Nusantara Journal of Multidisciplinary Science
Vol. 3, No. 10, Mei 2026
Hal 1477-1483
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Sistem Deteksi Serangan *Evil Twin* Menggunakan *ESP32* dan Bot Telegram

Airlangga Senja Dwitama[1] , Nasrul Faiz[2] , Farid Diaz Putra[3] , M. Danda Lazuardy Azka[4]
[1,2] Fakultas Teknik dan Industri, Universitas Pendidikan Indonesia, Bandung, Indonesia

Article Info

Article history:

Received Mei 5, 2026
Revised Mei 8, 2026
Accepted Mei 15, 2026

Kata Kunci:

ESP32,
Rogue Access Point,
Keamanan Wifi,
Telegram Bot,
Keamanan Jaringan

Keywords:

ESP32,
Rogue Access Point,
Wifi Security,
Telegram Bot,
Network Security

ABSTRAK

Penelitian ini bertujuan untuk meningkatkan keamanan jaringan WiFi melalui deteksi *Rogue Access Point (RAP)* menggunakan mikrokontroler ESP32. Penggunaan RAP menjadi ancaman serius dalam keamanan jaringan nirkabel karena dapat digunakan untuk melakukan serangan *Man-in-the-Middle* (MitM) guna mencuri data sensitif pengguna. Sistem yang dikembangkan memanfaatkan fitur pemindaian WiFi pada ESP32 untuk mengidentifikasi seluruh akses poin yang aktif di area tertentu dan membandingkannya dengan daftar akses poin resmi (*whitelist*) yang telah terdaftar. Jika terdeteksi adanya akses poin yang tidak dikenal atau mencurigakan, sistem akan mengirimkan notifikasi secara *real-time* kepada administrator melalui bot Telegram. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi kehadiran RAP dengan akurasi yang baik dan memberikan peringatan instan, sehingga memungkinkan penanganan ancaman keamanan secara lebih cepat dan efisien. Implementasi ini menawarkan solusi pemantauan jaringan yang portabel, berbiaya rendah, dan efektif untuk lingkungan institusi maupun akademik

ABSTRACT

This research aims to enhance WiFi Network security through the detection of Rogue Access Points (RAP) using the ESP32 microcontroller. The presence of RAP poses a significant threat to wireless Network security as it can be exploited for Man-in-the-Middle (MitM) attacks to steal sensitive user data. The developed system utilizes the WiFi scanning feature of the ESP32 to identify all active access points in a specific area and compares them against a registered whitelist of authorized access points. If an unauthorized or suspicious access point is detected, the system sends a real-time notification to the administrator via a Telegram bot. Test results demonstrate that the system can accurately detect RAP and provide instant alerts, enabling faster and more efficient responses to security threats. This implementation offers a portable, low-cost, and effective Network monitoring solution for institutional and academic environments.

Corresponding Author:

Airlangga Senja Dwitama
Fakultas Teknik dan Industri, Universitas Pendidikan Indonesia,
Bandung, Indonesia
Email: airlangga126@student.upi.edu

