e-XXXX-XXXX

Original Article

Studi Keamanan Data Pada Sistem Penyimpanan Lokal Terhadap Ancaman Malware

Wulang Sari[1]✉, Andry Aryshandy[2]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia
Korespondensi Email: wulansarisiddiq@gmail.com

Abstrak:

The rapid development of information technology has increased reliance on digital data in various individual and organizational activities. This condition was accompanied by a growing number of cybersecurity threats, particularly malware attacks targeting local storage systems. Although cloud-based services have continued to expand, local storage was still widely used due to the full control it provided over data. However, such systems showed a high level of vulnerability when they were not supported by adequate security mechanisms. This study aimed to examine data security in local storage systems against malware threats through a literature-based analysis. The research method used was descriptive qualitative with a literature review approach, drawing data from scientific journals, reference books, and cybersecurity reports. The results indicate that malware such as viruses, trojans, spyware, and ransomware poses significant threats to the principles of Confidentiality, Integrity, and Availability (CIA) in local storage systems. Therefore, the implementation of layered data security, through the use of antivirus software, data encryption, access control, regular data backups, and increased user awareness, plays an essential role in minimizing malware risks and maintaining the security of local storage systems.

Kata kunci: Data Security, Data Protection, Local Storage, Malware.e

Pendahuluan

Perkembangan teknologi informasi mendorong peningkatan penggunaan data digital dalam berbagai aktivitas individu maupun organisasi. Data digunakan untuk mendukung proses administrasi, pengelolaan informasi, serta penyimpanan dokumen penting yang bersifat pribadi maupun institusional. Dalam konteks ini, data tidak lagi

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

hanya berfungsi sebagai hasil dari suatu proses, tetapi telah menjadi aset penting yang memiliki nilai strategis. Keberadaan data yang akurat dan terlindungi sangat menentukan keberlangsungan operasional serta kualitas pengambilan keputusan. Oleh karena itu, keamanan data menjadi aspek yang sangat krusial, khususnya pada sistem penyimpanan yang digunakan untuk menampung dan mengelola data tersebut.

Sistem penyimpanan lokal merupakan salah satu media utama dalam penyimpanan data digital. Penyimpanan lokal mencakup perangkat seperti hard disk, solid state drive (SSD), serta media penyimpanan eksternal yang terpasang langsung pada perangkat pengguna. Sistem ini masih banyak digunakan karena memberikan kendali penuh terhadap data, kemudahan dalam pengelolaan, serta akses yang cepat tanpa ketergantungan pada koneksi internet. Selain itu, penyimpanan lokal memungkinkan pengguna untuk mengatur struktur data secara mandiri sesuai kebutuhan. Oleh sebab itu, penyimpanan lokal sering dimanfaatkan untuk menyimpan data penting dan sensitif, seperti dokumen kerja, arsip akademik, data keuangan, dan informasi pribadi lainnya.

Meskipun memiliki berbagai keunggulan, sistem penyimpanan lokal juga memiliki tingkat kerentanan yang cukup tinggi terhadap ancaman keamanan. Salah satu ancaman utama yang sering menyerang penyimpanan lokal adalah malware. Malware merupakan perangkat lunak berbahaya yang dirancang untuk menyusup ke dalam sistem dengan tujuan merusak data, mencuri informasi, atau mengganggu kinerja sistem. Ancaman malware menjadi semakin serius seiring dengan meningkatnya pertukaran data dan penggunaan perangkat digital, karena malware mampu menyebar melalui berbagai media, seperti perangkat USB, file unduhan, serta lampiran email yang terinfeksi.

Ancaman malware terhadap penyimpanan lokal dapat menimbulkan berbagai dampak yang merugikan. Virus dan worm dapat merusak atau menggandakan file, trojan membuka akses tidak sah, spyware mencuri informasi sensitif, dan ransomware mengenkripsi data sehingga tidak dapat diakses pemiliknya. Kondisi ini menunjukkan bahwa malware memiliki kemampuan untuk menyerang langsung data yang tersimpan secara lokal dan menimbulkan kerugian yang signifikan, baik secara teknis maupun non-teknis.

Kurangnya penerapan mekanisme keamanan yang memadai semakin memperbesar risiko serangan malware pada penyimpanan lokal. Banyak pengguna belum menerapkan perlindungan dasar seperti penggunaan antivirus yang diperbarui secara berkala, enkripsi data, serta pengaturan kontrol akses yang baik. Selain itu, rendahnya kesadaran pengguna terhadap praktik keamanan, seperti penggunaan perangkat eksternal tanpa pemindaian dan pengunduhan file dari sumber tidak terpercaya, turut meningkatkan peluang masuknya malware ke dalam sistem penyimpanan lokal.

