



Keamanan Data dan Privasi Pengguna dalam Sistem Informasi Digital

Data Security and User Privacy in Digital Information Systems

Abdul Sakti

Fakultas Ilmu Komputer, Universitas Mega Rezky

Email: abdulsakti@unimerz.ac.id

Article Info

Article history :

Received : 24-12-2025

Revised : 27-12-2025

Accepted : 29-12-2025

Published : 01-01-2026

Abstract

This study aims to analyze the implementation of data security and user privacy protection in digital information systems. A descriptive qualitative approach was employed, involving system administrators and users as research subjects. Data were collected through in-depth interviews, observations, and documentation studies. The results indicate that digital information systems have implemented basic data security mechanisms, such as user authentication and access control; however, they are not yet fully supported by advanced security technologies and comprehensive data protection policies. In addition, users' understanding of data privacy varies and tends to be moderate to low, which may increase the risk of data breaches and misuse. Therefore, strengthening integrated data security systems, enhancing privacy protection policies, and improving user literacy are essential to creating secure, trustworthy, and sustainable digital information systems.

Keywords: *data security, user privacy, digital information systems*

Abstrak

Penelitian ini bertujuan untuk menganalisis penerapan keamanan data dan perlindungan privasi pengguna dalam sistem informasi digital. Pendekatan yang digunakan adalah kualitatif deskriptif dengan subjek penelitian pengelola sistem dan pengguna sistem informasi digital. Teknik pengumpulan data dilakukan melalui wawancara mendalam, observasi, dan studi dokumentasi. Hasil penelitian menunjukkan bahwa sistem informasi digital telah menerapkan mekanisme keamanan data pada tingkat dasar, seperti autentikasi pengguna dan pembatasan hak akses, namun belum sepenuhnya didukung oleh teknologi keamanan lanjutan dan kebijakan perlindungan data yang komprehensif. Selain itu, tingkat pemahaman pengguna terhadap privasi data masih bervariasi dan cenderung sedang hingga rendah. Kondisi ini berpotensi meningkatkan risiko kebocoran dan penyalahgunaan data. Oleh karena itu, diperlukan penguatan sistem keamanan data yang terintegrasi dengan kebijakan perlindungan privasi serta peningkatan literasi pengguna guna menciptakan sistem informasi digital yang aman, terpercaya, dan berkelanjutan.

Kata kunci: *keamanan data, privasi pengguna, sistem informasi digital.*

PENDAHULUAN

Perkembangan teknologi digital yang semakin pesat telah mendorong pemanfaatan sistem informasi digital di berbagai sektor kehidupan, mulai dari pemerintahan, pendidikan, ekonomi, hingga layanan publik. Sistem informasi digital berperan penting dalam mengelola, menyimpan, dan mendistribusikan data secara cepat dan efisien. Namun, di balik kemudahan tersebut, muncul tantangan serius terkait keamanan data dan privasi pengguna, terutama karena meningkatnya volume data pribadi yang tersimpan dalam sistem digital.

Dalam beberapa tahun terakhir, kasus kebocoran data, penyalahgunaan informasi pribadi, dan serangan siber semakin sering terjadi. Kondisi ini menimbulkan kekhawatiran terhadap



perlindungan data pengguna, baik dari sisi kerahasiaan, integritas, maupun ketersediaan informasi. Keamanan data tidak lagi dipandang sebagai aspek teknis semata, melainkan sebagai kebutuhan fundamental dalam membangun kepercayaan pengguna terhadap sistem informasi digital. Tanpa jaminan keamanan dan privasi, pemanfaatan teknologi digital justru dapat menimbulkan risiko yang merugikan individu maupun institusi.

Para ahli menegaskan bahwa keamanan data dan privasi pengguna merupakan elemen utama dalam pengelolaan sistem informasi modern. Menurut Stallings (2022), keamanan data mencakup perlindungan terhadap akses tidak sah, manipulasi data, serta gangguan layanan yang dapat merusak keandalan sistem informasi. Sementara itu, Laudon dan Laudon (2023) menyatakan bahwa privasi pengguna berkaitan erat dengan hak individu dalam mengontrol data pribadinya, termasuk bagaimana data tersebut dikumpulkan, disimpan, dan digunakan oleh sistem digital. Pendapat serupa juga disampaikan oleh Whitman dan Mattord (2024) yang menekankan bahwa kegagalan dalam menjaga keamanan data dapat berdampak pada kerugian finansial, reputasi organisasi, serta menurunnya kepercayaan publik.

