



PELATIHAN KEAMANAN JARINGAN WIFI DAN INTERNET DI SEKOLAH

Adelya Pasya Nuraini ^{1*}, Amanda Depina ², Jesika Delistira ³

^{1,2,3}Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negri Sulthan Thaha Saifuddin Jambi

E-mail: adelyapasya18@gmail.com^{1*}, amandadepina05@gmail.com², delistirajesika@gmail.com³

ABSTRACT

The use of Wi-Fi and internet networks in schools has become essential for supporting digital learning, yet it is accompanied by increasing security risks. This study employs a literature review method to analyze network vulnerabilities in educational environments without involving specific research objects or locations. The findings indicate that low user security literacy, weak network configurations, and threats such as sniffing and unauthorized access are the main sources of vulnerability. The implementation of updated encryption, network segmentation, password management, and security training for teachers and students is required. These strategies can enhance network security and support safer and more effective digital learning processes.

Keywords: Network security, school Wi-Fi, cyber threats, network encryption, internet security.

ABSTRAK

Penggunaan jaringan Wi-Fi dan internet di sekolah semakin penting untuk mendukung pembelajaran digital, namun diiringi oleh meningkatnya risiko keamanan. Penelitian ini menggunakan metode studi literatur untuk menganalisis kerentanan jaringan sekolah tanpa melibatkan objek atau lokasi penelitian. Hasil kajian menunjukkan bahwa rendahnya literasi keamanan pengguna, lemahnya konfigurasi jaringan, serta ancaman seperti sniffing dan akses ilegal menjadi faktor utama kerentanan. Diperlukan penerapan enkripsi terbaru, segmentasi jaringan, manajemen kata sandi, serta pelatihan keamanan bagi guru dan siswa. Implementasi strategi tersebut dapat meningkatkan keamanan jaringan dan mendukung proses pembelajaran yang lebih aman dan efektif.

Kata Kunci: Keamanan jaringan, Wi-Fi sekolah, ancaman siber, enkripsi jaringan, keamanan internet.

Article History

Received: November 2025

Reviewed: November 2025

Published: November 2025

Plagiarism Checker No 235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)



1. PENDAHULUAN

Kemajuan teknologi informasi telah membawa perubahan besar dalam dunia pendidikan, terutama melalui penggunaan internet sebagai media pembelajaran. Salah satu fasilitas yang mendukung proses tersebut adalah jaringan Wi-Fi, yang memberikan akses cepat dan mudah ke berbagai sumber belajar daring. Di lembaga pendidikan, Wi-Fi menjadi salah satu infrastruktur penting yang digunakan untuk mendukung kegiatan pembelajaran berbasis teknologi (Ali, 2022).

Di era pembelajaran abad ke-21, infrastruktur jaringan komputer dan konektivitas internet merupakan komponen penting yang menunjang kegiatan belajar mengajar di sekolah seperti pembelajaran online. Menurut Moore et al., (2011) dalam penelitian (Firman F & Rahayu, 2020) mengungkapkan bahwa pembelajaran online merupakan kegiatan belajar mengajar yang membutuhkan jaringan internet dengan aksesibilitas, konektivitas, fleksibilitas, dan kemampuan untuk memunculkan berbagai jenis interaksi dalam proses pembelajaran. Sehingga jaringan internet sebagai salah satu komponen yang harus dipersiapkan oleh sekolah dalam menunjang pembelajarannya.

Namun, kemudahan akses Wi-Fi juga diiringi dengan tantangan keamanan yang semakin kompleks. Serangan siber, seperti pencurian data, akses tidak sah, dan eksploitasi jaringan, dapat terjadi jika keamanan jaringan tidak dikelola dengan baik. Hal ini meningkatkan risiko ancaman terhadap data pengguna dan kestabilan jaringan (S Faisal, 2021).

Selain itu, rendahnya pengetahuan pengguna tentang praktik keamanan jaringan memperburuk situasi. Sebagian besar pengguna tidak memahami pentingnya menjaga kerahasiaan kata sandi, memperbarui perangkat, atau menggunakan perangkat yang aman. Hal ini dapat membuka peluang bagi pihak yang tidak bertanggung jawab untuk mengakses jaringan secara ilegal.

