Journal of Information Technology and Computer Science (INTECOMS)
Volume 8 Nomor 5, Tahun 2025
e-ISSN : 2614-1574
p-ISSN : 2621-3249

PENGEMBANGAN MODUL IoT HEMAT ENERGI BERBASIS ESP32 UNTUK DETEKSI REAL-TIME SERANGAN DEAUTHENTICATION PADA JARINGAN WIFI DALAM PENINGKATAN LITERASI KEAMANAN DIGITAL

DEVELOPMENT OF ESP32-BASED ENERGY-EFFICIENT IOT MODULE FOR REAL-TIME DETECTION OF DEAUTHENTICATION ATTACKS ON WIFI NETWORKS TO IMPROVE DIGITAL SECURITY LITERACY

Faizal Riza[1], Dannie Febrianto Hendrakusuma[2], Budi Wibowo[3], Aji Nurrohman[4]
Institut Teknologi Budi Utomo[1,2,3,4]
faizalriza@itbu.ac.id[1]

ABSTRACT

This research was motivated by the increasing threat to WiFi network security, particularly Deauthentication attacks that can disconnect users and open up opportunities for further attacks such as Man-in-the-Middle and credential theft. This problem is even more complex in Indonesia due to low digital security literacy and limited affordable detection devices. The objective of this study is to develop an energy-efficient ESP32-based Internet of Things (IoT) module capable of detecting Deauthentication attacks in real-time. The research method was carried out in three stages, namely: (1) designing ESP32-based IoT hardware in monitor mode with OLED indicators; (2) developing firmware for analysing deauthentication and disassociation packet patterns with power consumption optimisation; and (3) validating performance through attack simulations using WiFi Deauther and testing on public WiFi networks. The results showed that the ESP32 prototype was capable of detecting attacks in real time with adequate accuracy and response. These findings have the potential to be implemented in public facilities to minimise the risk of cyber attacks and raise public awareness of digital security.

Keywords: *WiFi Network Security, Deauthentication Attacks, ESP32 IoT, Real-Time Detection, Digital Security Literacy.*

ABSTRAK

Penelitian ini dilatarbelakangi oleh meningkatnya ancaman keamanan jaringan WiFi, khususnya serangan Deauthentication yang dapat memutus koneksi pengguna dan membuka peluang serangan lanjutan seperti Man-in-the-Middle serta pencurian kredensial. Permasalahan ini semakin kompleks di Indonesia karena rendahnya literasi keamanan digital dan terbatasnya perangkat deteksi yang terjangkau. Tujuan penelitian ini adalah mengembangkan modul Internet of Things (IoT) berbasis ESP32 yang hemat energi dan mampu mendeteksi serangan Deauthentication secara real-time. Metode penelitian dilakukan melalui tiga tahap, yaitu: (1) perancangan perangkat keras IoT berbasis ESP32 dalam mode monitor dengan indikator OLED; (2) pengembangan firmware untuk analisis pola paket deauthentication dan disassociation dengan optimasi konsumsi daya; serta (3) validasi kinerja melalui simulasi serangan menggunakan WiFi Deauther dan pengujian di jaringan WiFi publik. Hasil penelitian menunjukkan bahwa prototipe ESP32 mampu mendeteksi serangan secara real-time dengan akurasi dan respons yang memadai. Temuan ini berpotensi diimplementasikan di fasilitas publik untuk meminimalisasi risiko serangan siber serta meningkatkan kesadaran masyarakat terhadap keamanan digital.

Kata Kunci: Keamanan Jaringan WiFi, Serangan Deauthentication, IoT ESP32, Deteksi Real Time, Literasi Keamanan Digital.

PENDAHULUAN

Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa penggunaan internet di Indonesia meningkat signifikan dari 66,48% populasi pada tahun 2022 menjadi 79,5% atau 221 juta pengguna pada tahun 2024. Peningkatan pengguna internet menunjukkan transformasi digital yang masif, diikuti dengan kebutuhan akses WiFi baik personal, bisnis maupun publik (Asosiasi Penyelenggara Jasa Internet Indonesia - Survei, n.d.). Seiring perkembangan penggunaan Internet of Thing (IoT) maka pertumbuhan akses WiFi ini meningkatkan risiko serangan keamanan jaringan, terutama deauthentication attack. Jenis serangan ini mencari celah pada protokol IEEE 802.11 untuk memutus koneksi pengguna dan

