ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Diseño de un candado Iot de seguridad logística con machine learning y geolocalizacion anti-spoofing

PROYECTO INTEGRADOR

Previo la obtención del Título de:

Ingeniero en Telemática

Presentado por:

Richard Dalton Núñez Torres

Arturo Daniel Parra Valencia

GUAYAQUIL - ECUADOR

Año: 2025

DEDICATORIA

Richard Dalton Núñez Torres

El presente proyecto lo dedico a mis padres, con profundo amor y gratitud, por su apoyo y por inspirarme a alcanzar mis metas con esfuerzo y dedicación.

Arturo Daniel Parra Valencia

A mis padres, por su amor y apoyo incondicional.

AGRADECIMIENTOS

Richard Dalton Núñez Torres

Agradezco al Magíster Néstor Arreaga, mi tutor, por su guía, a mi familia y amigos por su apoyo inquebrantable, y a mis profesores por su constante orientación.

Arturo Daniel Parra Valencia

Mi más sincero agradecimiento a mi familia por su constante apoyo. A mis profesores, por brindarme el conocimiento necesario para culminar este proyecto. Al ingeniero Cabrera, por su asesoría con el diseño mecánico del proyecto.

Declaración Expresa

Nosotros Richard Dalton Nuñez Torres, Arturo Daniel Parra Valencia acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al/los autor/es que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 30 de mayo del 2025.

Firmado electrónicamente por:
RICHARD DALTON NUÑEZ TORRES
Validar únicamente con FirmaEC

Richard Nuñez

Firmado electrónicamente por:
ARTURO DANIEL PARRA VALENCIA
Validar únicamente con FirmaEC

Arturo Parra

EVALUADORES

Maria Isabel Mera Collantes
Time Stamping Security Data

PhD María Isabel Mera

PROFESOR DE LA MATERIA

Firmado electrónicamente por:
NESTOR XAVIER ARREAGA ALVARADO
Validar únicamente con FirmaEC

Mgtr Néstor Arreaga

PROFESOR TUTOR

RESUMEN

La seguridad en la cadena de suministro ecuatoriana se ve comprometida por ataques que vulneran la integridad de la carga y la fiabilidad de los sistemas de rastreo. Este proyecto presenta el diseño de un candado inteligente IoT cuyo objetivo es garantizar la integridad y trazabilidad logística mediante la detección de anomalías físicas y la suplantación de señal GPS (spoofing). Para ello, se desarrolló un prototipo funcional que integró un microcontrolador ESP32, un sensor inercial MPU6050 y un módulo GPS. La detección de anomalías físicas se implementó a través de un modelo de Machine Learning tipo Random Forest, entrenado con datos empíricos de rutas reales y ataques simulados. Adicionalmente, se desarrolló un algoritmo anti-spoofing basado en la fusión de datos inerciales y la navegación por estima. Los resultados de la validación experimental demostraron una alta efectividad del sistema: el clasificador de anomalías alcanzó una precisión general del 99%, sin generar falsas alarmas, mientras que el mecanismo anti-spoofing logró identificar con éxito las señales de GPS fraudulentas. Se concluye que la fusión de sensores mediante un modelo de inteligencia artificial es una estrategia robusta y viable que ofrece una doble capa de protección contra las amenazas físicas y digitales en el transporte de mercancías.

Palabras Clave: Seguridad Logística, Internet de las Cosas, Machine Learning, GPS Spoofing.

ABSTRACT

Security in the Ecuadorian supply chain is compromised by attacks that threaten both cargo integrity and the reliability of tracking systems. This project presents the design of an intelligent IoT lock aimed at ensuring logistics integrity and traceability by detecting physical anomalies and GPS spoofing. To achieve this, a functional prototype was developed integrating an ESP32 microcontroller, an MPU6050 inertial sensor, and a GPS module. Physical anomaly detection was implemented using a Random Forest Machine Learning model, trained with empirical data from real routes and simulated attacks. Additionally, an anti-spoofing algorithm based on inertial data fusion and dead reckoning was developed. The results from the experimental validation showed the system's high effectiveness: the anomaly classifier achieved an overall accuracy of 99% without generating false alarms, while the anti-spoofing mechanism successfully identified fraudulent GPS signals. It is concluded that sensor fusion through an artificial intelligence model is a robust and viable strategy that offers a dual layer of protection against physical and digital threats in freight transport.

Keywords: Logistics Security, Internet of Things, Machine Learning, GPS Spoofing.

ÍNDICE GENERAL

ABREVIATURAS

API	Interfaz de Programación de Aplicaciones
ESPOL	Escuela Superior Politécnica del Litoral
GNSS	Sistema Global de Navegación por Satélite
GPS	Sistema de Posicionamiento Global
HTTPS	Protocolo de Transferencia de Hipertexto seguro
IMU	Unidad de Medición Inercial
IoT	Internet de las Cosas
JSON	Notación de Objetos de JavaScript
MCU	Unidad Microcontroladora
ML	Aprendizaje Automático
PCB	Placa de Circuito Impreso
REST	Transferencia de Estado Representacional
RMS	Valor Cuadrático Medio

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

El transporte de mercancías constituye un pilar esencial de la economía ecuatoriana. Sin embargo, enfrenta crecientes amenazas: entre enero de 2023 y mayo de 2024, se reportaron 240 casos de asaltos, secuestros y homicidios contra transportistas, con un aumento del 105% en robos en carretera entre 2023 y 2024 (Alai Secure, 2025). En particular, los delincuentes han perfeccionado sus métodos para vulnerar la seguridad física de los contenedores y, en algunos casos, incluso manipular digitalmente los sistemas de rastreo, logrando desviar camiones o abrir cargas sin ser detectados por los sistemas tradicionales de monitoreo (Cedillo-Campos et al., 2024).

Aunque el uso de GPS ha sido una solución ampliamente adoptada para rastrear vehículos y mercancías, no está exento de vulnerabilidades (Cedillo-Campos et al., 2024). Uno de los ataques más comunes en la actualidad es el llamado spoofing de GPS, que consiste en enviar señales falsas para engañar al receptor, haciéndole creer que se encuentra en una ubicación distinta a la real (Meng et al., 2022). Este tipo de ataque puede ser aprovechado para desviar una unidad de transporte sin que el sistema emita ninguna alerta, lo que pone en evidencia la necesidad de contar con mecanismos adicionales de protección y monitoreo (Khan et al., 2021).

