E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 10 No 7 Tahun 2025

SERANGAN SIBER DAN DAMPAKNYA TERHADAP INFRASTRUKTUR DIGITAL

M Rizki Anugrah[1], Edo Ramadhan[2] , Tata Sutabri
Universitas Bina Darma
e-mail: rizkianugrah1702@gmail.com[1], edoramadhan123@gmail.com[2])

Abstract
The rapid development of information and communication technology has accelerated digital transformation across various sectors, including government, industry, education, and public services. Digital infrastructure has become a critical backbone supporting these activities. However, the increasing reliance on digital systems is accompanied by a growing risk of cyber attacks. Cyber attacks such as malware, ransomware, phishing, and Distributed Denial of Service (DDoS) can disrupt service availability, compromise data integrity, and threaten information confidentiality. The impact of cyber attacks on digital infrastructure extends beyond technical damage, leading to significant economic losses, decreased public trust, and potential threats to national security. This article aims to examine common types of cyber attacks and analyze their impact on the stability and reliability of digital infrastructure. Furthermore, it highlights the importance of implementing comprehensive cybersecurity strategies that encompass technological measures, policy frameworks, and human resource awareness. Through effective prevention and mitigation efforts, cyber risks can be reduced, enabling digital infrastructure to operate securely and sustainably.
Keywords: *Cyber attack, Cyber security, Digital insfratucture*

Abstrak
Perkembangan teknologi informasi dan komunikasi telah mendorong percepatan digitalisasi di berbagai sektor, termasuk pemerintahan, industri, pendidikan, dan layanan publik. Infrastruktur digital menjadi tulang punggung utama dalam mendukung aktivitas tersebut. Namun, meningkatnya ketergantungan terhadap sistem digital juga diikuti oleh tingginya risiko serangan siber. Serangan siber seperti malware, ransomware, phishing, dan Distributed Denial of Service (DDoS) dapat mengganggu ketersediaan layanan, merusak integritas data, serta mengancam kerahasiaan informasi. Dampak serangan siber terhadap infrastruktur digital tidak hanya bersifat teknis, tetapi juga menimbulkan kerugian ekonomi, penurunan kepercayaan publik, serta potensi ancaman terhadap keamanan nasional. Artikel ini bertujuan untuk mengkaji jenis-jenis serangan siber yang umum terjadi serta menganalisis dampaknya terhadap stabilitas dan keandalan infrastruktur digital. Selain itu, dibahas pula pentingnya penerapan strategi keamanan siber yang komprehensif, mencakup aspek teknologi, kebijakan, dan peningkatan kesadaran sumber daya manusia. Dengan upaya pencegahan dan mitigasi yang tepat, risiko serangan siber dapat diminimalkan sehingga infrastruktur digital dapat berfungsi secara aman dan berkelanjutan.
Kata Kunci: Serangan siber, Keamanan siber, infrastruktur digital

Article History
Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Plagiarism Checker No 793
Prefix DOI : Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Digitalisasi telah diterapkan secara luas pada sektor pemerintahan, industri, pendidikan, kesehatan, dan layanan publik, sehingga infrastruktur digital menjadi komponen vital dalam menunjang aktivitas sehari-hari. Ketergantungan yang semakin tinggi terhadap sistem digital menjadikan keandalan, ketersediaan, dan keamanan infrastruktur digital sebagai faktor yang sangat penting.(Ear et al., 2025)

Namun, di balik manfaat yang ditawarkan, perkembangan teknologi digital juga menghadirkan berbagai tantangan, salah satunya adalah meningkatnya ancaman serangan siber. Serangan siber dapat dilakukan dalam berbagai bentuk, seperti malware, ransomware, phishing, dan Distributed Denial of Service (DDoS), yang bertujuan untuk mencuri data, merusak sistem, atau melumpuhkan layanan digital. Ancaman ini tidak hanya menargetkan organisasi besar, tetapi juga institusi pendidikan, usaha kecil, hingga pengguna individu.(Reddy, 2025)