Melalui penelitian ini, analisis dilakukan untuk mengidentifikasi tingkat keamanan jaringan Wi-Fi dan Internet, baik dari sisi teknis maupun perilaku pengguna. Temuan dari penelitian ini diharapkan dapat memberikan rekomendasi yang relevan untuk meningkatkan keamanan jaringan Wi-Fi di lingkungan sekolah, sehingga dapat mendukung pembelajaran berbasis teknologi secara lebih aman dan efektif (Sarjanoko, 2022)

Kesimpulan dari penelitian ini ditujukan untuk membantu sekolah meningkatkan keamanan jaringan, sehingga memungkinkan mereka menciptakan lingkungan belajar yang aman dan terlindungi dari segala ancaman digital.



2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur (*library research*) untuk mengkaji isu-isu tentang keamanan menjaga keamanan jaringan Wi-Fi dan internet khususnya di lingkungan sekolah. Metode ini dipilih karena sesuai dalam menggali pemahaman yang mendalam yang berasal dari berbagai sumber ilmiah tanpa melakukan pengumpulan data primer di lapangan.

Sumber data dalam penelitian ini adalah data sekunder yang berasal dari dokumen akademik terpercaya dan tersedia secara daring. Karena tidak melibatkan observasi langsung atau eksperimen di lapangan, maka penelitian ini tidak memiliki lokasi fisik yang spesifik, seluruh proses dilakukan secara daring dan literatur yang digunakan berasal dari berbagai konteks global, sehingga lokasi penelitian bersifat universal.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil telaah literatur dan analisis terhadap kondisi keamanan jaringan Wi-Fi di lingkungan sekolah, dapat disimpulkan bahwa masih terdapat berbagai permasalahan mendasar yang berkaitan dengan rendahnya pemahaman pengguna, tingginya potensi ancaman, serta kurang optimalnya penerapan kebijakan keamanan jaringan. Temuan ini menjadi dasar penyusunan pembahasan berikut yang menguraikan secara rinci tingkat pemahaman pengguna, identifikasi ancaman, pengelolaan keamanan, kebutuhan pelatihan, serta implementasi strategi keamanan dalam mendukung pembelajaran digital.

3.1 Tingkat Pemahaman Pengguna terhadap Keamanan Jaringan

Berdasarkan telaah literatur, tingkat pemahaman pengguna khususnya siswa dan tenaga pendidik terhadap keamanan jaringan masih tergolong rendah. Banyak pengguna belum memahami pentingnya menjaga kerahasiaan kata sandi Wi-Fi, penggunaan autentikasi yang kuat, serta melakukan pembaruan sistem operasi pada perangkat. Kondisi ini sejalan dengan temuan Sulaiman (2021), yang menyatakan bahwa rendahnya literasi keamanan menjadi salah satu faktor meningkatnya ancaman siber pada jaringan pendidikan.

Kurangnya pengetahuan mengenai langkah-langkah keamanan dasar tersebut menyebabkan tingginya peluang terjadinya akses ilegal serta eksploitasi jaringan, baik oleh pihak internal maupun eksternal sekolah.



3.2 Identifikasi Ancaman dan Risiko Pada Jaringan Wi-Fi Sekolah

Hasil analisis literatur menunjukkan bahwa jaringan Wi-Fi sekolah merupakan salah satu target mudah bagi serangan siber. Beberapa ancaman umum yang sering terjadi antara lain *sniffing*, *brute force*, dan *rogue access point*, terutama ketika jaringan tidak dilindungi dengan protokol keamanan yang memadai (Faisal, 2021).

Selain itu, perangkat siswa yang tidak memiliki perlindungan antivirus berpotensi menjadi sumber masuknya malware ke dalam jaringan sekolah. Risiko lain yang mungkin muncul meliputi kebocoran data pengguna, seperti identitas, riwayat aktivitas *browsing*, hingga informasi akademik. Hal ini menunjukkan perlunya penerapan kebijakan keamanan yang lebih komprehensif untuk menutup berbagai celah kerentanan tersebut (Sarjanoko, 2022).

3.3 Pengelolaan Keamanan Jaringan di Lingkungan Sekolah

Pengelolaan keamanan jaringan di sekolah tidak hanya bergantung pada aspek teknis, tetapi juga pada kebijakan serta perilaku pengguna. Beberapa mekanisme yang perlu diterapkan meliputi penggunaan WPA3 sebagai standar enkripsi terbaru untuk mencegah akses tidak sah, penerapan segmentasi jaringan antara guru, siswa, dan tamu guna meminimalkan risiko serangan lintas segmen, serta manajemen kata sandi melalui penggantian berkala dan penggunaan kombinasi karakter yang kuat. Penelitian Ali (2022). menegaskan bahwa upaya ini harus didukung oleh kebijakan resmi sekolah dan pelatihan rutin agar keamanan jaringan dapat terjaga secara berkelanjutan.

