BAB 2
TINJAUAN PUSTAKA

2.1 Landasan Teori

Pada sub-bab ini, diuraikan berbagai konsep dan teori dasar yang menjadi landasan dalam pelaksanaan penelitian. Pembahasan difokuskan pada prinsip kerentanan keamanan jaringan nirkabel, metode serangan *Evil Twin*, *deauthentication attack*, dan skenario *Man-in-the-Middle* (MITM), serta mekanisme pengalihan melalui *captive portal*. Selain itu, diuraikan pula spesifikasi teknis perangkat mikrokontroler ESP32 beserta protokol komunikasi UART yang menjustifikasi penggunaan arsitektur *dual-mikrokontroler* pada alat yang diimplementasikan.

2.1.1 Keamanan Jaringan Nirkabel

Keamanan jaringan nirkabel merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data yang dikirim melalui udara. Karena jaringan nirkabel menggunakan gelombang radio sebagai media transmisinya, data dapat ditangkap oleh siapa pun yang berada dalam jangkauan sinyal, sehingga meningkatkan risiko penyadapan dan manipulasi data. Berbeda dengan jaringan kabel yang memiliki jalur fisik dan tertutup, jaringan nirkabel bersifat terbuka dan dapat diakses oleh banyak perangkat secara bersamaan.

Untuk mengatasi kerentanan tersebut, berbagai protokol keamanan telah dikembangkan, seperti WEP, WPA, WPA2, hingga yang terbaru WPA3. Selain itu, sistem autentikasi seperti 802.1X, *MAC filtering*, dan metode enkripsi *end-to-end* juga sering digunakan untuk memperkuat keamanan jaringan (Boncella, 2002). Meskipun begitu, jaringan nirkabel masih menjadi sasaran empuk bagi berbagai jenis serangan, terutama jika pengguna atau administrator tidak memperhatikan pengaturan keamanan dasar.

2.1.2 Protokol WPA2

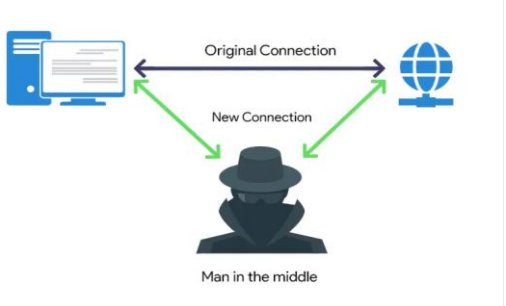
WPA2 (Wi-Fi Protected Access 2) merupakan standar keamanan nirkabel yang umum digunakan untuk melindungi jaringan dari akses yang tidak sah. Pada jaringan yang menggunakan otentikasi *WPA2-PSK (Pre-Shared Key)*, proses

pengamanan komunikasi antara *access point* dan perangkat klien tidak dilakukan dengan mengirimkan kata sandi secara polos *(plaintext)* melalui udara. Alih-alih demikian, protokol ini menggunakan mekanisme *4-Way Handshake* yang dienkapsulasi dalam protokol EAPOL *(Extensible Authentication Protocol over LAN)* (Ghanem & Ratnayake, 2016).

Mekanisme *4-Way Handshake* berfungsi untuk memverifikasi bahwa kedua belah pihak memiliki kunci rahasia yang sama (*passphrase* atau kredensial) dan menghasilkan kunci enkripsi sesi (*Pairwise Transient Key* / PTK) untuk melindungi pertukaran data selanjutnya. Proses ini melibatkan empat tahapan pertukaran pesan, di mana parameter acak (*nonce*) dan nilai integritas pesan (*Message Integrity Code* / MIC) saling dipertukarkan. Dalam konteks pengujian keamanan jaringan, paket-paket *4-Way Handshake* ini dapat direkam oleh pihak ketiga yang berada dalam jangkauan sinyal. Jika keseluruhan paket *handshake* berhasil ditangkap dan diekspor ke dalam format standar seperti HCCAPX, struktur kriptografi tersebut dapat dianalisis dan diretas secara luring (*offline cracking*) menggunakan metode *brute-force* atau serangan kamus (*dictionary attack*) untuk menemukan *Pre-Shared Key* aslinya.

