ABSTRAK

Perkembangan teknologi *Global Navigation Satellite System* (GNSS) telah membawa dampak besar dalam berbagai sektor, seperti transportasi, telekomunikasi, dan geolokasi. Meskipun demikian, sistem GNSS menghadapi tantangan besar berupa potensi serangan *GPS spoofing*, yang dapat merusak integritas data navigasi dengan memanipulasi sinyal GPS yang diterima. Ancaman ini bisa berisiko tinggi bagi aplikasi yang sangat bergantung pada akurasi data lokasi, seperti sistem navigasi otomatis dan aplikasi krusial lainnya. Masalah utama yang dibahas dalam penelitian ini adalah bagaimana cara mendeteksi serangan *GPS spoofing* secara efektif dengan biaya yang terjangkau untuk implementasi pada perangkat berbasis *Internet of Things* (IoT).

Penelitian ini mengusulkan solusi berupa sistem deteksi sinyal *spoofing* GPS berbasis IoT berbiaya rendah yang mengintegrasikan modul GPS u-blox NEO-6M V2 dengan mikrokontroler ESP32. Sistem ini mengakuisisi berbagai parameter sinyal GPS, namun metode deteksi yang digunakan berfokus pada analisis koordinat (*Latitude* dan *Longitude*). Deteksi dilakukan di sisi *backend* dengan pendekatan berbasis aturan (*rule-based*). Sistem menganalisis data koordinat yang masuk secara *real-time* dan membandingkannya dengan titik referensi yang valid. Jika deviasi dari koordinat yang diterima melebihi ambang batas (*threshold*) yang telah ditentukan, sistem akan mengklasifikasikannya sebagai sinyal *spoofing*. Hasil klasifikasi kemudian ditampilkan melalui *website monitoring* yang dibangun dengan Vercel.

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