membuka jalan bagi Evil Twin atau Man-in-the-Middle. Serangan ini mengancam privasi dan stabilitas layanan. Solusi konvensional seperti firewall dan enkripsi terbukti tidak memadai karena tidak mampu mendeteksi eksploitasi pada lapisan protokol IEEE 802.11 (Riza, 2023; Wibowo, 2024). Celah kemanan dari rekayasa sosial terhadap pengguna seperti rendahnya literasi keamanan digital di Indonesia ditambah minimnya alat deteksi terjangkau menjadikan penggunaan jaringan WiFi lebih rentan diretas. Kerentanan utama di fasilitas publik menjadi trust issue untuk meggunakan jaringan WiFi. Permasalahan utama yang disoroti dalam penelitian ini adalah: (1) bagaimana merancang sistem deteksi real-time serangan deauthentication yang hemat energi, portable dan berbiaya rendah; (2) bagaimana mengimplementasikan notifikasi insiden untuk meningkatkan kesadaran pengguna terhadap ancaman siber; serta (3) bagaimana mengoptimalkan ESP32 sebagai platform IoT untuk mengedukasi pengguna melalui notifikasi real-time. Urgensi penelitian ini terletak pada kebutuhan mendesak akan solusi yang tidak hanya mampu meningkatkan keamanan infrastruktur WiFi di Indonesia, tetapi juga mendorong literasi keamanan siber di tengah pesatnya transformasi digital di berbagai sektor kehidupan.

Penelitian "Analyzing and Detecting the De-Authentication Attack by Creating an Automated Scanner using Scapy" (Al-Nuaimi dan Ibrahim, 2023) melakukan deteksi serangan deauthentication menggunakan laptop dengan sistem operasi linux. NIC pada laptop difungsikan pada mode monitor. Simulasi serangan deauthentication menggunakan aireplay-ng. Analisis paket Dot11 dilakukan dengan scapy untuk mendeteksi serangan deauthentication. Kesamaan dengan penelitian kami adalah melakukan deteksi serangan deauthentication. Perbedaannya yaitu tujuan penelitian untuk deteksi serangan deauthentication dengan menggunakan NodeMCU ESP32 yang dilengkapi OLED serta fitur push notification sebagai indikator atau peringatan ketika adanya serangan deauthentication yang terdeteksi.

Penelitian "Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network" mengembangkan sistem berbasis Intrusion Detection System (IDS) untuk mengidentifikasi anomali lalu lintas jaringan. Namun, implementasi ini membutuhkan perangkat dengan spesifikasi tinggi serta konfigurasi yang kompleks. (Tufan, 2021). Sementara Kumar dan Kaur (2024) telah melakukan survei komprehensif terhadap *intrusion detection system* (IDS) dalam jaringan nirkabel, yang didorong oleh kebutuhan mendesak untuk mengatasi tantangan keamanan, terutama keterbatasan komputasi dan infrastruktur yang dihadapi IDS. Penelitian mencakup mekanisme pertahanan dasar dan berlanjut pada analisis mendalam sistem IDS. Analisis meliputi identifikasi jenis penyusup, perilaku intrusi, dasar-dasar keamanan, serta pembahasan berbagai varian IDS dan pendekatan yang digunakan untuk merancang sistem yang efektif. Penelitian ini juga mencakup perincian serangan kritis dan studi tentang *framework* IDS yang relevan. Penelitian memberikan gambaran menyeluruh tentang teknik-teknik terkini (*state-of-the-art*) dalam perlindungan jaringan nirkabel, mengedukasi pengguna mengenai ancaman dan solusi yang ada. Kontribusi utama dari survei ini adalah klasifikasi ancaman (termasuk perilaku intrusi dan serangan kritis), pemaparan solusi desain IDS yang efektif, dan identifikasi *framework* IDS untuk melawan serangan spesifik.

Penelitian "Analysis of Deauthentication Attack in IEEE 802.11 Networks And A Proposal For Its Detection" (Korolkov, 2021) menggunakan perangkat laptop, memanfaatkan sistem operasi Kali Linux, perangkat tambahan *Aircrack*-ng untuk meluncurkan serangan, serta aplikasi Wireshark untuk menangkap dan menganalisis frame IEEE 802.11.

