TEMATICS | Technology Management and Informatics Research Journals
E-ISSN : 2798-530X
POLITEKNIK IMIGRASI POLTEKIM

KAJIAN SISTEMATIS TERHADAP KERENTANAN JARINGAN NIRKABEL DALAM INFRASTRUKTUR KEIMIGRASIAN

A SYSTEMATIC REVIEW OF WIRELESS NETWORK VULNERABILITIES IN IMMIGRATION INFRASTRUCTURE

https://10.0.205.137/tematics.v8i1.910
Submitted: 03-05-2026 Reviewed: 17-05-2026 Published: 10-06-2026

Ibhar Avisina
Ibhar.avisina2@gmail.com
Politeknik Imigrasi dan Pemasyarakatan

Galuh Boy Hertantyo
galuhboyh@poltekim.ac.id
Politeknik Imigrasi dan Pemasyarakatan

Mila Rosmaya
milarosmaya@gmail.com
Politeknik Imigrasi dan Pemasyarakatan

Abstract *Wireless networks, particularly Wi-Fi, have become essential in supporting digital activities and public services, including institutional environments that manage sensitive data. However, their open transmission characteristics make them vulnerable to various security threats. This study aims to systematically review research related to vulnerabilities in wireless networks, with a focus on dominant attack types, security testing methods, and mitigation strategies Based on the selection process, 30 articles published were included in the review. The results indicate that the most frequently discussed threats are packet sniffing or eavesdropping, misconfiguration or weak authentication, deauthentication, brute force, rogue access point or evil twin, and man-in-the-middle (MITM) attacks. In addition, the most commonly applied approaches in previous studies are penetration testing, vulnerability assessment, and security testbed-based evaluation. The findings show that wireless network security remains a significant concern due to the open nature of data transmission and the strong influence of configuration quality and user awareness. This study highlights the importance of strengthening wireless security through proper configuration, continuous monitoring, and improved user awareness, especially in institutional environments that rely on secure digital services.*

Keywords: *wireless network; penetration testing; network security*

Abstrak *Jaringan nirkabel, khususnya Wi-Fi, telah menjadi bagian penting dalam mendukung aktivitas digital dan pelayanan publik, termasuk pada lingkungan institusi yang mengelola data sensitif. Namun, karakteristik transmisinya yang terbuka menyebabkan jaringan ini rentan terhadap berbagai ancaman keamanan. Penelitian ini bertujuan untuk mengkaji secara sistematis penelitian-penelitian yang membahas kerentanan pada jaringan nirkabel dengan fokus pada jenis serangan yang dominan, metode pengujian keamanan, dan strategi*

mitigasi yang digunakan. Berdasarkan proses seleksi, diperoleh 30 artikel yang diterbitkan. Hasil kajian menunjukkan bahwa ancaman yang paling sering dibahas meliputi packet sniffing atau eavesdropping, misconfiguration atau kelemahan autentikasi, deauthentication, brute force, rogue access point atau evil twin, dan man-in-the-middle (MITM). Selain itu, metode yang paling banyak digunakan dalam penelitian sebelumnya adalah penetration testing, vulnerability assessment, dan evaluasi keamanan berbasis security testbed. Temuan ini menunjukkan bahwa keamanan jaringan nirkabel masih menjadi isu penting karena sifat transmisi data yang terbuka serta pengaruh besar dari kualitas konfigurasi dan kesadaran pengguna. Oleh karena itu, penguatan keamanan jaringan nirkabel perlu dilakukan melalui konfigurasi yang tepat, pemantauan berkelanjutan, dan peningkatan kesadaran pengguna, khususnya pada lingkungan institusi yang bergantung pada layanan digital yang aman.

Kata kunci: ; *jaringan nirkabel; keamanan jaringan; penetration testing*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi mendorong peningkatan penggunaan jaringan nirkabel, khususnya Wi-Fi, dalam berbagai sektor, termasuk pemerintahan dan layanan publik. Dalam lingkungan keimigrasian, jaringan Wi-Fi mendukung operasional sistem informasi, pertukaran data, serta layanan digital yang menuntut ketersediaan dan kecepatan akses. Karena itu, keandalan dan keamanan jaringan nirkabel menjadi bagian penting dalam menjaga kualitas pelayanan dan kontinuitas operasional institusi.