1. PENDAHULUAN

Peningkatan ketergantungan masyarakat terhadap jaringan nirkabel (WiFi) di berbagai sektor, mulai dari perkantoran hingga institusi pendidikan, membawa konsekuensi logis berupa meningkatnya risiko keamanan. Salah satu ancaman yang paling krusial adalah kemunculan *Rogue Access Point* (RAP) [1]. RAP merupakan akses poin yang terpasang pada jaringan tanpa izin dari administrator, yang sering kali digunakan oleh penyerang untuk menyamar sebagai jaringan resmi, yang umumnya dikenal sebagai serangan *Evil Twin* [2]. Serangan berbasis RAP sangat berbahaya karena pengguna biasa sering kali tidak menyadari bahwa mereka terhubung ke perangkat palsu, yang dapat menyebabkan perangkat pengguna secara otomatis beralih ke AP palsu tersebut [2]. Begitu terhubung, penyerang dapat memantau seluruh lalu lintas data, melakukan pencurian kredensial, hingga penyuntikan *malware*, sehingga deteksi yang efektif sangat krusial [3]. Meskipun solusi keamanan jaringan tingkat perusahaan sudah tersedia, perangkat tersebut sering kali membutuhkan biaya investasi yang tinggi dan konfigurasi yang kompleks, sehingga memunculkan kebutuhan akan sistem yang adaptif, berbiaya rendah, dan mudah digunakan untuk audit keamanan [4]. Oleh karena itu, diperlukan sebuah sistem deteksi yang bersifat mandiri, portabel, dan konomis. Mikrokontroler ESP32 dipilih sebagai basis perangkat keras dalam penelitian ini karena memiliki prosesor *dual-core*, modul WiFi terintegrasi, serta kemampuan mengeksekusi *multitasking* secara efisien, yang memungkinkannya digunakan sebagai *sniffer* paket jaringan dengan konsumsi daya yang rendah [5]. Selain itu, integrasi peringatan keamanan secara *real-time* sangat dibutuhkan. Penggunaan *Bot API* dari aplikasi Telegram memungkinkan sistem untuk berinteraksi langsung dengan pengguna atau administrator jaringan melalui pesan singkat [6]. Dengan menggunakan Telegram, peringatan keamanan tidak lagi terbatas pada *log server*, melainkan langsung dikirimkan berupa notifikasi alarm ke perangkat seluler pemilik secara instan [7]. Perpaduan mikrokontroler ESP32 dengan Telegram Bot ini telah terbukti menghasilkan inovasi solusi keamanan berbasis IoT yang dapat dikendalikan dari jarak jauh, mudah diintegrasikan, dan memiliki biaya implementasi yang relatif rendah [8]. Penelitian ini memfokuskan pada pengembangan algoritma deteksi RAP yang membandingkan SSID dan BSSID di area cakupan dengan basis data akses poin yang sah. Melalui penelitian ini, diharapkan tercipta sebuah prototipe sistem keamanan WiFi yang dapat membantu tenaga IT atau administrator jaringan dalam mengawasi integritas area nirkabel mereka dari serangan akses poin ilegal secara lebih proaktif.

2. METODE

Penelitian ini menggunakan pendekatan eksperimental dengan merancang bangun sebuah sistem purwarupa pendeteksi *Rogue Access Point* (RAP) berbasis *Internet of Things* (IoT). Fokus utama sistem ini adalah mendeteksi serangan *Man-in-the-Middle* (MitM), khususnya tipe *Evil Twin* [2]. Penelitian ini dilakukan melalui tahapan studi literatur, perancangan perangkat keras dan lunak, pengujian, integrasi, serta analisis kinerja.

2.1 Arsitektur Sistem dan Konfigurasi Dinamis

Sistem ini beroperasi dengan prinsip kerja yang merujuk pada model referensi *Open Systems Interconnection* (OSI). Secara spesifik, NodeMCU ESP32 difungsikan sebagai sensor pada *Layer* 2 (*Data Link Layer*) untuk mengidentifikasi perangkat melalui parameter *Basic Service Set Identifier* (BSSID) [5]. Penempatan sistem pada lapisan ini sangat penting karena serangan *Evil Twin* memanipulasi identitas fisik akses poin. Pemetaan kerja sistem ini dapat diuraikan sebagai berikut: *Layer* 7 (*Application*) menggunakan API Telegram, *Layer* 4 (*Transport)* menggunakan HTTPS, *Layer* 3 (*Network*) menangani pengalamatan IP, *Layer* 2 (*Data Link*) sebagai fokus pemindaian MAC Address, dan *Layer* 1 (*Physical*) untuk transmisi sinyal WiFi. Implementasi fisik perangkat dimodifikasi melalui proses penyolderan antena eksternal secara langsung pada *board* mikrokontroler untuk meminimalisir atenuasi dan memperkuat daya tangkap sinyal [4]. Keseluruhan rangkaian komponen kemudian disusun

dengan rapi ke dalam sebuah kotak pelindung (*case*) guna memudahkan pengujian di lapangan. Implementasi bentuk fisik final dari perangkat sensor *Layer* 2 yang telah terlindungi kotak pelindung (*case*) ditunjukkan pada Gambar 1

