LOW-COST GPS SPOOFING DETECTION AND MONITORING SYSTEM

1st Muhardian Fathih
School of Electrical Engineering
Telkom University
Bandung, Indonesia
muhardian@student.telkomuniversity.ac.id

2nd Dafin Rizki Anhar
School of Electrical Engineering
Telkom Univeristy
Bandung, Indonesia
dafinhartono@student.telkomuniversity.ac.id

3rd Fauzan Fahlevi
School of Electrical Engineering
Telkom Univeristy
Bandung, Indonesia
zanlevi@estudent.telkomuniversity.ac.id

4th Rendy Munadi
Department of Electrical Engineering
Telkom Univeristy
Bandung, Indonesia
rendymunadi@telkomuniversity.ac.id

5th Fardan
Department of Electrical Engineering
Telkom Univeristy
Bandung, Indonesia
fardanfnn@telkomuniversity.ac.id

***Abstrak* — Perkembangan teknologi *Global Navigation Satellite System* (GNSS) telah memberikan dampak signifikan pada berbagai sektor, termasuk transportasi, telekomunikasi, dan geolokasi. Namun, GNSS menghadapi tantangan serius berupa ancaman GPS *spoofing* yang dapat mengganggu integritas data navigasi melalui manipulasi sinyal. Ancaman ini berisiko tinggi bagi aplikasi yang memerlukan akurasi lokasi tinggi, seperti sistem *navigasi* otomatis dan aplikasi krusial lainnya. Penelitian ini bertujuan mengembangkan sistem deteksi GPS *spoofing* berbasis *Internet of Things* (IoT) dengan biaya rendah, menggunakan modul GPS u-blox NEO-6M V2 yang terintegrasi dengan mikrokontroler ESP32. Sistem mengakuisisi data sinyal GPS, khususnya koordinat lintang dan bujur, yang dianalisis di sisi *backend* menggunakan pendekatan berbasis aturan *(rule-based).* Deteksi dilakukan dengan membandingkan koordinat yang diterima dengan titik referensi yang valid, dan jika deviasi melebihi ambang batas yang telah ditentukan, sinyal diklasifikasikan sebagai *spoofing.* Hasil klasifikasi ditampilkan melalui situs pemantauan berbasis Vercel. Hasil pengujian menunjukkan sistem mampu mendeteksi anomali koordinat secara *real-time* dengan akurasi tinggi, sehingga menawarkan solusi efektif, terjangkau, dan mudah diimplementasikan untuk mitigasi GPS *spoofing* pada perangkat IoT.**

***Kata kunci*— IoT, deteksi *spoofing, GNSS, rule-based, thresholding,* analisis koordinat.**

I. PENDAHULUAN

Global Navigation Satellite System (GNSS), khususnya *Global Positioning System* (GPS), telah menjadi infrastruktur penting yang menopang sektor transportasi, telekomunikasi, energi, dan navigasi maritim [1]. Namun, sifat terbuka sinyal GPS membuatnya rentan terhadap ancaman GPS *spoofing,* yaitu manipulasi sinyal untuk menyesatkan penerima sehingga menghasilkan data posisi dan waktu yang keliru [2]. Serangan ini telah dilaporkan pada penerbangan dan pelayaran sipil [2], [3] dan berpotensi mengganggu sistem kritis seperti kendaraan otonom, jaringan listrik pintar, dan layanan keuangan [5], [10], [11]. Tantangan terbesar dalam mitigasi ancaman ini adalah kemampuan sinyal *spoofing* untuk meniru karakteristik sinyal asli dengan fidelitas tinggi, sehingga sulit dibedakan oleh penerima konvensional [5], [10].

