Prosiding Seminar Nasional Sains dan Teknologi Seri 02
Fakultas Sains dan Teknologi, Universitas Terbuka
Vol. 1 No. 2 (2024)
e-ISSN: 3047-6569

ALAT *MONITORING* WI-FI BERBASIS ESP32-LORA UNTUK DETEKSI *ROGUE ACCESS POINT*

Suredsi Ulpada[1*], Ahmad Ridha[2]
[1] Program Studi Teknologi Rekayasa Komputer, Institut Pertanian Bogor, Bogor
[2] Program Studi Ilmu Komputer, Institut Pertanian Bogor, Bogor

**Penulis korespondensi: 21ulpada@apps.ipb.ac.id*

ABSTRAK

Popularitas jaringan Wi-Fi (WLAN) yang meningkat menghadirkan tantangan dalam hal keamanan karena WLAN rentan terhadap serangan berbahaya. Fasilitas WLAN yang dikonfigurasi menggunakan Pi-Hole untuk memblokir *adware* dan situs web berbahaya serta membatasi akses situs web selama jam kerja menjadi tidak efektif ketika karyawan menggunakan *access point* pribadi. Penelitian ini merancang sebuah alat *monitoring* Wi-Fi berbasis IoT menggunakan satu ESP32 sebagai *controller* dan dua ESP32 sebagai monitor. Modul LoRa digunakan untuk komunikasi antara monitor dan *controller*. Alat ini mendeteksi semua Wi-Fi di sekitarnya, lalu menyimpan data Wi-Fi tersebut dan melakukan *clustering* dengan algoritma K-Means untuk memperkiraan *access point* yang berada di dekat monitor. Alat dilengkapi dengan *aggressive mode* untuk melakukan *jamming* terhadap *rogue access point*.

Kata kunci: ESP32, *K-Means clustering*, LoRa, *rogue access point*, *Wi-Fi monitoring*

1. PENDAHULUAN

Jaringan area lokal nirkabel (WLAN) telah menjadi bagian tidak terpisahkan dari aktivitas sehari-hari, tetapi hal tersebut memunculkan tantangan untuk pengamanannya karena WLAN rentan terhadap serangan berbahaya (Korolkov & Kutsak, 2021). Meningkatnya penggunaan perangkat nirkabel membuat keamanan jaringan menjadi masalah yang sangat kritis. Keamanan jaringan yang tidak memadai dapat menyebabkan akses tidak sah, pencurian data, dan penyebaran *malware*, yang semuanya dapat berdampak buruk pada individu maupun organisasi.

Rogue Access Points (RAP) adalah *access point* (AP) yang tidak dipasang dan tidak disetujui oleh *administrator* jaringan setempat. RAP dapat dikategorikan menjadi empat jenis: *phishing* AP, RAP yang dipasang secara tidak benar oleh pengguna yang kurang berpengalaman, AP yang tidak sah yang terhubung ke WLAN tanpa izin, dan AP yang telah dikompromikan (Alotaibi & Elleithy, 2015). Keberadaan RAP ini sangat berbahaya karena mereka dapat melewati mekanisme keamanan yang ada, memberikan akses yang tidak sah ke jaringan, dan membuka pintu bagi berbagai jenis serangan siber. Penelitian sebelumnya telah mengusulkan pendekatan yang berfokus pada monitoring nilai RSSI antara client dan AP (Ahmad et al., 2015) untuk mendeteksi RAP.

Penelitian ini difokuskan pada RAP berupa perangkat Wi-Fi pribadi yang membuat ketentuan penggunaan jaringan di suatu lokasi, misalnya dengan Pi-Hole, menjadi tidak efektif. RAP seperti itu berpotensi menjadi celah masuknya ancaman keamanan seperti *worm* dan *trojan horse* ke perangkat pribadi yang kemudian bisa menyebar ke perangkat lain melalui pertukaran data.

Penelitian ini merancang sebuah alat *monitoring* Wi-Fi berbasis IoT dengan memanfaatkan satu buah ESP32 sebagai *controller* dan dua buah ESP32 sebagai monitor. Modul LoRa digunakan untuk komunikasi antara monitor dan *controller*. Alat ini diharapkan dapat mendeteksi keberadaan RAP secara real-time dan memberikan peringatan kepada administrator jaringan sehingga tindakan pencegahan dapat segera diambil.

2. METODE

2.1 Pengumpulan Data

Pengumpulan data dilakukan di PT. Semesta Integrasi Digital. Langkah pertama dalam pengumpulan data adalah pemindaian jaringan Wi-Fi di lokasi dengan perangkat ESP32 yang telah dipersiapkan. ESP32 mendeteksi jaringan Wi-Fi dalam suatu lokasi yang ditentukan dan mencatat informasi penting untuk tiap AP yang terdeteksi. Informasi yang dikumpulkan selama pemindaian termasuk *Service Set Identifier* (SSID), *Basic Service Set Identifier* (BSSID), dan *Received Signal Strength Indicator* (RSSI). Pemindaian akan dilakukan secara berkala untuk mendapatkan sampel data yang representatif.

