Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.3, June 2025, pp. 651~657
e-ISSN: 2548-6861

IMPLEMENTASI SISTEM DETEKSI SERANGAN JAMMING PADA JARINGAN IOT BERBASIS ESP32

Ronny Setiawan[1], Festy Winda Sari[2]
*Teknik Informatika, Politeknik Negeri Batam
ronny.setiawan3@student.polibatam.ac.id[1]
festy@polibatam.ac.id[2]

Article Info

Article history:

Received 2026-06-15
Revised 2026-06-19
Accepted 2026-06-19

Keyword:

Cybersecurity,
Internet of Things,
Jamming attack,
Signal Jammer,
ESP32,
Microcontroller,
Constant Jammer,
Keamanan Nirkabel

ABSTRACT

Perkembangan teknologi IoT (Internet of Things) yang memanfaatkan komunikasi nirkabel semakin meningkat di berbagai sektor. Namun, ketergantungan pada jaringan nirkabel juga menimbulkan risiko keamanan berupa serangan jamming. Serangan jamming bekerja dengan mengirimkan interferensi pada frekuensi komunikasi, sehingga mengganggu ketersediaan layanan dan menyebabkan kesalahan transmisi data. Jamming berkelanjutan (constant jamming) merupakan jenis serangan yang sangat mengganggu karena dapat menghasilkan gangguan sinyal yang terus menerus. Ancaman ini menunjukan akan kebutuhan sistem peringatan dini yang mampu mengidentifikasi gangguan komunikasi dengan cepat dan efisien. Tujuan penelitian ini adalah untuk mengembangkan sistem tersebut untuk mendeteksi serangan jamming berkelanjutan pada sistem komunikasi nirkabel berbasis IoT menggunakan mikrokontroler ESP32. Sistem ini memanfaatkan kemampuan pemrosesan dan pemantauan data ESP32 untuk mendeteksi akan tanda-tanda dari anomali sinyal yang disebabkan oleh interferensi yang disebabkan oleh serangan jamming. Pengujian dilakukan dengan memberikan kondisi yang mengganggu pada sistem komunikasi untuk menganalisis perubahan kinerja jaringan yang dihasilkan. Hasil penelitian ini bertujuan untuk menghasilkan sistem deteksi interferensi yang dapat digunakan sebagai mekanisme pertama untuk meningkatkan keamanan perangkat IoT terhadap interferensi pada lapisan fisik jaringan.
.

I. PENDAHULUAN

Perkembangan teknologi nirkabel yang semakin masif telah mendorong pemanfaatan perangkat *Internet of Things* (IoT) pada berbagai sektor, termasuk industri, keamanan, dan rumah pintar. Peningkatan jumlah perangkat yang beroperasi melalui komunikasi radio menjadikan aspek keandalan dan kontinuitas sinyal sebagai hal yang sangat krusial. Namun, ketergantungan tersebut sekaligus membuka peluang munculnya ancaman pada lapisan fisik jaringan, salah satunya serangan *jamming*. Serangan ini bekerja dengan memancarkan sinyal noise atau interferensi yang kuat untuk membanjiri kanal frekuensi, yang secara spesifik menargetkan aspek ketersediaan (*availability*) layanan agar komunikasi terputus[1].

Sejumlah kasus nyata yang menunjukkan dampak signifikan dari gangguan pada sistem komunikasi nirkabel. Sebagai contoh kasus yang pernah terjadi pada 13 Maret 2024 lalu, pesawat RAF yang membawa Menteri Pertahanan Inggris Grant Shapps mengalami gangguan GPS selama sekitar 30 menit saat melintas dekat Kaliningrad, wilayah Rusia di Laut Baltik. Pemerintah Inggris menduga bahwa gangguan tersebut merupakan tindakan GPS *jamming* oleh Rusia, meskipun tidak menimbulkan ancaman langsung terhadap keselamatan penerbangan. Insiden ini menyebabkan hilangnya konektivitas perangkat komunikasi dan memaksa pesawat menggunakan metode navigasi alternatif [2]. Selain ancaman bermotif militer dan politik, dampak destruktif gangguan frekuensi terhadap infrastruktur vital juga terlihat jelas pada insiden interferensi radar cuaca BMKG di Indonesia. Dalam tiga tahun terakhir, sejumlah radar cuaca BMKG di berbagai provinsi dilaporkan terganggu oleh penggunaan perangkat telekomunikasi pada pita 2,4 GHz dan 5,8 GHz yang tidak sesuai parameter teknis, sehingga radar kesulitan menganalisis pergerakan cuaca secara real time dan keselamatan penerbangan ikut terancam. Kasus ini menegaskan bahwa pelanggaran penggunaan spektrum frekuensi oleh pengguna sipil/komersial dapat menimbulkan risiko sistemik terhadap layanan publik dan mendorong pemerintah untuk langsung menerapkan sanksi pidana tanpa melalui tahapan sanksi administratif [3]. Selain ancaman yang bermotif kriminal, dampak destruktif dari penggunaan *jammer* sipil yang tidak terkontrol juga terlihat jelas pada insiden di Messanges, Prancis. Pada tanggal 17 Februari 2022 seorang warga menggunakan perangkat tersebut untuk membatasi akses internet anak-anaknya, namun secara tidak sengaja melumpuhkan jaringan seluler dan internet di seluruh kota tetangga setiap pukul 00.00 hingga 03.00 pagi. Kasus ini menegaskan bahwa penggunaan jammer pribadi memiliki

risiko *spillover* yang masif, di mana gangguan sinyal dapat merusak infrastruktur komunikasi publik jauh di luar target yang diinginkan [4].

Di antara berbagai klasifikasi serangan *jammer* yang pernah diuji, *constant jammer* merepresentasikan bentuk serangan yang paling agresif karena mekanisme operasionalnya yang memancarkan sinyal interferensi radio secara terus-menerus tanpa henti. Sifat frekuensi yang terbuka dan dapat diprediksi ini menjadi celah fatal bagi infrastruktur keamanan nirkabel [5].