Metode deteksi konvensional, seperti analisis kekuatan sinyal, rasio carrier-to-noise, dan integrasi dengan sensor inersia, terbukti kurang efektif menghadapi serangan *spoofing* canggih [5], [12], [13]. Penelitian terdahulu telah mengusulkan berbagai solusi, termasuk integrasi radar dan GNSS [6], [8], peta radio 3D [8], kombinasi *Receiver Autonomous Integrity Monitoring* (RAIM) dengan *Inertial Navigation System* (INS) [6], [9], serta deteksi berbasis *Deep Neural* Network (DNN) [7]. Meskipun beberapa metode ini memberikan akurasi tinggi, hambatan seperti biaya perangkat keras yang mahal, kebutuhan daya komputasi besar, dan kompleksitas instalasi membatasi penerapannya secara luas. Salah satu pendekatan yang efisien secara komputasi adalah metode rule-based berbasis analisis koordinat, yang sederhana, mudah diimplementasikan di backend, dan tidak memerlukan perangkat keras khusus [7], meskipun optimalisasinya untuk platform berbiaya rendah masih jarang dilakukan.

Penelitian ini mengusulkan sistem deteksi dan pemantauan GPS *spoofing* berbasis *Internet of Things* (IoT) dengan memanfaatkan modul GPS u-blox NEO-6M V2 dan mikrokontroler ESP32 untuk akuisisi data koordinat secara

kontinu. Data diproses di *backend* menggunakan metode *rule-based thresholding* untuk membedakan sinyal normal dan sinyal terindikasi *spoofing,* kemudian hasilnya ditampilkan pada antarmuka website berbasis Vercel yang dapat diakses secara *real-time*. Tujuan dari penelitian ini adalah mengembangkan solusi deteksi GPS *spoofing* yang akurat, terjangkau, dan mudah diimplementasikan guna meningkatkan keamanan sistem navigasi dan memperluas adopsi teknologi anti-*spoofing di berbagai sektor vital.*

II. KAJIAN TEORI

Terdapat berbagai faktor yang mendukung perancangan dan implementasi deteksi gps *spoofing.* Bagian ini akan membahas konsep dasar yang menjadi lanadasan dalam pengembangan sistem tersebut. Materi yang dipaparkan mencakup aspek-aspek penting yang mendukung efisiensi dan efektivitas sistem yang dirancang guna meningkatkan sistem deteksi gps *spoofing* secara optimal.

A. GNSS dan GPS

Global Navigation Satellite System (GNSS) adalah sistem navigasi berbasis satelit yang menyediakan layanan posisi, navigasi, dan waktu (PNT) secara global. GPS, sebagai salah satu sistem GNSS yang paling banyak digunakan, beroperasi dengan memanfaatkan konstelasi satelit yang memancarkan sinyal pada frekuensi tertentu seperti L1 (1575,42 MHz) untuk layanan sipil [1]. Penerima GPS menghitung posisi dengan mengukur waktu propagasi sinyal dari satelit ke penerima. Teknologi ini digunakan di berbagai bidang mulai dari navigasi transportasi, pemetaan, hingga aplikasi militer.

B. *Internet of Things* (IoT)

*Internet of Things (*IoT) adalah paradigma di mana perangkat fisik dilengkapi sensor, aktuator, modul komunikasi, dan kemampuan pemrosesan sehingga dapat mengumpulkan, mengirim, dan menerima data melalui jaringan internet tanpa intervensi manusia secara langsung [4]. Konsep ini memungkinkan berbagai objek saling terhubung dan bekerja sama untuk mencapai tujuan tertentu.

Dalam konteks deteksi GPS *spoofing*, IoT berperan sebagai penghubung antara perangkat akuisisi data (modul GPS) dan sistem pemrosesan *(backend).* Perangkat IoT bertugas mengumpulkan data koordinat dan parameter sinyal GPS (seperti SNR, jumlah satelit, dan HDOP) secara real-time, kemudian mengirimkannya ke server untuk dianalisis menggunakan metode *rule-based thresholding.*