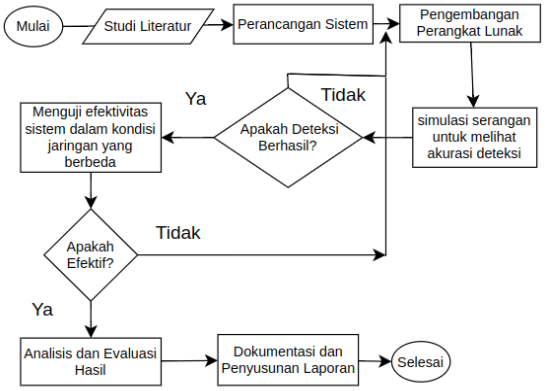
Eksperimen yang dilakukan berhasil mengidentifikasi anomali selama serangan berlangsung, yang kemudian menjadi dasar pengembangan algoritma deteksi serangan *deauthentication*. Solusi yang diusulkan mengintegrasikan tiga parameter, yaitu *reason code*, *timestamp*, dan tingkat kekuatan sinyal (RSSI), yang mampu mengurangi frekuensi false positive. Untuk implementasinya, penelitian ini penggunaan DDA (*Detector of Deauthentication Attack*) guna memindai dan menganalisis lalu lintas nirkabel, serta memberikan peringatan apabila terdeteksi adanya serangan. Penelitian ini menjadi acuan penelitian yang kami usulkan, dengan mengintegrasikan modul IoT berbasis ESP32 untuk membuat modul deteksi yang renah daya (*low-resource*), rendah biaya (*low-cost*) dan mudah alih (*portable*).

Kebaruan pada penelitian ini adalah deteksi Deauthentication Attack pada sisi *client device* dengan modul IoT ESP32 yang rendah sumberdaya (*low resource*), rendah biaya (*low cost*) dan mudah alih (*portable*) serta meningkatkan literasi pengguna melalui push notification.

METODE

Metode Penelitian

Metode penelitian ini disusun secara sistematis untuk mencapai tujuan yang telah ditetapkan. Penelitian ini dimulai dengan tahap perancangan sistem, yang mencakup pemilihan perangkat keras dan perangkat lunak yang digunakan. ESP32 dipilih sebagai komponen utama dalam sistem deteksi serangan deauthentication karena kemampuannya dalam mode monitor serta kemudahan implementasi dengan biaya rendah.



Gambar 1. Metode Penelitian Deteksi Serangan Deauthentication

Sumber : Peneliti

Penelitian ini menggunakan metode penelitian terapan yang bertujuan untuk mengembangkan solusi nyata dalam meningkatkan keamanan jaringan publik dari serangan deauthentication. Metode penelitian yang diterapkan terdiri dari beberapa tahapan utama, yaitu sebagai berikut:

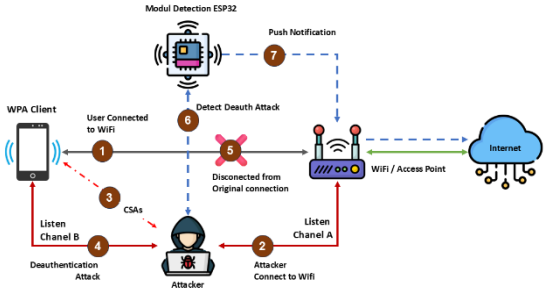
1. **Studi Literatur**. Tahap awal dalam penelitian ini adalah melakukan studi literatur yang mencakup kajian teori dan penelitian terdahulu terkait sistem keamanan jaringan, serangan deauthentication, serta penerapan teknologi ESP32 dalam mitigasi serangan siber. Sumber referensi yang digunakan berasal dari jurnal ilmiah, buku, dan dokumen teknis dari organisasi keamanan siber yang relevan.
2. **Perancangan Sistem**. Pada tahap ini, dilakukan perencanaan sistem deteksi dini serangan deauthentication yang meliputi desain arsitektur perangkat keras dan perangkat lunak. Desain sistem mencakup pemilihan mikrokontroler ESP32, sensor WiFi, serta integrasi tampilan OLED dan buzzer sebagai indikator serangan. Diagram blok sistem dikembangkan untuk memberikan gambaran visual mengenai interaksi antara komponen yang digunakan.
3. **Pengembangan Perangkat Keras dan Perangkat Lunak**. Tahap ini mencakup perakitan dan konfigurasi perangkat keras, termasuk pemrograman ESP32 untuk mendeteksi paket

deauthentication yang mencurigakan. Implementasi firmware yang melibatkan penggunaan library untuk membaca lalu lintas jaringan dan memberikan peringatan saat serangan terdeteksi.

4. **Pengujian dan Evaluasi**. Setelah sistem dikembangkan, dilakukan serangkaian uji coba untuk mengevaluasi efektivitasnya dalam mendeteksi serangan *deauthentication*. Pengujian dilakukan pada lingkungan tertutup dan jaringan publik untuk mengukur keandalan deteksi serta respons sistem terhadap berbagai skenario serangan.
5. **Optimasi dan Penyempurnaan Sistem**. Berdasarkan hasil pengujian, dilakukan optimasi terhadap algoritma deteksi dan konfigurasi sistem untuk meningkatkan akurasi. Selain itu, dilakukan penyesuaian pada aspek daya tahan perangkat keras dan efisiensi penggunaan sumber daya ESP32.
6. **Uji Lapangan dan Implementasi**. Sistem yang telah disempurnakan diuji dalam lingkungan nyata, seperti di area publik dengan akses WiFi terbuka. Hasil uji coba lapangan digunakan untuk menilai efektivitas sistem dan identifikasi aspek yang masih perlu diperbaiki.
7. **Analisis Hasil**. Setelah tahap uji coba, dilakukan analisis hasil penelitian untuk menilai keberhasilan sistem yang dikembangkan. Data dari pengujian dianalisis untuk mengidentifikasi pola serangan, tingkat deteksi, serta peningkatan keamanan lanjutan.