3.4 Pentingnya Pelatihan Keamanan Jaringan Wi-Fi dan Internet

Pelatihan keamanan jaringan Wi-Fi dan internet merupakan rekomendasi utama untuk meningkatkan keamanan jaringan sekolah karena terbukti mampu meningkatkan pemahaman pengguna terhadap berbagai ancaman digital serta mendorong kemampuan mereka dalam menerapkan praktik penggunaan jaringan yang aman (Firman & Rahayu, 2020). Materi pelatihan yang perlu diberikan mencakup pembuatan dan pengelolaan kata sandi yang kuat, pengenalan ancaman seperti *phishing* dan *malware*, langkah pengamanan perangkat sebelum terhubung ke jaringan sekolah, serta edukasi mengenai etika penggunaan internet. Pelatihan yang dilakukan secara terstruktur dan berkelanjutan akan membantu sekolah membangun budaya keamanan digital yang lebih baik.



3.5 Implementasi Strategi Keamanan dalam Mendukung Pembelajaran Digital

Implementasi strategi keamanan memiliki peran penting dalam mendukung pembelajaran digital karena Wi-Fi merupakan infrastruktur utama yang digunakan dalam proses belajar mengajar. Penerapan keamanan jaringan yang baik dapat mengurangi risiko *downtime* akibat serangan siber, melindungi data akademik, serta meningkatkan kepercayaan guru dan siswa terhadap sistem digital sekolah. Penelitian menunjukkan bahwa sekolah yang menerapkan kebijakan keamanan ketat memiliki tingkat keandalan jaringan yang lebih tinggi, sehingga proses pembelajaran digital dapat berlangsung lebih efektif (Moore et al., 2011) dalam (Firman & Rahayu, 2020).

KESIMPULAN

Berdasarkan hasil kajian, dapat disimpulkan bahwa keamanan jaringan Wi-Fi di sekolah masih perlu ditingkatkan karena pemahaman pengguna yang rendah dan konfigurasi jaringan yang belum optimal. Ancaman seperti *sniffing*, *brute force*, dan akses ilegal muncul akibat lemahnya pengelolaan keamanan. Untuk itu, sekolah perlu menerapkan enkripsi terbaru, segmentasi jaringan, serta manajemen kata sandi yang baik, yang harus didukung oleh kebijakan dan pengawasan berkelanjutan. Pelatihan keamanan bagi guru dan siswa juga terbukti penting untuk meningkatkan literasi digital dan mendorong perilaku penggunaan jaringan yang aman. Implementasi strategi keamanan yang tepat akan meningkatkan keandalan jaringan, melindungi data, serta mendukung kelancaran pembelajaran digital di lingkungan sekolah.

DAFTAR PUSTAKA

- [1] Ali, M. (2022). *Manajemen Keamanan Jaringan pada Institusi Pendidikan*. Jakarta: Penerbit Informatika Pendidikan.
- [2] Faisal, A. (2021). Analisis Kerentanan Jaringan Wi-Fi pada Lingkungan Sekolah Menggunakan Metode Pengujian Keamanan. *Jurnal Teknologi dan Keamanan Informasi*, 9(2), 112-120.
- [3] Firman, F., & Rahayu, S. (2020). Literasi Digital dan Hambatan Keamanan Siber pada Lingkungan Pendidikan Menengah. *Jurnal Pendidikan dan Teknologi Informasi*, 5(1), 45-53.
- [4] Moore, J., Jackson, T., & Yeung, K. (2011). Cybersecurity Practices in K-12 Education Systems. *Journal of Educational Technology Research*, 14(3), 201-215.
- [5] Sarjanoko, R. (2022). Evaluasi Risiko Keamanan Data pada Sistem Informasi Sekolah. *Jurnal Sistem dan Teknologi Informasi*, 7(1), 55-63.



[6] Sulaiman, A. (2021). Pengaruh Literasi Keamanan Informasi terhadap Risiko Ancaman Siber di Sekolah Menengah. *Jurnal Keamanan Siber Indonesia*, 3(2), 89-97.