En este contexto, el presente proyecto propone el diseño e implementación de un candado inteligente IoT con capacidad de detección de anomalías físicas en tiempo real, capaz de identificar intentos de manipulación, vibraciones sospechosas, impactos o torsiones que podrían indicar un intento de apertura no autorizada. Este candado integra un sensor inercial (MPU6050), que mide aceleraciones y giros en los tres ejes, y un microcontrolador ESP32, encargado de recolectar los datos y transmitirlos a una plataforma de análisis. Se realizarán pruebas en entornos controlados para validar la efectividad del sistema en la detección de manipulaciones y ataques de suplantación de

señal GPS.

Este trabajo busca contribuir al fortalecimiento de la seguridad en la logística de transporte, combinando tecnologías de hardware, inteligencia artificial y comunicaciones IoT. A través de la detección temprana de manipulaciones físicas, se pretende ofrecer una capa adicional de protección que complemente a los sistemas GPS existentes, haciendo frente a los desafíos actuales en la protección de activos durante su traslado.

1.1 Planteamiento del Problema

La seguridad en la cadena de suministro es un factor crítico para sectores productivos del Ecuador,como el bananero y camaronero, que representan pilares fundamentales de la economía nacional (Fares, 2024). El transporte terrestre de mercancías es uno de los eslabones más vulnerables de esta cadena. Según informes de gremios de transporte y de la Policía Nacional, las carreteras del país registran una alta incidencia de asaltos, especialmente en las rutas de la zona costera (Hora, 2025). La delincuencia organizada no solo utiliza métodos tradicionales, sino que también emplea tecnología avanzada, como inhibidores de comunicaciones celulares (jammers) y técnicas de manipulación de sistemas de geolocalización, para perpetrar sus actividades ilícitas (Ghanbarzade and Soleimani, 2025).

El problema central que este proyecto aborda es la insuficiencia de los sistemas de seguridad convencionales para detectar y responder a ataques de manipulación tecnológica avanzada, en particular el *GPS spoofing* y las manipulaciones físicas sutiles de los contenedores (Ghanbarzade and Soleimani, 2025). Actualmente, las empresas de logística invierten en plataformas de rastreo que dependen en gran medida de la veracidad de la señal GPS (“Global GPS Market and Its Applications”, 2025). Sin embargo, las señales GPS son susceptibles a ataques de spoofing, lo que permite a los delincuentes desviar vehículos o contenedores sin que los sistemas de monitoreo detecten anomalías (Dasgupta, Ahmed, et al., 2024).

Diversos estudios advierten que el *GPS spoofing* representa una amenaza creciente para el transporte y la logística, al permitir la alteración maliciosa de la ubicación reportada por los sistemas de rastreo (Clements et al., 2022). A esta vulnerabilidad tecnológica se suma la falta de mecanismos efectivos para detectar manipulaciones físicas sutiles en

los contenedores, como aperturas no autorizadas o vibraciones anómalas, que muchas veces pasan desapercibidas por los sistemas actuales (Renault et al., 2025).

Esta situación evidencia la necesidad de un sistema de seguridad inteligente que integre sensores inerciales, técnicas de machine learning y geolocalización resistente a interferencias (Dasgupta, Shakib, and Rahman, 2024). El desarrollo de este tipo de solución permitiría detectar tanto eventos físicos sospechosos como intentos de suplantación de ubicación, fortaleciendo la seguridad logística en Ecuador, reduciendo pérdidas económicas y mejorando la confiabilidad del sistema de transporte nacional.

1.2 Justificación

La necesidad de una solución robusta e inteligente para la seguridad logística en Ecuador es innegable, especialmente considerando los desafíos actuales en la cadena de suministro. Este proyecto se justifica por su impacto transformador en tres dimensiones clave: tecnológica, económica-social y académica.

- **Impacto Tecnológico:** El proyecto propone una solución innovadora al integrar *Machine Learning* directamente en un dispositivo IoT de bajo costo (un microcontrolador ESP32). A diferencia de las soluciones que dependen exclusivamente del procesamiento en la nube, este enfoque de computación en el borde (*edge computing*) permite la detección de anomalías en tiempo real y de forma autónoma, incluso si la conexión a internet es interrumpida. El desarrollo de un algoritmo anti-spoofing basado en la correlación de múltiples sensores (GPS y acelerómetro) representa un avance significativo sobre los sistemas de rastreo pasivos.

- **Impacto Económico y Social:** Al mejorar la seguridad y la trazabilidad de las cargas, se busca reducir directamente las pérdidas por robos y manipulaciones, que representan un costo significativo para la economía nacional (Alai Secure, 2025). Esto no solo beneficia a las empresas de transporte, sino que fortalece a sectores productivos enteros, alineándose con el **Objetivo de Desarrollo Sostenible (ODS) 12: Producción y consumo responsables**. Asimismo, al crear una infraestructura logística más segura y confiable, se fomenta la innovación y se robustece la industria, contribuyendo al **ODS 9: Industria, innovación e infraestructura**.

- **Impacto Académico:** El proyecto constituye una aplicación práctica y tangible de conocimientos avanzados en áreas como sistemas embebidos, Internet de las Cosas, inteligencia artificial y ciberseguridad. La validación del prototipo generará conocimiento empírico sobre la viabilidad y efectividad de ejecutar modelos de inferencia en microcontroladores con recursos limitados, sirviendo como base para futuras investigaciones y desarrollos en el campo de la logística inteligente.

1.3 Objetivos

Para abordar la problemática descrita y validar la hipótesis, se han definido los siguientes objetivos.

Objetivo General

Desarrollar un candado inteligente IoT que integre detección de anomalías de movimiento y geolocalización anti-spoofing utilizando técnicas de Machine Learning, con el fin de garantizar la integridad y trazabilidad de la cadena de suministro

Objetivos Específicos

1. Diseñar la arquitectura hardware-software del sistema, integrando un microcontrolador ESP32, un módulo GPS y un acelerómetro MPU6050.