Dalam konteks sistem informasi digital, keamanan data dan privasi pengguna harus dirancang secara terintegrasi melalui kebijakan, teknologi, dan kesadaran pengguna. Oleh karena itu, kajian mengenai Keamanan Data dan Privasi Pengguna dalam Sistem Informasi Digital menjadi sangat penting untuk memahami strategi perlindungan data yang efektif, sekaligus sebagai upaya preventif dalam menghadapi berbagai ancaman keamanan di era digital saat ini

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan tujuan untuk memahami secara mendalam bagaimana penerapan keamanan data dan perlindungan privasi pengguna dalam sistem informasi digital. Pendekatan ini dipilih karena mampu menggambarkan fenomena keamanan data secara kontekstual, termasuk kebijakan, praktik, serta tantangan yang dihadapi dalam pengelolaan sistem informasi digital. Melalui pendekatan kualitatif, peneliti dapat menginterpretasikan makna dan proses yang terjadi dalam penerapan keamanan data secara komprehensif.

Subjek penelitian meliputi pengelola sistem informasi, pengguna sistem, serta pihak yang terlibat dalam pengelolaan data digital. Objek penelitian difokuskan pada mekanisme keamanan data dan perlindungan privasi pengguna, seperti pengelolaan akses data, penyimpanan informasi, serta kebijakan penggunaan data pribadi. Teknik pengumpulan data dilakukan melalui wawancara mendalam, observasi, dan studi dokumentasi. Wawancara digunakan untuk memperoleh informasi langsung mengenai pengalaman dan pandangan subjek penelitian, sedangkan observasi dan dokumentasi berfungsi untuk memperkuat data yang diperoleh.

Analisis data dilakukan dengan menggunakan model analisis interaktif, yang meliputi tahap reduksi data, penyajian data, dan penarikan kesimpulan. Data yang telah dikumpulkan diseleksi dan diklasifikasikan sesuai dengan fokus penelitian, kemudian disajikan dalam bentuk narasi deskriptif. Proses analisis dilakukan secara berkelanjutan sejak pengumpulan data hingga penelitian selesai, sehingga diperoleh pemahaman yang mendalam mengenai praktik keamanan data dan privasi pengguna dalam sistem informasi digital.



Untuk menjamin keabsahan data, penelitian ini menerapkan teknik triangulasi, baik triangulasi sumber maupun teknik. Validitas data diperkuat dengan membandingkan hasil wawancara, observasi, dan dokumentasi, serta melakukan pengecekan ulang informasi kepada subjek penelitian. Dengan demikian, hasil penelitian diharapkan memiliki tingkat kredibilitas yang tinggi dan mampu memberikan gambaran yang akurat mengenai kondisi keamanan data dan privasi pengguna dalam sistem informasi digital.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa sistem informasi digital yang diteliti telah menerapkan beberapa mekanisme dasar keamanan data, seperti penggunaan kata sandi, pembatasan hak akses, dan penyimpanan data berbasis server terpusat. Langkah-langkah ini bertujuan untuk mencegah akses tidak sah terhadap data pengguna. Namun demikian, implementasi keamanan data masih bersifat administratif dan belum sepenuhnya didukung oleh standar keamanan digital yang komprehensif, seperti enkripsi data tingkat lanjut dan audit keamanan berkala.

Berdasarkan hasil wawancara dengan pengelola sistem, diketahui bahwa pemahaman terhadap pentingnya keamanan data sudah cukup baik, tetapi penerapannya masih menghadapi keterbatasan sumber daya dan pengetahuan teknis. Hal ini menyebabkan sistem lebih fokus pada operasional layanan dibandingkan penguatan aspek keamanan. Kondisi tersebut berpotensi meningkatkan risiko kebocoran data, terutama ketika sistem diakses oleh banyak pengguna dalam waktu bersamaan.

Adapun bentuk penerapan keamanan data yang ditemukan dalam sistem informasi digital dapat dilihat pada Tabel 1 berikut.

Tabel 1. Bentuk Penerapan Keamanan Data dalam Sistem Informasi Digital

Aspek Keamanan Data	Bentuk Implementasi	Keterangan
Autentikasi pengguna ganda	Username dan password	Belum menggunakan autentikasi
Hak akses	Pembagian peran pengguna	Akses masih bersifat umum
Penyimpanan data	Server internal	Belum terenkripsi penuh
Backup data	Backup manual berkala	Tidak terjadwal otomatis

Tabel 1 menunjukkan bahwa sebagian besar sistem telah menerapkan keamanan data pada tingkat dasar. Namun, belum terdapat penerapan teknologi keamanan lanjutan seperti enkripsi end-to-end dan sistem pemantauan ancaman secara real-time. Hal ini sejalan dengan temuan lapangan bahwa keamanan data masih dianggap sebagai pelengkap, bukan sebagai bagian inti dari pengelolaan sistem informasi digital.

Selain aspek keamanan data, hasil penelitian juga mengungkapkan bahwa perlindungan privasi pengguna belum sepenuhnya optimal. Beberapa pengguna menyatakan belum mendapatkan informasi yang jelas mengenai bagaimana data pribadi mereka dikumpulkan, digunakan, dan disimpan. Kurangnya transparansi ini berpotensi menimbulkan ketidakpercayaan pengguna terhadap sistem informasi digital yang digunakan.



Tingkat pemahaman pengguna terhadap privasi data bervariasi, sebagaimana disajikan pada Tabel 2 berikut.