2.2 Analisis Data

Selanjutnya, data diolah menggunakan *machine learning* dengan metode *clustering*. Penelitian ini menggunakan algoritma K-means yang mengelompokkan data menjadi sejumlah *cluster* (Altintas & Serif, 2011). Prinsip dasarnya adalah setiap kelompok terwakili oleh *centroid*-nya yakni nilai rata-rata fitur yang digunakan. Penelitian ini menggunakan K = 2 untuk mewakili kelompok data yang dekat dan yang jauh dari monitor. Tiap titik data direpresentasikan oleh RSSI dan waktu deteksi sebagai fitur . Waktu deteksi direpresentasikan sebagai jumlah menit sejak pukul 00.00. Sebagai contoh, waktu deteksi pukul 11.30 direpresentasikan sebagai 690. *Centroid* awal dipilih secara acak, lalu tiap titik data dimasukkan ke *cluster* dengan *centroid* terdekat. Proses diulang hingga posisi *centroid* tidak lagi berubah (Ahmad *et al*., 2015).

2.3 Prosedur Kerja

Metode pengembangan perangkat yang digunakan di dalam penelitian ini adalah *Hardware Development Life Cycle* yang terdiri atas analisis, perancangan, implementasi dan pengujian. Metode ini dipilih karena pengembangan ini cocok untuk proyek dengan skala kecil (Windarto *et al*., 2020)

2.3.1 Analisis

Tahap ini adalah proses untuk menemukan jawaban permasalahan yang terjadi disekitar tempat Perusahaan. Analisis data dilakukan dengan dua tahapan yaitu analisis masalah dan analisis kebutuhan. Analis masalah dilakukan melalui wawancara dengan *Chief Technology Officer* PT Semesta Integrasi Digital. Analisis masalah yang ditemukan dari wawancara tersebut menghasilkan kebutuhan adanya sebuah perangkat *monitoring* RAP.

2.3.2 Perancangan

Tahap perancangan dilakukan jika sudah menentukan, mengindetifikasi, serta menemukan inti permasalahan untuk kebutuhan yang diperlukan dalam penelitian alat *monitoring* RAP. Adapun proses perancangan yang dibutuhkan adalah membuat *flowchart*, diagram blok, dan desain skematik. Perancangan ini dibagi dua bagian yaitu perancangan *software* dan perancangan *hardware*.

2.3.3 Implementasi

Implementasi memaparkan mengenai bagaimana cara perangkat dibentuk, mulai dari pembentukan rangkaian elektronik, implementasi program, hingga pemasangan *casing*. Tahap ini menghasilkan perangkat untuk diuji pada tahap berikutnya.

2.3.4 Pengujian

Tahap ini menguji apakah alat dapat berfungsi dengan baik dan memenuhi kebutuhan. Pengujian mencakup pengiriman data antara monitor dan *controller* melalui LoRa, pengolahan data dengan metode K-Means *clustering* untuk membuat model *clustering* yang dapat mengelompokan RAP terdekat berdasarkan data yang diterima dari ESP32, hingga penyajiannya di *dashboard*.

3. HASIL DAN PEMBAHASAN

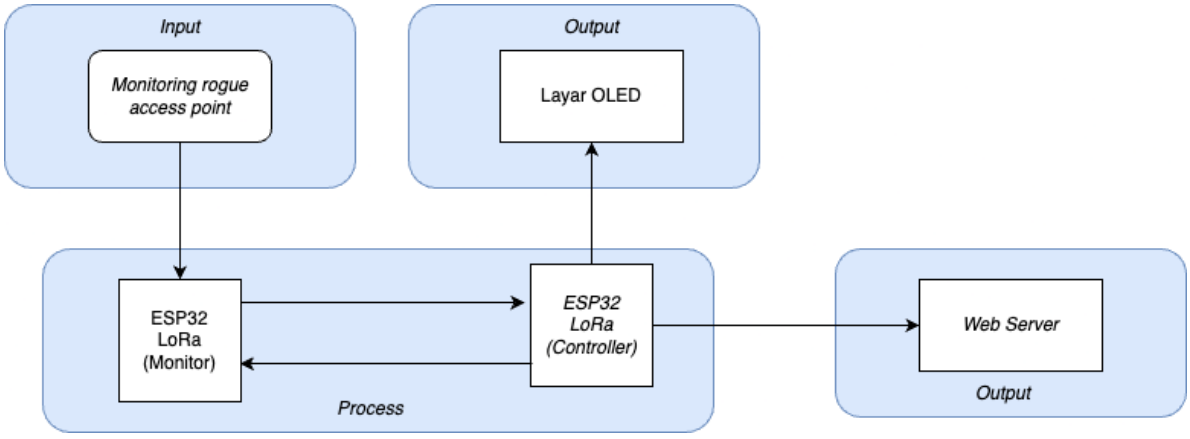
3.1 Analisis Kebutuhan

Analisis kebutuhan merupakan langkah awal yang dilakukan dalam penelitian. Tujuan dari tahap ini adalah untuk menemukan permasalahan terkait penelitian dan selanjutnya mengembangkan banyak solusi untuk mengatasinya. Dalam melakukan analisis masalah, interaksi yang terjalin dengan dosen lapangan merupakan langkah awal yang mendalam untuk membahas permasalahan yang dihadapi oleh PT Semesta Integrasi Digital. Hasil dari tahap ini mengonfirmasi bahwa perusahaan menghadapi tantangan yang substansial, dan analisis ini memberikan dasar yang diperlukan untuk menemukan solusi yang sesuai.