2. Implementar un algoritmo de anti-spoofing para la señal GPS, basado en el análisis de consistencia temporal y espacial de los datos recibidos.

3. Entrenar un modelo de Machine Learning para la detección de anomalías con datos de rutas legítimas y simulaciones de ataques.

4. Desarrollar una interfaz web para la visualización en tiempo real de la ubicación del candado, así como los eventos de anomalía y manipulación detectados .

1.4 Alcance

El desarrollo del presente proyecto considera la implementación de un candado inteligente orientado a reforzar la seguridad logística en el transporte terrestre de mercancías. El dispositivo estará dirigido principalmente a empresas de transporte, operadores logísticos y exportadores que requieren monitoreo físico y geoespacial de su carga en tiempo real. Para ello, el candado debe ser capaz de registrar eventos anómalos asociados a intentos de manipulación, impactos o movimientos no autorizados durante el trayecto.

El sistema estará conformado por un microcontrolador de bajo consumo, un sensor de movimiento y un módulo GPS, los cuales permitirán capturar información crítica del entorno físico y de ubicación del candado. Esta información será procesada localmente para identificar patrones inusuales y generar alertas, las cuales serán transmitidas a un servidor central mediante conexión Wi-Fi. De este modo, se garantizará una respuesta oportuna ante situaciones de riesgo, sin depender completamente de una conexión permanente a internet móvil.

Además, el diseño del candado considerará portabilidad, autonomía energética y facilidad de integración con los procesos logísticos existentes, de manera que pueda adaptarse a diversos entornos operativos y niveles de infraestructura tecnológica. Este enfoque permitirá que el sistema pueda ser utilizado en contextos urbanos, manteniendo su funcionalidad y efectividad bajo condiciones reales de operación.

1.5 Limitaciones del Proyecto

El desarrollo del presente proyecto contempla la implementación de un prototipo funcional de un candado inteligente IoT para la seguridad logística. Sin embargo, es necesario reconocer ciertas limitaciones técnicas y operativas inherentes a su diseño y entorno de aplicación. Una de las principales limitantes radica en la relación del sistema con respecto a la calidad de la señal GPS, la cual puede verse afectada negativamente en entornos urbanos densamente construidos, espacios interiores o condiciones atmosféricas adversas. Además, la presencia de interferencias deliberadas o accidentales (como jammers) puede degradar o anular la recepción satelital, comprometiendo la precisión de la geolocalización.

Asimismo, el prototipo ha sido diseñado con un enfoque en eficiencia energética y autonomía operativa, optimizando su funcionamiento para consumir la menor cantidad posible de energía en contextos donde el acceso a fuentes de alimentación constante es limitado. Debido a ello, se prescinde de la conexión directa a redes móviles (como 3G, 4G o LTE), ya que estos módulos presentan un consumo energético significativamente más alto en comparación con tecnologías de bajo consumo como Wi-Fi o LoRa. Esta decisión limita la capacidad de transmisión de datos en movimiento y obliga a operar el dispositivo en zonas con conectividad Wi-Fi estable o mediante sincronización periódica.

Finalmente, es importante señalar que la validación del prototipo se realizó bajo una metodología mixta. Si bien los datos de ”comportamiento normal” se capturaron en rutas reales para asegurar que el modelo aprenda de condiciones operativas auténticas (tal como se indica en los objetivos), las pruebas de ”comportamiento anómalo” (impactos, vibraciones forzadas, etc.) y la validación final del sistema se ejecutaron en entornos controlados. Esta decisión garantiza la seguridad, la repetibilidad de los experimentos y permite un análisis preciso de la respuesta del dispositivo frente a ataques simulados específicos.

1.6 Estado del Arte

La creciente complejidad y globalización de las cadenas de suministro han incrementado su exposición a una variedad de riesgos, que van desde interrupciones operativas hasta actos delictivos deliberados. En este contexto, la revisión de la literatura se centra en cuatro áreas fundamentales: las vulnerabilidades inherentes a los sistemas de navegación por satélite, las estrategias de defensa contra ataques tecnológicos, la aplicación de sensores inerciales para la detección de anomalías físicas, y las arquitecturas de referencia para sistemas IoT en el ámbito de la seguridad.

1.6.1 Vulnerabilidades en la Cadena de Suministro y Sistemas de Navegación Global por Satélite (GNSS)

La dependencia de la logística moderna en el Sistema de Posicionamiento Global (GPS) y otros GNSS es casi absoluta. Sin embargo, la naturaleza de la señal GPS civil,

que es pública, no cifrada y de baja potencia, la convierte en un objetivo vulnerable a interferencias y manipulaciones. Entre las amenazas más significativas se encuentra el ataque de suplantación de identidad o *spoofing*, en el cual un adversario transmite señales de GPS falsificadas con el objetivo de engañar a un receptor, haciéndole calcular una posición o tiempo incorrectos (Morillo Barragán, 2013).

Históricamente, la ejecución de un ataque de spoofing requería un alto nivel de conocimiento técnico y equipos costosos, limitando la amenaza a actores estatales o grupos con recursos significativos. No obstante, el panorama ha cambiado drásticamente con la proliferación de radios definidas por software (SDR) de bajo costo y generadores de señales GPS de código abierto. Hoy en día, es posible construir un dispositivo de spoofing portátil y efectivo con una inversión inferior a 300 USD. Esta ”democratización” de la tecnología de ataque representa una transformación fundamental del modelo de amenaza. El spoofing ha dejado de ser una vulnerabilidad teórica para convertirse en una herramienta práctica y accesible para organizaciones criminales, que pueden utilizarla para secuestrar cargamentos, desviar rutas y eludir los sistemas de monitoreo tradicionales, impactando directamente a sectores económicos vitales como los descritos en el Capítulo 1 (Ordenes Espíndola, 2012).

