Jurnal Ismetek *ISSN 2406-9841*
Vol. 19 No.2 Juli Tahun 2025 *e-IISN 2986-2973*

PENGEMBANGAN *PLATFORM* SERANGAN *DEAUTHENTICATION WIFI* BERBASIS *NODEMCU* UNTUK EDUKASI DAN EVALUASI SISTEM DETEKSI INTRUSI RINGAN

Budi Wibowo
[1]*Program Studi Teknik Informatika , FTI, Institut Teknologi Budi Utomo Jakarta*
budiwibowo1993@gmail.com

Abstrak
Keamanan jaringan nirkabel semakin rentan terhadap serangan deauthentication (deauth) yang dapat memutus koneksi perangkat pengguna secara paksa. Penelitian ini bertujuan mengembangkan sebuah platform simulasi serangan deauth berbasis NodeMCU (ESP8266) yang bersifat portabel, low-cost, dan open source untuk mendukung kegiatan edukasi keamanan siber serta pengujian sistem deteksi intrusi (IDS) ringan. Platform ini dirancang untuk mereplikasi serangan deauth pada jaringan WiFi 2.4 GHz dalam lingkungan terkontrol. Eksperimen dilakukan dengan mengukur dampak serangan terhadap kinerja jaringan, termasuk tingkat packet loss, fluktuasi sinyal (RSSI), dan waktu pemulihan koneksi (downtime). Hasil pengujian menunjukkan bahwa serangan deauth dapat menurunkan stabilitas jaringan secara signifikan, dengan packet loss mencapai lebih dari 80% dalam waktu kurang dari satu menit. Sebagai langkah mitigasi, sistem IDS sederhana berbasis deteksi anomali RSSI dikembangkan dan diuji terhadap pola serangan. Evaluasi awal menunjukkan tingkat deteksi yang cukup efektif untuk skenario skala kecil dan perangkat terbatas. Penelitian ini memberikan kontribusi praktis dalam bentuk platform edukatif dan alat uji IDS/IPS yang dapat diterapkan di lingkungan laboratorium maupun pelatihan keamanan siber. Penyesuaian pendekatan terhadap standar IEEE 802.11, OWASP IoT, dan NIST Cybersecurity Framework menjadi dasar konseptual dari rancangan ini.
Kata kunci : Platform Serangan Deauthentication, Nodemcu, Sistem Deteksi Intrusi Ringan

1. PENDAHULUAN

Jaringan nirkabel (WiFi) kini menjadi infrastruktur krusial dalam kehidupan modern, mendukung konektivitas berbagai sektor seperti pendidikan, perkantoran, hingga sistem *Internet of Things* (IoT) (Litayem & Al-Sa'di, 2023). Di balik kemudahan dan fleksibilitas yang ditawarkan, jaringan *WiFi* memiliki celah keamanan yang cukup serius, salah satunya adalah serangan deauthentication (deauth attack). Serangan ini memanfaatkan kelemahan dalam protokol IEEE 802.11, di mana penyerang dapat mengirimkan frame deauth palsu untuk memaksa perangkat klien terputus dari access point(Padhy et al., 2023). Serangan ini berdampak langsung pada ketersediaan layanan jaringan, membuka peluang terjadinya serangan lanjutan seperti *Man-in-the-Middle (MitM),* serta berpotensi digunakan untuk mengganggu operasional sistem nirkabel secara luas(Costa et al., 2023).