Dampak serangan siber terhadap infrastruktur digital sangat luas, mencakup gangguan operasional, kebocoran data, kerugian ekonomi, serta menurunnya kepercayaan masyarakat terhadap layanan digital. Dalam skala yang lebih besar, serangan siber terhadap infrastruktur kritis bahkan dapat mengancam stabilitas dan keamanan nasional. Oleh karena itu, pemahaman mengenai serangan siber dan dampaknya terhadap infrastruktur digital menjadi hal yang penting sebagai dasar dalam merumuskan strategi pencegahan dan penguatan keamanan siber di era digital.(Sendjaja et al., 2024)

KAJIAN LITERATUR

1. Konsep Serangan Siber

Serangan siber merupakan aktivitas yang dilakukan secara sengaja untuk mengganggu, merusak, atau mengambil alih sistem komputer dan jaringan tanpa izin. Menurut beberapa ahli, serangan siber bertujuan untuk mengeksploitasi celah keamanan pada sistem informasi guna memperoleh data, keuntungan finansial, atau kepentingan tertentu.(Huang et al., 2025) Serangan siber dapat dilakukan oleh individu, kelompok terorganisir, maupun aktor negara dengan tingkat kompleksitas yang beragam. Seiring dengan perkembangan teknologi, metode serangan siber juga semakin canggih dan sulit dideteksi.(Ogunsanya et al., 2025)

2. Jenis-Jenis Serangan Siber

Literatur menunjukkan bahwa terdapat berbagai jenis serangan siber yang umum terjadi. Malware merupakan perangkat lunak berbahaya yang dirancang untuk merusak atau mengendalikan sistem.(Syah et al., 2025) Ransomware adalah bentuk malware yang mengenkripsi data korban dan meminta tebusan agar data dapat dipulihkan. Phishing dilakukan dengan cara memanipulasi pengguna agar memberikan informasi sensitif melalui pesan atau situs palsu. Selain itu, serangan Distributed Denial of Service (DDoS) bertujuan untuk melumpuhkan layanan dengan membanjiri server menggunakan lalu lintas data dalam jumlah besar. Keempat jenis serangan ini sering menjadi ancaman utama bagi infrastruktur digital.(Tommy and Nasution, n.d.)

3. Infrastruktur Digital

Infrastruktur digital mencakup seluruh komponen teknologi yang mendukung pengelolaan dan pertukaran informasi secara elektronik, seperti jaringan komputer, pusat data, sistem cloud, perangkat lunak, dan sistem keamanan informasi. Infrastruktur digital berperan penting dalam menjaga keberlangsungan layanan digital dan efisiensi operasional suatu organisasi. Keandalan infrastruktur digital sangat bergantung pada sistem keamanan yang diterapkan serta kemampuan dalam mengelola risiko teknologi.(Swandanang et al., 2025)

4. Dampak Serangan Siber terhadap Infrastruktur Digital

Beberapa penelitian menyebutkan bahwa serangan siber dapat menyebabkan gangguan layanan, kerusakan sistem, dan kebocoran data yang berdampak luas. Selain kerugian finansial, organisasi juga menghadapi penurunan reputasi dan kepercayaan publik. Pada infrastruktur kritis, serangan siber berpotensi mengganggu layanan penting seperti energi, transportasi, dan komunikasi. Oleh karena itu, serangan siber dipandang sebagai ancaman serius yang memerlukan perhatian khusus.(Ilaina and Nugraha, 2025)

5. Upaya Keamanan dan Mitigasi Serangan Siber

Literatur terkait keamanan siber menekankan pentingnya pendekatan multidimensi dalam menghadapi serangan siber. Upaya mitigasi meliputi penerapan teknologi keamanan seperti firewall, sistem deteksi intrusi, enkripsi data, serta pembaruan sistem secara berkala. Selain itu, kebijakan keamanan dan peningkatan kesadaran sumber daya manusia melalui pelatihan juga menjadi faktor penting dalam memperkuat pertahanan infrastruktur digital.(Khairunnisa et al., n.d.)

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan pendekatan kualitatif deskriptif. Metode ini dipilih untuk memperoleh pemahaman yang komprehensif mengenai serangan siber serta dampaknya terhadap infrastruktur digital berdasarkan kajian dari berbagai sumber ilmiah yang relevan.