1.6.2 Estrategias para la Detección de Ataques de Suplantación de GPS (Spoofing)

Frente a la creciente amenaza del *spoofing*, la comunidad científica ha desarrollado diversas contramedidas. Las técnicas iniciales se basaban en el análisis de las características de la señal de radiofrecuencia (RF), como la potencia de la señal, el ángulo de llegada o la consistencia de los datos de múltiples satélites. Si bien son útiles contra ataques simplistas, estas técnicas pueden ser eludidas por atacantes más sofisticados que logran sincronizar y replicar las características de las señales auténticas (Warner and Johnston, n.d.).

Una estrategia considerablemente más robusta y que constituye la base de este proyecto es la fusión de sensores, específicamente la integración de datos de una Unidad de Medición Inercial (IMU) con los datos del receptor GPS. La IMU, que típicamente combina un acelerómetro y un giroscopio, proporciona mediciones de movimiento

(aceleración lineal y velocidad angular) de forma autónoma y contenida, sin depender de señales externas. Por lo tanto, no es susceptible a los mismos ataques de RF que afectan al GPS. El principio fundamental de esta defensa radica en la detección de una *inviabilidad física*. Un atacante puede generar una trayectoria GPS falsa que parezca suave y plausible; sin embargo, es prácticamente imposible que prediga y reproduzca de forma remota y en tiempo real las microvibraciones, las irregularidades del camino y las sutiles correcciones de la dinámica del vehículo que la IMU es capaz de medir con alta fidelidad(Jafarnia-Jahromi et al., 2012).

Un ataque de *spoofing* exitoso crea una disonancia en el sistema: el GPS reporta una trayectoria coherente pero falsa, mientras que la IMU reporta la ”firma” inercial del movimiento físico real. La discrepancia entre la aceleración derivada de las lecturas consecutivas del GPS y la aceleración medida directamente por la IMU se convierte en un indicador de una perturbación no esperada. El algoritmo de detección, por lo tanto, se encarga de cuantificar esta disonancia para generar una alerta fiable.

1.6.3 Detección de Anomalías Físicas mediante Sensores Inerciales y Machine Learning

Además de la suplantación de GPS, la seguridad de la carga se ve amenazada por manipulaciones físicas directas, como intentos de forzar cerraduras, impactos o aperturas no autorizadas. Los sensores inerciales, como el MPU6050, son herramientas excepcionalmente adecuadas para detectar este tipo de eventos. La literatura en campos como el Reconocimiento de Actividades Humanas (HAR) y la monitorización de maquinaria demuestra ampliamente la eficacia de las IMU para clasificar patrones de movimiento (Salas et al., 2023).

La metodología estándar, adoptada en este proyecto, consiste en un proceso de varias etapas. Primero, los datos brutos de la serie temporal de los seis ejes del sensor (tres de aceleración, tres de giroscopio) se segmentan en ventanas de tiempo fijas. Dentro de cada ventana, se realiza un proceso de ingeniería de características (*feature engineering*), donde se calculan diversos descriptores estadísticos como la media, la desviación estándar, el valor eficaz (RMS), la asimetría (skewness) y la curtosis. Este proceso transforma la serie temporal en un vector de características de dimensión fija que

resume la dinámica del movimiento en ese intervalo. Finalmente, este vector se utiliza como entrada para un modelo de aprendizaje automático (Machine Learning) entrenado para clasificar la actividad.

Diversos estudios han demostrado que los modelos de conjunto, y en particular el algoritmo *Random Forest*, ofrecen un rendimiento superior para este tipo de tareas de clasificación de series temporales (Parmar et al., 2019). Su robustez frente a características irrelevantes, su alta precisión y su relativa simplicidad de implementación lo convierten en una opción idónea. Un aspecto clave del diseño de este proyecto es la dualidad del vector de características inerciales. El mismo conjunto de 42 características extraídas de los datos del MPU6050 sirve a dos propósitos de seguridad distintos. Por un lado, permite la detección de anomalías físicas al identificar patrones de movimiento (impactos, vibraciones anómalas, torsiones) que se desvían de la ”huella” estadística del tránsito normal. Por otro lado, proporciona la base para el mecanismo anti-spoofing al permitir una comparación con los datos de movimiento derivados del GPS. Esta eficiencia en el diseño, donde un único flujo de datos de un sensor alimenta múltiples funciones de seguridad, es una de las fortalezas de la arquitectura propuesta.

1.6.4 Arquitecturas de Referencia en Sistemas IoT para Seguridad Logística

La arquitectura del sistema propuesto se alinea con los patrones de diseño establecidos en la literatura para sistemas de monitoreo basados en IoT. La estructura canónica de dichos sistemas consta de tres capas principales: una capa de percepción, compuesta por nodos sensores (en este caso, el candado inteligente con ESP32 y MPU6050) que adquieren datos del entorno físico; (2) una capa de red, que utiliza tecnologías de comunicación (como Wi-Fi) para transmitir los datos a un servidor central; y una capa de aplicación, donde los datos son almacenados, procesados, analizados (mediante algoritmos de Machine Learning) y presentados al usuario a través de una interfaz. Esta arquitectura modular y distribuida valida la decisión de delegar el procesamiento computacionalmente intensivo al backend, permitiendo que el dispositivo IoT se mantenga como un componente de bajo costo y bajo consumo energético, enfocado en la adquisición y transmisión de datos.

1.7 Marco Teórico

Seguridad en la cadena de logística

La cadena de suministro representa un sistema complejo de actividades interrelacionadas que van desde la producción hasta la distribución de bienes. En este contexto, la seguridad logística se vuelve un aspecto esencial, especialmente en sectores como el agrícola, pesquero y de exportación, donde los incidentes relacionados con robos, sabotajes y manipulación de la carga pueden generar pérdidas significativas (Liu et al., 2021). En América Latina, el robo de mercancías durante el transporte terrestre es un problema creciente, y Ecuador no es la excepción. Informes recientes indican que las rutas logísticas ecuatorianas, particularmente aquellas que conectan puertos con zonas industriales, presentan una alta incidencia de asaltos y manipulación de sistemas GPS mediante tecnologías como jammers y spoofing (BSI and TAPA EMEA, 2023).

