Vol 3 No. 2 April 2026 P-ISSN : 3047-9029 E-ISSN : 3047-9010, Hal 35 – 38

JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/vzqtrw67

ANALISIS KEAMANAN JARINGAN WI-FI PUBLIK TERHADAP SERANGAN EVIL TWIN

Rakhmadi Rahman[a*], Nurhalisah Ramli[b], Alya Putri Rahmadani[c]
[a] Jurusan Sistem Informasi; rakhmadi.rahman@ith.ac.id, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[b] Jurusan Sistem Informasi; nurhalisahramli23@gmail.com, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[c] Jurusan Sistem Informasi, aliyaputri1275@gmail.com, Institut Teknologi BJ Habibie, Jl. Pemuda Kota Parepare Provinsi Sulawesi Selatan
[*]Penulis Korespondensi: Rakhmadi Rahman

ABSTRACT

Public wireless networks (Wi-Fi) are widely used in educational institutions, offices, and public areas due to their ease of access and flexibility. However, this convenience is accompanied by significant security risks, particularly Man-In-The-Middle (MITM) attacks using the Evil Twin technique. This attack exploits fake access points that imitate legitimate networks to deceive users into connecting and transmitting sensitive data. This study aims to analyze the characteristics of Evil Twin attacks on public Wi-Fi networks, evaluate the effectiveness of Deauthentication and Web Phishing techniques, and assess network monitoring tools in detecting traffic anomalies. The research method applied is an experimental approach using penetration testing in a controlled environment. Several tools such as Aircrack-ng, Hostapd-WPE, Wireshark, Zui, and Wi-Fi Analyzer were utilized. The results indicate that Evil Twin attacks are highly effective in intercepting HTTP traffic and potentially compromising HTTPS sessions when users ignore digital certificate warnings. Monitoring based on metadata successfully detects abnormal traffic patterns, while the implementation of a Resilient Certificate Management System (RCMS) significantly improves network security by rejecting unauthorized certificates. This research provides practical recommendations for administrators and users to enhance public Wi-Fi security.

Keywords: *Public Wi-Fi; Evil Twin; Man-In-The-Middle; Penetration Testing; Network Security*

Abstrak

Jaringan nirkabel (Wi-Fi) publik banyak digunakan di lingkungan pendidikan, perkantoran, dan ruang publik karena kemudahan akses dan fleksibilitasnya. Namun, kondisi ini juga meningkatkan risiko keamanan informasi, terutama terhadap serangan Man-In-The-Middle (MITM) dengan teknik Evil Twin. Serangan ini memanfaatkan access point palsu yang menyerupai jaringan sah untuk mengelabui pengguna agar terhubung dan mengirimkan data sensitif. Penelitian ini bertujuan untuk menganalisis karakteristik serangan Evil Twin pada jaringan Wi-Fi publik, mengevaluasi efektivitas teknik Deauthentication dan Web Phishing, serta menguji kemampuan alat monitoring jaringan dalam mendeteksi anomali trafik. Metode penelitian yang digunakan adalah metode eksperimental dengan pendekatan penetration testing pada lingkungan terkontrol. Alat yang digunakan meliputi Aircrack-ng, Hostapd-WPE, Wireshark, Zui, dan Wi-Fi Analyzer. Hasil penelitian menunjukkan bahwa serangan Evil Twin sangat efektif dalam mengintersepsi trafik HTTP dan berpotensi mengeksploitasi sesi HTTPS ketika pengguna mengabaikan peringatan sertifikat digital. Monitoring berbasis metadata mampu mendeteksi lonjakan trafik abnormal, sedangkan implementasi Resilient Certificate Management System (RCMS) terbukti meningkatkan keamanan autentikasi jaringan. Penelitian ini diharapkan dapat menjadi referensi bagi administrator jaringan dan pengguna dalam meningkatkan keamanan Wi-Fi publik.