3.2 Perancangan

Setelah melakukan analisis kebutuhan dan mengidentifikasi permasalahan yang dihadapi oleh PT Semesta Integrasi Digital, dan langkah selanjutnya adalah merancang solusi yang akan diimplementasikan. Diagram blok yang mengilustrasikan proses komunikasi antara ESP32 dan *controller* ESP32 menggunakan teknologi LoRa disajikan pada **Gambar 1**.

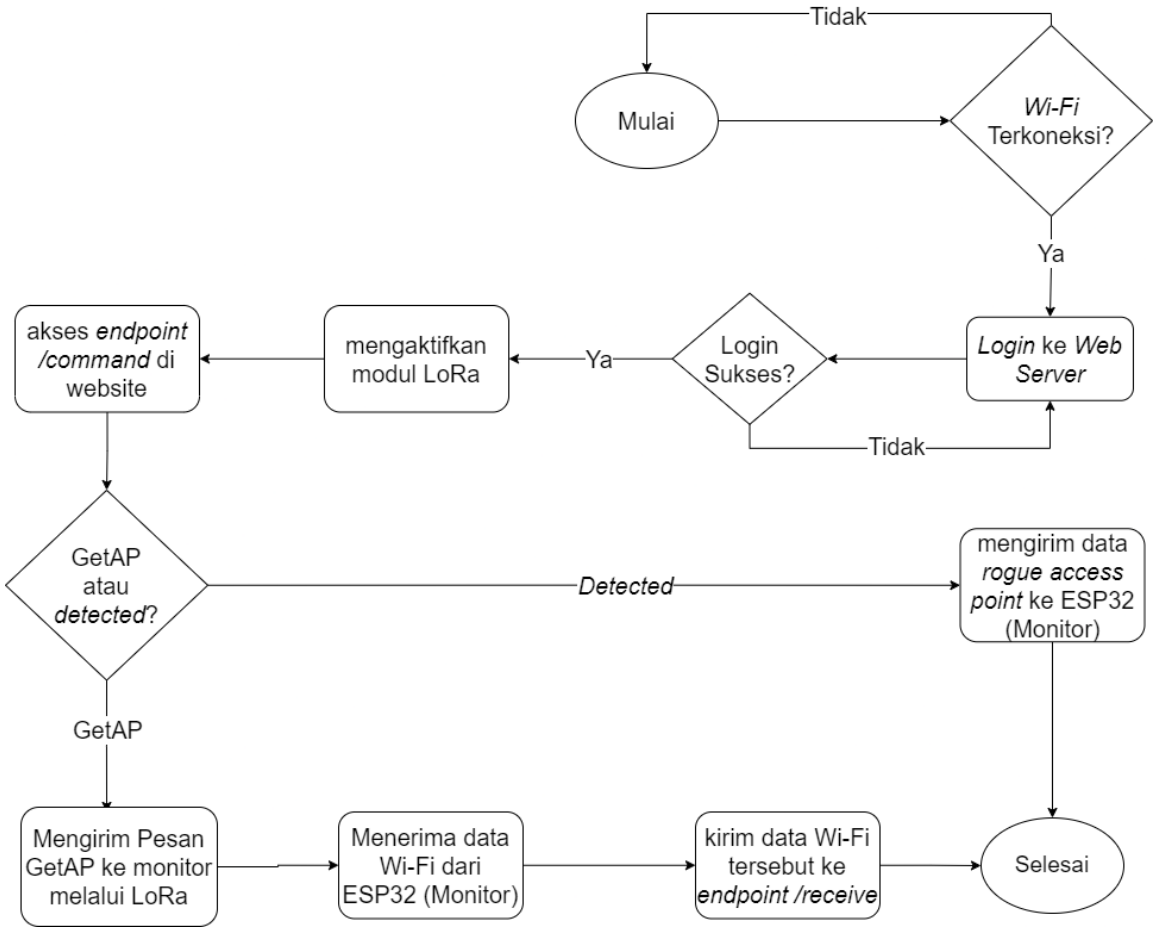
Monitor mengirimkan data AP sekitarnya ke controller melalui LoRa. Kemudian, controller mengidentifikasi AP yang perlu dilindungi dan mengirimkan informasinya kembali ke monitor. Controller mendeteksi RAP, dan jika terdeteksi, controller melaporkan ke monitor. Selanjutnya, monitor dapat melakukan jamming terhadap RAP yang terdeteksi jika aggressive mode diaktifkan. Jika ada dua monitor yang digunakan, controller akan memberikan perintah kepada masing-masing monitor secara sekuensial.