2.1.3 Man-in-the-Middle (MITM) Attack

Serangan *Man-in-the-Middle* (MITM) adalah salah satu teknik paling berbahaya dalam dunia jaringan karena memungkinkan pihak penyusup berada di antara dua pihak yang berkomunikasi. Data dalam komunikasi tersebut dapat disadap (*eavesdropping*), diubah, atau disisipkan tanpa diketahui oleh kedua belah pihak (Mallik, 2019). Dalam konteks pengujian keamanan, MITM biasanya terjadi ketika pengguna terhubung ke *access point* palsu yang dikendalikan oleh penyerang, sebagaimana diilustrasikan pada Gambar 2.1 (Beagle Security, 2020).

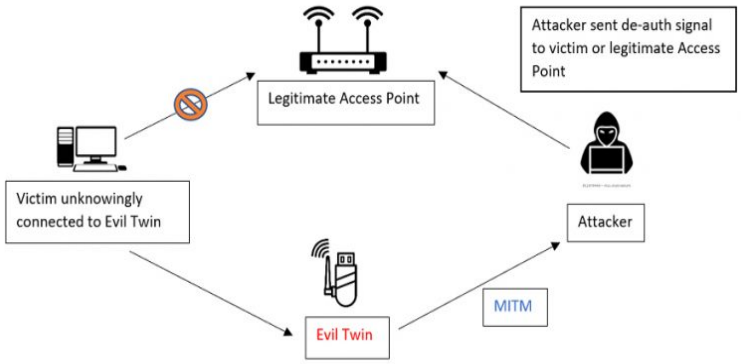


Gambar 2.1 *Man in The Middle*

Setelah koneksi terbentuk, seluruh lalu lintas jaringan dari perangkat korban dapat dialihkan melalui perangkat peretas. Dengan bantuan perangkat lunak seperti Wireshark atau *tcpdump*, aktivitas internet korban dapat dipantau, hingga perekaman kredensial yang dikirim melalui protokol yang tidak terenkripsi dapat dilakukan. MITM menjadi sangat berbahaya karena meskipun jaringan terlihat normal di sisi pengguna, semua aktivitas sebenarnya telah dimonitor secara diam-diam.

2.1.4 Evil Twin attack

Evil Twin merupakan salah satu bentuk eksploitasi jaringan nirkabel. Dalam serangan ini, sebuah *access point* palsu dibuat dengan *Service Set Identifier* (SSID) yang menyerupai jaringan WiFi asli (Selvarathinam dkk., 2019). Ketika pengguna secara tidak sadar terhubung ke jaringan palsu ini, lalu lintas jaringan dapat dipantau, dan korban dapat diarahkan ke *captive portal* palsu untuk mencuri informasi penting seperti *username*, *password*, atau data sensitif lainnya, seperti yang ditunjukkan pada Gambar 2.2 (Networkguru.ru, 2022).



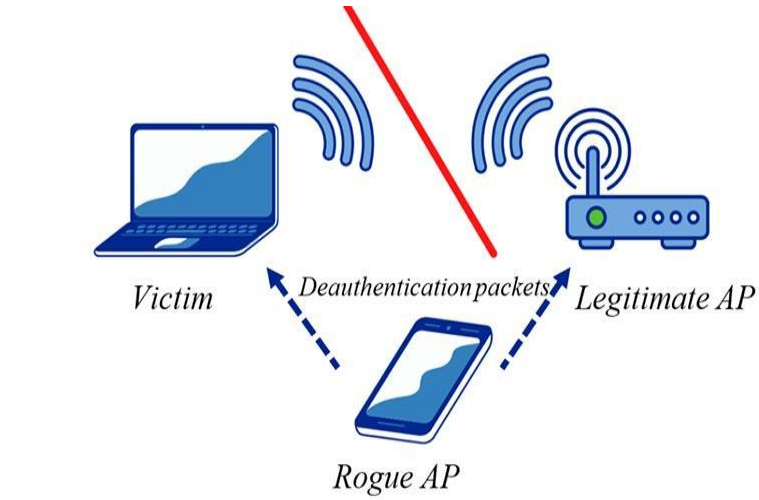
Gambar 2.2 *Evil Twin*

Serangan ini umumnya disimulasikan atau terjadi di tempat-tempat umum seperti bandara, kafe, atau kampus, di mana perangkat cenderung mudah terhubung ke jaringan WiFi tanpa memverifikasi keasliannya. Karena nama jaringan (SSID) yang ditampilkan dapat disamakan dengan jaringan asli, pengguna sering kali tidak menyadari bahwa koneksi tersebut dikendalikan oleh penyerang. Hal ini membuktikan bahwa selain aspek teknis, kesadaran pengguna terhadap keamanan

juga sangat penting dalam mencegah keberhasilan eksploitasi ini.