Meskipun metode mitigasi canggih seperti *spectrum patrol* telah tersedia, masih banyak hal disekitar kita yang masih memiliki kerentanan terhadap serangan *jammer*, salah satu contohnya adalah sektor *smart home* yang masih memiliki kerentanan signifikan yang mengancam keselamatan penghuni. Perangkat IoT juga menjadi target yang menarik bagi para penyerang siber, terutama melalui serangan pada lapisan fisik, ancaman seperti *jamming* terbukti sulit dideteksi oleh sistem keamanan tradisional yang membuat masalah ini semakin kompleks akibat minimnya solusi proteksi yang menawarkan efisiensi biaya serta fleksibilitas implementasi di lapangan[6]. Kondisi tersebut mendasari kebutuhan pengembangan sistem peringatan dini (*early warning system*) yang mampu mengidentifikasi gangguan sinyal secara cepat guna mencegah kelumpuhan layanan yang lebih fatal. Merespons urgensi tersebut, penelitian ini berfokus pada perancangan sistem deteksi *jamming* berbasis ESP32, sebuah *system on a chip* (SoC) yang mengintegrasikan kemampuan komputasi prosesor dual core dengan modul komunikasi nirkabel. Arsitektur ini memungkinkan pengembangan perangkat deteksi anomali sinyal yang responsif, sehingga sangat relevan untuk menjawab kebutuhan keamanan nirkabel sehari-hari [7].

II. METODE

Bagian ini membahas desain dan implementasi alat deteksi serangan pengacauan sinyal pada jaringan *Internet of Things* (IoT) berbasis ESP32.

2.1 Metode Penelitian

Metode penelitian yang digunakan dalam studi ini adalah eksperimental dan desain sistem (desain dan pembuatan). Metode ini dipilih karena penelitian berfokus pada desain, konstruksi, dan pengujian perangkat deteksi gangguan berbasis ESP32 yang sederhana, bukan pada analisis teoritis atau pengembangan algoritma yang kompleks. Sistem ini dirancang untuk memantau kondisi komunikasi nirkabel di sekitarnya dan memberikan indikasi ketika interferensi terdeteksi yang dapat mengindikasikan aktivitas pengacauan[8].

2.2 Analisa Kebutuhan Perancangan

Analisis kebutuhan desain dilakukan sebagai tahap awal dalam mendesain detektor dan pengacau sinyal telepon seluler berbasis ESP32. Penelitian ini bertujuan untuk memastikan bahwa sistem yang dikembangkan mampu mendeteksi keberadaan pengacau sinyal perangkat nirkabel pada rentang frekuensi tertentu. Berdasarkan tujuan dari penelitian ini, sejumlah komponen ditentukan untuk mendukung desain dan implementasi sistem.

Tabel 1 Analisis Kebutuhan Perancangan

No	Nama Komponen	Jumlah
1	ESP32 Devkit v4	2 unit
2	Modul nRF24L01 + PA + LNA	3 unit
3	TFT OLED *Graphic Display* ILLI 9488	2 unit
4	Kapasitor 10 µF	3 unit
5	PCB	2 unit

2.3 Alat dan Perangkat

Berikut merupakan alat dan perangkat utama yang digunakan dalam penelitian ini. Perangkat-perangkat tersebut berperan sebagai komponen pendukung dalam proses perancangan, implementasi, dan pengujian alat pendeteksi serangan *signal jamming* berbasis ESP32. Pemilihan setiap alat dilakukan dengan mempertimbangkan kesesuaian fungsi, kemudahan dalam proses implementasi, serta ketersediaan komponen, sehingga sistem yang dirancang dapat beroperasi sesuai dengan tujuan penelitian.

Tabel 2 Spesifikasi Perangkat Pengujian

Komponen perangkat	Spesifikasi
CPU *(Processor)*	Intel(R) i5-7300U
RAM	8GB
Disk/Storage	M.2 Sata SSD 256 GB
Sistem Operasi	Windows 10 Pro 64-bit
Jaringan	Wi-Fi

Tabel 3 Perangkat Lunak

Tools	Fungsi
Arduino IDE	Digunakan untuk pemrograman ESP32 dan pengunggahan kode program.
Library ESP32 dan nRF24L01	Digunakan untuk mendukung komunikasi dan pengolahan data sinyal.

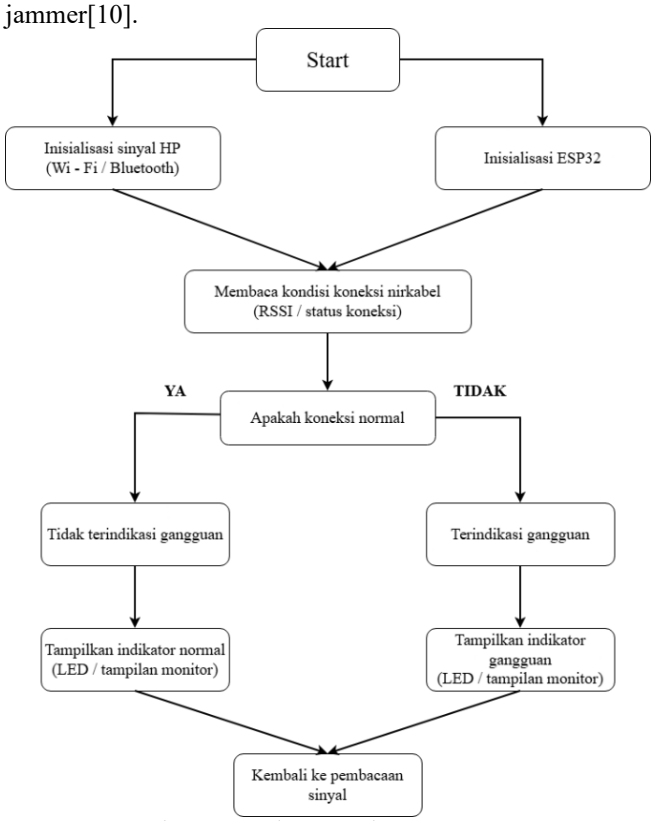
III. HASIL

Bab ini menyajikan hasil pengujian dan analisis sistem deteksi serangan *jamming* pada komunikasi nirkabel berbasis *Internet of Things* (IoT). Pengujian dilakukan dengan menerapkan gangguan (*constant jammer*) terhadap sistem komunikasi menggunakan perangkat ESP32 untuk mengetahui pengaruh interferensi sinyal terhadap performa jaringan. Analisis dilakukan berdasarkan perubahan parameter komunikasi seperti kekuatan sinyal, keberhasilan pengiriman data, dan tingkat gangguan yang terjadi sebelum dan sesudah adanya serangan *jamming*[9].