1. Jenis dan Pendekatan Penelitian

Jenis penelitian yang digunakan adalah penelitian kualitatif deskriptif. Pendekatan ini bertujuan untuk mendeskripsikan fenomena serangan siber secara sistematis dan mendalam tanpa melakukan pengujian hipotesis secara kuantitatif. Fokus penelitian diarahkan pada analisis konsep, jenis, serta dampak serangan siber terhadap infrastruktur digital.

2. Teknik Pengumpulan Data

Data penelitian diperoleh melalui studi literatur yang bersumber dari buku teks, artikel jurnal ilmiah, prosiding konferensi, laporan resmi lembaga terkait, serta publikasi daring yang membahas keamanan siber dan infrastruktur digital. Sumber-sumber tersebut dipilih berdasarkan relevansi, kredibilitas, dan keterkinian informasi.

3. Teknik Analisis Data

Data yang telah dikumpulkan dianalisis menggunakan teknik analisis deskriptif-kualitatif. Proses analisis dilakukan dengan cara mengelompokkan informasi berdasarkan tema, seperti jenis serangan siber, dampak terhadap infrastruktur digital, dan upaya mitigasi. Selanjutnya, data dianalisis untuk menemukan pola, hubungan, dan implikasi yang berkaitan dengan keamanan infrastruktur digital.

4. Prosedur Penelitian

Prosedur penelitian diawali dengan identifikasi topik dan perumusan tujuan penelitian. Tahap selanjutnya adalah pengumpulan literatur yang relevan, kemudian dilakukan penelaahan dan pencatatan informasi penting. Setelah itu, dilakukan analisis data dan penyusunan hasil kajian secara sistematis agar mudah dipahami dan sesuai dengan tujuan penelitian.

5. Batasan Penelitian

Penelitian ini dibatasi pada pembahasan serangan siber secara umum dan dampaknya terhadap infrastruktur digital berdasarkan sumber literatur yang tersedia. Penelitian ini tidak melibatkan pengumpulan data lapangan atau analisis teknis mendalam terhadap sistem tertentu.

PEMBAHASAN

Berdasarkan hasil analisis data yang diperoleh dari berbagai sumber literatur ilmiah, laporan keamanan siber, dan penelitian terdahulu, ditemukan bahwa serangan siber merupakan ancaman yang terus meningkat seiring dengan berkembangnya infrastruktur digital. Jenis serangan siber yang paling dominan meliputi malware, ransomware, phishing, dan Distributed Denial of Service (DDoS). Serangan-serangan tersebut terbukti berdampak langsung terhadap ketersediaan layanan, integritas data, dan kerahasiaan informasi dalam sistem digital.

Hasil kajian juga menunjukkan bahwa infrastruktur digital dengan tingkat keamanan yang rendah lebih rentan mengalami gangguan operasional dan kebocoran data. Organisasi yang belum menerapkan pembaruan sistem secara berkala serta minim pelatihan keamanan siber bagi sumber daya manusia cenderung mengalami dampak serangan yang lebih besar. Selain itu, sektor-sektor yang mengelola data penting dan infrastruktur kritis memiliki risiko yang lebih tinggi apabila tidak didukung oleh sistem keamanan yang memadai.

1. Analisis Kajian

Analisis kajian dilakukan dengan mengaitkan hasil pemaparan data dengan teori dan temuan penelitian sebelumnya. Berdasarkan teori keamanan informasi, kerentanan sistem sering kali tidak hanya disebabkan oleh kelemahan teknis, tetapi juga oleh faktor manusia dan kebijakan organisasi. Hal ini sejalan dengan hasil kajian yang menunjukkan bahwa serangan phishing masih efektif karena rendahnya kesadaran pengguna terhadap keamanan siber.

Penelitian sebelumnya juga menyatakan bahwa serangan siber terhadap infrastruktur digital dapat menimbulkan dampak multidimensional, mulai dari gangguan teknis hingga kerugian ekonomi dan sosial. Temuan tersebut diperkuat oleh hasil kajian ini yang menunjukkan adanya hubungan antara intensitas serangan siber dan menurunnya kepercayaan pengguna terhadap layanan digital. Dengan demikian, dapat disimpulkan bahwa penguatan infrastruktur digital tidak hanya memerlukan teknologi keamanan yang canggih, tetapi juga pendekatan strategis yang mencakup kebijakan, manajemen risiko, dan peningkatan kompetensi sumber daya manusia.