2.1.5 Deauthentication Attack

Deauthentication attack adalah teknik yang digunakan untuk memutus koneksi antara perangkat pengguna dan *access point* yang sah. Teknik ini memanfaatkan kelemahan dalam protokol IEEE 802.11, di mana *frame deauthentication* dapat dikirim secara terbuka tanpa memerlukan proses autentikasi (Arora, 2018). Akibatnya, *frame* tersebut dapat disisipkan dan dikirimkan secara sepihak ke klien target untuk memaksanya terputus dari jaringan, sebagaimana diilustrasikan pada Gambar 2.3 (Sepio Cyber, 2021).



Gambar 2.3 *Deauthentication Attack*

Setelah perangkat korban terputus, sistem operasi perangkat umumnya akan mencoba menyambung kembali ke jaringan yang sama secara otomatis. Pada momen ini, *access point* palsu (*Evil Twin*) dengan nama SSID yang sama disisipkan agar memancar lebih kuat. Karena proses penyambungan dilakukan secara otomatis oleh perangkat keras korban, koneksi beralih ke *access point* palsu dapat terjadi tanpa disadari oleh pengguna. Teknik ini menjadi langkah awal yang paling umum digunakan dalam skenario serangan nirkabel.

2.1.6 Captive portal

Captive portal merupakan halaman *web* yang muncul otomatis ketika sebuah perangkat terhubung ke jaringan WiFi, yang biasanya digunakan untuk keperluan *login* atau persetujuan syarat penggunaan sebelum mendapatkan akses internet

(Larose dkk., 2020). Secara umum, *captive portal* digunakan di lingkungan publik seperti hotel, bandara, dan kampus sebagai pintu masuk otorisasi jaringan, seperti yang terlihat pada Gambar 2.4 (honoki.net, 2015).

Gambar 2.4 *Captive portal*

Namun dalam konteks pengujian keamanan, *captive portal* dapat dimodifikasi untuk meniru halaman *login* resmi. Halaman tiruan ini umumnya dibangun menggunakan HTML, CSS, dan JavaScript agar tampak sangat meyakinkan. Setelah informasi *login* dimasukkan oleh pengguna, data kredensial tersebut dikirim dan direkam ke dalam sistem yang dikendalikan oleh pihak penguji atau penyerang. Teknik ini sering diintegrasikan dalam *Evil Twin attack* sebagai metode utama pencurian kredensial, terutama apabila target tidak mewaspadai tanda-tanda ketidakabsahan jaringan.

2.1.7 Packet sniffing

Packet sniffing adalah teknik pencegatan dan perekaman lalu lintas data yang melintas di dalam sebuah jaringan komunikasi. Pada jaringan nirkabel (IEEE 802.11), *packet sniffing* dapat dilakukan dengan mengubah mode operasi *Network Interface Card* (NIC) menjadi *promiscuous mode*. Dalam mode standar, antarmuka jaringan akan mengabaikan paket data yang tidak ditujukan pada alamat MAC-nya sendiri. Namun, saat *promiscuous mode* diaktifkan, antarmuka akan menangkap

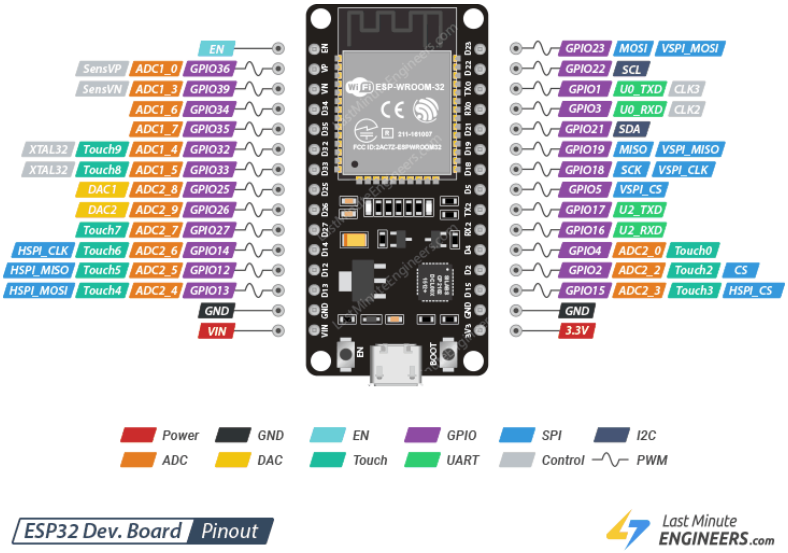
seluruh lalu lintas paket (*raw frames*) yang mengudara pada saluran frekuensi (*channel*) tertentu, tanpa memedulikan alamat tujuannya (Setiawan dkk., 2025).