Di sisi lain, karakteristik transmisi melalui media udara menjadikan jaringan nirkabel lebih mudah dipantau, diintersepsi, atau disusupi dibandingkan jaringan kabel. Kajian terdahulu menunjukkan bahwa ancaman pada jaringan wireless banyak dipengaruhi oleh kelemahan konfigurasi, kualitas autentikasi, serta mekanisme perlindungan yang tidak diterapkan secara memadai (Aslan et al., 2023). Pada jaringan Wi-Fi enterprise, masalah validasi sertifikat, rogue access point, dan pencurian kredensial juga masih menjadi isu penting yang berdampak langsung pada kerahasiaan data dan keamanan akses (Palama et al., 2023).

Berbagai penelitian telah mengidentifikasi bentuk ancaman yang berulang pada jaringan Wi-Fi, seperti packet sniffing atau eavesdropping, man-in-the-middle, deauthentication, brute force, dan evil twin. Selain dipengaruhi oleh aspek teknis, sejumlah studi menunjukkan bahwa tingkat kesadaran pengguna dan kualitas tata kelola keamanan juga berpengaruh besar terhadap efektivitas pengamanan jaringan (Halbouni et al., 2023). Dalam konteks keimigrasian, kerentanan tersebut menjadi semakin krusial karena berkaitan dengan perlindungan data identitas, dokumen perjalanan, serta layanan publik yang bersifat sensitif.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk melakukan kajian sistematis terhadap literatur yang membahas kerentanan jaringan nirkabel, khususnya Wi-Fi, dengan fokus pada jenis serangan yang dominan, metode pengujian keamanan, serta implikasinya terhadap infrastruktur keimigrasian. Penelitian dilakukan dengan pendekatan Systematic Literature Review (SLR) menggunakan pedoman PRISMA agar proses seleksi artikel berlangsung terstruktur dan dapat dipertanggungjawabkan (Snyder, 2019; Page et al., 2021). Hasil kajian memperlihatkan bahwa penelitian masih banyak berfokus pada identifikasi celah keamanan dan simulasi serangan, sementara penguatan mekanisme pertahanan adaptif mulai berkembang sebagai arah penelitian berikutnya.

2. METODE PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) dengan pedoman PRISMA 2020 untuk mengidentifikasi, menyeleksi, dan mensintesis hasil penelitian terdahulu secara sistematis (Snyder, 2019; Page et al., 2021). Proses penelusuran artikel dilakukan melalui Google Scholar, Semantic Scholar, dan Garuda dengan kata kunci wireless security, Wi-Fi vulnerability, penetration testing Wi-Fi, keamanan Wi-Fi, dan kerentanan jaringan nirkabel. Artikel yang dipilih dibatasi pada publikasi tahun 2020-2026, tersedia dalam bahasa Indonesia atau bahasa Inggris, dapat diakses penuh, dan relevan dengan isu kerentanan, serangan, metode pengujian, maupun mitigasi keamanan jaringan nirkabel.

Seleksi artikel mengikuti empat tahap PRISMA, yaitu identification, screening, eligibility, dan included. Pada tahap identification, seluruh artikel yang ditemukan dari basis data dikumpulkan berdasarkan kata kunci yang telah ditetapkan. Tahap screening dilakukan dengan menyeleksi judul, abstrak, tahun publikasi, bahasa artikel, dan ketersediaan naskah lengkap. Artikel yang lolos kemudian dibaca secara penuh pada tahap eligibility untuk memastikan kesesuaian tujuan, metode, dan hasil penelitian. Tahap included menghasilkan 30 artikel yang dianalisis lebih lanjut. Data dari artikel terpilih diekstraksi ke dalam unsur penulis, tahun, fokus kajian, metode, platform atau tools, serta temuan utama untuk dianalisis secara deskriptif tematik (Rethlefsen et al., 2021).

Tabel 1. Pengumpulan Data Artikel

Source	Studi Menemukan "WiFi Security"	Kandidat	Artikel Terpilih
Google Scholar	8439	25	17
Semantic Scholar	3476	19	8
Garuda	303	44	5
Total	12.218	88	30

3. PEMBAHASAN

Berdasarkan proses seleksi literatur, diperoleh 30 artikel yang memenuhi kriteria dan selanjutnya dianalisis untuk melihat pola ancaman, metode pengujian, serta arah perkembangan penelitian keamanan jaringan nirkabel. Hasil telaah menunjukkan bahwa sebagian besar artikel menempatkan Wi-Fi sebagai objek utama kajian karena sifat transmisinya yang terbuka, penggunaan yang luas, dan ketergantungan organisasi terhadap akses wireless dalam mendukung layanan digital.