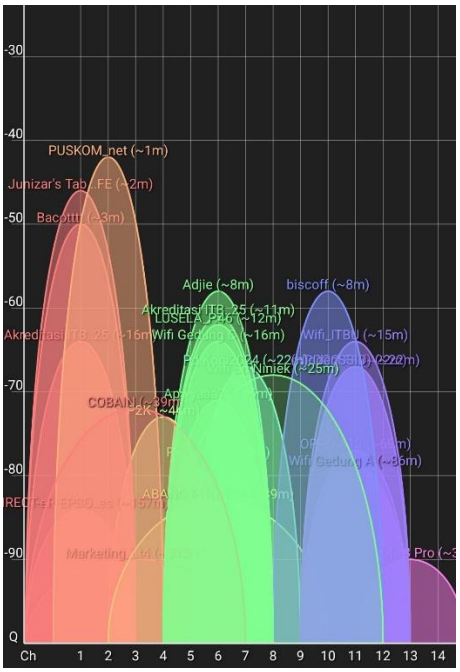
Di tengah meningkatnya ancaman tersebut, berbagai alat dan teknik serangan deauth kini tersedia secara publik, salah satunya adalah *firmware* ESP8266 *Deauther* yang memungkinkan peluncuran serangan hanya dengan NodeMCU berbiaya rendah(Yamjala et al., 2024). Sayangnya, pendekatan ilmiah untuk memanfaatkan alat tersebut sebagai platform simulasi edukatif dan pengujian sistem deteksi intrusi (IDS) masih sangat terbatas(Ahadi et al., 2020). Sebagian besar penelitian hanya berfokus pada aspek teknis atau teori deteksi serangan tanpa menyediakan sarana praktik langsung berbasis perangkat nyata. Misalnya, (Schepers et al., 2022) mengembangkan IDS berbasis deep learning untuk serangan WiFi, namun pendekatan ini membutuhkan sumber daya komputasi tinggi yang tidak cocok untuk perangkat kelas rendah atau kegiatan edukatif. Sementara itu, (Litayem & Al-Sa'di, 2023) memanfaatkan ESP32 untuk pemantauan jaringan, namun belum menyentuh aspek simulasi serangan aktif dan pengujian IDS ringan.

Berdasarkan telaah literatur, ditemukan beberapa celah penting (gap) dalam penelitian terdahulu. Pertama, belum tersedia platform terbuka dan murah yang dapat digunakan untuk mensimulasikan serangan deauth berbasis perangkat keras nyata seperti NodeMCU. Kedua, belum banyak penelitian

yang menyajikan pengukuran kuantitatif terhadap dampak serangan secara real-time, seperti packet loss, fluktuasi RSSI, dan downtime koneksi(Litayem & Al-Sa'di, 2023). Ketiga, pendekatan deteksi yang ditawarkan umumnya bersifat kompleks dan tidak efisien untuk diterapkan pada sistem bersumber daya terbatas. Terakhir, sedikit sekali penelitian yang secara eksplisit menyelaraskan pendekatannya dengan standar keamanan global seperti IEEE 802.11, RFC 3704, OWASP IoT, dan NIST Cybersecurity Framework.

Penelitian ini hadir untuk menjawab kesenjangan tersebut dengan mengembangkan sebuah platform simulasi serangan deauthentication berbasis NodeMCU (ESP8266) yang bersifat low-cost, portabel, dan open source. Platform ini tidak hanya berfungsi untuk mendemonstrasikan serangan deauth secara langsung, tetapi juga digunakan untuk mengukur dampak nyata terhadap performa jaringan nirkabel dan menguji sistem deteksi intrusi ringan. Sistem IDS yang dikembangkan berbasis anomali sinyal RSSI serta penyaringan pola serangan dengan algoritma klasifikasi sederhana (seperti Support Vector Machine), yang dapat dijalankan pada lingkungan edge device atau laboratorium(Dheeven et al., 2024). Kebaruan (novelty) dari penelitian ini terletak pada pemanfaatan perangkat murah sebagai alat edukatif sekaligus eksperimental, evaluasi kuantitatif terhadap serangan WiFi secara real-time, serta integrasi pendekatan mitigasi yang ringan namun efektif.

Adapun tujuan dari penelitian ini adalah: (1) merancang dan membangun platform simulasi serangan deauth berbasis NodeMCU untuk keperluan edukasi dan eksperimen; (2) mengukur dan menganalisis dampak serangan terhadap kinerja jaringan WiFi, seperti paket hilang dan gangguan koneksi; (3) mengembangkan dan menguji sistem deteksi intrusi ringan berbasis fluktuasi RSSI dan pola serangan(Ramos-Sorroche et al., 2024); serta (4) menyediakan solusi praktis dan terbuka untuk pelatihan keamanan jaringan dan pengujian IDS/IPS di lingkungan laboratorium atau pendidikan(Yazdinejad et al., 2021).