3.1 Pengumpulan Data

Tahap pengumpulan data dilakukan untuk memperoleh beberapa informasi dan parameter yang dibutuhkan dalam proses perancangan sistem deteksi serangan *jamming* pada

komunikasi nirkabel berbasis *Internet of Things* (IoT). Parameter yang menjadi acuan dalam pengumpulan data meliputi bagaimana cara kerja *signal jammer*, tipe jaringan apa saja yang terdampak terhadap serangan jammer, bagaimana cara membedakan koneksi yang aman dan koneksi yang terganggu atau terdampak dari serangan jammer[10].



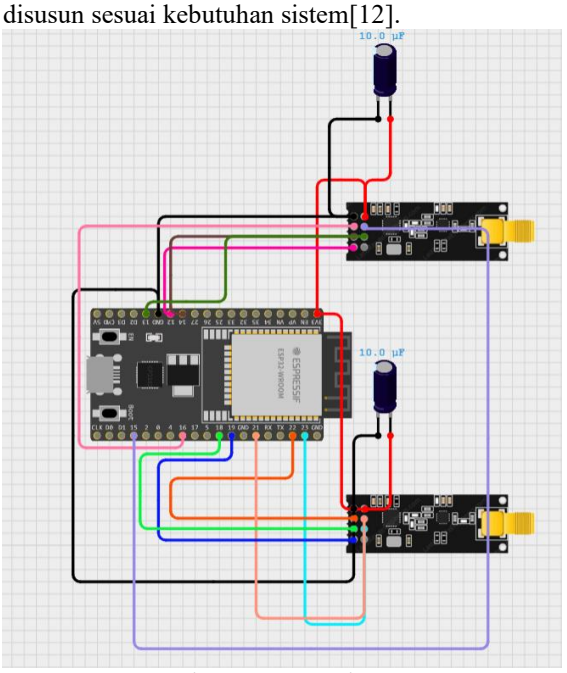
Gambar 1 Diagram Alir Sistem Deteksi Jamming

3.2 Pengumpulan Komponen

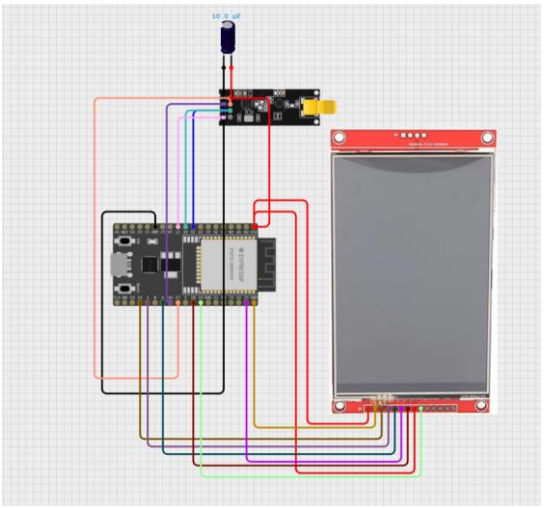
Tahap pengumpulan komponen dilakukan untuk mempersiapkan perangkat apa saja yang dibutuhkan dalam perancangan sistem. Komponen utama yang digunakan yaitu ESP32 sebagai mikrokontroler untuk proses pengolahan data dan nRF24L01+PA+LNA sebagai modul komunikasi radio, dan ILLI 9488 OLED *display* untuk menampilkan output dari hasil deteksi. Selain itu, digunakan komponen pendukung seperti breadboard, kabel jumper, dan sumber daya sebagai media perakitan sistem. Perangkat lunak yang digunakan adalah Arduino IDE untuk melakukan pemrograman dan konfigurasi perangkat. Pemilihan komponen disesuaikan dengan kebutuhan sistem dalam melakukan pengiriman data, pemantauan komunikasi, serta analisis gangguan akibat interferensi sinyal[11].

3.3 Perancangan Sistem

Tahap perancangan sistem dilakukan dengan membuat desain rangkaian perangkat keras sebagai gambaran awal sebelum proses implementasi. Perancangan ini bertujuan untuk menentukan jalur antar komponen. Rangkaian sistem dirancang dengan ESP32 sebagai pusat pengolahan data, modul nRF24L01+ sebagai media komunikasi nirkabel, serta TFT ILI9488 OLED Display sebagai *output display* untuk menampilkan kondisi komunikasi dan hasil deteksi gangguan. Selain itu, komponen pendukung seperti sumber daya, kabel penghubung, dan modul tambahan disusun sesuai kebutuhan sistem[12].



Gambar 2 Rancangan Signal Jammer

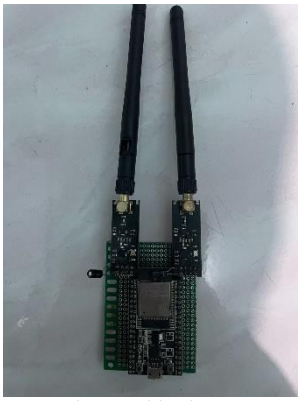


Gambar 3 Rancangan Jammer Detector

3.4 Desain Sistem

Tahap desain sistem dilakukan berdasarkan hasil perancangan rangkaian yang telah dibuat sebelumnya. Sistem terdiri dari dua perangkat utama, yaitu perangkat *jammer* sebagai penghasil gangguan sinyal dan perangkat *jammer detector* sebagai pendeteksi dan pemantau komunikasi. Perangkat *jammer* dirancang menggunakan ESP32 dan modul nRF24L01+PA+LNA untuk menghasilkan interferensi pada frekuensi yang digunakan sebagai media pengujian. Sementara itu, perangkat deteksi

menggunakan ESP32, modul nRF24L01+PA+LNA, serta TFT ILI9488 OLED Display sebagai media informasi untuk memantau kondisi komunikasi. Selain perakitan perangkat keras, dilakukan juga pembuatan program pada kedua sistem menggunakan Arduino IDE. Program pada *jammer detector* digunakan untuk melakukan komunikasi, membaca perubahan kondisi jaringan, dan menampilkan status sistem pada layar. Hasil implementasi ini kemudian digunakan sebagai perangkat uji pada tahap pengujian untuk mengetahui kemampuan sistem dalam mendeteksi serangan *jammer*.