Data mentah hasil *sniffing* tersebut kemudian dienkapsulasi dan disimpan ke dalam format PCAP (*Packet Capture*). Format PCAP merupakan standar industri yang digunakan untuk menyimpan rekaman lalu lintas jaringan, yang terdiri dari *header* global (*global header*) yang menyimpan informasi meta seperti zona waktu dan standar tautan data, serta diikuti oleh *header* paket (*packet header*) dan muatan paket sesungguhnya. Format ini memastikan interoperabilitas data sehingga hasil rekaman dapat diekspor, diunduh, dan dianalisis secara mendalam menggunakan perangkat lunak analisis protokol jaringan pihak ketiga, seperti Wireshark.

2.1.8 Arsitektur Mikrokontroler ESP32

ESP32 merupakan keluarga sistem-dalam-cip (*System-on-a-Chip / SoC*) berbiaya rendah yang terintegrasi dengan modul WiFi dan Bluetooth (Espressif Systems, 2023). Dalam pengembangan sistem uji penetrasi pada penelitian ini, terdapat kebutuhan fungsional di mana antarmuka pengguna, layanan *web*, dan manipulasi radio perlu dijalankan secara spesifik. Untuk memenuhi kebutuhan tersebut, pemisahan tugas secara fisik pada dua varian arsitektur ESP32 yang berbeda diterapkan.

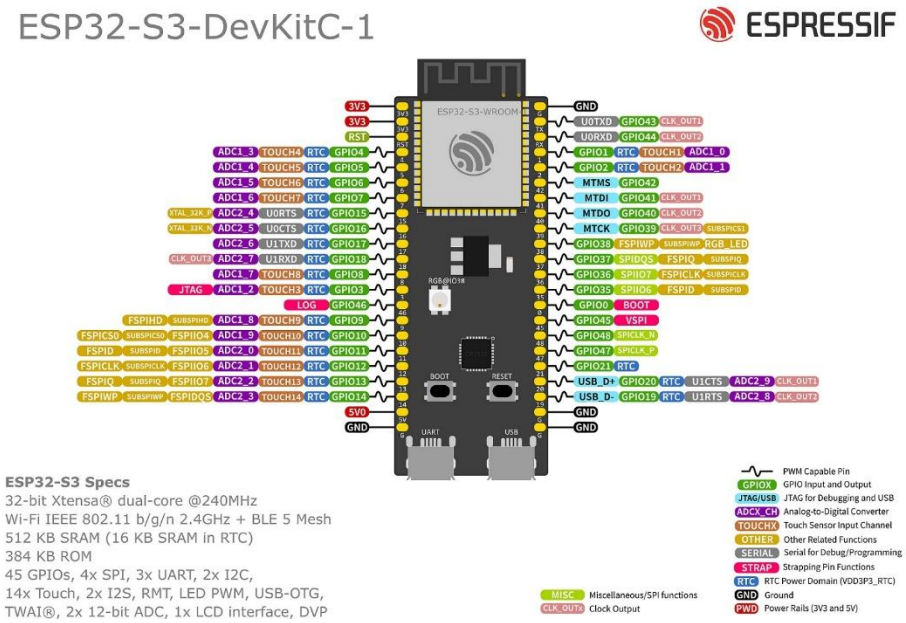
Varian pertama adalah ESP32 standar atau klasik yang umumnya dibangun berbasis pada arsitektur Xtensa *Dual-Core* 32-bit LX6. Tata letak pin (*pinout*) dari mikrokontroler varian ini dapat dilihat pada Gambar 2.5.