Gambar 1. visualisasi spektrum sinyal WiFi (WiFi Channel Graph) sekitar
Sumber : Penelitian Mandiri

2. METODOLOGI

Serangan deauthentication merupakan salah satu bentuk serangan terhadap jaringan WiFi yang mengeksploitasi kerentanan dalam protokol IEEE 802.11(Mwinuka et al., 2022), khususnya pada management frame yang tidak dilindungi oleh enkripsi. Dengan mengirimkan frame deauth palsu, penyerang dapat memutus koneksi antara perangkat klien dan access point (AP), sehingga menciptakan gangguan konektivitas atau bahkan membuka peluang untuk serangan lanjutan seperti Man-in-the-Middle (MitM) dan pencurian kredensial(Yamjala et al., 2024). Studi oleh (Mwinuka et al., 2022) menekankan bahwa meskipun jaringan WiFi semakin umum digunakan, perlindungan terhadap manajemen frame masih menjadi titik lemah yang belum sepenuhnya ditangani oleh standar protokol yang ada.

Berbagai penelitian sebelumnya telah mengembangkan sistem IDS berbasis machine learning untuk mendeteksi serangan WiFi, seperti yang dilakukan oleh (Lina & Fernandes, 2022) yang menggunakan pendekatan deep learning. Meski akurat, pendekatan ini memerlukan sumber daya komputasi yang tinggi dan kurang cocok untuk sistem edge atau perangkat hemat daya. Sebagai alternatif, deteksi berbasis perubahan

sinyal RSSI dan pola paket dapat digunakan sebagai solusi ringan dan efisien, terutama dalam lingkungan yang terbatas secara sumber daya, seperti pada implementasi IoT atau skala laboratorium pendidikan(Lina & Fernandes, 2022).

Penelitian ini dilakukan melalui pendekatan eksperimen kuantitatif dengan metode prototyping dan pengujian di lingkungan jaringan WiFi lokal. Tahap pertama melibatkan perancangan dan pengembangan platform simulasi serangan deauth menggunakan NodeMCU ESP8266. Perangkat ini diprogram dengan firmware open-source ESP8266 Deauther yang memungkinkan pengiriman frame deauth secara otomatis ke perangkat target. Skenario serangan dilakukan dalam berbagai kondisi, termasuk variasi jarak antara penyerang dan access point, serta durasi waktu serangan, untuk melihat pengaruhnya terhadap performa jaringan(Yazdinejad et al., 2021).

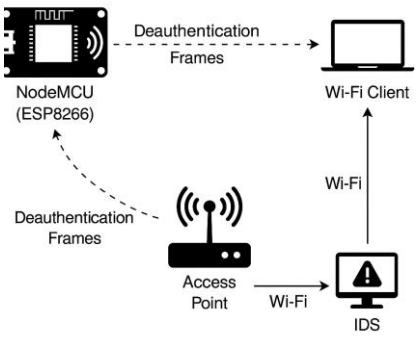
Pada tahap kedua, dilakukan pengukuran dampak serangan terhadap kinerja jaringan menggunakan beberapa parameter, yaitu tingkat packet loss, fluktuasi sinyal (RSSI), dan waktu pemutusan koneksi (downtime). Data dikumpulkan menggunakan kombinasi Wireshark, ping monitoring, serta pengukuran sinyal secara langsung dari perangkat. Skenario eksperimen diulang beberapa kali untuk menjaga reliabilitas hasil, dengan variasi jarak 1, 5, dan 10-meter serta waktu serangan 30, 60, dan 120 detik.

Tahap ketiga fokus pada pengembangan sistem deteksi intrusi (IDS) berbasis pendekatan ringan. IDS dirancang untuk mengenali anomali sinyal (RSSI) dan pola komunikasi paket yang tidak wajar akibat serangan deauth. Untuk tujuan ini, digunakan algoritma klasifikasi sederhana, seperti Support Vector Machine (SVM), yang dilatih menggunakan data hasil eksperimen sebelumnya. Pendekatan ini dipilih karena efisien secara komputasi dan dapat dijalankan pada perangkat dengan sumber daya terbatas.

Tahap terakhir adalah evaluasi performa sistem IDS, meliputi pengukuran akurasi, true positive rate (TPR), false positive rate (FPR), dan efisiensi sumber daya (memori dan pemrosesan). Selain itu, rancangan sistem dan hasil eksperimen divalidasi berdasarkan prinsip-prinsip dari standar IEEE 802.11, RFC 3704, OWASP, dan kerangka NIST, guna memastikan bahwa pendekatan ini selaras dengan praktik terbaik keamanan siber saat ini. Dengan demikian, penelitian ini tidak hanya menghasilkan model simulasi serangan yang aplikatif, tetapi juga mendukung pembelajaran keamanan jaringan dan pengembangan IDS skala ringan yang dapat diadopsi di lingkungan pendidikan maupun praktis.