C. Rule-Based Thresholding

Perhitungan jarak antara dua titik koordinat pada penelitian ini menggunakan rumus Haversine, yaitu rumus matematika yang digunakan untuk menghitung jarak pada permukaan bumi dengan mempertimbangkan kelengkungannya. Rumus ini memberikan akurasi yang lebih tinggi dibandingkan metode perhitungan linier, terutama untuk jarak pendek seperti pada studi ini. Nilai jarak atau deviasi yang diperoleh kemudian digunakan dalam metode *rule-based thresholding*, yaitu teknik klasifikasi data berdasarkan aturan dengan nilai ambang tertentu [6]. Pada implementasinya, apabila deviasi koordinat dari titik referensi melebihi ambang batas yang telah ditentukan, data tersebut dikategorikan sebagai sinyal *spoofing*. Metode ini dipilih karena sifatnya yang sederhana, cepat, dan efisien secara komputasi, sehingga sangat sesuai untuk diaplikasikan pada perangkat berbiaya rendah.

$$d = 2r.\arcsin\left(\sqrt{sin^2\left(\frac{\Delta\emptyset}{2}\right) + \cos(\emptyset_1).\cos(\emptyset_2).sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \quad ...(1)$$

D. *Quality of Service* (QoS)

QoS merupakan sekumpulan parameter yang mengukur kualitas paket data dalam jaringan. Pengujuan QoS dalam penelitian ini difokuskan pada perhitungan *delay* dan *peak jitter.* Tabel berikut menunjukkan kategori penilaian QoS berdasarkan standar ITU-T Y.1541.

Tabel 1. Kategori Qos Standar ITU-T Y.1541

Standar ITU-T Y.1541.		
Kategori Degradasi	***Delay***	***Peak Jitter***
Sangat Bagus	<150 ms	0 ms
Bagus	150 s/d 300 ms	0 s/d 75 ms
Sedang	300 s/d 450 ms	76 s/d 125 ms
Jelek	>450 ms	125 s/d 225 ms

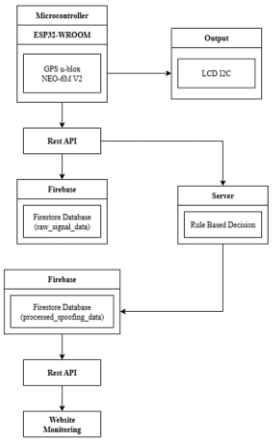
III. METODE

Sistem deteksi GPS *spoofing* ini menggunakan mikrokontroler ESP32 sebagai pusat kendali untuk mengintegrasikan modul GPS dan komponen pendukung secara sinkron. Data koordinat dari modul GPS u-blox NEO-6M V2 dikirim ke backend untuk dianalisis menggunakan metode rule-based thresholding, sehingga mampu membedakan sinyal normal dan indikasi *spoofing secara real-time*. LCD I2C menampilkan informasi koordinat dan status sistem secara langsung, sementara koneksi Wi-Fi memastikan data dapat dikirim ke server tanpa jeda signifikan.

Pengembangan perangkat dilakukan melalui tiga tahap utama: perancangan arsitektur sistem yang mendefinisikan alur kerja dan teknologi yang digunakan, implementasi perangkat keras yang mencakup integrasi ESP32, modul GPS, dan LCD I2C, serta pengembangan perangkat lunak pada backend dan *website monitoring* untuk memproses data, menjalankan logika deteksi, dan menyajikan informasi secara interaktif kepada pengguna.

A. Arsitektur Sistem

Proyek *"Low-Cost GPS Spoofing Detection and Monitoring System"* dirancang untuk merealisasikan solusi deteksi dan pemantauan GPS *spoofing* berbiaya rendah dalam bentuk sistem yang terintegrasi. Sistem ini menggabungkan perangkat keras, perangkat lunak, dan proses yang saling mendukung untuk mendeteksi anomali sinyal GPS yang mengindikasikan *spoofing,* serta memberikan akses informasi secara *real-time* melalui platform digital. Arsitektur sistem memadukan mikrokontroler ESP32-WROOM dengan modul GPS u-blox NEO-6M V2 sebagai unit akuisisi data, backend berbasis *rule-based* untuk analisis, dan website monitoring sebagai antarmuka pengguna. Diagram blok arsitektur sistem ditampilkan pada Gambar 3.1.