Laporan Lanskap Keamanan Siber Indonesia 2024 yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa serangan siber masih banyak menargetkan sistem lokal dan server. Insiden ransomware Brain Cipher yang menyerang Pusat Data Nasional Sementara (PDNS) menjadi contoh nyata bahwa ancaman malware tidak hanya berdampak pada jaringan, tetapi juga pada sistem penyimpanan data. Insiden tersebut menegaskan bahwa perlindungan data harus dilakukan secara menyeluruh dan tidak hanya berfokus pada aspek jaringan, tetapi juga pada tingkat penyimpanan lokal.

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

Berdasarkan kondisi tersebut, keamanan data pada sistem penyimpanan lokal terhadap ancaman malware menjadi isu yang penting untuk dikaji secara mendalam. Pemahaman yang baik mengenai jenis-jenis malware, dampaknya terhadap data, serta upaya perlindungan yang dapat diterapkan sangat diperlukan untuk meminimalkan risiko kehilangan dan kerusakan data. Tanpa adanya pengamanan yang memadai, sistem penyimpanan lokal berpotensi menjadi titik lemah dalam sistem informasi secara keseluruhan.

Oleh karena itu, penelitian ini dilakukan untuk mengkaji keamanan data pada sistem penyimpanan lokal terhadap ancaman malware. Fokus penelitian diarahkan pada identifikasi jenis ancaman malware yang berpotensi menyerang penyimpanan lokal, analisis dampaknya terhadap keamanan data berdasarkan prinsip Confidentiality, Integrity, dan Availability, serta pengkajian upaya perlindungan yang dapat diterapkan. Diharapkan hasil penelitian ini dapat memberikan kontribusi akademik serta menjadi referensi dalam meningkatkan kesadaran dan penerapan keamanan data pada sistem penyimpanan lokal.

Metode

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur. Pendekatan ini dipilih untuk memperoleh pemahaman yang komprehensif mengenai keamanan data pada sistem penyimpanan lokal berdasarkan kajian teoritis dan empiris dari berbagai sumber ilmiah yang relevan. Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh dari jurnal ilmiah, buku referensi, prosiding, laporan keamanan siber, serta publikasi lembaga resmi yang membahas topik keamanan data, malware, dan sistem penyimpanan lokal. Pengumpulan data dilakukan melalui studi literatur dan telaah dokumen dengan cara mengidentifikasi, mengelompokkan, serta menganalisis informasi yang berkaitan dengan fokus penelitian. Selanjutnya, analisis data dilakukan secara sistematis melalui proses identifikasi permasalahan, pengkajian konsep keamanan data dan jenis-jenis malware, serta penarikan kesimpulan berdasarkan hasil kajian pustaka yang telah dilakukan.

Hasil dan Pembahasan

Hasil penelitian menunjukkan bahwa penyimpanan lokal masih banyak digunakan untuk menyimpan data penting dan sensitif karena memberikan kontrol penuh kepada pengguna. Data tersebut meliputi dokumen akademik, data administrasi, laporan keuangan, arsip organisasi, serta data pribadi. Tingginya nilai dan sensitivitas data menjadikan sistem penyimpanan lokal sebagai target potensial berbagai ancaman keamanan, khususnya serangan malware.

Meningkatnya ketergantungan terhadap data digital berbanding lurus dengan meningkatnya risiko serangan siber pada penyimpanan lokal. Malware dapat masuk ke dalam sistem melalui berbagai media, seperti perangkat penyimpanan eksternal, unduhan file dari internet, email phishing, serta celah keamanan pada sistem operasi dan aplikasi. Sistem penyimpanan lokal yang tidak dilengkapi mekanisme keamanan yang memadai terbukti memiliki tingkat kerentanan yang tinggi terhadap serangan tersebut. Berdasarkan hasil penelitian, jenis malware yang paling sering menyerang sistem penyimpanan lokal meliputi virus, worm, trojan, spyware, dan ransomware. Virus ditemukan sebagai malware yang paling umum karena menyisipkan diri ke dalam file

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

atau aplikasi lain dan aktif ketika file dijalankan. Worm memiliki kemampuan menyebar secara otomatis melalui jaringan tanpa interaksi pengguna, sedangkan trojan menyamar sebagai aplikasi yang tampak sah namun membuka akses tidak sah ke sistem. Spyware beroperasi secara tersembunyi untuk mengumpulkan data sensitif, sementara ransomware menjadi ancaman paling serius karena mengenkripsi data sehingga tidak dapat diakses.