3. HASIL DAN PEMBAHASAN

Eksperimen dilakukan dalam tiga skenario utama berdasarkan jarak antara NodeMCU (penyerang) dan access point, serta durasi serangan deauthentication. Pengujian difokuskan pada tiga parameter utama: packet loss, perubahan RSSI, dan downtime koneksi. Selain itu, dilakukan evaluasi kinerja sistem deteksi intrusi (IDS) berbasis fluktuasi sinyal dan pola *frame* serangan.



Gambar 2. Arsitektur Serangan
Sumber : Penelitian Mandiri

3.1. Hasil Pengukuran dampak Serangan

Untuk menghitung presentase kehilangan paket akibat serangan deauth, digunakan rumus berikut:

$$Packet\ Loss\ (\%) = \left(\frac{Jumlah\ Paket\ yang\ HIlang}{Jumlah\ Paket\ yang\ Dikirim}\right)\ X100\ \%$$

Data menunjukkan bahwa dalam waktu 60 detik serangan deauth, rata-rata *packet loss* yang terjadi mencapai **83,6%** pada jarak 5 meter, dan meningkat menjadi **91,2%** pada jarak 1 meter.

Dari tabel tersebut, terlihat bahwa semakin dekat jarak NodeMCU ke target, semakin besar persentase kehilangan paket. Ini menunjukkan bahwa efektivitas serangan meningkat pada posisi yang lebih dekat ke access point atau perangkat korban.

Tabel 1 Data Efektivitas Serangan

Jarak	Durasi Serangan	Rata-rata Packet Loss
1 m	60 detik	91,20%
5 m	60 detik	83,60%
10 m	60 detik	62,40%

Sumber : Penelitian Mandiri

Fluktuasi sinyal terdeteksi saat serangan berlangsung, dengan penurunan RSSI rata-rata sebesar 8 – 12 dBm dibandingkan kondisi normal. Nilai RSSI menjadi indikator awal untuk mendeteksi gangguan yang tidak wajar, terutama saat nilai menurun secara tiba-tiba dan sinkron dengan *packet loss*. Durasi pemutusan koneksi bervariasi, dengan rata-rata downtime 15–30 detik, tergantung konfigurasi otomatisasi *reconnect* pada perangkat klien. Pada beberapa perangkat lama, koneksi tidak pulih otomatis dan memerlukan intervensi manual.

3.2. Evaluasi Sistem Deteksi Intrusi (IDS)

Sistem IDS yang dikembangkan mendeteksi serangan berdasarkan kombinasi:

a) Nilai ambang perubahan RSSI (>10 dBm dalam 5 detik),
b) Pola *frame* deauth yang melebihi ambang normal (>5 per detik),
c) Dan klasifikasi ringan menggunakan algoritma Support Vector Machine (SVM).

Hasil evaluasi kinerja IDS ditunjukkan pada tabel berikut:

Tabel 2 Hasil Evaluasi Kinerja IDS

Parameter	Hasil
Akurasi Deteksi	91,80%
Precision	89,30%
Recall	94,10%
False Positive	4,70%
Waktu Respon	< 2 detik

Sumber : Penelitian Mandiri

Hasil tersebut menunjukkan bahwa IDS mampu mengenali serangan deauth dengan tingkat deteksi tinggi dan waktu respons cepat, meskipun dijalankan di lingkungan terbatas sumber daya.