Internet de las Cosas (IoT) en la Logística

El Internet de las Cosas (IoT) ha transformado las operaciones logísticas al permitir la interconexión de dispositivos que recopilan, transmiten y analizan datos en tiempo real. Esta tecnología permite no solo monitorear la ubicación de un contenedor, sino también variables como temperatura, vibración o apertura no autorizada (Lu et al., 2022). La integración de sensores inerciales, GPS y plataformas de análisis en la nube ha facilitado la visibilidad de extremo a extremo de las cadenas de suministro (Lu et al., 2022).

Spoofing de señal GPS y vulnerabilidades tecnológicas

El spoofing de señal GPS es una técnica mediante la cual un atacante emite señales falsas para engañar a un receptor GPS, haciéndole creer que se encuentra en una ubicación diferente. Esta técnica ha sido utilizada para desviar vehículos o interrumpir operaciones logísticas, y constituye una amenaza creciente debido al bajo costo y fácil acceso a equipos capaces de realizar este tipo de ataque (Bhatti and Humphreys, 2017). La ausencia de mecanismos anti-spoofing en dispositivos de rastreo comunes agrava esta vulnerabilidad (Bhatti and Humphreys, 2017).

Navegación por estima (Dead reckoning)

La navegación por estima es un método utilizado para determinar la posición de un vehículo basándose en los vectores de desplazamiento obtenidos mediante sensores

de orientación y aceleración (Kao, 1991). Aunque su uso a largo plazo no es factible debido al arrastre de errores, tiene una precisión alta al determinar la trayectoría de un vehículo en intervalos cortos o medianos(Steinhoff and Schiele, 2010). Al no depender de elementos externos, es una buena alternativa para determinar posición en situaciones donde un GPS se encuentre inhabilitado.

Sensores inerciales y detección de anomalías

El uso de sensores inerciales como el MPU6050, que combina un acelerómetro y giroscopio de tres ejes, permite detectar patrones de movimiento anómalos como impactos, vibraciones o torsiones. Estos patrones pueden ser característicos de intentos de manipulación física del candado o contenedor (Zhang et al., 2021). La extracción de características estadísticas de las señales inerciales, media, desviación estándar, curtosis, asimetría, entre otras, es una técnica común en aplicaciones de clasificación y reconocimiento de patrones (Lu et al., 2022).

Machine Learning aplicado a la seguridad IoT

El aprendizaje automático (Machine Learning, ML) ha demostrado ser eficaz en tareas de clasificación de eventos anómalos, incluso en entornos con ruido o incertidumbre. Modelos como el Random Forest son especialmente útiles por su capacidad de manejar variables correlacionadas y ofrecer interpretabilidad del proceso de decisión (Breiman, 2001). En el contexto de dispositivos IoT con recursos limitados, se ha optado por implementar estos modelos en arquitecturas edge, donde el procesamiento se realiza directamente en el microcontrolador (ESP32), permitiendo respuestas autónomas incluso cuando no hay conectividad (Panchatcharam et al., 2022).

Sistemas embebidos y ciberseguridad

El diseño de sistemas embebidos para aplicaciones críticas, como la seguridad logística, requiere un enfoque integral que contemple no solo la funcionalidad del hardware, sino también la protección frente a ataques físicos y digitales (Lee and Chang, 2020). La implementación de mecanismos de autenticación, encriptación y monitoreo de eventos anómalos es indispensable para garantizar la integridad de la solución (Sicari et al., 2015).

CAPÍTULO 2

2. METODOLOGÍA

Esta sección describe el enfoque sistemático adoptado para el diseño, implementación y validación del sistema de candado inteligente. Se detalla la arquitectura general, la metodología específica de aprendizaje automático empleada para la detección de anomalías y el marco de pruebas para evaluar el rendimiento y la eficacia del prototipo.

2.1 Arquitectura del Sistema

En este proyecto, se ha diseñado una arquitectura completa que une el dispositivo físico con toda la infraestructura digital. El sistema funciona en dos grandes áreas: por un lado, el dispositivo IoT , que se encarga de sentir lo que ocurre a su alrededor y actuar físicamente; y por otro, el back-end en la nube, que funciona como el cerebro digital, procesando, guardando y analizando toda la información de manera inteligente.

2.1.1 Hardware

El corazón del proyecto es un candado inteligente cuyo diseño electrónico se centra en tres pilares: sentir, pensar y comunicar. Como se puede ver en la Figura 2.1, varios componentes clave trabajan en conjunto. El cerebro del dispositivo es un microcontrolador ESP32, elegido por ser una pieza potente y versátil que ya incluye conexión Wi-Fi, lo que facilita enormemente la comunicación. Su capacidad de procesamiento es fundamental para leer los sensores, controlar el mecanismo de cierre y hablar constantemente con el servidor en la nube sin consumir demasiada energía.

Para detectar cualquier anomalía, el candado cuenta con un módulo de sensores muy completo. Incluye un sensor de movimiento MPU6050, que mide la aceleración y

la rotación para identificar patrones que puedan sugerir un golpe o una manipulación forzada. A su lado, un módulo GPS NEO-6M V2 se encarga de reportar la ubicación exacta del candado, una función vital para el seguimiento y la seguridad. Cuando el sistema decide sidebe abrirse o cerrarse, envía una señal a un servomotor de 5V. Este pequeño motor es el músculo del sistema, moviendo un pestillo para operar el mecanismo de bloqueo de forma segura y remota. Toda la comunicación con el exterior se realiza a través del módulo Wi-Fi del ESP32, que actúa como un puente para enviar datos de los sensores hacia la nube y recibir órdenes.

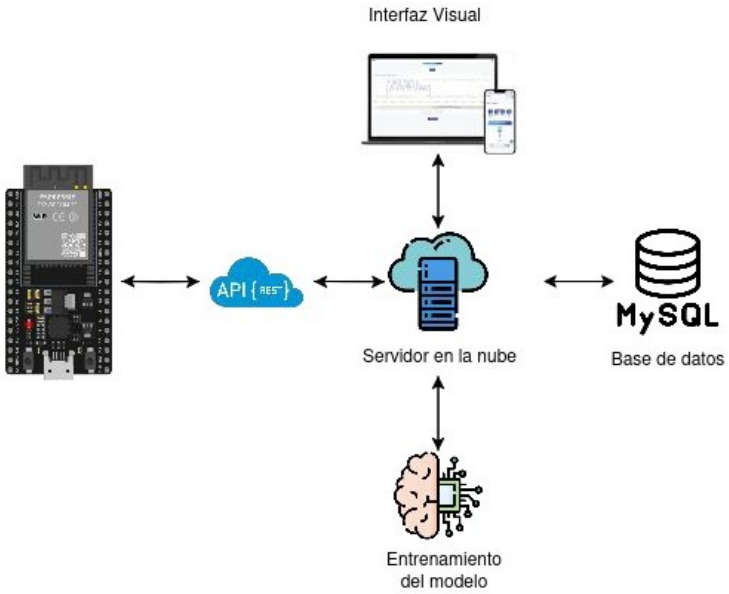

Figura 2.1: Diagrama de la arquitectura de hardware del candado inteligente.