Gambar 1. Diagram blok

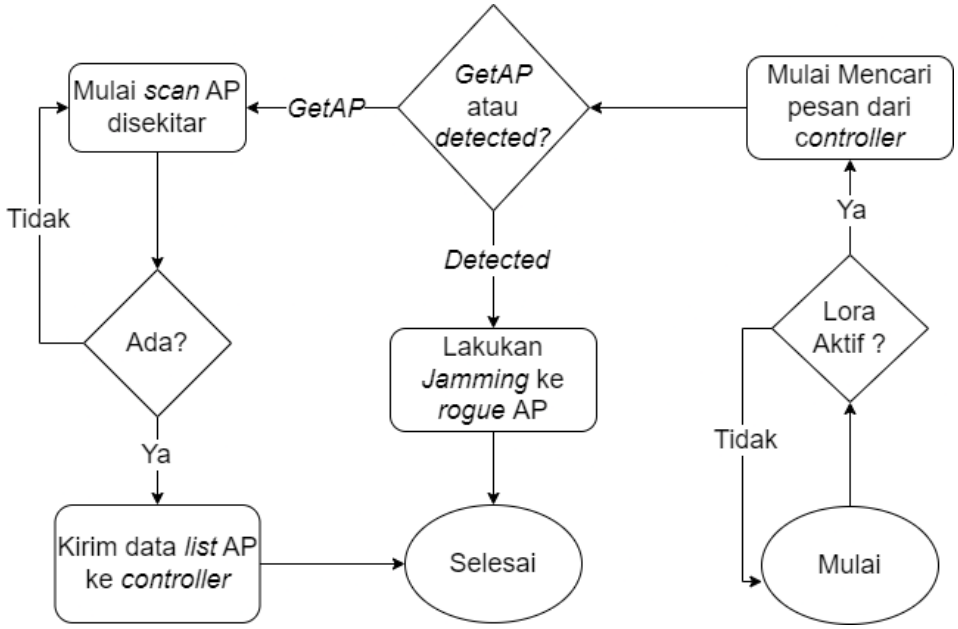
Flowchart untuk *controller* yang lebih detail disajikan pada **Gambar 2.** Proses dimulai dari memastikan koneksi Wi-Fi aktif. Jika Wi-Fi terkoneksi, langkah berikutnya adalah *controller* akan *login* ke *web server* untuk memasukkan data. Apabila *login* gagal, proses juga akan berhenti. Namun, jika *login* berhasil, *controller* akan mengakses *endpoint* "/command" di *website* dan mengaktifkan modul LoRa untuk melanjutkan proses komunikasi.

Setelah modul LoRa aktif, *controller* akan mengecek respons dari *endpoint* "/command" untuk menentukan apakah respons yang diterima adalah "GetAP" atau "detected". Jika responsnya adalah "GetAP", *controller* akan mengirim pesan "GetAP" ke monitor melalui modul LoRa. Monitor akan melakukan pendeteksian AP di sekitarnya dan mengirimkan kembali data tersebut ke *controller*. Setelah menerima data AP terbaru, *controller* akan mengirim data tersebut ke API pada *endpoint* "/receive".



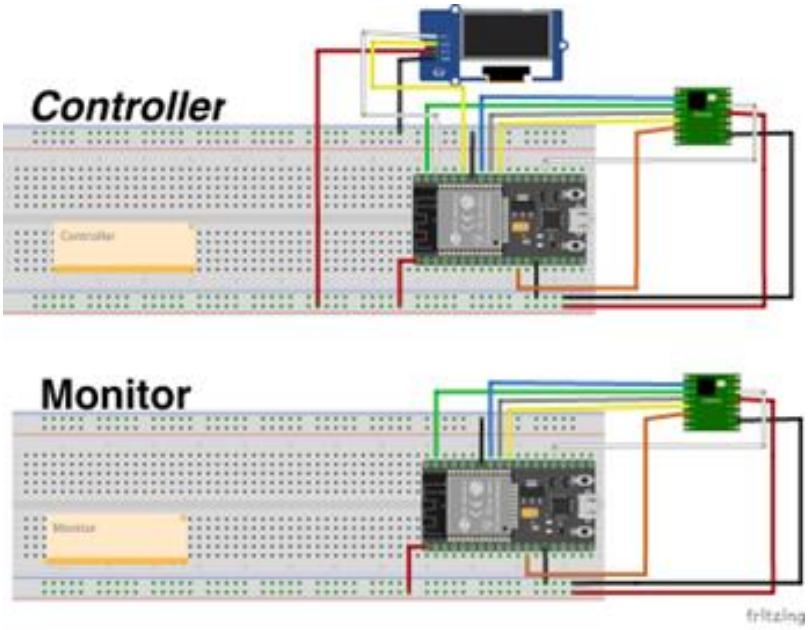
Gambar 2. *Flowchart* di sisi controller

Respons dari *endpoint* "/command" berupa "detected" menunjukkan ada RAP yang terdeteksi. *Controller* mengirim informasi berupa SSID dan BSSID dari RAP tersebut ke monitor melalui modul LoRa. Monitor akan melakukan tindakan yang diperlukan terhadap. RAP yang terdeteksi. Flowchart untuk monitor disajikan pada Gambar 3. Ketika LoRa aktif, ESP32 mencari pesan "GetAP" atau "detected" dari controller. Jika pesan yang diterima adalah "GetAP", monitor akan mendeteksi AP di sekitarnya dan langsung mengirimkan hasilnya ke controller melalui modul LoRa. Jika pesan yang diterima adalah "detected", jamming dilakukan selama 60 detik.