Kerentanan Jaringan Nirkabel

Kerentanan pada jaringan nirkabel umumnya berakar pada dua hal utama, yaitu sifat media transmisinya yang terbuka dan kualitas konfigurasi keamanan yang diterapkan. Sinyal yang dipancarkan melalui udara membuat lalu lintas data lebih mudah dipantau, sehingga packet sniffing atau eavesdropping tetap menjadi ancaman yang sering dibahas dalam literatur. Di samping itu, pengaturan autentikasi yang lemah, konfigurasi access point yang tidak optimal, serta mekanisme validasi yang kurang kuat memperbesar peluang terjadinya penyusupan dan pencurian kredensial (Aslan et al., 2023).

Pada jaringan enterprise, ancaman seperti rogue access point, evil twin, dan pencurian kredensial menunjukkan bahwa persoalan keamanan tidak hanya terletak pada protokol, tetapi juga pada perilaku pengguna dan tata kelola sistem. Temuan Palama et al. (2023) memperlihatkan bahwa rendahnya validasi sertifikat dan awareness pengguna masih membuka ruang eksploitasi yang signifikan. Di sisi lain, telaah terhadap WPA3 juga menunjukkan bahwa perbaikan protokol belum sepenuhnya menutup semua celah, terutama jika implementasi dan konfigurasi lapangannya tidak diperkuat (Halbouni et al., 2023).

Metode Pengujian Keamanan Jaringan

Metode yang paling dominan digunakan dalam artikel-artikel terpilih adalah penetration testing, vulnerability assessment, dan security analysis. Pada studi kasus lokal, penetration testing paling sering diterapkan untuk menguji celah autentikasi, konfigurasi access point, serta kemungkinan eksploitasi serangan brute force atau deauthentication. Tools yang muncul secara berulang antara lain Aircrack-ng, Wireshark, Kali Linux, dan perangkat uji sederhana seperti NodeMCU pada skenario simulasi serangan.

Pada studi internasional, evaluasi keamanan lebih banyak dikembangkan melalui security testbed dan framework analisis yang memungkinkan peneliti mensimulasikan serangan serta menguji mekanisme pertahanan dalam lingkungan yang lebih terkontrol. Kampourakis et al. (2023) menegaskan bahwa security testbed penting untuk menguji kombinasi skenario serangan, kontrol keamanan, dan ketahanan sistem. Sementara itu, pengembangan framework dan intrusion detection juga mulai menonjol sebagai bagian dari upaya

pergeseran dari sekadar identifikasi celah menuju pertahanan yang lebih adaptif (Imran et al., 2025; Dang et al., 2024).

Penelitian Terdahulu

Untuk memperoleh gambaran yang lebih komprehensif mengenai arah penelitian, sejumlah artikel representatif dipilih dan diringkas berdasarkan fokus, metode, dan temuan utamanya. Ringkasan tersebut disajikan pada Tabel 2.