Gambar 4 Produk Jadi Jammer

Gambar 5 Produk Jadi Sistem Deteksi Jammer

Parameter yang digunakan dalam pengujian sistem deteksi jamming terdiri dari empat parameter utama yang membentuk mekanisme *multi-layer detection.* Parameternya ditunjukkan pada Tabel berikut:

Tabel 4 Parameter Pengujian

Parameter	Deskripsi
Delta Baseline (L1)	Mengukur selisih antara nilai spektrum hasil pemindaian dengan nilai *baseline* untuk mendeteksi perubahan kondisi kanal.
Variance Spike Detection (L2)	Menganalisis variasi distribusi energi pada seluruh kanal untuk mengidentifikasi pola interferensi yang tidak normal.
Channel Entropy (L3)	Mengukur tingkat penyebaran energi antar kanal menggunakan nilai *entropy* untuk membedakan komunikasi normal dan gangguan jamming.
Consecutive Hit Counter (L4)	Menghitung konsistensi kemunculan gangguan pada beberapa siklus pemindaian sebagai validasi deteksi.
Threat Score	Nilai hasil pembobotan keempat parameter yang menunjukkan tingkat ancaman komunikasi.
Alert Counter	Penghitung yang bertambah ketika gangguan terdeteksi secara konsisten dan digunakan untuk mengurangi *false positive*.

Sistem melakukan pemindaian spektrum frekuensi 2,4 GHz secara *real-time*, kemudian menghitung nilai *Delta Baseline, Variance Spike Detection, Channel Entropy, dan Consecutive Hit Counter*. Keempat parameter tersebut digabungkan untuk menghasilkan *threat score,* sedangkan *alert counter* digunakan sebagai mekanisme validasi agar keputusan deteksi tidak hanya bergantung pada satu kali pembacaan spektrum. Berdasarkan kombinasi kedua parameter tersebut, sistem mengklasifikasikan kondisi menjadi Aman, Sinyal Mencurigakan, atau *Jammer* Terdeteksi.

3.5 Pengujian

Tahap pengujian dilakukan untuk mengetahui kinerja sistem *jammer* dan sistem deteksi *jamming* yang telah dirancang. Pengujian dilakukan dengan menjalankan perangkat *jammer* sebagai sumber gangguan dan perangkat *jammer detector* untuk monitoring kondisi komunikasi nirkabel. Pengujian dilakukan dengan membandingkan tiga kondisi utama, yaitu status aman, sinyal mencurigakan, dan jammer terdeteksi. Kondisi status aman merupakan kondisi ketika sistem komunikasi berjalan tanpa adanya gangguan, sehingga nilai spektrum sinyal berada pada kondisi normal. Kondisi sinyal mencurigakan merupakan kondisi *false positive*, yaitu ketika sistem memberikan indikasi adanya gangguan namun belum menunjukkan serangan *jammer* yang sebenarnya. Kondisi ini terjadi saat nilai spektrum sinyal berada pada rentang 25–50% dan ditampilkan sebagai peringatan awal. Selain itu, kondisi *false positive* juga diuji pada rentang 50–75%, yaitu ketika sistem menunjukkan status *jammer* terdeteksi berdasarkan peningkatan spektrum sinyal, tetapi kondisi tersebut masih dikategorikan sebagai kesalahan deteksi karena belum mencapai tingkat gangguan maksimum. Sementara itu, kondisi *jammer* terdeteksi yang sebenarnya terjadi ketika

nilai spektrum sinyal mencapai 100%, yang menunjukkan adanya interferensi kuat akibat aktivasi *jammer*. Data hasil pengujian kemudian dianalisis dengan membandingkan nilai spektrum sinyal dan status yang ditampilkan melalui TFT ILI9488 OLED Display untuk mengetahui tingkat keberhasilan sistem dalam membedakan kondisi normal, *false positive*, dan serangan *jamming*[8].

3.5.1 Cara Kerja *Jammer* 2.4GHz

Jammer 2.4GHz bekerja dengan prinsip membanjiri frekuensi radio dengan sinyal acak (*noise*) yang jauh lebih kuat sehingga perangkat yang digunakan dengan frekuensi sinyal yang sama tidak bisa lagi untuk mendengar atau menerima sinyal aslinya. *Jammer* yang digunakan pada penelitian kali ini menggunakan modul nRF24L01+PA+LNA yang bekerja pada rentang frekuensi 2.4GHz dan modul ini memiliki 2 komponen penting yaitu PA (*Power Amplifier*) berfungsi untuk memperkuat sinyal yang dipancarkan dan LNA (*Low Noise Amplifier*) berfungsi untuk memperkuat sinyal yang diterima[13]. Ada 3 langkah utama cara kerja jammer, yaitu:

3.5.1.1 Pertama, jammer akan terus menerus memancarkan sinyal acak (noise) pada rentang frekuensi 2.4GHz tanpa ada membawa data apapun.

3.5.1.2 Kedua, karena *WiFi* dan *Bluetooth* juga beroperasi pada frekuensi yang sama, sinyal acak dari *jammer* akan bertumpukan (*overlap*) dengan sinyal asli yang sedang dikirim oleh router atau perangkat lain. Ketika dua sinyal bertumpukan pada frekuensi yang sama, perangkat penerima tidak dapat membedakan mana data yang valid dan mana yang merupakan gangguan, sehingga data yang diterima menjadi rusak atau tidak terbaca (disebut interferensi).

3.5.1.3 Ketiga, jika daya sinyal jammer cukup kuat dan dipancarkan pada cakupan frekuensi yang luas biasa disebut *jamming broadband*, maka hampir seluruh channel komunikasi pada rentang 2.4GHz akan terganggu secara bersamaan. Hal ini menyebabkan perangkat WiFi gagal terhubung ke jaringan, koneksi yang sudah terhubung menjadi putus, atau perangkat Bluetooth tidak dapat melakukan pairing dengan perangkat lain[14].

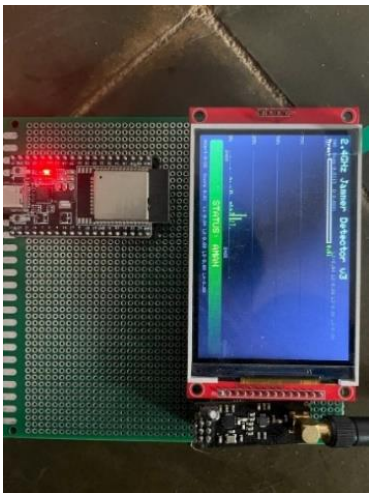
3.5.2 Analisis Kondisi Status Aman

Pada kondisi ini, sistem menampilkan indikator berwarna hijau dengan status "STATUS: AMAN". Nilai threat score yang ditampilkan sangat rendah, yaitu 0.01, dengan alert counter berada pada 0/20. Kondisi ini menunjukkan bahwa aktivitas jaringan pada frekuensi 2.4GHz berjalan normal, ditandai dengan skor dari spektrum sinyal yang relatif rendah dan stabil tanpa adanya lonjakan signifikan yang ditampilkan pada layar. Skenario pengujian pada kondisi ini dilakukan tanpa mengaktifkan perangkat jammer, sehingga jaringan WiFi dan Bluetooth di sekitar lokasi pengujian berjalan secara normal, dan pengujian dilakukan sebanyak tiga iterasi dengan durasi masing-masing satu menit[15].