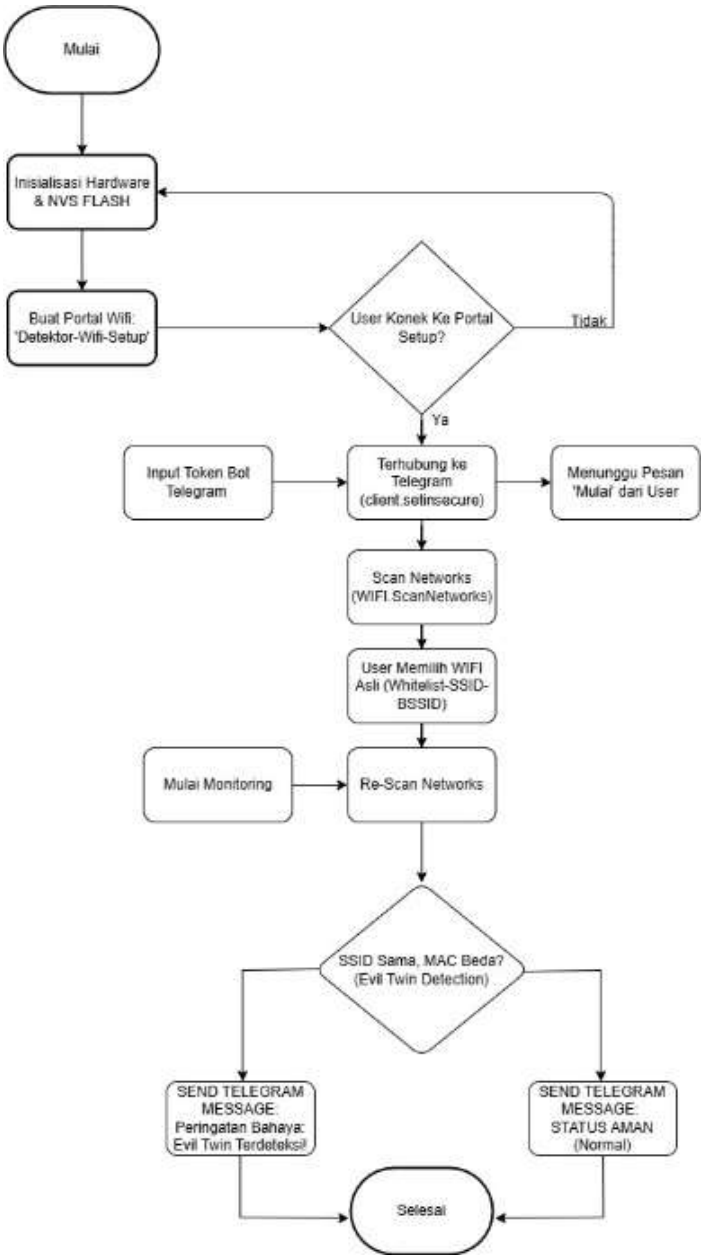
Gambar 1. Implementasi Fisik Final Perangkat Sensor Deteksi Rogue AP

Selain bentuk fisik akhir, perancangan interkoneksi antarkomponen juga dilakukan untuk mengoptimalkan kinerja perangkat. Modifikasi utama dilakukan dengan menyolder langsung antena eksternal pada titik kontak (*pad*) RF di papan sirkuit ESP32, guna meminimalisir redaman sinyal yang sering terjadi pada penggunaan kabel konektor biasa. Selain itu, ditambahkan pula sebuah tombol *reset* manual yang terhubung pada pin khusus. Tombol ini berfungsi secara praktis untuk memicu kembali mode *Captive Portal* apabila administrator perlu merubah konfigurasi jaringan sewaktu-waktu tanpa harus melakukan *flash* ulang program. Detail skema interkoneksi komponen elektronik dan letak penyolderan ini ditunjukkan pada Gambar 2.