2.1.2 Software

Toda la gestión del sistema reside en una sólida arquitectura de software en la nube, diseñada para recibir, procesar y analizar el flujo de datos que llega desde el candado. La Figura 2.2 muestra cómo interactúan los distintos componentes de este ecosistema digital. La comunicación entre el candado y el servidor se realiza a través de una API REST, un método estándar y flexible que permite un diálogo claro y eficiente. Este servidor, que es el núcleo de toda la operación, está desarrollado en Python con el framework FastAPI, una tecnología moderna y de alto rendimiento. Para mantener el código ordenado y fácil de mantener, se ha estructurado en módulos, separando la lógica de la API, los servicios de Machine Learning, los modelos de datos y la gestión de la base

de datos.

El servidor en la nube, que para nuestro caso se despliega con Uvicorn para asegurar su estabilidad, orquesta todas las tareas. Gestiona las peticiones que llegan desde el candado, se comunica con la base de datos para guardar y leer información, y utiliza el modelo de Machine Learning para realizar predicciones. Para el almacenamiento de datos a largo plazo, se utiliza una base de datos MySQL. En ella, una tabla llamada ”mpu data” guarda el historial completo de lecturas del sensor, mientras que otra tabla, ”officialtrainingdata”, almacena el conjunto de datos curado y etiquetado que sirve para entrenar al modelo de inteligencia artificial. Este modelo, un RandomForestClassifier guardado en un archivo, se carga en el servidor y está siempre listo para analizar nuevos datos y decidir si una actividad es normal o sospechosa. Finalmente, una interfaz visual, como una página web o una aplicación móvil, permite a los usuarios interactuar con el sistema para ver el estado del candado, su ubicación y recibir alertas.

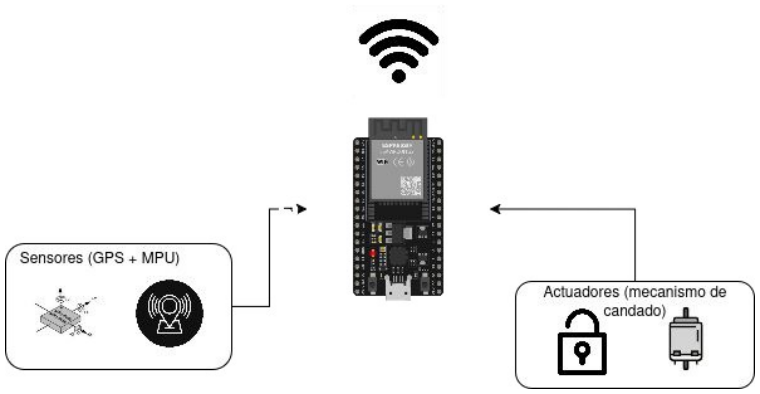

Figura 2.2: Diagrama de la arquitectura del software del candado inteligente.

2.2 Metodología de Machine Learning

El núcleo de la inteligencia del sistema reside en su capacidad para clasificar patrones de movimiento. A continuación, se detalla el pipeline de Machine Learning implementado.

2.2.1 Definición del Problema de Clasificación

El problema se formula como una tarea de clasificación binaria supervisada. El objetivo del modelo es, a partir de una ventana de datos de sensores, predecir una de dos posibles clases:

- **Clase 0 (Normal):** Representa el comportamiento esperado del candado durante un tránsito legítimo, incluyendo vibraciones normales del vehículo y movimientos menores.
- **Clase 1 (Anomalía):** Representa cualquier desviación significativa del comportamiento normal. Esto incluye eventos físicos como golpes, caídas, torsiones o vibraciones intensas que sugieran un intento de manipulación, así como la detección de una inconsistencia lógica con la señal GPS que indique un posible ataque de spoofing.

2.2.2 Construcción del Conjunto de Datos de Entrenamiento

La calidad y representatividad del conjunto de datos de entrenamiento son fundamentales para el éxito de cualquier modelo de Machine Learning. Para este proyecto, el conjunto de datos se construyó a través de un debido proceso de recolección de datos empíricos, utilizando el prototipo funcional del candado IoT. El proceso de recolección se dividió en dos categorías bien diferenciadas para generar un conjunto de datos etiquetado, indispensable para el entrenamiento supervisado:

1. **Captura de Comportamiento ”Normal”:** Se instaló el prototipo en un vehículo que realizó varios trayectos en distintas superficies. Esto permitió registrar una amplia gama de vibraciones, aceleraciones y patrones inerciales que corresponden a las condiciones de un transporte legítimo.
2. **Simulación de Eventos ”Anómalos”:** Para enseñar al modelo a reconocer amenazas, se ejecutaron y grabaron sistemáticamente una serie de eventos anómalos controlados. Estas simulaciones incluyeron:
    - Impactos secos y agudos con herramientas metálicas.
    - Vibraciones de alta frecuencia, simulando el uso de herramientas de corte.
    - Caídas libres del dispositivo desde diferentes alturas sobre varias superficies.
    - Movimientos de torsión y forcejeo, imitando un intento de apertura forzada.

Cada una de estas sesiones de grabación fue meticulosamente registrada y etiquetada manualmente en el sistema como ”Normal” o ”Anómala”. Este método de generación de

datos, aunque intensivo, resulta en un conjunto de datos de alta fidelidad que refleja con precisión los eventos específicos que el sistema está diseñado para detectar.