Tabel 2. Ringkasan Penelitian Terdahulu yang Representatif

No	Peneliti	Tahun	Judul Penelitian	Metode	Temuan Utama
1	Anshori, Azwar, dan Yuliana	2025	Analisis kualitas layanan jaringan internet WiFi Pusdiskom dengan metode penetration testing	Penetration testing	Jaringan Wi-Fi institusi masih memiliki celah keamanan dan memerlukan evaluasi berkala.
2	Ariyanto, Irham, dan Cahyadi	2024	An evaluation of wireless network security with penetration testing method at PT PLN UP2D S2JB	Penetration testing	Masih ditemukan titik lemah yang dapat dimanfaatkan untuk serangan pada jaringan wireless institusi.
3	Mulyanto, Herfandi, dan Kirana	2022	Analisis keamanan WLAN terhadap serangan brute force dengan metode penetration testing	Penetration testing	Serangan brute force dapat mengeksploitasi mekanisme autentikasi yang lemah.
4	Fitrian et al.	2026	Security evaluation of WPA2 vs WPA3 against deauthentication and brute force attacks	Eksperimen keamanan	WPA3 memiliki ketahanan lebih baik dibanding WPA2, tetapi konfigurasi tetap menjadi faktor penentu.
5	Imran, Neyman, dan Rahmawan	2025	Development of a penetration testing framework for WiFi vulnerability solutions	Pengembangan framework	Framework membantu identifikasi dan penelusuran solusi atas kerentanan jaringan Wi-Fi.
6	Halbouni, Ong, dan Leow	2023	Wireless security protocols WPA3: A systematic literature review	SLR	WPA3 memperbaiki kelemahan protokol sebelumnya, tetapi belum sepenuhnya bebas dari celah keamanan.
7	Aslan et al.	2023	A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions	Comprehensive review	Ancaman pada jaringan nirkabel menuntut pendekatan keamanan berlapis.
8	Kampourakis, Gkioulos, dan Katsikas	2023	A systematic literature review on wireless security testbeds	SLR	Security testbed penting untuk mengevaluasi serangan dan mekanisme pertahanan jaringan wireless.
9	Palama et al.	2023	Attacks and vulnerabilities of Wi-Fi Enterprise networks	Eksperimen keamanan	Wi-Fi enterprise tetap rentan terhadap pencurian kredensial ketika validasi dan awareness pengguna rendah.
10	Dang, Fazio, dan Voznak	2024	A novel deep learning framework for intrusion detection systems in wireless network	Pengembangan IDS	Intrusion detection berpotensi memperkuat mitigasi ancaman pada jaringan wireless.

Ringkasan pada Tabel 2 menunjukkan bahwa penelitian lokal cenderung berfokus pada studi kasus dan pengujian teknis melalui penetration testing, sedangkan penelitian internasional lebih banyak menyoroti protokol, framework, testbed, dan mekanisme deteksi. Perbedaan tersebut menunjukkan bahwa riset

keamanan jaringan nirkabel bergerak dari pendekatan identifikasi kerentanan menuju pengembangan pertahanan yang lebih terukur dan adaptif.

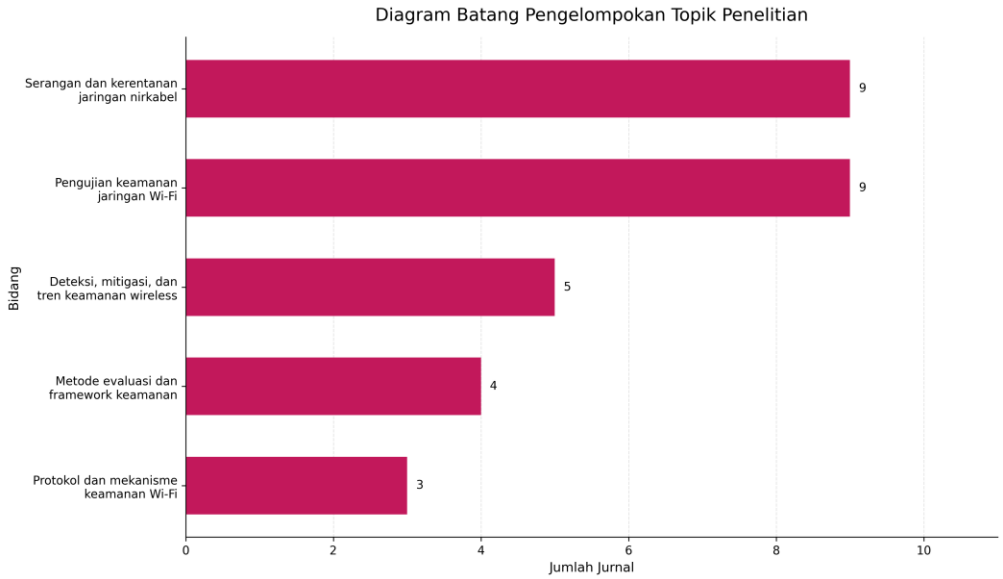
Pengelompokan Topik Pembahasan

Dalam penelitian ini, jurnal yang ditelaah selanjutnya diklasifikasikan ke dalam beberapa kategori utama berdasarkan fokus pembahasannya masing-masing. Klasifikasi tersebut dilakukan untuk menyajikan gambaran yang lebih terstruktur mengenai arah perkembangan penelitian dalam konteks yang beragam. Melalui pengelompokan tersebut, pembahasan dapat disusun secara lebih sistematis serta memudahkan dalam mengidentifikasi fokus dan kecenderungan tren penelitian yang berkembang pada periode kajian.