Gambar 3. *Flowchart* monitor

Skema alat pada **Gambar 4** merupakan prototipe yang berhasil dikembangkan menggunakan aplikasi Fritzing. Alat ini terdiri atas dua komponen utama yakni *controller* dan perangkat *monitoring* RAP.



Gambar 4. Skema alat

3.3 Implementasi

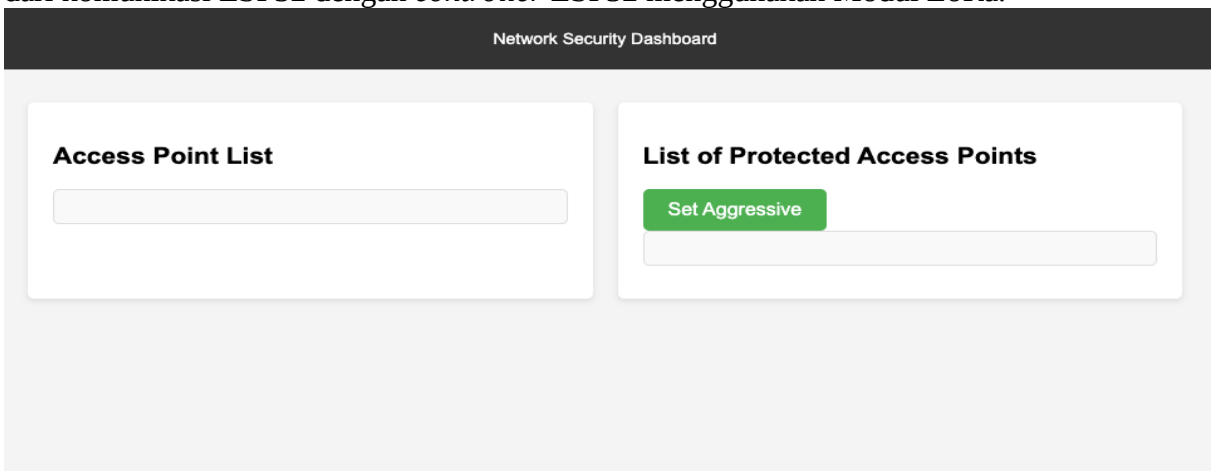
Implementasi ini merupakan tahapan untuk penerapan alat *monitoring* menjadi bentuk fisik dari alat dan bahan yang dirancang. Implementasi mencakup perakitan rangkaian dan perangkat serta pembuatan *monitoring dashboard*. Alat menggunakan mikrokontroller ESP32 yang terlihat pada **Gambar 5**. LCD OLED berfungsi untuk menampilkan status komunikasi. Modul LoRa RFM95 digunakan untuk komunikasi antara *controller* dan monitor karena kualitas transmisinya yang sangat baik (Yanziah *et al*., 2020).

Gambar 5. Implementasi rangkaian elektronik ESP32

Tampilan halaman web untuk *monitoring dashboard* disajikan pada **Gambar 6**. Halaman menampilkan daftar AP yang terdeteksi, lengkap dengan informasi SSID, BSSID, dan kekuatan sinyal. Pengguna dapat melihat detail setiap AP dan menggunakan tombol "Protect AP" untuk mengamankan AP tertentu melalui perangkat LoRa. Selain itu, terdapat tombol "Set Aggressive" atau "Set Monitoring" untuk menentukan apakah *controller* hanya memonitor atau menyerang RAP dalam *mode* agresif.