Gambar 2. Skema Rangkaian Elektronika Sistem dengan Modifikasi Antena dan Tombol *Reset*

2.2 Logika Algoritma Deteksi

Setelah perakitan perangkat keras, sistem diprogram menggunakan Arduino IDE. Algoritma pendeteksian didasarkan pada pemindaian (*scanning*) parameter BSSID dari jaringan yang aktif [4]. Sistem menyimpan daftar akses poin yang sah ke dalam memori sebagai *whitelist*. Pemindaian dilakukan secara terus-menerus untuk membandingkan parameter jaringan yang tertangkap. Indikasi serangan *Evil Twin* terjadi apabila sistem menemukan adanya duplikasi nama jaringan (SSID) yang persis sama dengan target, namun memancarkan alamat fisik (BSSID) yang berbeda [1]. Urutan proses keseluruhan dari sistem pendeteksian ini diilustrasikan secara rinci melalui diagram alir pada Gambar 3.



Gambar 3. Rangkaian Flowchart Algoritma Deteksi

3.3 Mekanisme Notifikasi

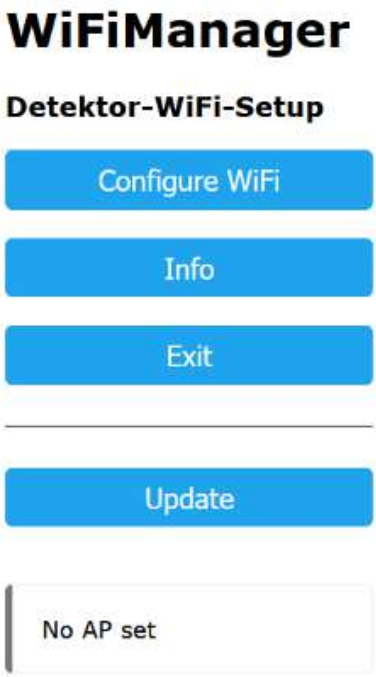
Sistem terintegrasi secara langsung dengan API Telegram untuk memberikan peringatan dini [6]. Mekanisme pengiriman pesan pada ESP32 dirancang berbasis perubahan status (*state-change based*) [7]. Sistem ini diatur agar hanya mengirimkan notifikasi *real-time* ketika terjadi anomali pertama kali, sehingga mencegah perangkat administrator menerima tumpukan pesan *spam* yang berulang-ulang [3].

3. HASIL DAN PEMBAHASAN

Bab ini menguraikan hasil implementasi dan pengujian dari purwarupa sistem pendeteksi *Rogue Access Point berbasis* ESP32 yang telah dirancang. Pengujian dilakukan untuk mengevaluasi kinerja sistem dalam kondisi operasional, dengan fokus pada tiga aspek utama: kemudahan konfigurasi perangkat lunak melalui *Captive Portal*, kecepatan dan akurasi algoritma dalam mendeteksi skenario serangan *Evil Twin*, serta evaluasi jangkauan deteksi fisik setelah dilakukan modifikasi antena. Rangkaian pengujian ini bertujuan untuk memastikan bahwa sistem mampu beroperasi secara efektif sesuai dengan parameter keamanan yang telah ditetapkan pada metodologi penelitian [4].

3.1 Implementasi Perangkat Lunak dan Konfigurasi

Penerapan *library* WiFiManager memungkinkan administrator melakukan konfigurasi secara dinamis tanpa mengubah kode sumber [8]. Saat perangkat pertama kali dijalankan, sistem akan memancarkan sinyal WiFi konfigurasi yang menampilkan halaman utama *Captive Portal* seperti pada Gambar 2. Administrator kemudian dapat memasukkan SSID target pemantauan serta Token Bot Telegram melalui formulir pengaturan yang ditunjukkan pada Gambar 3.