Tabel 3. Pengelompokan Jurnal Berdasarkan Topik Pembahasan

Bidang	Implementasi	Jumlah
Pengujian keamanan jaringan Wi-Fi	Implementasi penetration testing pada jaringan Wi-Fi atau WLAN di lingkungan instansi, kampus, sekolah, dan rumah sakit	9
Metode evaluasi dan framework keamanan	Penerapan PTES, security testbed, framework penetration testing, dan evaluasi keamanan jaringan	4
Protokol dan mekanisme keamanan Wi-Fi	Analisis keamanan WPA2, WPA3, dan Wi-Fi Easy Connect sebagai mekanisme perlindungan jaringan nirkabel	3
Serangan dan kerentanan jaringan nirkabel	Kajian mengenai brute force, deauthentication, rogue access point, eavesdropping, ancaman APT, serta kerentanan pada berbagai lingkungan wireless	9
Deteksi, mitigasi, dan tren keamanan wireless	Pembahasan mengenai IDS, mitigasi ancaman, keamanan wireless berbasis IoT, serta perkembangan tren keamanan jaringan nirkabel	5

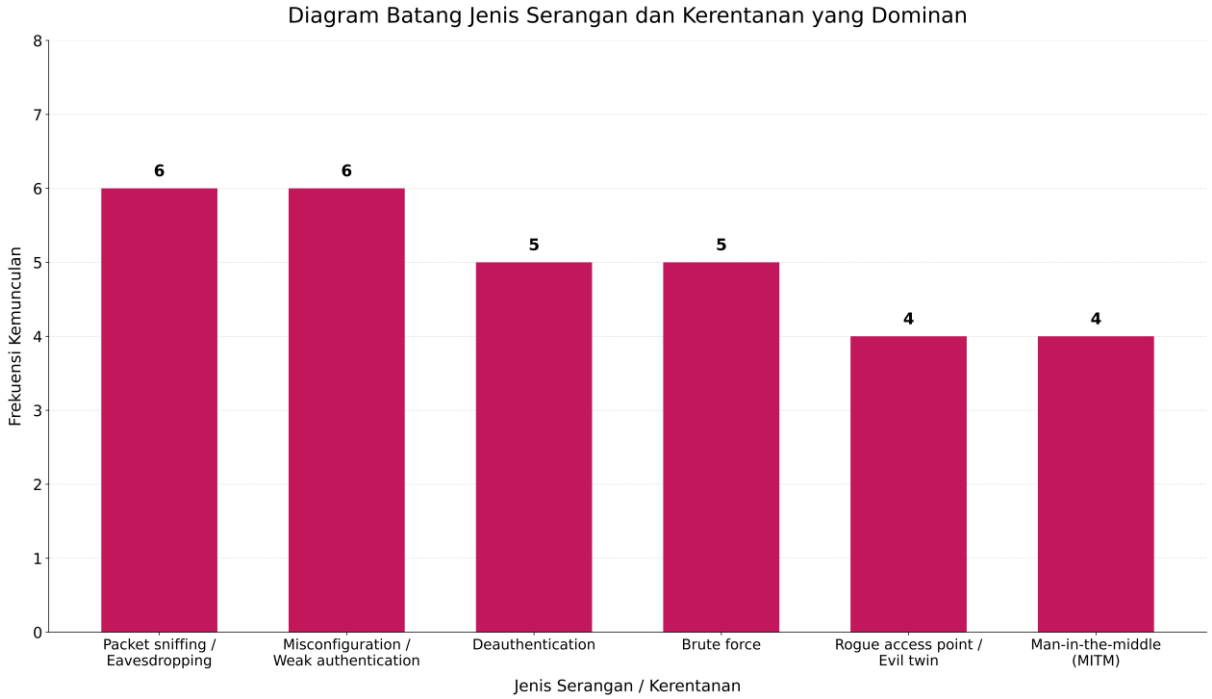
Berdasarkan Tabel 3, bidang yang paling dominan dalam penelitian yang dikaji adalah pengujian keamanan jaringan Wi-Fi serta serangan dan kerentanan jaringan nirkabel, masing-masing berjumlah 9 artikel. Hal ini menunjukkan bahwa perhatian penelitian masih banyak difokuskan pada identifikasi celah keamanan dan simulasi serangan terhadap jaringan wireless. Sementara itu, bidang deteksi, mitigasi, dan tren keamanan wireless menempati urutan berikutnya dengan 5 artikel, diikuti metode evaluasi dan framework keamanan sebanyak 4 artikel, serta protokol dan mekanisme keamanan Wi-Fi sebanyak 3 artikel. Temuan ini menunjukkan bahwa penelitian keamanan jaringan nirkabel tidak hanya berfokus pada serangan, tetapi juga mulai berkembang ke arah penguatan mekanisme pertahanan dan evaluasi keamanan secara sistematis.