Gambar 2.5 *Pinout* Mikrokontroler ESP32

Keunggulan utama varian ini dalam konteks keamanan nirkabel terletak pada dukungan pustaka dasar (*base library*) yang sangat matang untuk manipulasi paket (*raw frame*) nirkabel pada *Data Link Layer*. Karakteristik tersebut menjadikannya andal untuk didelegasikan secara khusus dalam mengoperasikan *deauthentication attack*, *packet sniffing*, dan *WPA handshake capture*.

Varian kedua adalah mikrokontroler ESP32-S3 yang dikembangkan menggunakan arsitektur Xtensa *Dual*-Core 32-bit LX7. Susunan tata letak pin (*pinout*) untuk varian ESP32-S3 diilustrasikan pada Gambar 2.6.

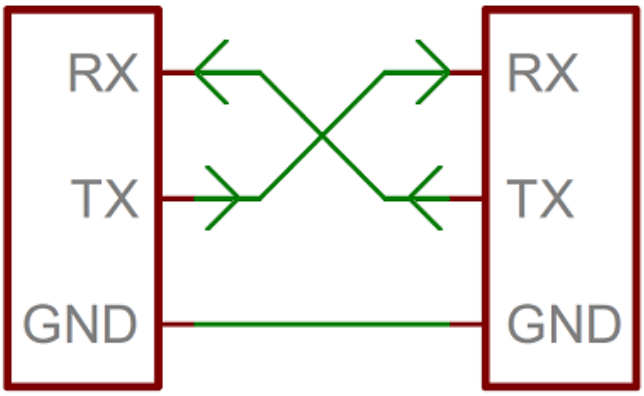


Gambar 2.6 *Pinout* Mikrokontroler ESP32-S3

Peningkatan arsitektur pada varian ESP32-S3 menawarkan performa komputasi yang memadai serta ketersediaan antarmuka *General-Purpose Input/Output* (GPIO) yang lebih banyak dibandingkan pendahulunya (Espressif Systems, 2026). Kelebihan ini membuatnya sangat ideal untuk difungsikan sebagai otak pengendali utama yang menjalankan antarmuka layar visual, pembacaan matriks tombol, pemindaian jaringan (*scanning*), pemancaran *Evil Twin*, serta penyediaan *web server* untuk *captive portal*.

2.1.9 Komunikasi Serial UART

Universal Asynchronous Receiver-Transmitter (UART) merupakan salah satu protokol komunikasi serial asinkron yang paling umum digunakan untuk mentransfer data antar perangkat mikrokontroler. Tidak seperti protokol sinkron (seperti SPI atau I2C) yang membutuhkan jalur sinyal *clock* terpisah, UART bekerja secara asinkron dengan menyepakati kecepatan transmisi data atau *baudrate* (misalnya 115200 bit per detik) antara perangkat pengirim dan penerima.



Gambar 2.7 Jalur komunikasi UART antar mikrokontroler

Protokol UART hanya membutuhkan dua jalur komunikasi utama, yaitu TX (*Transmit*) untuk mengirim data dan RX (*Receive*) untuk menerima data. Untuk membentuk komunikasi dua arah, pin TX pada perangkat pertama harus dihubungkan secara menyilang (*cross-over*) ke pin RX pada perangkat kedua, dan sebaliknya (Dhineshkaarthi dkk., 2016). Dalam implementasi arsitektur mikrokontroler ganda, UART sering digunakan sebagai jalur tulang punggung komunikasi antar-perangkat, di mana paket data biner, instruksi operasional, atau muatan informasi dikirim dengan struktur bingkai (*frame*) tertentu dan sering kali

dilengkapi dengan mekanisme pengecekan galat (*checksum*) untuk memastikan integritas data selama transmisi.

2.2 Penelitian Terdahulu

Pengujian keamanan nirkabel melalui simulasi serangan *Evil Twin* telah banyak dieksplorasi dalam berbagai penelitian terdahulu. Sebagian besar penelitian berfokus pada pembuktian kerentanan jaringan menggunakan perangkat keras berbiaya rendah. Implementasi pada lingkungan akademik dan perusahaan telah dilakukan menggunakan modul tunggal ESP8266 (Sigit dkk., 2024). Melalui pengujian tersebut, berhasil dibuktikan bahwa perangkat mikrokontroler tunggal mampu menjalankan serangan *deauthentication* dan menyajikan *captive portal* untuk mengecoh pengguna jaringan yang diamankan dengan WPA2-PSK. Kerentanan serupa juga ditemukan pada implementasi jaringan rumahan dengan *router* standar (Rahmat Mauluddin & Desyani, 2024) serta pada jaringan berbasis Mikrotik (Andris & Sutresna, 2024), di mana konfigurasi keamanan bawaan terbukti tidak cukup untuk menahan eksploitasi pembuatan *access point* palsu.