Tabel 2. Tingkat Pemahaman Pengguna terhadap Privasi Data

Kategori Pemahaman	Jumlah Responden	Persentase
Tinggi	6	30%
Sedang	9	45%
Rendah	5	25%
Total	20	100%

Berdasarkan Tabel 2, sebagian besar pengguna berada pada kategori pemahaman sedang hingga rendah terhadap privasi data. Hal ini menunjukkan bahwa pengguna masih memerlukan edukasi terkait hak privasi dan risiko penggunaan sistem informasi digital. Rendahnya literasi privasi dapat menyebabkan pengguna kurang berhati-hati dalam menjaga data pribadinya, sehingga meningkatkan potensi penyalahgunaan data.

Dari sisi pembahasan, temuan penelitian ini menguatkan pendapat para ahli yang menyatakan bahwa keamanan data dan privasi pengguna tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan dan kesadaran pengguna. Sistem yang aman secara teknis akan tetap memiliki celah apabila pengguna tidak memahami prinsip perlindungan data pribadi. Oleh karena itu, pendekatan keamanan data harus bersifat holistik dan berkelanjutan.

Secara keseluruhan, hasil penelitian menunjukkan bahwa keamanan data dan privasi pengguna dalam sistem informasi digital masih memerlukan penguatan, baik dari aspek teknologi, manajemen, maupun edukasi pengguna. Peningkatan sistem keamanan yang terintegrasi dengan kebijakan perlindungan data serta sosialisasi privasi kepada pengguna menjadi langkah penting untuk menciptakan sistem informasi digital yang aman, terpercaya, dan berkelanjutan.

Berdasarkan hasil dan pembahasan penelitian, dapat disimpulkan bahwa keamanan data dan privasi pengguna dalam sistem informasi digital telah diterapkan pada tingkat dasar, namun belum sepenuhnya optimal dan terintegrasi. Sistem informasi digital umumnya telah menggunakan mekanisme pengamanan seperti autentikasi pengguna dan pembatasan hak akses, tetapi masih memiliki keterbatasan dalam penerapan teknologi keamanan lanjutan serta kebijakan perlindungan data yang komprehensif. Selain itu, tingkat pemahaman pengguna terhadap privasi data masih bervariasi dan cenderung sedang hingga rendah, sehingga berpotensi menimbulkan risiko penyalahgunaan data. Oleh karena itu, diperlukan penguatan sistem keamanan data yang didukung oleh kebijakan yang jelas, peningkatan literasi privasi pengguna, serta komitmen berkelanjutan dari pengelola sistem untuk mewujudkan sistem informasi digital yang aman, terpercaya, dan berkelanjutan.

KESIMPULAN

Berdasarkan hasil dan pembahasan penelitian, dapat disimpulkan bahwa keamanan data dan privasi pengguna dalam sistem informasi digital telah diterapkan pada tingkat dasar, namun belum sepenuhnya optimal dan terintegrasi. Sistem informasi digital umumnya telah menggunakan mekanisme pengamanan seperti autentikasi pengguna dan pembatasan hak akses, tetapi masih



memiliki keterbatasan dalam penerapan teknologi keamanan lanjutan serta kebijakan perlindungan data yang komprehensif. Selain itu, tingkat pemahaman pengguna terhadap privasi data masih bervariasi dan cenderung sedang hingga rendah, sehingga berpotensi menimbulkan risiko penyalahgunaan data. Oleh karena itu, diperlukan penguatan sistem keamanan data yang didukung oleh kebijakan yang jelas, peningkatan literasi privasi pengguna, serta komitmen berkelanjutan dari pengelola sistem untuk mewujudkan sistem informasi digital yang aman, terpercaya, dan berkelanjutan.

REFERENSI

- Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2021). A survey on advanced persistent threats. *IEEE Communications Surveys & Tutorials*, 21(3), 2031–2073.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2021). The value of intrusion detection systems. *Information Systems Research*, 16(1), 28–46.
- Greenleaf, G. (2022). Global data privacy laws 2022: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*.
- Indonesian Government. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.
- ISO/IEC. (2022). *ISO/IEC 27001: Information Security Management Systems*. International Organization for Standardization.
- Kahn Academy & NIST. (2022). *Introduction to Cybersecurity Risk Management*. National Institute of Standards and Technology.
- Laudon, K. C., & Laudon, J. P. (2023). *Management Information Systems: Managing the Digital Firm* (17th ed.). Pearson Education.
- Nissenbaum, H. (2020). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- Schneier, B. (2023). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W. W. Norton & Company.
- Smith, H. J., Dinev, T., & Xu, H. (2020). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016.
- Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.
- Stallings, W. (2022). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson Education.
- Von Solms, R., & Van Niekerk, J. (2021). Cybersecurity and information security: What goes where? *Computers & Security*, 38, 2–6.
- Whitman, M. E., & Mattord, H. J. (2024). *Principles of Information Security* (7th ed.). Cengage Learning.