Gambar 1. Diagram Batang Pengelompokan Topik Penelitian

Jenis Serangan dan Kerentanan yang Dominan

Untuk memberikan gambaran yang lebih jelas mengenai bentuk ancaman yang paling sering dibahas dalam literatur, hasil kajian selanjutnya divisualisasikan dalam bentuk diagram batang berdasarkan jenis serangan dan kerentanan yang dominan. Penyajian ini bertujuan untuk memudahkan pembaca dalam melihat kecenderungan ancaman keamanan jaringan nirkabel yang paling banyak dibahas dalam penelitian sebelumnya.



Gambar 2. Diagram Batang Jenis Serangan dan Kerentanan yang Dominan

Berdasarkan hasil sintesis terhadap artikel-artikel terpilih, jenis serangan dan kerentanan yang paling dominan dibahas dalam penelitian adalah packet sniffing atau eavesdropping serta misconfiguration atau weak authentication, masing-masing muncul sebanyak 6 kali. Selanjutnya, serangan deauthentication dan brute force masing-masing ditemukan sebanyak 5 kali, sedangkan rogue access point atau evil twin dan man-in-the-middle (MITM) muncul sebanyak 4 kali. Temuan ini menunjukkan bahwa perhatian penelitian keamanan jaringan nirkabel masih banyak difokuskan pada kerentanan yang berkaitan dengan penyadapan lalu lintas data, kelemahan autentikasi, dan eksploitasi konfigurasi jaringan yang tidak aman. Dominasi serangan tersebut juga menegaskan bahwa keamanan jaringan Wi-Fi tidak hanya dipengaruhi oleh kekuatan protokol yang digunakan, tetapi juga oleh kualitas konfigurasi sistem dan perilaku pengguna dalam mengelola akses jaringan.

Implikasi terhadap Infrastruktur Keimigrasian

Bagi lingkungan keimigrasian, temuan-temuan tersebut memiliki implikasi langsung terhadap perlindungan layanan dan data institusi. Infrastruktur keimigrasian memproses informasi identitas, dokumen perjalanan, dan data administrasi yang bersifat sensitif. Karena itu, kelemahan pada jaringan wireless berpotensi menimbulkan gangguan operasional, kebocoran data, hingga penyalahgunaan akses jika tidak diantisipasi secara berlapis.

Hasil kajian ini menunjukkan bahwa penguatan keamanan jaringan nirkabel pada institusi keimigrasian tidak cukup hanya melalui pembaruan protokol, tetapi juga perlu didukung hardening access point, segmentasi jaringan, audit keamanan berkala, pemantauan lalu lintas, serta peningkatan awareness pengguna. Dengan demikian, keamanan Wi-Fi perlu diposisikan sebagai bagian dari tata kelola keamanan informasi yang menyeluruh, bukan sekadar persoalan teknis pada lapisan jaringan.

4. KESIMPULAN

Berdasarkan hasil Systematic Literature Review terhadap 30 artikel terpilih, dapat disimpulkan bahwa penelitian mengenai keamanan jaringan nirkabel masih didominasi oleh pembahasan terkait kerentanan, jenis serangan, metode pengujian keamanan, serta upaya mitigasi pada jaringan Wi-Fi. Hasil kajian menunjukkan bahwa serangan yang paling banyak dibahas dalam literatur meliputi packet sniffing atau eavesdropping, misconfiguration atau kelemahan autentikasi, deauthentication, brute force, rogue access point atau evil twin, serta man-in-the-middle (MITM), yang menegaskan bahwa jaringan nirkabel memiliki tingkat risiko tinggi karena sifat transmisinya yang terbuka dan dipengaruhi oleh kualitas konfigurasi keamanan yang diterapkan. Selain itu, metode yang paling banyak digunakan adalah penetration testing, vulnerability assessment, dan evaluasi keamanan berbasis security testbed. Dalam konteks infrastruktur keimigrasian, hasil kajian ini menunjukkan bahwa keamanan jaringan Wi-Fi harus

menjadi perhatian serius karena berkaitan langsung dengan perlindungan data, layanan digital, dan keberlangsungan operasional institusi.