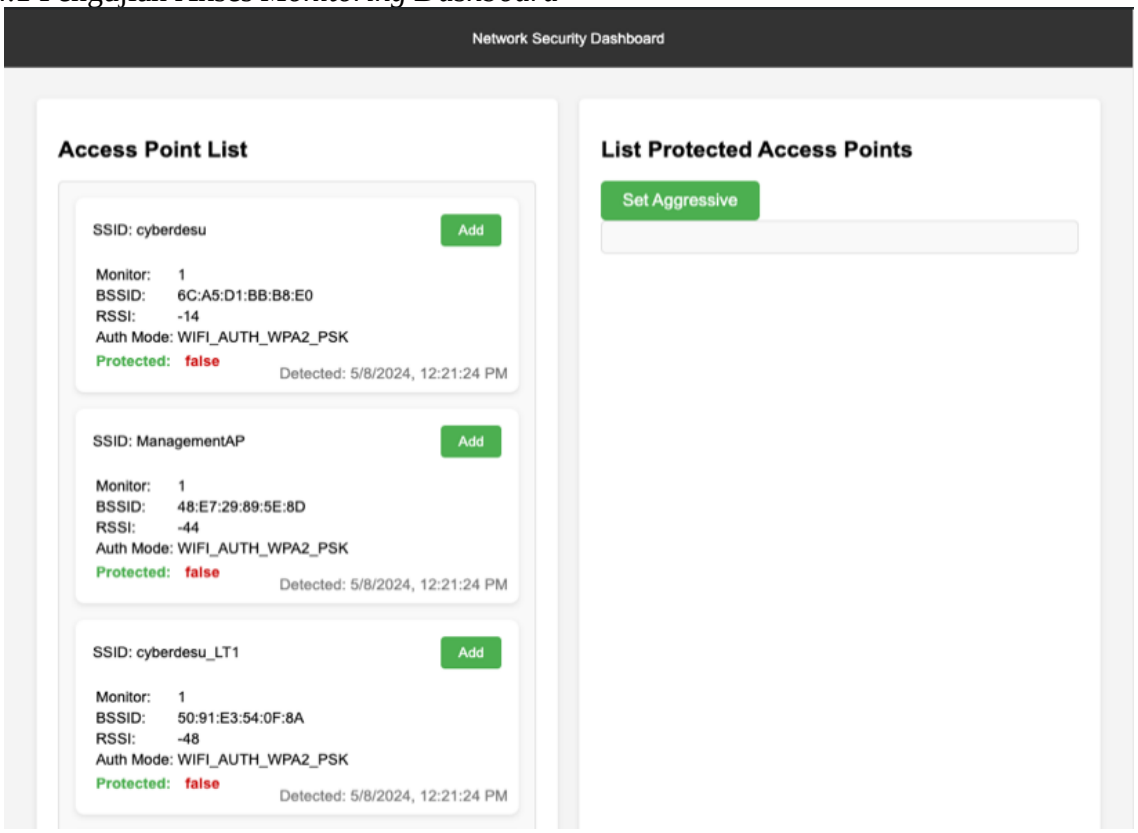
3.4 *Pengujian*

Tahap pengujian adalah tahap terakhir sekaligus menguji terlebih dahulu apakah alat dapat berfungsi dengan baik dan memenuhi hasil akhir kebutuhan serta fungsi yang sesuai. Mulai dari komunikasi ESP32 dengan *controller* ESP32 menggunakan Modul LoRa.



Gambar 6. Tampilan halaman web untuk *monitoring*

3.4.1 Pengujian Akses *Monitoring Dashboard*

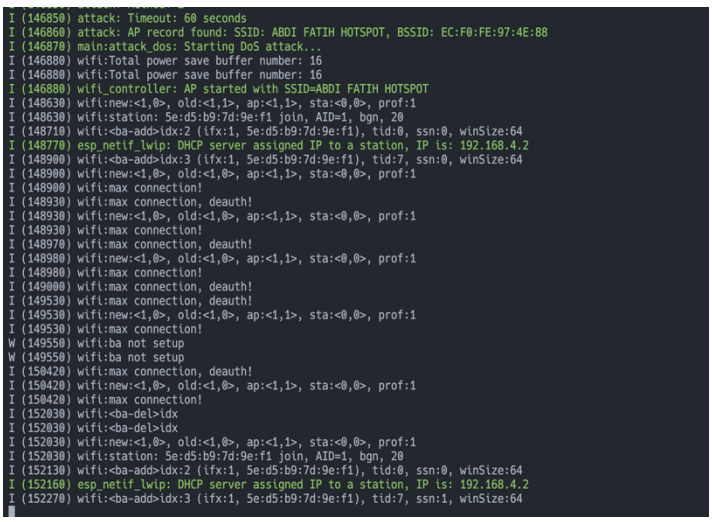


Gambar 7. Tampilan *dashboard* saat aktif

Gambar 7 merupakan tampilan *dasboard* ketika *controller* berhasil mengirim data terkini terkait AP ke API "/receive" yang secara otomatis akan ditampilkan di sisi *frontend website dasboard* ini. Lalu ketika ada AP yang ditambahkan ke daftar "protected AP", semua AP selain dari "protected AP" akan dianggap RAP.

3.4.2 Pengujian Deteksi RAP

Gambar 8 memperlihatkan sebuah *serial log* dari alat monitor, yang menandakan ketika RAP terdeteksi, monitor akan melakukan *jamming* yang menyebabkan *client* tidak dapat mengakses Wi-Fi tersebut.