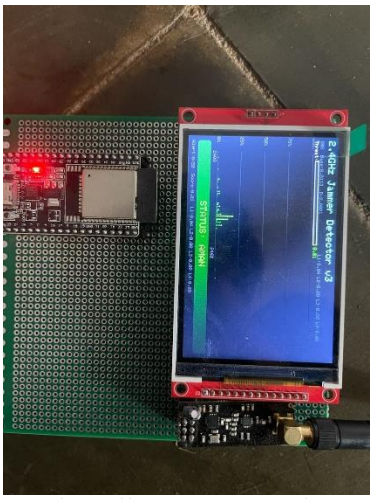
Tabel 5 Pengujian Pertama Kondisi Status Aman

Iterasi	Threat Score	Volume Spektrum	Hasil di Smartphone	Status Sistem
1	0.01	Rendah, tidak ada lonjakan	Wifi dan Bluetooth terdeteksi normal	AMAN
2	0.03	Rendah, lonjakan tidak signifikan	Wifi dan Bluetooth terdeteksi normal	AMAN
3	0.25	25-50%, lonjakan sesaat	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN

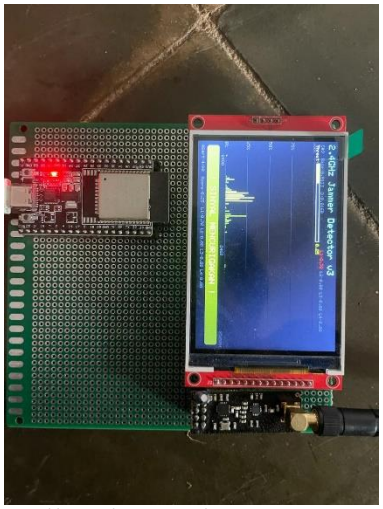
Berdasarkan tabel di atas di iterasi ketiga sistem sempat menampilkan status "SINYAL MENCURIGAKAN" dengan threat score 0.25 dalam waktu singkat sebelum kembali ke status aman. Kondisi sinyal mencurigakan ini tidak diprovokasi secara sengaja dan merupakan respons alami sistem terhadap lonjakan trafik jaringan WiFi dan Bluetooth yang wajar di sekitar lokasi pengujian. Karena lonjakan tersebut bersifat sesaat dan tidak bertahan secara konsisten, sistem secara otomatis kembali ke status aman, dan jaringan WiFi 2.4GHz pada perangkat smartphone terpantau masih terdeteksi secara normal selama iterasi berlangsung. Oleh karena itu, kondisi sinyal mencurigakan pada iterasi ketiga dikategorikan sebagai *false positive* yang muncul sebagai bagian dari perilaku normal sistem, bukan sebagai indikasi gangguan *jamming* yang sesungguhnya[16].



Gambar 6 Indikator Tanpa Gangguan Pertama



Gambar 7 Indikator Tanpa Gangguan Kedua



Gambar 8 Indikator False Positive Selama Pengujian Tanpa Jammer

3.5.3 Analisis Kondisi Sinyal Mencurigakan (*False Positive* Tahap Awal)

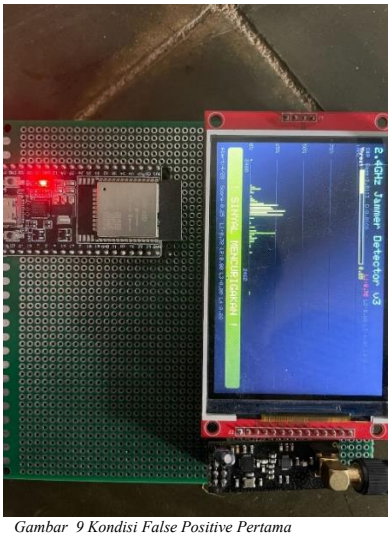
Kondisi yang ditandai dengan indikator berwarna kuning dan status "! SINYAL MENCURIGAKAN !", dengan *threat score* meningkat dari 0.01 ke 0.25 dan alert counter naik ke 4/20. Spektrum sinyal pada layar menunjukkan beberapa peningkatan aktivitas dibanding kondisi aman, namun belum mencapai tingkat yang mengindikasikan gangguan penuh. Kondisi ini dikategorikan sebagai *false positive* karena sistem baru memberikan peringatan awal ak ibat adanya kenaikan sinyal yang belum tentu berasal dari aktivitas *jamming*, melainkan dapat disebabkan oleh peningkatan trafik jaringan WiFi atau Bluetooth yang wajar. Berbeda dengan kondisi pengujian lainnya yang dapat direproduksi secara sengaja, kondisi *false positive* tidak dapat diprovokasi secara terkontrol karena kemunculannya bergantung sepenuhnya pada fluktuasi trafik jaringan di sekitar lokasi pengujian. Oleh karena itu, lima iterasi yang ditampilkan pada tabel berikut merupakan data yang dikumpulkan secara alami dari keseluruhan rangkaian pengujian, yaitu setiap kali sistem menampilkan status sinyal mencurigakan dari awal hingga akhir sesi pengujian berlangsung dan lima iterasi berikut dilakukan dalam kurun waktu pengujian selama lima menit, dalam kurun waktu tersebut terdapat lima kali lonjakan spektrum yang tidak wajar sehingga pada *jammer detector* terdeteksi sinyal mencurigakan.[17].