5. HASIL

Hasil penelitian ini memperlihatkan bahwa kajian keamanan jaringan nirkabel masih lebih banyak diarahkan pada identifikasi celah dan simulasi serangan daripada implementasi mekanisme pertahanan yang adaptif. Secara teoretis, temuan ini memperkuat pandangan bahwa keamanan Wi-Fi dipengaruhi secara simultan oleh faktor teknis, kualitas konfigurasi, dan perilaku pengguna. Dengan demikian, studi ini memberikan kontribusi konseptual dengan memetakan kecenderungan ancaman, metode pengujian, dan arah perkembangan penelitian keamanan jaringan wireless.

Dari sisi praktis, hasil kajian ini dapat menjadi rujukan bagi institusi yang bergantung pada layanan digital, khususnya instansi keimigrasian, untuk merancang audit keamanan berkala, penguatan konfigurasi access point, penerapan intrusion detection, dan program peningkatan kesadaran pengguna. Penelitian selanjutnya disarankan untuk lebih memfokuskan kajian pada efektivitas mekanisme pertahanan, hardening access point, segmentasi jaringan, serta evaluasi protokol keamanan terbaru dalam konteks operasional institusi publik.

REFERENSI

Adbeib, K. A. (2023). Comprehensive study on Wi-Fi security protocols by analyzing WEP, WPA, and WPA2. African Journal of Advanced Pure and Applied Sciences, 2(4), 385–402. https://doi.org/10.65418/ajapas.v2i4.659

Anshori, A., Azwar, M. H., & Yuliana, A. (2025). Analisis kualitas layanan jaringan internet WiFi Pusdiskom dengan metode penetration testing. JICode: Jurnal Informatika dan Komputer, 1(1), 9–12. https://doi.org/10.30599/jicode.v1i1.3288

Ariyanto, T., Irham, I., & Cahyadi, E. F. (2024). An evaluation of wireless network security with penetration testing method at PT PLN UP2D S2JB. Jurnal INFOTEL, 16(1). https://doi.org/10.20895/infotel.v16i1.1057

As-sajid, A. B. N., & Putra, R. E. (2023). Analisis dan pengujian dictionary attack terhadap WPA3 berbasis script. JINACS, 5(2), 216–222. https://doi.org/10.26740/jinacs.v5n02.p216-222

Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. Journal of Information Security and Applications, 64, 103058. https://doi.org/10.1016/j.jisa.2021.103058

Dang, K. D. N., Fazio, P., & Voznak, M. (2024). A novel deep learning framework for intrusion detection systems in wireless network. Future Internet, 16(8), 264. https://doi.org/10.3390/fi16080264

Dar, M. D. P., Lorch, R., Sadeghi, A., Sorcigli, V., Gollier, H., Tinelli, C., Vanhoef, M., & Chowdhury, O. (2025). SAECRED: A state-aware, over-the-air protocol testing approach for discovering parsing bugs in SAE handshake implementations of COTS Wi-Fi access points. In Proceedings of the IEEE Symposium on Security and Privacy (pp. 3691–3709). https://doi.org/10.1109/SP61157.2025.00211

Fitrian, H. P., Eriyana, E., Ibrahim, H. M., Rizqullah, R. P., & Meliansyah, S. P. (2026). Security evaluation of WPA2 vs WPA3 wireless network against deauthentication and brute force attacks using Aircrack-ng. Jurnal Ilmiah Sistem Informasi, 5(1). https://doi.org/10.51903/gy968e07

Ghanim, A. A., & Thanoun, M. Y. (2025). Evaluating the effectiveness of WPA3 protocol against advanced hacking attacks. International Journal of Wireless and Microwave Technologies, 15(4), 1–18. https://doi.org/10.5815/ijwmt.2025.04.01