Gambar 8. Pengujian *rogue access point*

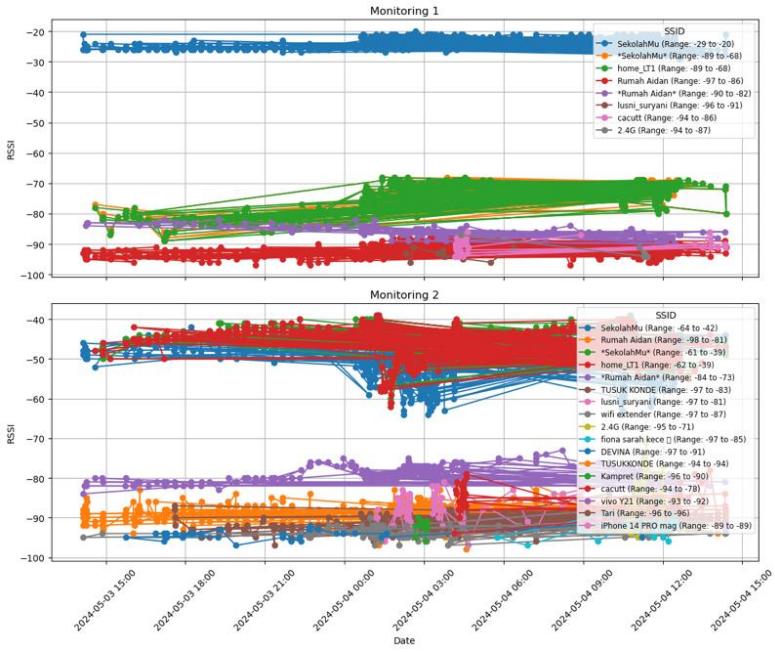
Metode pertama yang digunakan untuk *jamming* yaitu dengan cara menggunakan *evil twin attack* (ETA) yakni sebuah situasi jaringan Wi-Fi yang tidak aman menyediakan lingkungan yang menarik bagi penyerang. ETA mengacu pada sebuah RAP yang menyamar sebagai AP yang sah (*Legitimate Access Point*/LAP) untuk menyadap data Wi-Fi pengguna (Nakhila & Zou, 2016).

Kebanyakan sistem operasi modern dikonfigurasikan untuk terhubung ke AP yang menyediakan kekuatan sinyal lebih tinggi jika terdapat beberapa AP yang menggunakan SSID yang sama. Dalam kehadiran AP *evil twin*, jika kekuatan sinyal dari AP *evil twin* melebihi kekuatan sinyal dari AP yang asli, klien akan terhubung ke AP *evil twin*. Kekuatan sinyal yang lebih tinggi menghasilkan *throughput* yang lebih tinggi dan kehilangan *frame* yang lebih sedikit. Oleh karena itu, *client* selalu lebih memilih AP yang menawarkan kekuatan sinyal lebih tinggi (Agarwal *et al*., 2018).

Metode kedua yang digunakan untuk melakukan *jamming* ialah menggunakan *Denial of Service* (DoS). Jenis serangan DoS pada WiFi dapat menyebabkan kelumpuhan komunikasi antarperangkat yang terhubung. Serangan dilakukan melalui proses autentikasi dengan mengirim *broadcast address* dan mengubah *broadcast address* pada target yang diserang. Serangan ini disebut *deauthentication attack* (Kristiyanto & Ernastuti, 2020).

3.4.3 Pengujian Hasil Pengambilan data Wi-Fi

Gambar 9 menyajikan dua grafik: "Monitoring 1" dan "Monitoring 2", yang masing-masingnya menunjukkan nilai RSSI untuk berbagai SSID Wi-Fi selama periode waktu tertentu. Sumbu x menunjukkan tanggal dan waktu, dari 31 Mei 2024 pukul 15.00 hingga 1 Juni 2024 pukul 15.00, sementara sumbu y menunjukkan nilai RSSI dari -100 hingga -20, dengan nilai yang lebih tinggi menunjukkan sinyal yang lebih kuat. Setiap grafik memiliki beberapa SSID dengan garis dan titik berwarna yang menunjukkan variasi kekuatan sinyal untuk setiap jaringan. Legenda di samping grafik mencantumkan SSID dan rentang fluktuasi sinyal RSSI yang disebabkan oleh berbagai faktor seperti *multipath propagation* dan *non-line of sight* (NLOS) (Xue *et al*., 2017).



Gambar 9. Hasil pengambilan data Wi-Fi

3.4.4 Pengujian hasil K-Means

Gambar 10 merupakan tampilan untuk memberikan informasi mengenai perubahan kedekatan berbagai SSID terhadap monitor tertentu dalam rentang waktu yang ditentukan. Dengan menggunakan data yang dikumpulkan, analisis ini membantu dalam memahami bagaimana sinyal Wi-Fi dari berbagai SSID berubah dalam hal kedekatan ke monitor. Misalnya, SSID "SekolahMu" lebih dekat dengan monitor 1 dan monitor 2 dari pukul 10.24 hingga 10.58. Selain itu, SSID "*home_LT1*" terdeteksi lebih dekat dari monitor 2 antara pukul 11.00 hingga 11.30 dan terdeteksi lebih jauh dari monitor 1 dari pukul 10.31 hingga 10.58. Analisis ini membantu pengguna untuk memantau kekuatan sinyal Wi-Fi terhadap monitor yang mengindikasikan posisinya.