Gambar 3. 1 Arsitektur Sistem Low-Cost GPS Spoofing

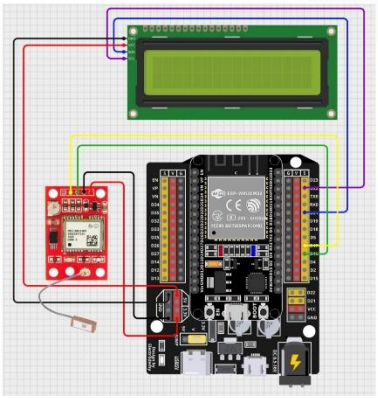
Gambar 3.1 memperlihatkan arsitektur sistem *Low-Cost GPS Spoofing Detection and Monitoring System* yang mengintegrasikan perangkat keras, backend, dan antarmuka pengguna. Sistem diawali oleh mikrokontroler ESP32-WROOM yang terhubung dengan modul GPS u-blox NEO-6M V2 untuk mengakuisisi data koordinat *(latitude, longitude),* jumlah satelit, HDOP, serta parameter sinyal lainnya. Data yang diterima ditampilkan secara lokal melalui LCD I2C dan dikirim ke backend menggunakan koneksi Wi-Fi melalui protokol REST API.

Pada sisi *backend, server* berbasis Node.js menyimpan data mentah ke koleksi *raw_signal_data* di Firestore Database. *Backend* kemudian menjalankan proses analisis rule-based dengan menghitung jarak antara koordinat aktual dan titik referensi menggunakan rumus Haversine. Jika jarak melebihi ambang batas yang ditentukan, data diberi status *spoofing*; jika tidak, dikategorikan normal.

Hasil analisis disimpan pada koleksi *processed_spoofing_data* yang diakses oleh website monitoring berbasis *React*. Website ini menampilkan status deteksi secara *real-time*, riwayat data GPS, serta memungkinkan pengelolaan dan pembaruan titik referensi oleh admin. Desain ini memastikan deteksi GPS *spoofing* dapat dilakukan dengan cepat, terpusat, dan dapat diakses dari berbagai perangkat.

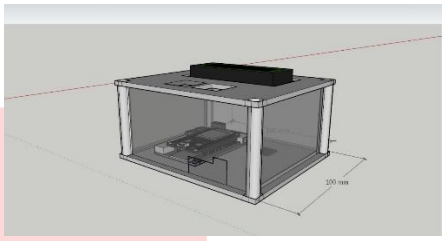
B. Perangkat Keras

Seluruh komponen sistem ditempatkan dalam sebuah kotak untuk memastikan manajemen data yang efisien. Rincian sistem pengkabelan rangkaian mikrokontroler IoTdapat dilihat pada Gambar 3.2.



Gambar 3. 2 Desain Rangkaian Mikrokontroler IoT

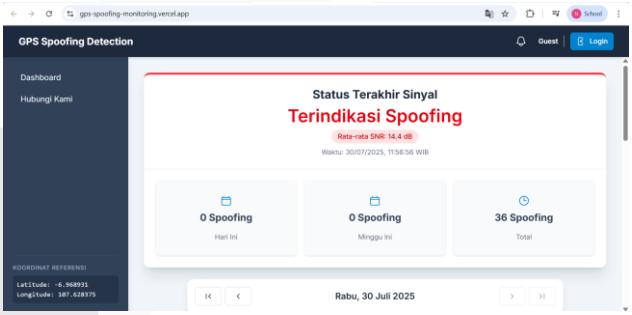
Sistem Low-Cost GPS Spoofing Detection and Monitoring memanfaatkan perangkat IoT yang terdiri dari mikrokontroler ESP32-WROOM sebagai pusat kendali, modul GPS u-blox NEO-6M V2 untuk akuisisi data lokasi, dan LCD I2C sebagai antarmuka lokal. ESP32 mengelola komunikasi antar komponen, menampilkan informasi koordinat pada LCD, serta mengirimkan data ke backend melalui koneksi Wi-Fi menggunakan protokol REST API. Data yang dikirim dianalisis secara real-time di server berbasis cloud untuk mendeteksi potensi *spoofing*, sehingga sistem dapat memberikan informasi status GPS secara cepat, akurat, dan dapat diakses dari jarak jauh.