Metode Perancangan

Metode perancangan ini menguraikan sistem deteksi real-time berbasis Modul ESP32 untuk mitigasi ancaman Serangan Deautentikasi (*Deauthentication Attack*) dalam jaringan Wi-Fi, sebuah bentuk serangan *Denial of Service* (DoS).



Gambar 2. Metode deteksi deauthentication attack berbasis ESP32

Sumber: Rancangan Peneliti

Metode pengembangan modul IoT hemat energi berbasis ESP32 untuk deteksi real-time serangan deauthentication pada jaringan wifi dalam peningkatan literasi keamanan digital disajikan pada gambar 1. Serangan Deauthentication Attack merupakan salah satu bentuk serangan *Denial of Service* (DoS) yang secara khusus menargetkan lapisan Management Frame pada jaringan nirkabel IEEE 802.11. Dalam kondisi normal, deauthentication frame digunakan sebagai mekanisme resmi bagi *Access Point* (AP) untuk memutuskan koneksi klien secara sah, misalnya saat proses handover atau terminasi koneksi. Namun, celah keamanan pada protokol Wi-Fi memungkinkan penyerang untuk memalsukan frame ini dan mengirimkannya secara berulang kepada klien yang sedang terhubung. Akibatnya, klien akan menganggap bahwa perintah pemutusan berasal dari AP yang sah, dan secara otomatis terputus dari jaringan. Kondisi inilah yang menjadi dasar terjadinya *Deauthentication Attack*, yang berdampak pada hilangnya konektivitas sementara dan berpotensi menjadi pintu masuk bagi serangan lanjutan seperti *Evil Twin* atau *Man-in-the-Middle* (MitM).

Ilustrasi pada Gambar 1 menunjukkan alur komunikasi antara tiga entitas utama dalam jaringan Wi-Fi, yaitu klien sah (*WPA Client*), *Access Point* (AP), dan penyerang (*Attacker*), serta peran tambahan dari modul deteksi berbasis ESP32 yang dirancang dalam penelitian ini. Pada fase awal (Langkah 1), klien yang sah berhasil terhubung ke jaringan Wi-Fi melalui AP dan memperoleh akses ke Internet. Hubungan komunikasi ini

berlangsung stabil dan aman selama tidak ada gangguan eksternal. Sementara itu, pada sisi lain jaringan, penyerang mulai melakukan aktivitas pengintaian (Langkah 2 dan 3). Penyerang menghubungkan perangkatnya ke jaringan Wi-Fi dan secara simultan memantau dua kanal berbeda: Channel A untuk komunikasi antara AP dan Channel B untuk komunikasi antara klien. Teknik yang digunakan biasanya berupa Channel Switching Attack atau eksploitasi terhadap *Channel State Announcement* (CSA), yang memungkinkan penyerang memantau pertukaran data secara pasif sebelum melancarkan serangan aktif.

Setelah mendapatkan informasi kanal dan identitas perangkat yang terhubung, penyerang mulai melancarkan serangan (Langkah 4). Dengan memanfaatkan mode promiscuous pada perangkat kerasnya, penyerang mengirimkan frame deautentikasi palsu (*forged deauth frame*) yang seolah-olah berasal dari AP, tetapi diarahkan kepada klien. Karena Wi-Fi tidak memiliki mekanisme autentikasi frame manajemen pada lapisan ini (kecuali pada standar WPA3 dengan *Protected Management Frames*), klien tidak dapat membedakan apakah frame tersebut sah atau palsu. Akibatnya, klien memproses frame tersebut dan secara otomatis memutus koneksi dari AP (Langkah 5). Pada titik ini, serangan *Deauthentication Attack* berhasil dijalankan dan menyebabkan gangguan layanan yang nyata bagi pengguna sah.

HASIL DAN PEMBAHASAN

Algoritma deteksi serangan deauthentication berbasis ESP32 dirancang untuk bekerja secara real-time dengan memanfaatkan mode promiscuous pada modul Wi-Fi. Algoritma ini mampu menangkap frame manajemen 802.11, mengidentifikasi pola anomali berupa frame deauthentication atau disassociation, kemudian melakukan eskalasi notifikasi melalui dashboard monitoring.