Di sisi lain, keberhasilan serangan *Evil Twin* tidak hanya bergantung pada kemampuan perangkat keras, melainkan juga pada faktor psikologis target. Pendekatan analisis *social engineering* dalam serangan nirkabel menunjukkan bahwa desain *captive portal* berbasis HTML/CSS yang meyakinkan menjadi faktor penentu utama (Lina & Fernandes, 2022). Hasil pengujian di lingkungan kampus menegaskan bahwa mayoritas target sering kali tidak memverifikasi validitas *access point* sebelum memasukkan kredensial pribadi mereka.

Untuk memudahkan perbandingan dan mengidentifikasi celah dari berbagai metode yang telah diusulkan sebelumnya, ringkasan studi kasus, teknologi, hasil, beserta keterbatasan dari masing-masing penelitian disajikan pada Tabel 2.1.

Tabel 2.1 Ringkasan Penelitian Terdahulu

Peneliti	Studi Kasus	Teknologi	Hasil	Keterbatasan Utama
(Sigit dkk., 2024)	STT Wastukancana	ESP8266, Arduino IDE	Serangan *deauth* dan *captive portal* berhasil mengecoh pengguna.	Menggunakan pendekatan mikrokontroler tunggal yang belum dirancang untuk mengeksekusi

Peneliti	Studi Kasus	Teknologi	Hasil	Keterbatasan Utama
				deauthentication attack secara bersamaan dengan aktifnya *Evil Twin* dan *captive portal*.
(Anggriani, 2023)	Jaringan Perusahaan	ESP8266	Berhasil membuktikan kerentanan WPA2-PSK melalui *captive portal*	Kurangnya fitur perekaman (*sniffing*) data mentah nirkabel untuk keperluan forensik jaringan lanjutan
(Mauluddin & Desyani, 2024)	Jaringan rumah (TL-WR840N)	ESP8266, TL-WR840N	Jaringan rumah sangat rentan terhadap *access point* palsu.	Masih menggunakan pendekatan mikrokontroler tunggal dalam implementasi serangannya
(Lina & Fernandes, 2022)	Mahasiswa di lingkungan kampus	ESP8266, taktik *social engineering*	Faktor psikologis sangat mempengaruhi keberhasilan serangan	Berfokus pada aspek sosial, arsitektur alat penyerang masih bersifat konvensional (perangkat tunggal)
(Andris & Sutresna, 2024)	Mikrotik RB941-2ND	ESP8266, Mikrotik	Menunjukkan kerentanan SSID terhadap serangan *deauth* dan pengelabuan.	Tidak menawarkan pembaruan pada arsitektur perangkat keras uji penetrasi yang digunakan

Berdasarkan tinjauan pada Tabel 2.1, dapat ditarik kesimpulan bahwa seluruh penelitian terdahulu masih mengandalkan penggunaan modul mikrokontroler tunggal (seperti ESP8266 atau ESP32 standar) untuk mengeksekusi seluruh rangkaian pengujian. Namun, pada proses pengembangan penelitian ini, ditemukan kebutuhan implementasi yang lebih spesifik. Terdapat kebutuhan operasional agar proses pemutusan jaringan (*deauthentication attack*) dapat terus berlangsung secara bersamaan ketika *access point* palsu dan layanan *captive portal* sedang aktif melayani target. Pendekatan mikrokontroler tunggal yang digunakan pada penelitian sebelumnya belum dapat mengakomodasi kebutuhan skenario

operasional tersebut secara utuh.

Oleh karena itu, penelitian ini dirancang untuk memenuhi kebutuhan implementasi tersebut melalui penerapan arsitektur dua mikrokontroler. Dengan memisahkan fungsi antarmuka pengguna, *Evil Twin*, dan *captive portal* pada modul ESP32-S3, serta mendelegasikan fungsi injeksi paket *deauthentication* dan perekaman lalu lintas (*packet sniffing*) jaringan pada ESP32, skenario simulasi serangan dapat dijalankan sesuai dengan kebutuhan pengujian.