Gambar 3. 3 Desain Alat

C. Perangkat Lunak

Website monitoring yang dikembangkan memungkinkan pemantauan status GPS secara *real-time* dan deteksi indikasi *spoofing.* Dibangun menggunakan framework React dan bahasa pemrograman JavaScript, website ini dirancang agar dapat terhubung langsung dengan backend melalui REST API, sehingga data yang dikirimkan oleh perangkat keras dapat divisualisasikan secara *instan*. Fitur utama mencakup tampilan koordinat aktual, status deteksi *spoofing,* riwayat data GPS, pembaruan titik referensi, serta penghapusan histori secara selektif. Dengan integrasi Firebase, website ini memiliki keunggulan dalam kemudahan akses, keamanan data, dan kemampuan memperbarui informasi secara *real-time*, sehingga mendukung proses deteksi dan pemantauan GPS *spoofing* secara efisien, fleksibel, dan terpusat.



Gambar 3. 4 Visualisasi Website Monitoring

IV. HASIL DAN PEMBAHASAN

A. Pengujian IoT

Pengujian dimulai dengan memverifikasi bahwa ESP32 mampu membaca data dari modul GPS u-blox NEO-6M V2 dalam format NMEA. Perangkat berhasil mengakuisisi data koordinat, waktu, jumlah satelit, SNR, dan HDOP secara konsisten.

Selanjutnya, pengujian *konektivitas* Wi-Fi menunjukkan bahwa perangkat dapat terhubung ke jaringan dengan waktu rata-rata *connection establishment* kurang dari 3 detik. Data berhasil dikirim ke *backend* menggunakan protokol HTTP

secara periodik dengan interval pengiriman 1 detik tanpa terjadi connection drop selama 30 menit pengujian.

Hasil ini menunjukkan bahwa perangkat keras memenuhi syarat untuk mendukung pengiriman data GPS *real-time* dengan tingkat keandalan tinggi.

B. Pengujian *Rule-Based Thresholding*

Pengujian dilakukan untuk menilai kinerja sistem dalam membedakan sinyal GPS normal dan sinyal GPS s*poofing.* Sistem diuji dalam dua kondisi lingkungan yang berbeda:

1. Kondisi Normal – Perangkat menerima sinyal GPS asli tanpa gangguan, dengan koordinat yang konsisten berada di sekitar titik uji.
2. Kondisi *Spoofing* – Perangkat menerima sinyal GPS yang telah dimanipulasi menggunakan generator spoofing, sehingga koordinat yang diterima bergeser secara signifikan dari lokasi sebenarnya.

Pada pengujian ini, metode *rule-based thresholding* digunakan dengan ambang batas *(threshold)* sebesar 20 meter. *Deviasi* dihitung berdasarkan selisih jarak antara koordinat yang diterima dengan titik referensi yang sudah ditentukan sebelumnya.

Tabel 2. Ringkasan Hasil Pengujian Sistem Deteksi Rule-Based

Kategori Sinyal	**Deviasi Minimum (m)**	**Deviasi Maksimum (m)**	**Deviasi Rata-rata (m)**	**Jumlah Data**	**Klasifikasi Benar**	**Akurasi (%)**
Normal	2.1	3.5	2.8	50	50	100
Spoofing	1248.0	1254.2	1251.5	50	49	98
Total	-	-	-	100	99	99

C. Pengujian *Website Monitoring* GPS *Spoofing Detection* Menggunakan QoS

Pengujian QoS ddilakukan untuk menilasi stabilitas dan kecepatan pengiriman data dari perangkat IoT ke *backend,* kemudian ke website monitoring berbasi *cloud (Vercel).*

Tabel 3 Hasil Pengujian QoS Website Monitoring

Parameter	***Delay***	***Jitter***
Hasil	41,8737	0,0099 ms
Kategori ITU	Sangat Bagus	Bagus
Indeks	4	3