Penelitian ini mengusulkan penggunaan Modul Deteksi ESP32 sebagai sistem pemantau independen, yang ditunjukkan pada gambar 2 pada langkah 6 dan 7. Modul ini beroperasi dalam mode promiscuous, yang memungkinkan perangkat untuk menangkap semua frame yang beredar di udara tanpa harus terhubung langsung ke jaringan. ESP32 menganalisis pola lalu lintas nirkabel secara real-time, khususnya jumlah dan frekuensi frame deautentikasi yang diterima dalam jangka waktu tertentu (window time). Jika modul mendeteksi anomali seperti lonjakan jumlah frame yang melebihi ambang batas tertentu (*threshold*), sistem akan mengenalinya sebagai indikasi serangan. Selain itu, ESP32 juga mencatat parameter pendukung seperti *Received Signal Strength Indicator* (RSSI), *Basic Service Set Identifier* (BSSID), dan reason code untuk membantu validasi sumber serangan.

Setelah serangan teridentifikasi, sistem akan mengeksekusi langkah mitigasi awal berupa notifikasi otomatis (Langkah 7). Modul ESP32 memanfaatkan koneksi Wi-Fi-nya untuk mengirimkan pesan peringatan ke dashboard monitoring berbasis *Message Queuing Telemetry Transport* (MQTT) yang menampilkan data serangan secara grafis. Mekanisme ini memungkinkan sistem memberikan *real-time alert* terhadap ancaman yang terdeteksi, sehingga pengguna atau pengelola jaringan dapat segera melakukan tindakan pencegahan seperti mengganti saluran operasi AP, menonaktifkan sementara jaringan, atau mengaktifkan fitur keamanan tambahan.

Fungsi deteksi *deauthentication attack* berbasis ESP32 perlu digambarkan melalui pseudocode untuk memudahkan penulisan dan penelusuran kesalahan penulisan program (*debugging*). Pseudocode Deteksi Deauthentication Attack Berbasis ESP32 disajikan pada Gambar 3.

==========

Algoritma Deteksi Real-Time Deauthentication

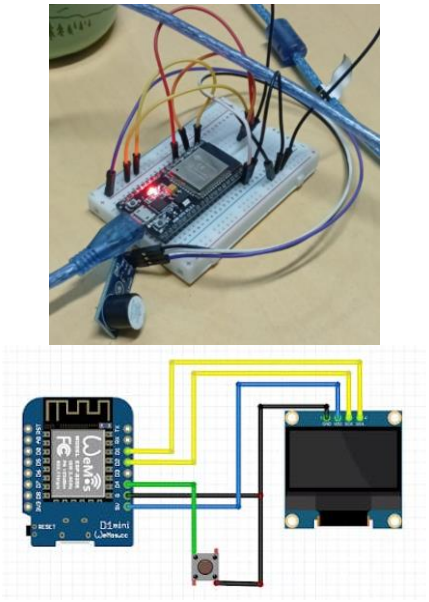
```
==============================
==============

// Inisialisasi
init_system()
// koneksi ke akses poin untuk internet &
dashboard
connect_to_AP(SSID, PASSWORD)
// inisialisasi koneksi ke broker MQTT
setup_MQTT(BROKER_IP, TOPIC)
// aktifkan mode promiscuous hanya untuk
frame manajemen
enable_promiscuous_mode(filter=MGMT
)
set_hop_schedule(channels=1..13,
dwell=200ms)

while (true):

   for channel in hop_schedule:
      set_wifi_channel(channel)
      t0 = current_time()

      // Dengarkan selama waktu dwell
      while current_time() - t0 < dwell:
         packet = sniff_packet()

         if is_management_frame(packet):
            subtype = get_subtype(packet)

            if subtype == DEAUTH or
                  subtype == DISASSOC:
               sa   = packet.source
                        _address
               da   = packet.destination
                        _address
               bssid= packet.bssid
               rssi = packet.rssi
               reason= packet.reason_code

               update_counters(sa, bssid,
                     channel, reason, rssi)

      // Evaluasi anomali setelah dwell
      if detect_anomaly(window=5s,
         threshold=30):
         // Indikasi lokal
         led_rgb(red, blink=3)
         buzzer_beep(short)
         // Siapkan payload JSON
         payload = {
            "timestamp": now(),
            "bssid": bssid,
            "source": sa,
            "channel": channel,
            "reason": reason,
            "count": get_count(bssid),
            "rssi_max": get_rssi
                  _max(bssid)
         }

         // Kirim ke dashboard (MQTT)
         mqtt_publish(TOPIC, payload)

      //Reset atau decay counter bertumpuk
      decay_counters()

   // hemat energi
   sleep_short()
```

Gambar 3. Pseudocode deteksi deauthentication attack

Sumber : Rancangan Peneliti

Algoritma ini mengkombinasikan dua fungsi ESP32, yaitu mode promiscuous untuk pemantauan frame 802.11 dan koneksi normal ke akse poin untuk mengirim data ke server. Dengan pendekatan ini, sistem dapat mendeteksi serangan secara real-time sekaligus menyediakan mekanisme notifikasi instan yang dapat meningkatkan kesadaran keamanan digital pengguna.