Serangan malware berdampak langsung terhadap prinsip dasar keamanan informasi, yaitu Confidentiality, Integrity, dan Availability (CIA). Dari aspek confidentiality, malware seperti spyware dan trojan terbukti mampu mencuri data sensitif yang tersimpan secara lokal. Dari aspek integrity, virus dan worm dapat merusak, mengubah, atau menghapus data. Sementara itu, dari aspek availability, ransomware menyebabkan data tidak dapat diakses dalam jangka waktu tertentu atau bahkan secara permanen. Selain faktor teknis, hasil penelitian juga menunjukkan bahwa faktor manusia berperan besar dalam meningkatnya risiko serangan malware. Kebiasaan pengguna yang kurang memperhatikan keamanan, seperti mengunduh file dari sumber tidak terpercaya dan membuka lampiran email mencurigakan, menjadi celah utama masuknya malware ke dalam sistem penyimpanan lokal. Keamanan data pada sistem penyimpanan lokal merupakan aspek yang tidak dapat diabaikan dalam sistem informasi modern. Tingginya intensitas penggunaan penyimpanan lokal tanpa diimbangi dengan penerapan mekanisme keamanan yang memadai meningkatkan potensi terjadinya pelanggaran keamanan data. Kondisi ini menegaskan bahwa kontrol penuh yang dimiliki pengguna atas penyimpanan lokal juga diiringi dengan tanggung jawab penuh terhadap keamanannya.

Temuan mengenai dominasi malware seperti virus, worm, trojan, spyware, dan ransomware menunjukkan bahwa ancaman terhadap penyimpanan lokal bersifat kompleks dan terus berkembang. Virus dan worm tidak hanya berdampak pada kinerja sistem, tetapi juga mengancam integritas data. Trojan dan spyware memperlihatkan bahwa ancaman terhadap kerahasiaan data semakin serius, terutama ketika data tidak dilindungi oleh enkripsi dan kontrol akses yang memadai. Dampak malware terhadap prinsip Confidentiality, Integrity, dan Availability menunjukkan bahwa satu jenis serangan dapat memengaruhi lebih dari satu aspek keamanan informasi. Hal ini memperkuat pandangan bahwa pendekatan keamanan parsial tidak cukup untuk melindungi penyimpanan lokal. Keamanan data harus dipahami sebagai sistem yang saling terintegrasi, bukan sekadar penerapan satu teknologi tertentu.

Penerapan keamanan data pada sistem penyimpanan lokal perlu dilakukan secara berlapis (*defense in depth*). Penggunaan antivirus yang selalu diperbarui merupakan langkah awal yang penting, namun tidak cukup untuk menghadapi malware modern yang semakin canggih. Oleh karena itu, diperlukan mekanisme tambahan seperti enkripsi data, kontrol akses yang ketat, serta sistem pencadangan data yang terencana. Enkripsi data menjadi solusi penting dalam menjaga kerahasiaan data yang tersimpan secara lokal. Dengan enkripsi, data tetap terlindungi meskipun malware berhasil mengakses sistem. Selain itu, kontrol akses berbasis peran membantu membatasi hak pengguna sesuai kebutuhan, sehingga mengurangi risiko penyalahgunaan data dan menjaga integritas informasi.

Dari aspek ketersediaan data, mekanisme pencadangan secara rutin terbukti menjadi langkah paling efektif dalam menghadapi serangan ransomware. Backup yang disimpan pada media terpisah memungkinkan pemulihan data dilakukan tanpa harus

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

memenuhi tuntutan tebusan. Hal ini menunjukkan bahwa availability data sangat bergantung pada kesiapan sistem pemulihan yang dimiliki pengguna atau organisasi. Selain penerapan teknologi, faktor manusia menjadi aspek yang tidak kalah penting dalam pembahasan keamanan data. Rendahnya kesadaran pengguna terhadap keamanan informasi memperbesar peluang masuknya malware. Oleh karena itu, edukasi dan pelatihan keamanan informasi perlu dilakukan secara berkelanjutan agar pengguna mampu menerapkan praktik keamanan yang baik dalam penggunaan penyimpanan lokal.