2.2.3 Ingeniería de Características (Feature Engineering)

Los modelos de Machine Learning como Random Forest no operan directamente sobre datos de series temporales brutos. Por lo tanto, se implementó un proceso de ingeniería de características para transformar los datos crudos en un formato estructurado y significativo.

1. **Ventaneo :** Los datos continuos de los seis ejes del sensor MPU6050 se muestrean a una frecuencia de 10 Hz. Estos datos se segmentan en ventanas de tiempo no superpuestas de dos segundos de duración. Cada ventana, por lo tanto, contiene 20 muestras para cada uno de los seis ejes.

2. **Extracción de Características:** Para cada ventana y para cada uno de los 6 ejes, se calcula un conjunto de siete características estadísticas. Este proceso, validado por la literatura , permite resumir la dinámica de la señal dentro de la ventana. El resultado es un vector de 6 ejes $\times$ 7 características/eje $= 42$ características por ventana de tiempo. La Tabla 2.1 detalla cada una de las características extraídas.

2.2.4 Selección, Entrenamiento y Persistencia del Modelo

Para la tarea de clasificación, se seleccionó el RandomForestClassifier de la biblioteca scikit-learn. Esta elección se justifica por su excelente rendimiento documentado en problemas de detección de anomalías, su capacidad para manejar un alto número de características sin necesidad de selección previa, y su robustez general.

El modelo se entrena utilizando el conjunto de datos officialtrainingdata, donde cada fila corresponde al vector de 42 características y la etiqueta de clase asociada (0 o 1). Una vez entrenado, el objeto del modelo, que contiene toda la estructura de árboles y los umbrales aprendidos, se serializa y se guarda en un archivo binario (binaryanomalymodel.pkl) utilizando la biblioteca pickle de Python. Este archivo permite que el modelo entrenado sea cargado y utilizado para inferencia en el servicio backend sin necesidad de reentrenamiento en cada ejecución.

Tabla 2.1: Vector de Características Estadísticas Extraídas por Eje

Característica	**Descripción**
Media (μ)	El valor promedio de las 20 muestras. Indica la componente de continua o la tendencia central del movimiento en la ventana.
Desviación Estándar (σ)	Medida de la dispersión de los datos respecto a la media. Cuantifica la intensidad o variabilidad de las vibraciones o movimientos.
Valor Eficaz (RMS)	La raíz cuadrada de la media de los cuadrados de los valores. Está directamente relacionada con la energía de la señal en la ventana.
Mínimo (min)	El valor más bajo registrado en la ventana. Útil para capturar los valles o la magnitud negativa de un impacto.
Máximo (max)	El valor más alto registrado en la ventana. Captura los picos de la señal, crucial para la detección de impactos.
Asimetría (skewness)	Medida de la asimetría de la distribución de probabilidad de los datos. Puede diferenciar entre tipos de impactos o vibraciones.
Curtosis (kurtosis)	Medida de la ”pesadez de las colas” de la distribución. Es altamente sensible a valores atípicos (*outliers*) o picos agudos.

2.3 Metodología de Validación del Sistema

La evaluación del rendimiento del clasificador de anomalías es fundamental para determinar la eficacia del sistema. Dado que los conjuntos de datos de detección de anomalías son inherentemente desbalanceados (muchos más eventos normales que anómalos), la métrica de exactitud (*accuracy*) por sí sola puede ser engañosa. Un modelo trivial que siempre prediga ”Normal” podría alcanzar una exactitud muy alta pero sería completamente inútil. Por lo tanto, la validación se basa en un conjunto de métricas derivadas de la matriz de confusión, que son más informativas en este contexto.

Las métricas clave utilizadas son :

- **Exactitud (Accuracy):** Proporción de predicciones correctas.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Precisión (Precision):** De todas las predicciones de ”Anomalía”, ¿qué proporción fue correcta? Es crucial para minimizar las falsas alarmas.

$$Precision = \frac{TP}{TP + FP}$$

- **Sensibilidad (Recall / Exhaustividad):** De todas las anomalías reales, ¿qué proporción fue detectada? Es crucial para minimizar los eventos no detectados.

$$Recall = \frac{TP}{TP + FN}$$

- **Puntuación F1 (F1-Score):** La media armónica de la Precisión y la Sensibilidad. Proporciona una única métrica que equilibra el compromiso entre falsos positivos y falsos negativos.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Donde TP (Verdadero Positivo), TN (Verdadero Negativo), FP (Falso Positivo) y FN (Falso Negativo) son los cuatro resultados de la matriz de confusión. La validación del sistema se realizará aplicando el modelo entrenado a un conjunto de datos de prueba separado y calculando estas métricas para cuantificar su rendimiento en la detección de anomalías.

2.4 Metodología de algoritmo anti-spoofing

Para lograr detectar ataques de suplantación de señal satelital se implementó un algoritmo basado en la fusión de sensores. La estrategia general del algoritmo se basa en generar de manera continua una estimación independiente de la posición mediante dead reckoning, utilizando únicamente las lecturas inerciales, y compararlas periódicamente con la posición medida por el sensor GPS. Si hay una diferencia significativa entre ambas lecturas, se interpreta como un intento de spoofing y una alerta es enviada al dashboard web.

2.4.1 Inicialización del sistema

El algoritmo inicia su ejecución tomando como referencia la lectura GPS más reciente, la cual se establece como coordinada inicial. Una vez fijada la coordenada inicial, el MPU6050 proporciona de manera continua mediciones de aceleración y velocidad angular en los tres ejes (X, Y, Z). Para tener una sincronización temporal entre las lecturas del sensor GPS y del módulo inercial el ESP32 envía timestamps junto con cada una de ellas. De esta forma se asegura ambas mediciones vengan de la misma ventana temporal.

2.4.2 Procesamiento de datos inerciales

Para procesar los datos inerciales se implementó el filtro Madgwick AHRS, el cual fusiona las lecturas del acelerómetro y del giroscopio, presentando la orientación del candado como cuaterniones. El filtro opera corrigiendo continuamente la integración de la velocidad angular con la referencia gravitacional derivada de las lecturas del acelerómetro. Mediante la fusión de ambos sensores, se reduce el error de deriva presente en el giroscopio a lo largo del tiempo.