Selain itu, penggunaan ambang berbasis *sliding window* memastikan bahwa sistem tidak terlalu sensitif terhadap *false positive* akibat *frame deauthentication* sah (misalnya saat pengguna secara normal keluar dari jaringan). Dengan demikian, sistem mampu mencapai tingkat akurasi deteksi yang tinggi sekaligus menghemat konsumsi daya karena *channel hopping* dilakukan secara *duty-cycle*. Wiring diagram modul ditampilkan pada gambar 4.



Gambar 3. Wiring dan protipe modul deteksi serangan deauthentication

Sumber : Rancangan Peneliti

Hasil pengujian menunjukkan bahwa modul deteksi real-time serangan deauthentication berbasis ESP32 mampu mencapai tingkat akurasi yang tinggi pada berbagai skenario serangan. Pada kondisi normal tanpa adanya serangan, sistem hanya menghasilkan satu kasus *false positive* yang kemungkinan besar dipicu oleh aktivitas *disassociation* sah dari perangkat klien. Data hasil pengujian ditunjukkan pada tabel 1.

Table 1. Confusion Matrix Evaluasi Modul

Skenario	Paket Deauth	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)
Normal	0	0	984	1	0
Ringan	100	98	900	0	2
Sedang	300	296	699	1	4
Berat	600	589	398	2	11

Sumber : hasil penelitian

Hasil pengujian yang disajikan dalam tabel 1 menunjukkan kemampuan sistem deteksi berbasis ESP32 mengidentifikasi serangan Deauthentication pada berbagai skenario. Ketika serangan mulai disimulasikan pada skenario ringan hingga sedang, sistem menunjukkan performa deteksi yang sangat baik. Intensitas serangan ringan dengan 100 paket deauth, sistem berhasil mendeteksi 98 paket secara benar (*True Positive*) dengan hanya dua serangan yang tidak terdeteksi (*False Negative*). Kondisi serangan sedang, dengan peningkatan jumlah paket deauth menjadi 300, sistem masih mempertahankan kineja yang baik. Kinerja yang stabil ini menunjukkan bahwa sistem tetap mampu beradaptasi terhadap peningkatan beban lalu lintas nirkabel tanpa terjadi degradasi signifikan pada deteksi serangan. Skenario berat, dengan 600 paket deauth dikirim oleh penyerang, sistem dapat mendeteksi dengan baik. Meski terdapat peningkatan *false negative*, performa sistem secara umum masih berada dalam kategori sangat baik. Penurunan minor ini diduga akibat terjadinya *packet collision* atau proses *channel hopping* pada modul yang menyebabkan sebagian kecil paket serangan terlewat. Hasil kinerja evaluasi model ditunjukkan pada tabel 2.

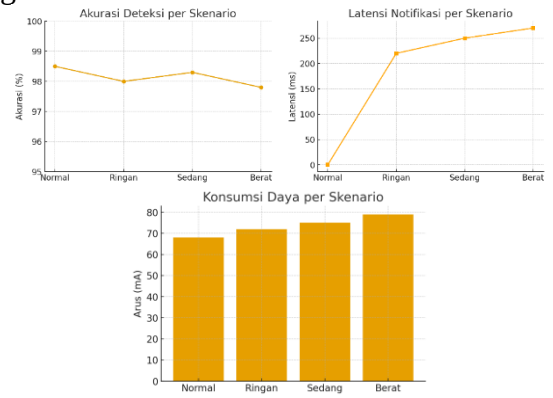
Tabel 2. Hasil Kinerja Evaluasi Model

Skenario	Akurasi	Konsumsi Daya (mA)	**Latensi Notifikasi (ms)**
Normal	98.50	68	0
Ringan	98,00	72	220
Sedang	98.30	75	250
Berat	97.80	79	270