Kata Kunci: Wi-Fi Publik; Evil Twin; Man-In-The-Middle; Penetration Testing; Keamanan Jaringan

Naskah Masuk 5 Januari 2026; Revisi 6 Januari 2026; Diterima 11 Januari 2026; Tersedia 12 Januari 2026

1. PENDAHULUAN

Penggunaan jaringan Wi-Fi publik mengalami peningkatan signifikan seiring dengan kebutuhan mobilitas dan akses informasi yang cepat. Di lingkungan kampus, sekolah, dan fasilitas umum, Wi-Fi publik menjadi infrastruktur utama pendukung aktivitas akademik dan administratif. Namun, rendahnya kesadaran keamanan pengguna menyebabkan jaringan ini rentan terhadap berbagai serangan siber.

Salah satu serangan yang paling berbahaya adalah Man-In-The-Middle (MITM), khususnya menggunakan teknik Evil Twin. Serangan ini dilakukan dengan membuat access point palsu yang memiliki identitas serupa dengan jaringan resmi. Dengan memanfaatkan kecenderungan perangkat klien yang otomatis memilih sinyal terkuat, penyerang dapat mengalihkan koneksi pengguna tanpa disadari.

Berdasarkan penelitian sebelumnya, kombinasi Evil Twin dengan teknik Deauthentication dan Web Phishing mampu mencuri kredensial pengguna dalam waktu singkat. Oleh karena itu, penelitian ini difokuskan pada analisis pola serangan tersebut serta pengujian metode mitigasi yang efektif dan mudah diterapkan.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan Wi-Fi Publik

Jaringan Wi-Fi publik merupakan jaringan nirkabel yang dapat diakses oleh banyak pengguna tanpa autentikasi ketat. Menurut Akhyasi dan Muflih [1], jaringan jenis ini memiliki tingkat kerentanan tinggi terhadap serangan MITM karena tidak adanya mekanisme verifikasi access point yang kuat.

2.2. Serangan Evil Twin

Evil Twin adalah teknik serangan dengan membuat access point palsu yang meniru SSID jaringan sah. Aman [2] menjelaskan bahwa serangan ini sering dikombinasikan dengan Deauthentication untuk memutus koneksi pengguna dari jaringan asli.

2.3. Teknik Deauthentication dan Web Phising

Deauthentication merupakan serangan pada frame manajemen IEEE 802.11 yang memaksa klien terputus dari jaringan. Lina dan Fernandes [3] menyatakan bahwa teknik ini sangat efektif ketika digabungkan dengan captive portal palsu untuk mencuri kredensial pengguna.

2.4. Metode Mitigasi Serangan Evil Twin

Daldoul [4] mengusulkan Resilient Certificate Management System (RCMS) sebagai solusi mitigasi dengan memverifikasi sertifikat digital access point. Sistem ini mampu menolak sertifikat palsu dan mencegah koneksi ke jaringan tidak sah.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan literature review. Penelitian ini menggunakan metode eksperimental dengan pendekatan penetration testing. Metode ini dipilih untuk mensimulasikan kondisi serangan nyata pada jaringan Wi-Fi publik dalam lingkungan terkontrol. Tahapan penelitian meliputi reconnaissance jaringan, persiapan serangan, eksploitasi menggunakan Evil Twin dan Deauthentication, monitoring trafik, serta analisis dan mitigasi menggunakan RCMS.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Simulasi Serangan Evil Twin

Hasil pengujian menunjukkan bahwa kombinasi teknik Evil Twin dan Deauthentication mampu memaksa perangkat korban berpindah dari access point asli ke access point palsu dalam waktu yang relatif singkat. Berdasarkan simulasi selama 10 menit, teridentifikasi peningkatan signifikan pada jumlah paket HTTP yang melewati perangkat penyerang.

Tabel 1. Ringkasan Hasil Simulasi Serangan

Parameter Pengujian	Hasil Pengamatan
Durasi simulasi	10 menit
Jumlah klien terputus (deauth)	8 perangkat

Klien berhasil terhubung ke Evil Twin	6 perangkat
Paket HTTP terintersepsi	±600 paket
Paket HTTPS terdeteksi	Tinggi (terenskripsi)

Sumber : [1] Hasil Pengujian dan analisis Penulis (2026)

Data pada Tabel 1 menunjukkan bahwa mayoritas klien yang terkena serangan Deauthentication secara otomatis melakukan reassociation ke jaringan Evil Twin dengan sinyal lebih kuat.