Secara keseluruhan, hasil dan analisis kajian ini memberikan jawaban atas permasalahan penelitian dengan membuktikan bahwa serangan siber memiliki dampak signifikan terhadap keandalan infrastruktur digital. Oleh karena itu, diperlukan upaya mitigasi yang komprehensif dan berkelanjutan untuk meningkatkan ketahanan infrastruktur digital terhadap ancaman siber.

KESIMPULAN

Berdasarkan hasil kajian dan analisis yang telah dilakukan, dapat disimpulkan bahwa serangan siber merupakan ancaman nyata dan terus berkembang terhadap infrastruktur digital. Berbagai jenis serangan siber, seperti malware, ransomware, phishing, dan Distributed Denial of Service (DDoS), terbukti dapat mengganggu ketersediaan layanan, merusak integritas data, serta mengancam kerahasiaan informasi. Dampak yang ditimbulkan tidak hanya bersifat teknis, tetapi juga mencakup kerugian ekonomi, penurunan kepercayaan pengguna, serta potensi gangguan terhadap stabilitas layanan publik dan infrastruktur kritis.

Hasil penelitian menunjukkan bahwa tingkat kerentanan infrastruktur digital sangat dipengaruhi oleh kualitas sistem keamanan, kebijakan organisasi, dan kesadaran sumber daya manusia. Infrastruktur digital yang tidak dilengkapi dengan mekanisme keamanan yang memadai dan pengelolaan risiko yang baik cenderung lebih rentan terhadap serangan siber dan mengalami dampak yang lebih besar. Oleh karena itu, penguatan keamanan siber perlu dilakukan secara komprehensif melalui penerapan teknologi keamanan yang tepat, pembaruan sistem secara berkala, peningkatan literasi keamanan siber, serta dukungan kebijakan dan regulasi yang jelas.

Dengan penerapan strategi mitigasi yang terintegrasi dan berkelanjutan, ketahanan infrastruktur digital terhadap serangan siber dapat ditingkatkan sehingga mampu mendukung transformasi digital secara aman dan berkelanjutan.

DAFTAR PUSTAKA

Ear, E., Remy, J.L.C., Chang, C., Que, Q., Feffer, A., Xu, S., 2025. Characterizing Cyber Attacks against Space Infrastructures with Missing Data: Framework and Case Study. https://doi.org/10.48550/arXiv.2512.02414

Huang, S., Poskitt, C.M., Shar, L.K., 2025. Security Modelling for Cyber-Physical Systems: A Systematic Literature Review. ACM Trans. Cyber-Phys. Syst. 3776549. https://doi.org/10.1145/3776549

Ilaina, A.S.A., Nugraha, I.F., 2025. KESENJANGAN KAPABILITAS KEAMANAN SIBER INDONESIA DALAM MITIGASI SERANGAN SIBER PADA LAYANAN PUBLIK DIGITAL TAHUN 2020-2025. Open Access 8.

Khairunnisa, P.A., Annisa, N., Parhusip, J., n.d. Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia.

Ogunsanya, V.A., Adesokan, A., Eleweke, I., Udoka, A., Afolabi, R., Abbas, R., 2025. Cybersecurity Incidents on Digital Infrastructure and Industrial Networks 34.

Reddy, R.P., 2025. Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age. IJCTT 73, 7–17. https://doi.org/10.14445/22312803/IJCTT-V73I2P102

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., Fatmawati, E., 2024. Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. IJSOC 6, 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

Swandanang, I., Aulya, M.Z., Wijaya, N., 2025. Keamanan Siber dalam Era Digital : Tantangan dan Solusi dengan Zero Trust Architecture 8.

Syah, E., Weharima, H., Susilo, T., Basuki, T., Akad, A.M., 2025. Serangan Siber terhadap Infrastruktur Kritis: Ancaman Bagi Keamanan dan Kesejahteraan Masyarakat. JSIM 6, 145–154. https://doi.org/10.54543/syntaximperatif.v6i2.678

Tommy, S., Nasution, M.I.P., n.d. Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN).