BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

1.1.1 Latar Belakang Masalah

Pemanfaatan Sistem Navigasi Satelit Global (GNSS), khususnya *Global Positioning System* (GPS), telah menjadi pilar utama yang menyokong operasional berbagai sektor vital [1]. Namun, seiring meluasnya adopsi teknologi ini, muncul pula kerentanan terhadap ancaman siber yang signifikan, yaitu *GPS spoofing* [2]. Serangan ini merupakan suatu bentuk manipulasi di mana pihak tidak bertanggung jawab memancarkan sinyal GPS palsu untuk mengelabui perangkat penerima, sehingga menghasilkan informasi lokasi dan waktu yang tidak akurat [2].

Ancaman ini telah menjadi masalah faktual yang dampaknya semakin terasa, dengan meningkatnya insiden yang menargetkan penerbangan dan pelayaran sipil [2], [3]. Hal inilah yang mendorong penelitian ini, yaitu adanya kebutuhan mendesak untuk merancang sebuah sistem pendeteksian dan pemantauan serangan *spoofing* GPS yang tidak hanya efektif tetapi juga memiliki biaya implementasi yang rendah [4], [5]. Akar permasalahan ini terletak pada tantangan teknis untuk mengidentifikasi sinyal *spoofing* yang dirancang sangat identik dengan sinyal GPS otentik, di mana banyak solusi yang ada masih mengandalkan perangkat keras khusus yang mahal, seperti perangkat berbasis radio terdefinisi perangkat lunak atau Software Defined Radio [4], [6], [7].

Sebagai jawaban atas tantangan tersebut, penelitian ini mengajukan sebuah arsitektur sistem yang mengintegrasikan perangkat *Internet of Things* (IoT) berbiaya rendah dengan sistem pemrosesan di *backend* yang berbasis aturan (*rule-based*) [8]. Sistem ini dirancang untuk melakukan akuisisi data koordinat GPS secara *real-time* dan menganalisisnya. Deteksi anomali didasarkan pada perbandingan data *Latitude* dan *Longitude* yang masuk terhadap ambang batas (*threshold*) yang telah dihitung secara statik dari koordinat referensi yang valid [8]. Luaran dari sistem ini adalah klasifikasi sinyal ke dalam dua kategori: Sinyal Normal atau Terindikasi *Spoofing*, yang hasilnya dapat dipantau secara langsung melalui sebuah *website monitoring* [8].

1.2 Analisa Masalah

Untuk memahami urgensi dan dampak dari pengembangan sistem deteksi *spoofing* GPS yang terjangkau, diperlukan analisis dari berbagai sudut pandang.

1.2.1 Aspek Teknis

Dari sisi teknis, tantangan terbesar terletak pada kemampuan sinyal *spoofing* untuk meniru karakteristik sinyal GPS asli dengan fidelitas tinggi, sehingga sulit dibedakan oleh penerima konvensional dan berpotensi menyebabkan kegagalan navigasi fatal [9], [16]. Banyak teknologi deteksi yang ada hanya mampu mengenali anomali sederhana, sementara serangan modern yang lebih canggih memerlukan metode analisis yang jauh lebih mendalam [10], [12]. Solusi berbasis aturan (*rule-based*) yang diimplementasikan pada *backend* dalam riset ini menawarkan pendekatan yang efisien dan efektif. Metode ini bekerja dengan menganalisis deviasi data koordinat (*Latitude* dan *Longitude*) secara *real-time* terhadap titik referensi yang telah dikonfigurasi, sehingga mampu mengidentifikasi anomali posisi secara akurat tanpa memerlukan komputasi yang kompleks [13].

1.2.2 Aspek Ekonomi

Faktor ekonomi, khususnya biaya implementasi, menjadi kendala utama yang menghambat adopsi luas teknologi anti-*spoofing* [10], [14]. Solusi yang tersedia di pasaran saat ini, seperti yang berbasis radar atau *Inertial Navigation Systems* (INS), cenderung melibatkan investasi perangkat keras yang signifikan, sehingga berada di luar jangkauan banyak organisasi [11], [15]. Lebih jauh lagi, ketergantungan infrastruktur kritis seperti jaringan listrik (sinkronisasi waktu), telekomunikasi, dan jaringan keuangan pada sinyal GPS membuat serangan *spoofing* berpotensi menyebabkan gangguan layanan yang berdampak pada kerugian ekonomi berskala luas. Dengan demikian, sebuah pendekatan yang memanfaatkan komponen IoT berbiaya rendah dapat mendemokratisasi akses terhadap teknologi keamanan ini, memungkinkan penerapannya di lebih banyak sektor vital.