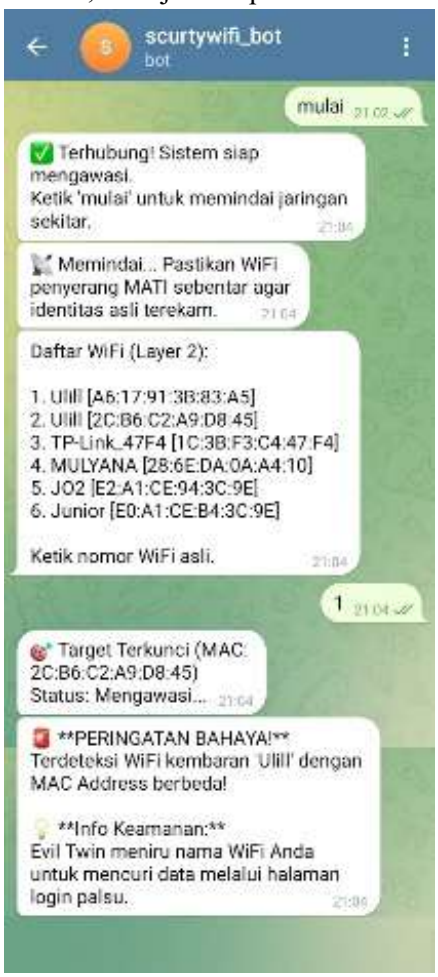
Gambar 4. Tampilan Halaman Utama *Captive Portal*

Gambar 5. Antarmuka Konfigurasi Parameter Jaringan

3.2 Pengujian Serangan *Evil Twin* dan Notifikasi *Real-Time*

Pada tahap pengujian keamanan, sistem dihadapkan pada skenario serangan *Evil Twin*, di mana sebuah akses poin ilegal memancarkan SSID target ("Ulill") namun memiliki BSSID yang tidak

terdaftar dalam *database whitelist* [2]. Algoritma pemindaian *Layer* 2 berhasil mengidentifikasi anomali tersebut secara instan. Seketika itu juga, sistem memicu pengiriman notifikasi peringatan ke perangkat ponsel administrator [7]. Hasil pesan peringatan yang diterima melalui aplikasi Telegram, yang memuat detail ancaman dan informasi keamanan, ditunjukkan pada Gambar 6.



Gambar 6. Tampilan Notifikasi Telegram saat Terjadi Serangan

3.3 Pengujian Jangkauan Deteksi dan Pengaruh Antena Eksternal

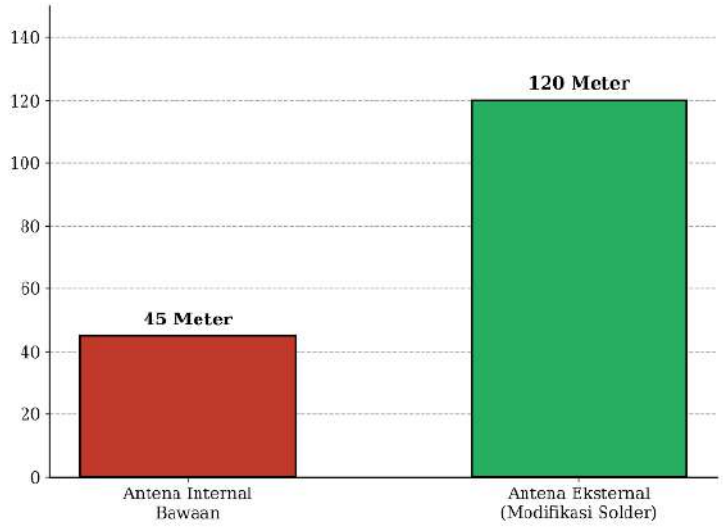
Untuk memastikan sistem pemantauan dapat mencakup area nirkabel yang luas, dilakukan pengujian jangkauan penerimaan sinyal (SSID) oleh mikrokontroler ESP32 [5]. Pengujian ini membandingkan kemampuan daya tangkap sensor dalam dua kondisi operasional perangkat keras: menggunakan antena internal bawaan modul dan menggunakan tambahan antena eksternal hasil modifikasi penyolderan langsung pada *board.* Rekapitulasi hasil perbandingan jarak deteksi maksimal secara *Line of Sight* (LoS) disajikan pada Tabel 1.