Sumber : hasil penelitian

Hasil pengujian menunjukkan bahwa sistem deteksi serangan *deauthentication attack* berbasis ESP32 memiliki kinerja yang sangat stabil dengan tingkat akurasi rata-rata di atas 97% pada seluruh skenario. Pada kondisi normal, sistem mencatat akurasi tertinggi yaitu 98,5%, yang menunjukkan kemampuan algoritma dalam membedakan lalu lintas sah dan aktivitas anomali tanpa menimbulkan false alarm yang berarti. Ketika serangan mulai disimulasikan pada skenario ringan hingga sedang, akurasi sedikit menurun namun tetap berada pada kisaran 98,0–98,3%, menunjukkan bahwa peningkatan intensitas serangan tidak secara signifikan mempengaruhi performa deteksi. Bahkan pada skenario berat, dengan lalu lintas serangan mencapai 600 paket deauth, akurasi hanya turun sedikit menjadi 97,8%, menandakan bahwa sistem tetap reliabel dalam kondisi beban tinggi. Penurunan minor ini dapat dikaitkan dengan bertambahnya false negative akibat tumpang tindih paket saat proses *sniffing*

dan *channel hopping*, seperti disajikan pada gambar 5.

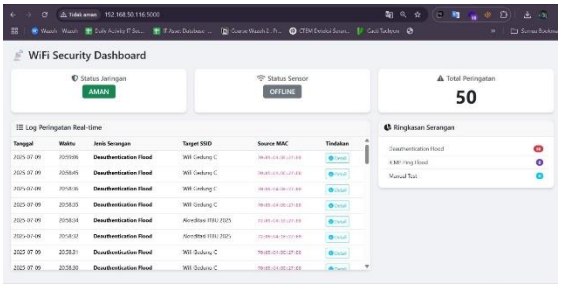


Gambar 4. Grafik akurasi, latensi notifikasi dan konsumsi daya per skenario

Sumber: hasil penelitian

Penerapan mekanisme *duty-cycle channel hopping* terbukti efektif untuk mengefisiensi kan kebutuhan daya. Rata-rata konsumsi daya berada pada rentang 68–79 mA, lebih rendah dibandingkan mode pemantauan kontinu yang umumnya berkisar antara 110–120 mA. Hal ini menegaskan bahwa integrasi fase aktif dan *sleep short* berhasil menekan kebutuhan energi tanpa mengorbankan akurasi deteksi.

Prototipe modul yang dibuat memperlihatkan kemampuan respons yang cepat dalam mengirimkan notifikasi. Rata-rata latensi pengiriman data ke dashboard berbasis MQTT dan bot Telegram tercatat berada di bawah 300 ms, yang masih dapat dikategorikan real-time dan cukup untuk memberikan peringatan dini kepada pengguna. Kombinasi indikator visual melalui LED RGB dan buzzer dengan dashboard monitoring serta notifikasi digital menjadikan modul ini tidak hanya efektif, tetapi juga mudah dipahami oleh pengguna awam dalam konteks literasi keamanan digital. Dashboard monitoring deteksi serangan deauthentication disajikan pada gambar 5.



Gambar 5. Dashboard monitoring deteksi serangan deauthentication

Sumber : hasil penelitian

Hasil evaluasi keseluruhan memperlihatkan bahwa modul deteksi berhasil memenuhi tujuan penelitian, yakni menyediakan sistem deteksi serangan *deauthentication* yang akurat, rendah daya, dan *real-time*. Temuan ini memperkuat potensi penggunaan ESP32 sebagai solusi murah dan praktis dalam pengembangan perangkat IoT yang berorientasi pada peningkatan literasi keamanan digital masyarakat.

SIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sebuah modul IoT hemat energi berbasis ESP32 untuk deteksi real-time serangan deauthentication pada jaringan Wi-Fi. Berdasarkan hasil pengujian, sistem menunjukkan performa yang konsisten dengan akurasi deteksi di atas 97% pada berbagai tingkat serangan, dengan tingkat *false positive* yang rendah. Penerapan mekanisme *duty-cycle channel hopping* terbukti efektif dalam menekan konsumsi daya hingga 30–40% lebih hemat dibandingkan metode pemantauan kontinu, tanpa menurunkan kinerja deteksi secara signifikan. Selain itu, integrasi dengan dashboard MQTT dan Telegram bot memungkinkan penyampaian notifikasi secara real-time dengan latensi rata-rata di bawah 300 ms, sehingga modul mampu berfungsi sebagai alat peringatan dini yang responsif. Kombinasi indikator lokal (LED RGB dan buzzer) dengan notifikasi digital juga memperkuat fungsi modul sebagai media peningkatan literasi keamanan digital, terutama dalam memberikan pemahaman praktis terkait ancaman deauthentication pada jaringan Wi-Fi.