Tabel 6 Pengujian Kedua Kondisi Sinyal Mencurigakan

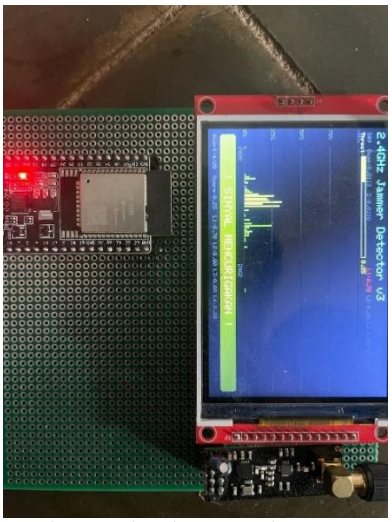
Iterasi	Threat Score	Volume Spektrum	Hasil di Smartphone	Status Sistem
1	0.25	25–50%, lonjakan sesaat pada sebagian channel	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN
2	0.25	25–50%, lonjakan sesaat pada sebagian channel	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN
3	0.25	25–50%, lonjakan sesaat pada sebagian channel	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN
4	0.25	25–50%, lonjakan sesaat pada sebagian channel	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN
5	0.35	25–50%, lonjakan sesaat dengan intensitas lebih tinggi	Wifi dan Bluetooth terdeteksi normal	SINYAL MENCURIGAKAN

Berdasarkan tabel di atas, kelima iterasi menunjukkan hasil yang konsisten sebagai kondisi false positive, ditandai dengan nilai threat score yang berada pada rentang 0.25–0.35 dan lonjakan spektrum yang bersifat

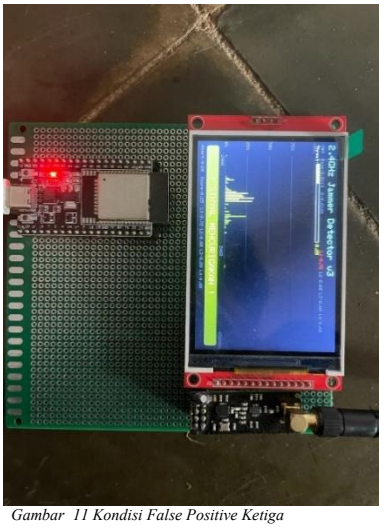
sesaat serta tidak bertahan secara konsisten dari waktu ke waktu. Pada seluruh iterasi, jaringan WiFi 2.4GHz pada perangkat smartphone masih dapat terdeteksi secara normal, membuktikan bahwa meskipun sistem menampilkan peringatan, tidak terdapat gangguan nyata pada komunikasi nirkabel di sekitar lokasi pengujian.



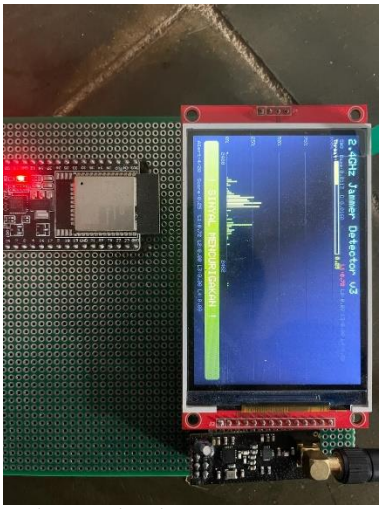
Gambar 9 Kondisi False Positive Pertama



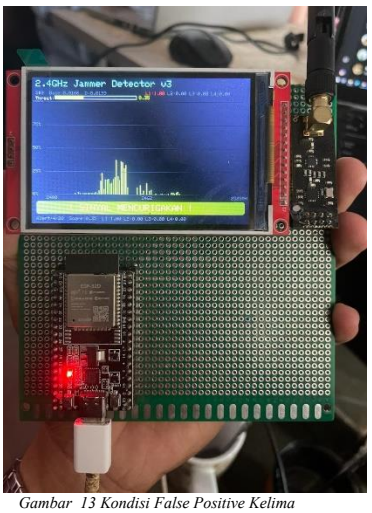
Gambar 10 Kondisi False Positive Kedua



Gambar 11 Kondisi False Positive Ketiga



Gambar 12 Kondisi False Positive Keempat



Gambar 13 Kondisi False Positive Kelima

3.5.4 Analisis Kondisi Jammer Terdeteksi dengan Spektrum Tidak Maksimal (False Positive Tahap Lanjut)

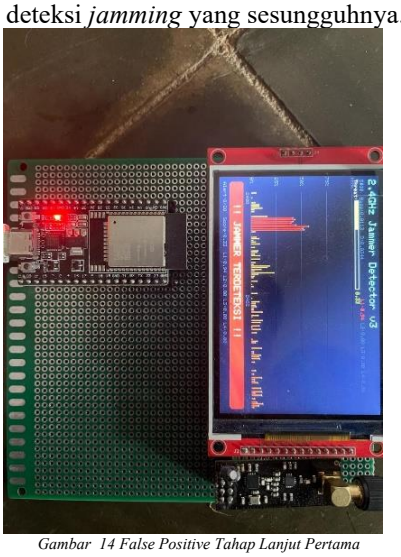
Pada kondisi ini, sistem telah menampilkan status "!! JAMMER TERDETEKSI !!" dengan indikator merah, threat score sebesar

0.33, dan alert counter mencapai 8/20. Meskipun status yang ditampilkan sudah berupa peringatan tinggi, pengamatan terhadap layar menunjukkan bahwa lonjakan sinyal hanya berlangsung sesaat dan tidak konsisten atau tidak bertahan lama pada pemindaian-pemindaian berikutnya. Hal ini menjadi poin penting dalam membedakan gangguan jamming yang sesungguhnya dengan lonjakan sinyal biasa, karena jammer — baik dengan daya tinggi maupun daya rendah — secara fisik selalu memancarkan sinyal secara konsisten dan terus-menerus selama aktif. Sebaliknya, trafik WiFi dan Bluetooth yang berjalan normal bersifat naik-turun, yaitu mengirim data sebentar lalu berhenti, sehingga sesekali dapat memunculkan lonjakan yang menyerupai gangguan meskipun sebenarnya bukan dampak dari gangguan jamming. Karena lonjakan pada kondisi ini tidak bertahan secara konsisten dari waktu ke waktu, kondisi ini lebih tepat dikategorikan sebagai kesalahan deteksi (false positive) yang dipicu oleh aktivitas jaringan yang wajar, bukan oleh interferensi jamming yang sesungguhnya. Temuan ini menunjukkan bahwa status "jammer terdeteksi" pada sistem masih dapat muncul akibat lonjakan sesaat, sehingga durasi dan konsistensi sinyal perlu menjadi pertimbangan tambahan untuk meningkatkan akurasi deteksi pada pengembangan selanjutnya. Pengujian pada kondisi ini dilakukan selama lima menit, berbeda dari sebelumnya, pada pengujian ini terdapat tiga iterasi yang menunjukkan lonjakan spektrum yang tidak wajar sehingga pada alat deteksi menunjukkan indikator "JAMMER TERDETEKSI" dalam kurun waktu pengujian selama lima menit[7].

