluasi sistem secara berkala untuk mendeteksi celah keamanan, menganalisis insiden, dan memperbaiki kelemahan sistem.
6. Edukasi dan peningkatan kesadaran pengguna agar memahami prosedur keamanan dan mengurangi risiko human error.
7. Segmentasi jaringan untuk membatasi penyebaran serangan dan melindungi sistem kritis dari akses tidak sah.
8. Penerapan autentikasi multifaktor untuk memperkuat kontrol akses dan mengurangi risiko penyalahgunaan akun.
9. Backup data secara rutin dan implementasi rencana pemulihan bencana untuk menjamin ketersediaan informasi ketika terjadi gangguan atau serangan.
10. Pemantauan aktivitas pengguna dan sistem secara real-time untuk mendeteksi aktivitas mencurigakan sejak dini.

Tantangan dan Peluang Keamanan Informasi :

Keamanan informasi menghadapi berbagai tantangan, antara lain perkembangan ancaman siber yang sangat cepat, meningkatnya adopsi teknologi baru seperti cloud computing dan Internet of Things (IoT), serta keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber. Tantangan lainnya adalah rendahnya kesadaran pengguna terhadap pentingnya menjaga keamanan informasi.

Di sisi lain, terdapat peluang besar dalam peningkatan keamanan informasi melalui pemanfaatan teknologi baru seperti kecerdasan buatan, machine learning, dan cyber threat intelligence. Pemanfaatan teknologi kecerdasan buatan dapat meningkatkan deteksi serangan dan meningkatkan respons terhadap insiden keamanan (Nguyen et al., 2023;

JIKUM
JURNAL ILMU KOMPUTER

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

Rahman et al., 2024). Penerapan standar dan regulasi keamanan informasi juga memberikan peluang bagi organisasi untuk membangun sistem keamanan yang lebih terstruktur. Dengan memanfaatkan peluang tersebut, organisasi dapat meningkatkan ketahanan sistem informasi secara berkelanjutan.

Selain itu, otomatisasi proses keamanan menggunakan AI dan machine learning dapat mempercepat deteksi dan respons terhadap serangan siber. Pemanfaatan analitik data besar memungkinkan identifikasi pola ancaman yang sebelumnya sulit dikenali. Kolaborasi antar organisasi dan pertukaran informasi ancaman siber meningkatkan kemampuan deteksi dini dan mitigasi risiko. Penerapan kerangka kerja manajemen risiko secara konsisten membantu organisasi fokus pada ancaman yang paling kritis. Pengembangan sumber daya manusia melalui pelatihan dan sertifikasi keamanan siber memperkuat kompetensi internal.

Kesadaran dan edukasi pengguna dapat mengurangi risiko kesalahan manusia yang sering menjadi pintu masuk serangan. Integrasi teknologi keamanan dengan kebijakan dan prosedur organisasi memastikan perlindungan yang lebih menyeluruh. Penggunaan enkripsi dan autentikasi multifaktor memperkuat kerahasiaan dan integritas data. Pemantauan sistem secara real-time memungkinkan respons cepat terhadap insiden keamanan. Dengan memanfaatkan peluang ini secara strategis, organisasi dapat membangun budaya keamanan yang proaktif dan adaptif terhadap ancaman siber yang terus berkembang.

KESIMPULAN

Keamanan dalam bidang informasi merupakan aspek penting dalam menjaga keberlangsungan dan keandalan sistem informasi. Berdasarkan hasil kajian literatur, ancaman keamanan informasi terus berkembang dan menargetkan baik aspek teknis maupun faktor manusia. Oleh karena itu, penerapan keamanan informasi tidak dapat hanya bergantung pada teknologi semata.

Keamanan informasi dipengaruhi oleh berbagai faktor, termasuk pengamanan sistem dan jaringan, penerapan kriptografi, kebijakan dan standar keamanan, manajemen risiko, serta kesadaran pengguna. Pendekatan keamanan yang holistik dan terintegrasi sangat diperlukan agar aset informasi dapat terlindungi secara optimal dan berkelanjutan.