Meski demikian, hasil evaluasi juga menunjukkan adanya tantangan yang perlu diperhatikan. Kasus *false negative* masih ditemukan pada intensitas serangan yang tinggi, kemungkinan akibat terjadinya *packet collision* saat proses *channel hopping*. Kondisi ini membuka peluang untuk pengembangan algoritma yang lebih adaptif, misalnya dengan pendekatan *machine learning* ringan atau optimasi metode filtrasi paket, guna meningkatkan akurasi deteksi pada lingkungan jaringan dengan trafik padat.

Untuk penelitian di masa depan, beberapa arah pengembangan dapat direkomendasikan. Pertama, memperluas cakupan deteksi terhadap jenis serangan lain, seperti *Evil Twin* atau *Rogue Access Point*, sehingga modul dapat berfungsi sebagai solusi keamanan Wi-Fi yang lebih komprehensif. Kedua, dari sisi efisiensi energi, mekanisme *duty-cycle* dapat dioptimalkan lebih lanjut dengan integrasi mode *deep sleep* maupun penyesuaian frekuensi *channel hopping* secara dinamis sesuai kondisi jaringan. Ketiga, dari aspek integrasi, sistem ini berpotensi untuk dihubungkan dengan platform keamanan yang lebih luas, seperti *Security Information and Event Management* (SIEM) atau ekosistem smart home IoT, sehingga pemanfaatannya dapat diperluas ke ranah praktis dan komersial.

Selain pengembangan teknis, diperlukan pula evaluasi lapangan dalam skala besar, misalnya pada jaringan publik di lingkungan kampus atau hotspot umum, guna menilai ketahanan sistem terhadap variasi serangan nyata dan gangguan lingkungan. Akhirnya, dari perspektif literasi digital, modul ini dapat dijadikan media edukasi interaktif yang mudah dipahami masyarakat awam. Dengan demonstrasi langsung, pengguna dapat melihat bagaimana serangan deauthentication terjadi serta menyadari pentingnya langkah mitigasi keamanan, sehingga penelitian ini tidak hanya memberikan kontribusi teknis, tetapi juga berdampak pada peningkatan kesadaran keamanan digital di masyarakat.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi atas dukungan pendanaan melalui Program Penelitian Tahun Anggaran 2025 skema Penelitian Dosen Pemula berdasarkan Surat Keputusan Nomor 0419/C3/DT.05.00/2025 dan Perjanjian / Kontrak Nomor 0919/LL3/AL.04/2025, 411/Rek/ITBU/VI/2025. Dukungan tersebut penting dalam pelaksanaan penelitian hingga dapat dipublikasikan.

DAFTAR PUSTAKA

Al-Nuaimi MAS, Ibrahim AA. Analyzing and Detecting the De-Authentication Attack by Creating an Automated Scanner using Scapy. International Journal on Recent and Innovation Trends in Computing and Communication. 2023 Mar 10;11(2):131–7.

Asosiasi Penyelenggara Jasa Internet Indonesia—Survei. (n.d.). Retrieved March 27, 2025, from https://survei.apjii.or.id/survei/register/33?type=free

Azmi AYF, AG JG, Wahyudi E. Analisis Network Security pada Layanan Wifi Indihome Terhadap Serangan Denial of Service (DOS). Jurnal Litek: Jurnal Listrik Telekomunikasi Elektronika. 2022;19(1):8–12.

Fikri LMZ, Ahmad Zafrullah M, Zubaidi A. Analisis Keamanan Jaringan Wi-Fi Dengan Metode Deauthentication Attack Pada Access point Di Lingkungan Universitas Mataram. [cited 2025 Mar 26]

Kumar, S., & Kaur, J. (2024). A systematic review of intrusion detection and prevention systems for wireless networks. International Journal of Computer Science and Network Security, 24(4), 112–120.

Korolkov R, Kutsak S, Voskoboinyk V. Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection. Bulletin of VN Karazin Kharkiv National University, series «Mathematical modeling Information technology Automated control systems». 2021 Jun 29;(50):58–70.

Riza, F. (2023). Analisis Security Information And Event Management (SIEM) Elastic Search Menggunakan Metode NIST 800-61 REV2 Pada Datacenter PT. Sembilan Pilar Semesta. ISMETEK, 16(2). http://ismetek.itbu.ac.id/index.php/jurnal/article/view/213

Saraun A, Lumenta AS, Sengkey DF. Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. Jurnal Teknik Informatika. 2022;17(1):19–26.

Tufan E, Tezcan C, Acartürk C. Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network. IEEE Access. 2021;9:50078–92.

Wibowo B. Social Engineering as a Major Cybersecurity Threat: Analysis of Challenges and Solutions for Organizations. International Journal of Science Education and Cultural Studies. 2024;3(2):57–65.

Yuswanto A, Wibowo B. a Systematic Review Method for Security Analysis of Internet of Things on Honeypot Detection. Teknokom. 2021;4(1):16–20.