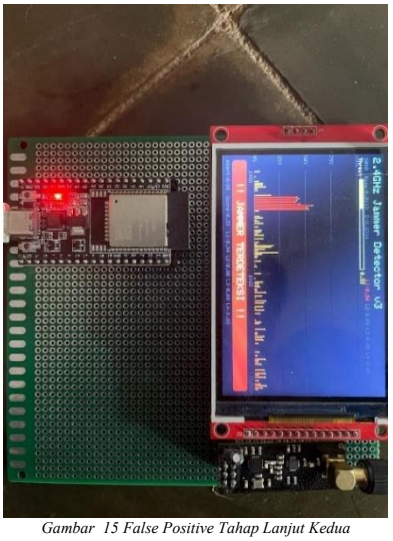
Tabel 7 Pengujian Ketiga Kondisi Jammer Terdeteksi Dengan Spektrum Tidak Maksimal

Iterasi	Threat Score	Volume Spektrum	Hasil di Smartphone	Status Sistem
1	0.33	50–75%, lonjakan tidak menyeluruh pada sebagian channel	Wifi dan Bluetooth terdeteksi normal tanpa gangguan	JAMMER TERDETEKSI
2	0.33	50–75%, lonjakan tidak menyeluruh pada sebagian channel	Wifi dan Bluetooth terdeteksi normal tanpa gangguan	JAMMER TERDETEKSI
3	0.33	50–75%, lonjakan tidak menyeluruh pada sebagian channel	Wifi dan Bluetooth terdeteksi normal tanpa gangguan	JAMMER TERDETEKSI

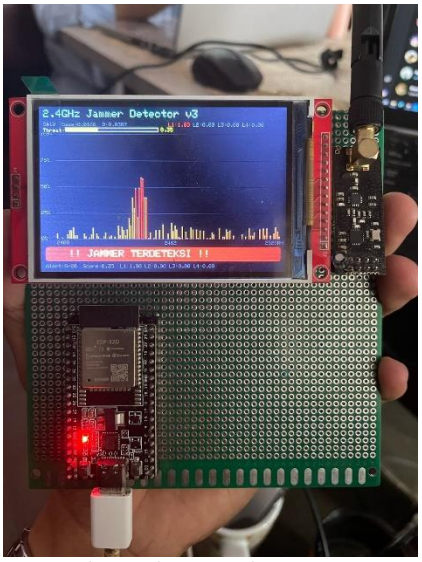
Berdasarkan ketiga iterasi diatas menunjukkan hasil yang konsisten dengan *threat score* pada rentang 0.33–0.35 dan *alert counter* yang hanya mencapai 8/20, jauh di bawah nilai maksimum. Spektrum sinyal pada layar menunjukkan peningkatan aktivitas yang terpusat pada sebagian *channel* saja dan tidak merata ke seluruh rentang frekuensi 2.4GHz, serta jaringan WiFi 2.4GHz pada perangkat smartphone masih dapat terdeteksi selama seluruh pengujian berlangsung. Kombinasi kedua temuan ini memperkuat kategorisasi kondisi ini sebagai *false positive* tahap lanjut, bukan sebagai deteksi *jamming* yang sesungguhnya.



Gambar 14 False Positive Tahap Lanjut Pertama



Gambar 15 False Positive Tahap Lanjut Kedua



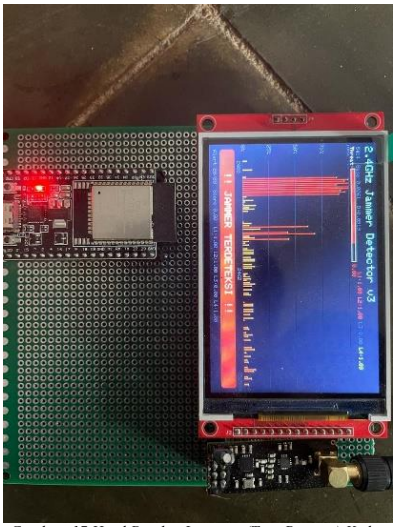
Gambar 16 False Positive Tahap Lanjut Ketiga

3.5.5 Analisis Kondisi Jammer Terdeteksi dengan Spektrum Maksimal (True Positive)

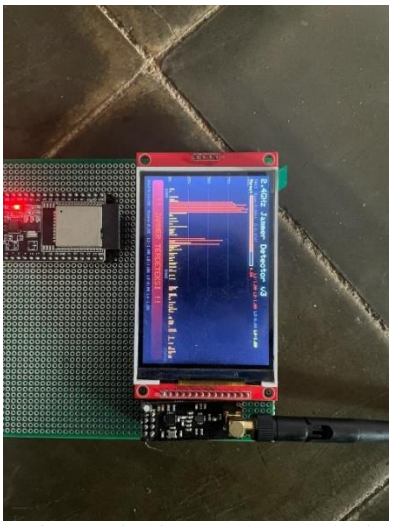
Kondisi ini merupakan hasil deteksi yang sebenarnya, ditandai dengan *alert counter* mencapai nilai maksimum 20/20 dan *threat score* sebesar 0.80, di mana lonjakan sinyal bertahan secara konsisten dan merata di hampir seluruh *channel* frekuensi 2.4GHz sesuai karakteristik *jammer broadband* menggunakan modul nRF24L01+PA+LNA. Validitasnya diperkuat oleh hasil pengamatan langsung pada perangkat *smartphone* yang menunjukkan seluruh jaringan WiFi 2.4GHz di sekitar lokasi pengujian hilang sepenuhnya dari daftar jaringan sementara jaringan 5GHz tetap normal, sehingga gangguan ini dapat dipastikan sebagai *jamming* yang sesungguhnya (*true positive*) karena hasil pembacaan sistem konsisten dengan dampak nyata yang terjadi di lapangan, bukan sekadar kesalahan deteksi. Pengujian pada kondisi ini dilakukan sebanyak dua iterasi dengan mengaktifkan *jammer* pada daya pancar optimal[15].