Analysis Result

SSID	Closer to	Farther from	Start Time	End Time
SekolahMu	monitor 1 and monitor 2		10:24	10:58
SekolahMu	monitor 2		10:24	10:58
SekolahMu		monitor 1	10:31	10:58
home_LT1	monitor 2		10:24	10:58
home_LT1		monitor 1	10:31	10:58
Rumah Aidan		monitor 1	10:31	10:56
Rumah Aidan		monitor 2	10:24	10:58
Rumah Aidan		monitor 1	10:39	10:58
Rumah Aidan		monitor 2	10:31	10:58
TUSUK KONDE		monitor 2	10:31	10:58
2.4G		monitor 2	10:39	10:58
wifi extender		monitor 2	10:39	10:52
fiona sarah kece 😀		monitor 2	10:33	10:33

Gambar 10. Tampilan hasil K-means di website

4. KESIMPULAN

Alat pemantauan Wi-Fi berbasis ESP-32-LoRa mampu memantau AP Wi-Fi di sekitarnya secara *real-time* dan memiliki fitur untuk mendeteksi dan memblokir RAP. Sistem ini terdiri atas dua komponen utama, yaitu perangkat *controller* dan perangkat *monitoring* yang berkomunikasi menggunakan teknologi LoRa. Penggunaan metode *machine learning*, khususnya K-Means *clustering*, memungkinkan alat ini untuk mengelompokkan data sinyal RSSI yang akan ditampilkan ke *website* berupa informasi mengenai perubahan kedekatan berbagai SSID terhadap monitor tertentu dalam rentang waktu yang ditentukan. Untuk ke depannya, pengujian lebih lanjut di berbagai lokasi dengan kondisi jaringan yang berbeda perlu dilakukan untuk memastikan alat ini dapat berfungsi dengan baik di berbagai lingkungan.

Perangkat yang telah dikembangkan belum memiliki fitur notifikasi karena ditujukan untuk digunakan langsung di lapangan. Fitur notifikasi akan berguna jika perangkat ini akan digunakan untuk *monitoring* jarak jauh. Komunikasi antara perangkat *monitoring* dan *controller* juga belum dienkripsi. Ini diperlukan untuk melindungi data yang dikirimkan dari kemungkinan serangan pihak ketiga. Tampilan *dashboard* masih relatif sederhana karena belum mendukung penyajian data selama lebih dari satu hari. Oleh karena itu, pengembangan *dashboard* yang lebih ramah pengguna dengan visualisasi data yang lebih lengkap dan pengujian dari segi *usability* sangat diperlukan. Selain itu, metode *trilateration* dapat diterapkan untuk menentukan lokasi RAP yang terdeteksi dengan lebih akurat. Metode ini membutuhkan penggunaan minimal tiga monitor.

UCAPAN TERIMA KASIH

Terima kasih penulis ucapkan kepada Bapak Chaerul Akbar beserta staf karyawan PT. Semesta Integrasi Digital yang telah menyediakan tempat penelitian dan Sdr. Muhammad Agusrian Ilka di Program Studi Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor yang membantu dalam pengolahan data.

DAFTAR PUSTAKA

Agarwal, M., Biswas, S., & Nandi, S. (2018). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. *International Journal of Wireless Information Networks*, *25*(2), 130–145. https://doi.org/10.1007/s10776-018-0396-1

Ahmad, N. M., Amin, A. H. M., Kannan, S., Abdollah, M. F., & Yusof, R. (2015). A RSSI-based rogue access point detection framework for Wi-Fi hotspots. *ISTT 2014 - 2014 IEEE 2nd International Symposium on Telecommunication Technologies*. https://doi.org/10.1109/ISTT.2014.7238186

Alotaibi, B., & Elleithy, K. (2015). A passive fingerprint technique to detect fake access points. *Wireless Telecommunications Symposium (WTS), IEEE*, 1–8.

Altintas, B., & Serif, T. (2011). Improving RSS-based indoor positioning algorithm via K-means clustering. *17th European Wireless Conference 2011, EW 2011*.

Korolkov, R. Y., & Kutsak, S. V. (2021). Received-signal-strength-based approach for detection and 2D indoor localization of evil twin rogue access point in 802.11. *International Journal of Safety and Security Engineering*, *11*(1), 13–20. https://doi.org/10.18280/ijsse.110102

Kristiyanto, Y., & Ernastuti. (2020). Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. *CommIT Journal*, *14*(1), 45–51. https://doi.org/10.21512/commit.v14i1.6337

Nakhila, O., & Zou, C. (2016). User-side Wi-Fi evil twin attack detection using random wireless channel monitoring. *Proceedings - IEEE Military Communications Conference MILCOM*. https://doi.org/10.1109/MILCOM.2016.7795501

Windarto, Y. E., Samosir, B. M. W., & Assariy, M. R. (2020). Monitoring Ruangan Berbasis Internet of Things Menggunakan Thingsboard dan Blynk. *Walisongo Journal of Information Technology*, *2*(2), 145. https://doi.org/10.21580/wjit.2020.2.2.5798

Xue, W., Qiu, W., Hua, X., & Yu, K. (2017). Improved Wi-Fi RSSI Measurement for Indoor Localization. *IEEE Sensors Journal*, *17*(7). https://doi.org/10.1109/JSEN.2017.2660522

Yanziah, Asma., Soim, S., & Rose, M. M. (2020). Analisis Jarak Jangkauan Lora Dengan Parameter Rssi Dan Packet Loss Pada Area Urban. *Jurnal Teknologi Technoscientia*, *13*(1).