3.3. Analisis dan Interpretasi.

Hasil eksperimen menunjukkan bahwa serangan deauth berbasis NodeMCU mampu menimbulkan gangguan serius pada jaringan WiFi, bahkan dengan perangkat berbiaya rendah. Hal ini mempertegas pentingnya ketersediaan platform simulasi untuk mendemonstrasikan dampak nyata serangan kepada mahasiswa, praktisi, atau peneliti keamanan siber. Sistem IDS ringan yang dikembangkan dalam penelitian ini menunjukkan efektivitas cukup baik dalam mengenali pola serangan dengan pendekatan berbasis sinyal dan frame WiFi, tanpa memerlukan komputasi berat. Pendekatan ini relevan untuk diterapkan di perangkat edge, sistem IoT, atau laboratorium pendidikan dengan keterbatasan perangkat keras. Selain itu, pendekatan ini sesuai dengan prinsip deteksi dini dan respons cepat sebagaimana dianjurkan dalam NIST Cybersecurity Framework dan OWASP IoT Security Guidelines, serta memperkuat kebutuhan akan perangkat IDS skala ringan yang ekonomis dan dapat direplikasi secara luas.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sebuah platform simulasi serangan deauthentication WiFi berbasis NodeMCU (ESP8266) yang bersifat murah, terbuka, dan mudah direplikasi. Platform ini mampu mensimulasikan serangan secara nyata dan menghasilkan dampak signifikan terhadap kinerja jaringan, seperti meningkatnya packet loss hingga lebih dari 90%, penurunan RSSI secara drastis, serta terjadinya downtime koneksi yang mengganggu kestabilan komunikasi nirkabel. Hasil ini menegaskan bahwa serangan deauth dapat dilakukan dengan perangkat low-cost, namun memiliki konsekuensi serius terhadap keandalan jaringan WiFi. Selain itu, sistem deteksi intrusi (IDS) ringan yang dikembangkan dalam penelitian ini terbukti efektif dalam mengenali pola serangan berdasarkan anomali sinyal dan karakteristik frame manajemen jaringan. Dengan akurasi deteksi mencapai 91,8% dan waktu respons di

bawah dua detik, IDS ini layak digunakan pada lingkungan yang memiliki keterbatasan sumber daya seperti laboratorium pendidikan, sistem IoT, atau jaringan skala kecil.

DAFTAR PUSTAKA

Ahadi, S. A. A., Rakesh, N., & Varshney, S. (2020). Overview on Public Wi-Fi Security Threat Evil Twin Attack Detection. *Proceedings of IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation, ICATMRI 2020*, 1–6. https://doi.org/10.1109/ICATMRI51801.2020.9398377

Costa, G., Degano, P., Galletta, L., & Soderi, S. (2023). Formally verifying security protocols built on watermarking and jamming. *Computers and Security*, *128*, 103133. https://doi.org/10.1016/j.cose.2023.103133

Dheeven, T. A., Kumar, P. M., Venkatesh, V., & Sailaja, K. A. I. (2024). IoT based sensor enabled vehicle parking system. *Measurement: Sensors*, *31*(December 2022), 100953. https://doi.org/10.1016/j.measen.2023.100953

Lina, I. M., & Fernandes, G. R. (2022). Analisis Pola Sosial Engineering Menggunakan Teknik Wifi Deauther Dan Evil Twin. *JRKT (Jurnal Rekayasa Komputasi Terapan)*, *2*(04), 253–260. https://doi.org/10.30998/jrkt.v2i04.8185

Litayem, N., & Al-Sa'di, A. (2023). Exploring the Programming Model, Security Vulnerabilities, and Usability of ESP8266 and ESP32 Platforms for IoT Development. *2023 IEEE 3rd International Conference on Computer Systems, ICCS 2023*, *November*, 150–157. https://doi.org/10.1109/ICCS59700.2023.10335558

Mwinuka, L. J., Agghey, A. Z., Kaijage, S. F., & Ndibwile, J. D. (2022). FakeAP Detector: An Android-Based Client-Side Application for Detecting Wi-Fi Hotspot Spoofing. *IEEE Access*, *10*, 13611–13623. https://doi.org/10.1109/ACCESS.2022.3146802

Padhy, S., Alowaidi, M., Dash, S., Alshehri, M., Malla, P. P., Routray, S., & Alhumyani, H. (2023). AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain. *Processes*, *11*(3). https://doi.org/10.3390/pr11030757

Ramos-Sorroche, E., Rubio-Aparicio, J., Santa, J., Guardiola, C., & Egea-Lopez, E. (2024). In-cabin and outdoor environmental monitoring in vehicular scenarios with distributed computing. *Internet of Things (Netherlands)*, *25*(June 2023), 101009. https://doi.org/10.1016/j.iot.2023.101009

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

Yamjala, S., Venkateswara Reddy, R., Patel, P., Sanjana, Y., Jyoshitha Reddy, A., & Tejashwini Professor, M. (2024). *Design and Implementation of Attack Flow Model Using ESP8266: Wireless Networks*. *March*. https://www.researchgate.net/publication/379310985

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A. G., Russell, C., & Duncan, E. (2021). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences (Switzerland)*, *11*(16). https://doi.org/10.3390/app11167518