Table 1. Hasil Perbandingan Jangkauan Deteksi ESP32

Kondisi Pengujian	Jarak Maksimal	Kualitas Penerimaan
Antena Internal Bawaan	45 Meter	Rendah / Sering Drop
Antena Eksternal (Solder)	120 Meter	Stabil dan Sangat Baik

Berdasarkan pengujian, jangkauan deteksi sistem meluas secara signifikan. Jika sebelumnya perangkat hanya bisa memvalidasi ancaman hingga jarak 45 meter, modifikasi fisik berupa penyolderan antena eksternal berhasil meluaskan cakupan keamanan hingga 120 meter. Hal ini membuktikan bahwa

intervensi perangkat keras sangat krusial untuk mengoptimalkan *coverage area* pengawasan jaringan [1].



Gambar 7. Grafik Perbandingan Jangkauan Deteksi Antena

4. KESIMPULAN

Penelitian ini berhasil merancang dan membangun sistem keamanan WiFi untuk mendeteksi *Rogue Access Point berbasis Internet of Things* (IoT). Sistem terintegrasi secara fungsional dengan NodeMCU ESP32, antena eksternal, dan aplikasi Telegram. ESP32 yang beroperasi sebagai sensor *Layer* 2 terbukti efektif mendeteksi serangan *Evil Twin* dengan mengenali duplikasi SSID yang memiliki MAC Address berbeda. Sistem juga menawarkan kemudahan melalui konfigurasi dinamis WiFiManager dan modifikasi antena fisik yang berhasil meningkatkan jangkauan pemantauan dari 45 meter menjadi 120 meter. Peringatan dini juga terkirim secara *real-time* ke Telegram administrator tanpa *delay* yang mengganggu, menjadikannya solusi pemantauan jaringan yang portabel dan efisien.

REFERENSI

[1] N. A. Aljehane, "Invisible Scout: A *Layer* 2 Anomaly System for Detecting *Rogue Access Point (RAP)*," International Journal of Software Engineering, 2021.
[2] M. AL-Makhadmeh and A. Tolba, "Investigation of WiFi Security Auditing Tools for *Evil Twin* Attacks and Detection," IEEE Access, 2023.
[3] J. Wang, et al., "Convolutional neural *Network* based *Evil Twin* attack detection in WiFi *Network*s," MATEC Web of Conferences, 2021.
[4] A. Kurniawan, "Pengembangan Purwarupa Alat Packet Capture dan Analisis Untuk Deteksi Rogue Access Point," ETD Universitas Gadjah Mada, 2020.
[5] R. S. Putra, "Dual-Interface WiFi Packet *Sniffer* System using ESP32-CAM with *Real-time* PCAP Generation for IoT *Network* Analysis," Makara Journal of Technology, 2022.
[6] S. R. Kumar, "Webpage And Telegram Bot Controlled Home Automation System Using Raspberry Pi3," International Journal of Scientific & Technology Research, 2020.
[7] F. A. Rahman, "Designing Home Security With Esp32-Cam and IoT-Based Alarm Notification Using Telegram," bit-Tech Journal, 2021.
[8] D. Prasetyo, "Pemanfaatan Telegram Bot pada Sistem Keamanan Rumah Berbasis IoT dengan Mikrokontroler ESP32," Jurnal Senatib, 2022