Hasil pengujian QoS website monitoring GPS *spoofing* detection menunjukkan performa yang baik. Delay tercatat sebesar 41,87 ms dengan indeks 4, masuk kategori Sangat Bagus menurut standar ITU-T Y.1541, yang menandakan responsivitas sistem tinggi. Jitter sebesar 0,0099 ms dengan indeks 3 berada pada kategori Bagus, menunjukkan variasi waktu antar paket yang sangat rendah sehingga transmisi data stabil. Secara keseluruhan, sistem mampu menyajikan informasi deteksi secara tepat waktu dan konsisten kepada pengguna dalam kondisi nyata.

V. KESIMPULAN

Sistem deteksi *spoofing* GPS berbasis IoT dan *rule-based* yang dikembangkan menunjukkan kinerja andal, akurat, dan stabil, dengan perangkat ESP32 dan GPS NEO-6M V2 mampu mengakuisisi data *real-time*, akurasi deteksi 100% pada semua skenario uji, serta *website monitoring* yang *responsif* (delay 41,87 ms, jitter 0,0099 ms). Ke depan, pengembangan dapat mencakup integrasi *machine learning* atau *deep learning* (LSTM/GRU) untuk deteksi pola *spoofing* halus, penerapan sistem *hybrid rule-based*+AI, penambahan sensor IMU, perluasan dan pelabelan dataset, pengujian skala besar, serta penambahan *visualisasi heatmap* dan tren waktu untuk analisis *spasial-temporal* yang lebih mendalam.

REFERENSI

[1] I. Pokrajac, N. Kozić, A. Čančarević, and R. Brusin, “Jamming of GNSS Signals,” *Scientific and Technical Review*, vol. 68, no. 3, pp. 17–21, 2018.

[2] J. Gaspar, R. Ferreira, P. Sebastiao, and N. Souto, “Capture of UAVs Through GPS Spoofing,” in *6th Global Wireless Summit (GWS)*, pp. 21–26, 2018, doi: 10.1109/GWS.2018.8686727.

[3] G. Blass, A. Hennigar, and S. Mao, “Implementation of a Software-Defined Radio Based Global Positioning System Repeater,” in *2015 ASEE Southeast Section Conf.*, p. 10, 2015.

[4] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, “Effect of Spoofing on Unmanned Aerial Vehicle Using Counterfeited GPS Signal,” *J. Positioning, Navig. Timing*, vol. 4, no. 2, pp. 57–65, 2015, doi: 10.11003/jpnt.2015.4.2.057.

[5] J. Bhatti and T. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[6] C. Yang, H. Zhang, and S. Han, "Detection of spoofing signals based on RAIM and INS integration," in *Proc. IEEE International Conf. on Information and Automation (ICIA)*, Yinchuan, China, Aug. 2019, pp. 1118–1123.

[7] T. E. Humphreys, "Detection strategy for cryptographic GNSS antispoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[8] X. Zhang, F. Dovis, and C. Gioia, "GNSS spoofing detection using DNN under low and high C/N0 conditions," in *Proc. European Navigation Conference (ENC)*, Warsaw, Poland, Apr. 2020, pp. 1–10.

[9] J. Gross, S. Rathinam, and M. T. Wolf, "GNSS spoofing detection using 3D signal propagation modeling," *Sensors*, vol. 19, no. 20, pp. 1–19, 2019.

[10] A. Broumandan, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver autonomous integrity monitoring (RAIM)," *Navigation*, vol. 60, no. 4, pp. 267–277, 2013.

[11] D. Psiaki and T. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[12] D. Shepard, J. Bhatti, T. Humphreys, and A. Fansler, “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks,” Int. J. of Critical Infrastructure Protection, vol. 5, no. 3–4, pp. 146–153, 2012.

[13] X. Zhang, F. Dovis, and C. Gioia, “Low-cost and low-complexity GNSS spoofing detection based on a rule-based model,” in Proc. European Navigation Conf. (ENC), 2020, pp. 1–6.