4.2 Analisis Trafik Jaringan

Analisis menggunakan Wireshark memperlihatkan bahwa data sensitif seperti username dan password dapat terbaca dalam bentuk plain text ketika dikirim melalui protokol HTTP. Sementara itu, monitoring menggunakan Zui menampilkan lonjakan trafik HTTP/SSL yang disertai indikator anomali seperti alert, weird, dan capture_loss.

Tabel 2. Indikator Trafik Anomali Selama Serangan

Jenis Indikator	Deskripsi	Status
Alert	Aktivitas mencurigakan pada sesi autentikasi	Terdeteksi
Weird	Ketidaksesuaian pola protocol	Terdeteksi
Capture_loss	Kehilangan paket akibat trafik tinggi	Terdeteksi

Sumber : [2] Analisis trafik jaringan menggunakan Wireshark dan Zui (2026).

4.3 Evaluasi Implementasi Mitigasi RCMS

Implementasi Resilient Certificate Management System (RCMS) diuji untuk memverifikasi efektivitasnya dalam mencegah koneksi ke access point palsu. Hasil pengujian menunjukkan bahwa RCMS mampu menolak sertifikat self-signed yang digunakan oleh Evil Twin dan menampilkan peringatan keamanan kepada pengguna.

Tabel 3. Perbandingan Kondisi Sebelum dan Sesudah RCMS

Aspek Pengujian	Tanpa RMCS	Dengan RMCS
Deteksi AP palsu	Rendah	Tinggi
Risiko MITM	Tinggi	Rendah
Keamanan Autentikasi	Rendah	Kuat

Sumber : [3] Perbandingan hasil pengujian sebelum dan sesudah implementasi RCMS oleh penulis (2026).

Dengan demikian, RCMS terbukti efektif sebagai lapisan pertahanan tambahan dalam meningkatkan keamanan jaringan Wi-Fi publik.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa jaringan Wi-Fi publik memiliki tingkat kerentanan yang tinggi terhadap serangan Man-In-The-Middle (MITM) dengan teknik Evil Twin. Kombinasi teknik Deauthentication dan Web Phishing terbukti efektif dalam memaksa pengguna berpindah ke access point palsu serta memungkinkan penyerang mengintersepsi data sensitif, khususnya pada komunikasi berbasis HTTP. Selain itu, hasil monitoring trafik menunjukkan adanya pola anomali yang dapat dideteksi menggunakan alat analisis jaringan seperti Wireshark dan Zui. Implementasi Resilient Certificate Management System (RCMS) mampu meningkatkan keamanan jaringan dengan menolak sertifikat tidak sah dan mengurangi risiko koneksi ke access point palsu.

Berdasarkan kesimpulan tersebut, disarankan agar administrator jaringan Wi-Fi publik menerapkan mekanisme keamanan tambahan seperti autentikasi berbasis sertifikat digital, melakukan monitoring jaringan

secara berkala, serta membatasi penggunaan protokol tidak terenkripsi. Selain itu, pengguna Wi-Fi publik diharapkan lebih waspada terhadap jaringan yang tidak dikenal dan memperhatikan peringatan keamanan sertifikat pada perangkat yang digunakan. Penelitian selanjutnya dapat mengembangkan pengujian pada skala jaringan yang lebih besar serta membandingkan efektivitas metode mitigasi lainnya untuk meningkatkan keamanan jaringan nirkabel.

DAFTAR PUSTAKA

[1] Akhyasi Ulfiah, G. Z. (2025). Eksploitasi dan Pencegahan Serangan Man In The Middle (MITM) Dengan Teknik Evil Twin Pada Jaringan WI-FI Publik. *RJTI (Riau Jurnal Teknik Informatika), Vol. 4 No. 2*, 316-323.

[2] Daldoul, Y. (2021). A Robust Certificate Management System to Prevent Evil Twin Attacks in IEEE 802.11 Networks. 1-10.

[3] Sharma Priyanka, P. K. (2015). Survey on Evil Twin Attack. *International Journal of Scientific Engineering and Research (IJSER)* , 23447-3878.