Tabel 8 Pengujian Keempat Kondisi Jammer Terdeteksi Dengan Spektrum Maksimal

Iterasi	Threat Score	Volume Spektrum	Hasil di Smartphone	Status Sistem
1	0.80	100%, merata di hampir seluruh channel	WiFi 2.4GHz hilang, koneksi bluetooth terganggu, sementara koneksi wifi 5GHz tetap normal	JAMMER TERDETEKSI
2	0.80	100%, merata di hampir seluruh channel	WiFi 2.4GHz hilang, koneksi bluetooth terganggu, sementara koneksi wifi 5GHz tetap normal	JAMMER TERDETEKSI



Gambar 17 Hasil Deteksi Jamming (True Positive) Kedua



Gambar 18 Hasil Deteksi Jamming (True Positive) Kedua

Gambar 19 Hasil Pengujian Menunjukkan Semua Sinyal 2.4GHz Terganggu

IV. KESIMPULAN

4.1 Kesimpulan

Berdasarkan hasil perancangan dan pengujian sistem deteksi serangan *jammer* pada penelitian ini, dapat disimpulkan bahwa sistem berhasil dirancang menggunakan ESP32, modul nRF24L01+ PA/LNA, dan TFT ILI9488 sebagai media pemantauan kondisi komunikasi. Sistem yang dibuat terdiri dari perangkat *jammer* sebagai sumber gangguan dan perangkat *jammer detector* sebagai pemantau serta pendeteksi perubahan kondisi sinyal pada rentang frekuensi 2.4GHz. Hasil pengujian menunjukkan bahwa sistem ini mampu mengidentifikasi kondisi komunikasi berdasarkan perubahan spektrum sinyal, serta membedakan antara kondisi normal tanpa gangguan, kondisi sinyal mencurigakan, dan kondisi *jammer* terdeteksi. Pengujian juga mengungkap bahwa penentu utama antara kondisi *false positive* dan *true positive* bukan terletak pada seberapa tinggi nilai spektrum yang terbaca sesaat, melainkan pada konsistensi sinyal tersebut dari waktu ke waktu; lonjakan yang muncul sebentar lalu mereda cenderung merupakan trafik jaringan normal, sedangkan sinyal yang bertahan tinggi secara terus-menerus mengindikasikan adanya sumber gangguan yang benar-benar aktif. Validitas kondisi jammer terdeteksi pada pengujian ini turut diperkuat melalui pengamatan langsung di lokasi pengujian, yang menunjukkan hilangnya seluruh jaringan WiFi berfrekuensi 2.4GHz secara bersamaan ketika status *jamming* tertinggi tercapai, sementara jaringan berfrekuensi 5GHz tetap berjalan normal, sehingga membuktikan bahwa hasil pembacaan sistem konsisten dengan dampak nyata pada komunikasi nirkabel di sekitar lokasi pengujian.

DAFTAR PUSTAKA

[1] Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, and Fried Sinlae, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," *J. Zetroem*, vol. 6, no. 1, pp. 114–119, 2024, doi: 10.36526/ztr.v6i1.3376.

[2] "Russia suspected of jamming GPS signal on aircraft carrying Grant Shapps | Grant Shapps | The Guardian." Accessed: Dec. 22, 2025. [Online]. Available: https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps?

[3] "Tiga Tahun Terakhir Banyak Radar BMKG Terinterferensi - Seputar DJID - Info - Direktorat Jenderal Infrastruktur Digital." Accessed: Jul. 20, 2026. [Online]. Available: https://www.postel.go.id/berita-tiga-tahun-terakhir-banyak-radar-bmkg-terinterferensi-27-5507

[4] "Dad takes down town's internet by mistake to get his kids offline." Accessed: Dec. 22, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/technology/dad-takes-down-towns-internet-by-mistake-to-get-his-kids-offline/

[5] L. Arcangeloni, G. S. Member, E. Testi, A. Giorgetti, and S. Member, "Detection of Jamming Attacks via Source Separation and Causal Inference," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4793–4806, 2023, doi: 10.1109/TCOMM.2023.3281467.

[6] C. Elindria, "Serangan Pada Jaringan Wireless," 2007.

[7] R. Bangun *et al.*, "Rancang bangun alat pendeteksi dan jammer sinyal," 2025.

[8] N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A Wireless Intrusion Detection System for 802.11 WPA3 Networks," *2022 14th Int. Conf. Commun. Syst. NETworkS, COMSNETS 2022*, vol. 3, pp. 384–392, 2022, doi: 10.1109/COMSNETS53615.2022.9668542.

[9] Kruthika V H, Gagana M Aradhyamatt, Bharat K, Bhuvan S, DR. Sujay Routh, "Ai based rf jamming and mitigation 1," vol. 13, no. 12, pp. 39–45, 2025.

[10] Ratih Agustiningsih, Dedy Suryadi, Dasril "Rancang Bangun Alat Pemblocking Sinyal (Jammer) Pada Sistem Telekomunikasi Jaringan Seluler Global System For Mobile (Gsm) Di Area Bebas Sinyal GSM," J. Teknik, E. Fakultas, and U, Tanjungpura, 2018.

[11] "ESP32 Bluetooth Jammer with NRF24L01 – DIY Build Guide." Accessed: Jun. 19, 2026. [Online]. Available: https://circuitdigest.com/tutorial/esp32-bluetooth-jammer-using-nrf24l01

[12] A. M. Avianty, Y. Suprapto, and T. Warsito, "Rancangan Monitoring Interferensi Frekuensi pada Komunikasi VHF Air to Ground Berbasis Arduino Uno Menggunakan Receiver RTL-SDR R820T," *SNITP Semin. Nas. Inov. Teknol. Penerbangan*, 2021.

[13] Yanuar Agung Pratama, "Tugas akhir rancang bangun jammer seluler gsm," J. Teknik, E. Fakultas, and U.

Semarang, 2021.
[14] M. N. Djamin, E. I. Alwi, and S. M. Abdullah, "Analisis Serangan Jammer Pada Jaringan Wireless," *Lit. Inform. Komput.*, vol. 2, no. 1, p. pp xx-xx, 2025.
[15] Citra Rizki Utami, "Perancangan Model Deteksi Dan Klasifikasi Serangan Jamming Pada Jaringan Nirkabel Berbasis Machine Learning," vol. 23221064, 2023.
[16] Ferdi Kuswandi, Andi Rukmana, Adiyanto, "Keamanan Siber Dalam Era Internet of Things:Tantangan dan Solusi Teknologi Terkini" vol. 13, no. 1, pp. 57–62, 2025.
[17] Alvin Mufidha Ahmad and Fauzi Adi Rafrastara, "Improving Internet of Things Cyber Attack Detection with Information Gain and Decision Tree," *INOVTEK Polbeng - Seri Inform.*, vol. 10, no. 3, pp. 1888–1896, 2025, doi: 10.35314/p2c33t87.