1.2.3 Aspek Keamanan

Pada intinya, isu ini adalah masalah keamanan. GPS *spoofing* membuka celah bagi berbagai skenario serangan dengan potensi dampak yang merusak. Secara spesifik, ancaman ini mencakup manipulasi navigasi militer yang dapat membahayakan aset strategis negara, hingga menyesatkan sistem navigasi pesawat yang berisiko menyebabkan kecelakaan fatal. Dampak lainnya adalah pembajakan kendaraan otonom, disrupsi jaringan listrik pintar (*smart grid*), pengalihan *drone* untuk tujuan jahat, hingga manipulasi aset militer [16], [17]. Dari sisi penegakan hukum, spoofing juga dapat dimanfaatkan untuk memfasilitasi kegiatan kriminal dan terorisme, seperti penyelundupan, perdagangan manusia, atau melumpuhkan sistem pelacakan dengan memanipulasi data lokasi. Seiring dengan semakin dalamnya integrasi

teknologi GPS dalam kehidupan sehari-hari, pengembangan sistem deteksi yang andal menjadi sebuah keharusan untuk melindungi infrastruktur dan menjamin keselamatan publik [9], [17].

1.2.4 Aspek Lingkungan

Meskipun tidak secara langsung, dampak serangan *spoofing* terhadap lingkungan dapat bersifat katastropik. Sebagai contoh, sebuah kapal tanker pengangkut minyak mentah atau bahan kimia berbahaya yang sistem navigasinya dimanipulasi dapat menyebabkan kecelakaan fatal. Kecelakaan ini dapat berupa kandasnya kapal atau masuknya kapal ke area perairan terlarang, yang berujung pada tumpahan minyak di perairan lepas dan memicu bencana ekologis [9], [16]. Oleh karena itu, sistem deteksi *spoofing* yang efektif juga berperan sebagai garda pertahanan untuk mencegah potensi kerusakan lingkungan akibat kegagalan navigasi [9].

1.3 Analisa Solusi yang Ada

Sejumlah pendekatan telah dieksplorasi untuk menanggulangi serangan *GPS spoofing*. Namun, setelah dianalisis, banyak dari solusi tersebut yang masih memiliki keterbatasan, terutama dalam hal biaya dan kerumitan teknis. Beberapa penelitian telah mengkaji berbagai metode, mulai dari penggunaan perangkat keras tambahan hingga implementasi algoritma yang kompleks. Berikut adalah rangkuman dari beberapa solusi yang telah ada:

Tabel 1. 1 Analisa solusi yang sudah ada

Solusi	Hasil	Keterbatasan
Sistem deteksi menggunakan radar dan GNSS [11], [14].	Mampu mendeteksi *spoofing* dengan menggabungkan sinyal dari kedua sumber.	Memerlukan perangkat keras radar yang sangat mahal, sehingga tidak cocok untuk aplikasi berbiaya rendah.
Sistem deteksi berbasis peta radio 3D [14].	Efektif untuk mendeteksi *spoofing* pada *Unmanned Aerial Vehicle* (UAV).	Membutuhkan proses pemetaan radio yang kompleks dan mahal untuk menghasilkan peta yang akurat.
Sistem deteksi RAIM dengan integrasi INS [11], [15].	Menggabungkan *Receiver Autonomous Integrity*	Memerlukan perangkat *Inertial Navigation* yang

	Monitoring (RAIM) dengan data navigasi inersia untuk deteksi.	mahal, sehingga tidak ideal untuk solusi berbiaya rendah.
Sistem deteksi berbasis *Deep Neural Network* (DNN) [13].	Memberikan akurasi klasifikasi yang tinggi, terutama pada *Signal-to-Noise Ratio* (SNR) sedang hingga tinggi.	Kinerja dapat menurun pada C/N0 yang rendah dan sering kali membutuhkan daya komputasi yang signifikan.
Rule-Based Threshold pada Koordinat [13].	Efisien secara komputasi dan mudah diimplementasikan di *backend*. Mampu mendeteksi anomali posisi dengan membandingkan data *real-time* terhadap titik referensi yang valid.	Keakuratannya sangat bergantung pada kualitas dan stabilitas titik referensi yang dikonfigurasi. Mungkin kurang efektif melawan serangan *spoofing* yang sangat lambat dan bertahap (*slow-drift attacks*).

Berdasarkan Tabel 1.1, terlihat bahwa analisis terhadap berbagai solusi tersebut menggarisbawahi adanya kesenjangan yang signifikan, seperti belum ada sistem deteksi *spoofing* yang secara simultan memenuhi kriteria akurat, terjangkau, dan mudah diimplementasikan. Ketergantungan pada perangkat keras mahal serta kebutuhan daya komputasi tinggi menjadi hambatan utama adopsi. Oleh karena itu, penelitian ini bertujuan mengisi kesenjangan tersebut dengan mengusulkan sebuah sistem yang menyinergikan efisiensi analisis data berbasis aturan (*rule-based*) dengan efektivitas biaya dari perangkat IoT, guna menghasilkan solusi yang dapat diakses secara lebih luas.