Selain ancaman malware, faktor kelalaian pengguna juga menjadi salah satu penyebab utama terjadinya kebocoran dan kerusakan data pada sistem penyimpanan lokal. Penggunaan perangkat lunak tidak resmi, keterlambatan pembaruan sistem, serta lemahnya pengelolaan kata sandi meningkatkan peluang eksploitasi oleh pihak tidak bertanggung jawab. Kondisi ini menunjukkan bahwa keamanan data tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada kesadaran dan perilaku pengguna dalam mengelola data. Di sisi lain, penerapan mekanisme pengamanan berlapis pada penyimpanan lokal menjadi langkah penting untuk meminimalkan risiko serangan. Penggunaan antivirus, firewall, serta enkripsi data mampu memberikan perlindungan tambahan terhadap akses tidak sah dan aktivitas berbahaya. Namun, efektivitas mekanisme tersebut sangat bergantung pada konsistensi penerapan dan pemeliharaan sistem keamanan secara berkala.

Lebih lanjut, prinsip kerahasiaan, integritas, dan ketersediaan data perlu dijadikan dasar dalam pengelolaan penyimpanan lokal. Kerahasiaan menjamin bahwa data hanya dapat diakses oleh pihak yang berwenang, integritas memastikan data tetap akurat dan tidak berubah tanpa izin, sedangkan ketersediaan menjamin data dapat diakses ketika dibutuhkan. Ketiga prinsip ini saling berkaitan dan harus diterapkan secara seimbang agar keamanan data dapat terjaga secara optimal.

Kesimpulan

Keamanan data pada sistem penyimpanan lokal merupakan aspek krusial dalam pengelolaan sistem informasi karena seluruh tanggung jawab pengamanan berada pada pengguna atau organisasi. Sistem ini memiliki tingkat kerentanan yang tinggi terhadap ancaman malware, seperti virus, trojan, spyware, dan ransomware, yang dapat mengganggu prinsip Confidentiality, Integrity, dan Availability (CIA). Ancaman tersebut tidak hanya disebabkan oleh kelemahan teknis, tetapi juga oleh faktor manusia serta kurangnya kebijakan keamanan yang terstruktur. Oleh karena itu, diperlukan penerapan keamanan berlapis melalui antivirus, enkripsi data, kontrol akses, dan pencadangan data, disertai peningkatan kesadaran dan edukasi pengguna untuk meminimalkan risiko serangan malware.

Saran

Berdasarkan tujuan penelitian, disarankan agar pengguna dan organisasi meningkatkan pengamanan sistem penyimpanan lokal untuk melindungi data dari ancaman malware. Upaya yang dapat dilakukan meliputi penggunaan perlindungan keamanan yang sesuai, pengelolaan akses data yang lebih baik, serta pencadangan data secara berkala. Selain itu, diperlukan peningkatan kesadaran pengguna dalam menerapkan perilaku aman saat mengelola dan menyimpan data digital.

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

Daftar Pustaka

Awan Pintar. (2025). *Laporan ancaman digital semester I 2025*.

Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia 2024*. Badan Siber dan Sandi Negara.

Fitria, G., Dhini, A., Purba, A. V., Cindiasyahwa, D., & Gunawan, I. (2025). Ilmu keamanan sistem informasi dalam mengatasi ancaman, kerentanan, dan penanggulangan di dalam penggunaan perangkat. *Gudang Jurnal Multidisiplin Ilmu Keamanan Sistem Informasi*, 3(1):26–31.

Gunawan, I. (2021). *Keamanan data: Teori dan implementasi*. CV Jejak, Bandung.

No, V., Hal, J., Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya sistem keamanan database untuk melindungi data pribadi. 1(2):44–47.

Prasetyo, F., Putra, E., Zulfikri, A., & Huda, M. A. (2023). Analisis keamanan jaringan dari serangan malware menggunakan firewall filtering dengan port blocking. 3(2):857–863.

Sulianta, F. (2025). *Malware*. Feri Sulianta.

Ventures, C. (2025). Konsep keamanan data dalam jaringan. *Journal of Innovative and Creativity*, 5(2):497–505.

Widiyasono, N. (2025). *Pengantar ilmu analisa malware*. Literasi Langsung Terbit, Padang.

Wisnu, M. (n.d.). Pentingnya antivirus dalam melindungi data pribadi dan keamanan siber di era digital.

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026