Selain itu, manajemen risiko yang berkelanjutan membantu organisasi dalam mengidentifikasi, menilai, dan memitigasi ancaman yang paling kritis. Pemantauan dan audit keamanan secara rutin memastikan bahwa kebijakan dan prosedur dijalankan dengan konsisten. Penggunaan enkripsi dan autentikasi multifaktor meningkatkan perlindungan terhadap akses tidak sah dan manipulasi data. Segmentasi jaringan dan kontrol akses yang tepat membatasi potensi penyebaran serangan di dalam sistem.

Edukasi dan pelatihan pengguna menjadi kunci dalam membangun budaya keamanan yang kuat. Pemanfaatan teknologi baru seperti kecerdasan buatan dan machine learning dapat meningkatkan kemampuan deteksi ancaman secara proaktif. Kolaborasi antara tim TI, manajemen, dan pihak terkait lainnya memperkuat koordinasi dalam menjaga keamanan informasi. Standar dan regulasi keamanan memberikan pedoman yang jelas bagi organisasi dalam mengelola aset informasi. Backup data dan rencana pemulihan bencana memastikan ketersediaan informasi saat terjadi insiden. Dengan penerapan strategi yang menyeluruh, organisasi dapat menghadapi ancaman siber secara lebih efektif dan menjaga kepercayaan pengguna.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Teknik Informatika, Universitas Malikussaleh, atas dukungan dan fasilitas yang diberikan dalam penyusunan penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pengampu mata kuliah dan seluruh pihak yang telah memberikan arahan, masukan, serta dukungan sehingga penelitian ini dapat diselesaikan dengan baik.

REFERENSI

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.
ISO/IEC. (2022). ISO/IEC 27001: Information Security Management Systems. ISO.
NIST. (2020). Cybersecurity Framework Version 1.1. National Institute of Standards and Technology.
Rahardjo, B. (2020). Keamanan informasi sebagai aset strategis organisasi. Jurnal Teknologi Informasi, 7(1), 1–10.
Nugroho, A. (2021). Implementasi ISO/IEC 27001 dalam sistem manajemen keamanan informasi. Jurnal Sistem Informasi, 17(2), 101–110. Shinta Nurul, A., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi. JEMSI, 3(5), 564–571.
Kaspersky. (2021). IT Security Risks Survey Report. Kaspersky Lab.
IBM Security. (2022). Cost of a Data Breach Report. IBM Corporation.
Cisco. (2023). Cybersecurity Threat Trends Report. Cisco Systems.
Microsoft. (2024). Digital Defense Report. Microsoft Corporation.
Alasmary, W., et al. (2021). Measuring cyber security awareness. Computers & Security, 104, 102211.
Alzahrani, A., & Alomar, N. (2020). Cybersecurity challenges. Journal of Information Security, 11(3), 145–160.

JIKUM
JURNAL ILMU KOMPUTER

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

Behl, A., & Behl, K. (2022). Cybersecurity and cyberwar. Technological Forecasting and Social Change, 175, 121347.
Conti, M., et al. (2021). A survey on man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 23(3), 2021–2048.
Kumar, S., & Somani, G. (2020). Security issues in cloud computing. Journal of Cloud Computing, 9(1), 1–14.
Nguyen, T., et al. (2023). Network intrusion detection using ML. IEEE Access, 11, 55632–55645.
Rahman, A., et al. (2024). Cyber threat intelligence. Future Internet, 16(2), 45.
Singh, J., et al. (2021). Ransomware attacks and mitigation. Journal of Cyber Security Technology, 5(2), 65–82.
Sarker, I. H. (2021). Cybersecurity data science. Computers & Security, 102, 102166.
Zhao, R., et al. (2025). Advances in information security management. Information Systems Frontiers, 27(1), 1–15.