Halbouni, A., Ong, L.-Y., & Leow, M.-C. (2023). Wireless security protocols WPA3: A systematic literature review. IEEE Access, 11, 112438–112450. https://doi.org/10.1109/ACCESS.2023.3322931

Imran, A., Neyman, S. N., & Rahmawan, H. (2025). Development of a penetration testing framework for identifying security vulnerability solutions in WiFi networks. Telematika: Jurnal Informatika dan Teknologi Informasi, 22(1). https://doi.org/10.31315/telematika.v22i1.14767

Kampourakis, V., Gkioulos, V., & Katsikas, S. K. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. Computers & Security, 133, 103383. https://doi.org/10.1016/j.cose.2023.103383

Kohlios, C., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. Electronics, 7(11), 284. https://doi.org/10.3390/electronics7110284

Kurniawan, T. A. (2020). Analisa keamanan jaringan WiFi terhadap serangan packet sniffing. Jurnal Ilmiah Fakultas Teknik LIMITS, 16(2), 11–15. https://teknik.usni.ac.id/jurnal/2.%20T.Adi.pdf

Leevy, J. L., & Khoshgoftaar, T. M. (2020). A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. Journal of Big Data, 7, 104. https://doi.org/10.1186/s40537-020-00382-x

Lo Cigno, R., Gringoli, F., Bartoletti, S., Cominelli, M., Ghiro, L., & Zanini, S. (2025). Communication and sensing: Wireless PHY-layer threats to security and privacy for IoT systems and possible countermeasures. Information, 16(1), 31. https://doi.org/10.3390/info16010031

Mulyanto, Y., Herfandi, H., & Kirana, R. C. (2022). Analisis keamanan wireless local area network (WLAN) terhadap serangan brute force dengan metode penetration testing (Studi kasus: RS H. L. Manambai Abdulkadir). JINTEKS, 4(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mulyanto, Y., Qanita, S. S., Wiryatari, D., & Idifitriani, F. (2025). Analisis perbandingan kinerja dan keamanan protokol WPA2 dan WPA3 dengan metode penetration testing. Jurnal Informatika dan Rekayasa Elektronik, 8(1), 140–148. https://doi.org/10.36595/jire.v8i1.1539

Natkaniec, M., & Bednarz, M. (2023). Wireless local area networks threat detection using 1D-CNN. Sensors, 23(12), 5507. https://doi.org/10.3390/s23125507

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-

Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Palama, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. Computer Communications, 212, 129–140. https://doi.org/10.1016/j.comcom.2023.10.003

Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., Koffel, J. B., & PRISMA-S Group. (2021). PRISMA-S: An extension to the PRISMA Statement for reporting literature searches in systematic reviews. Systematic Reviews, 10(1), 39. https://doi.org/10.1186/s13643-020-01542-z

Schepers, D., Ranganathan, A., & Vanhoef, M. (2021). Let numbers tell the tale: Measuring security trends in Wi-Fi networks and best practices. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 100–105). https://doi.org/10.1145/3448300.3468286

Schepers, D., Ranganathan, A., & Vanhoef, M. (2022). On the robustness of Wi-Fi deauthentication countermeasures. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 245–256). https://doi.org/10.1145/3507657.3528548

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Tleuberdin, S., Issainova, A., Adamova, A., Aidynov, T., Samashova, G., & Satybaldina, D. (2025). Analysis of vulnerabilities and practical attacks on WPA3-Enterprise in corporate wireless networks. Procedia Computer Science, 272, 613–618. https://doi.org/10.1016/j.procs.2025.10.256

Wang, K., Evans, D., Hui, P., Lo, D., & Li, J. (2022). Assessing certificate validation user interfaces of WPA supplicants. In Proceedings of the 28th Annual International Conference on Mobile Computing and Networking (pp. 501–513). https://doi.org/10.1145/3495243.3517026

Xu, M., Zhang, Y., Liu, H., Ma, L., & Li, Q. (2024). Beamforming made malicious: Manipulating Wi-Fi traffic via beamforming feedback forgery. In Proceedings of the 30th Annual International Conference on Mobile Computing and Networking (pp. 908–922). https://doi.org/10.1145/3636534.3690669

Zaidan, D. T. (2021). Analyzing attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols. Periodicals of Engineering and Natural Sciences, 9(4), 1093–1101. https://doi.org/10.21533/pen.v9i4.1011