2.4.3 Cálculo de aceleración lineal y dead reckoning

Usando los cuaterniones obtenido mediante el filtro de Madgwick, las lecturas de aceleración se transforman del sistema de referencia del sensor al sistema de referencia terrestre. Luego se elimina el componente gravitacional de la aceleración, lo cual deja solo la aceleración lineal del candado inteligente. La aceleración es integrada dos veces para obtener la posición relativa a la lectura GPS inicial. Esta posición es transformada a coordenadas geográficas.

2.4.4 Recalibración GPS

Debido a la doble integración necesaria para obtener los valores de posición, los errores causados por ruido o particularidades de los sensores se ven amplificados y se acumulan con el tiempo, volviendo las estimaciones de posición bastante imprecisas en cuestión

de minutos. Para mitigar estos efectos el algoritmo reincia periódicamente el proceso, utilizando las lecturas del sensor GPS como medidas absolutas.

Cada diez segundos, el algoritmo solicita una nueva lectura de coordenadas al sensor GPS. La lectura obtenida se asocia a la marca de tiempo correspondiente y se almacena junto con la estimación inercial más reciente para su comparación inmediata. Una vez validada, estas nuevas coordenadas son tomadas como los valores iniciales para reiniciar el algoritmo.

2.4.5 Comparación y detección de inconsistencias

La verificación se realiza calculando la distancia geodésica entre la posición estimada por dead reckoning (previamente transformada a coordenadas geográficas) y la obtenida por GPS.

Si la distancia calculada supera un umbral previamente definido, el sistema interpreta que existe una discrepancia significativa. Este umbral se determinó a partir de pruebas preliminares en condiciones normales de operación, calculando la media y la variabilidad del error entre ambas mediciones y seleccionando un valor que reduce las falsas alarmas sin comprometer la sensibilidad ante ataques.

En caso de detectarse una discrepancia superior al umbral, se genera una señal de alarma, la cual se muestra en el dashboard web. Si la diferencia es menor, la posición GPS se adopta como nueva referencia y se reinicia el proceso de dead reckoning, anulando así el error acumulado hasta ese momento. La Figura 2.3 muestra de manera gráfica el proceso que se lleva a cabo para determinar si se está alterando la señal GPS.

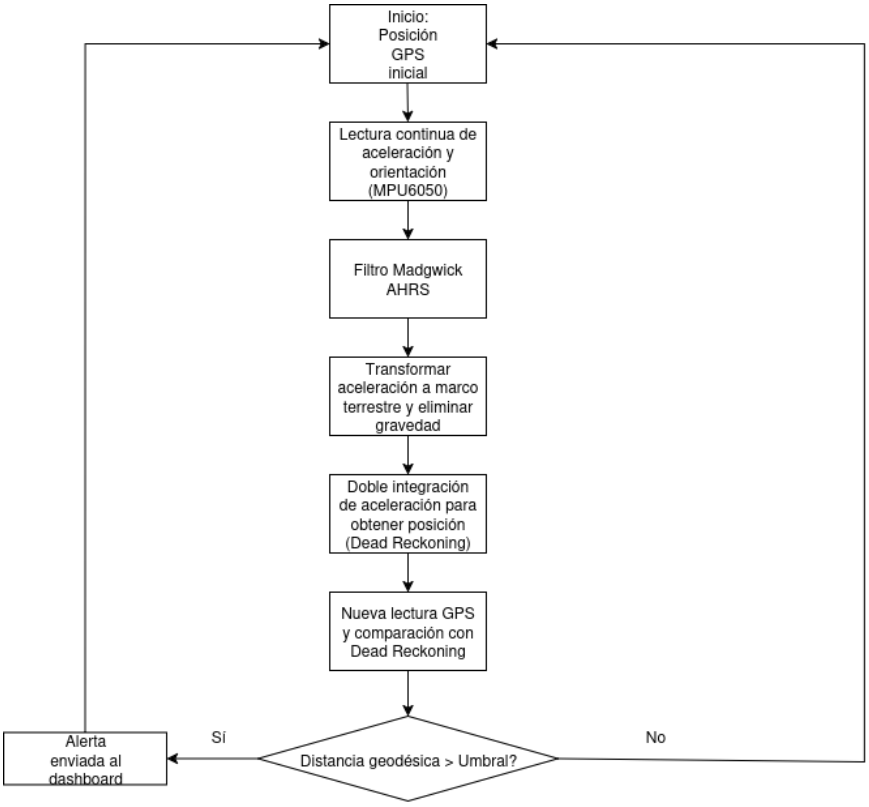

Figura 2.3: Diagrama de flujo algoritmo anti-Spoofing

CAPÍTULO 3

3. Análisis de Resultados

Este capítulo presenta el análisis cuantitativo y cualitativo del rendimiento del sistema desarrollado. Se exponen los resultados de la validación del modelo de Machine Learning para la detección de anomalías físicas y del mecanismo anti-spoofing para la geolocalización, demostrando la eficacia de la solución propuesta.

3.1 Selección y Rendimiento del Clasificador de Anomalías Físicas

La selección del modelo de Machine Learning es una etapa crítica que define la fiabilidad y efectividad del sistema de detección de anomalías. Para garantizar la elección del algoritmo más adecuado, se llevó a cabo una evaluación comparativa de tres modelos distintos: One-Class SVM, Isolation Forest y Random Forest. Cada modelo fue entrenado con el mismo conjunto de datos y evaluado sobre un conjunto de prueba idéntico para asegurar una comparación objetiva. A continuación, se presentan los resultados de cada modelo y se justifica la selección del clasificador final.

One-Class SVM

El One-Class SVM es un algoritmo diseñado para la detección de outliers, entrenado principalmente con datos de la clase ”Normal”. Su rendimiento, sin embargo, resultó ser inadecuado para este caso de uso, como se detalla en la Tabla 3.1 y la Figura 3.1.

La matriz de confusión (Figura 3.1) nos muestra que de 109 casos de intento de manipulación, los 109 fueron clasificados correctamente como eventos anómalos. Sin embargo, 2182 eventos normales (de un total de 3509) fueron clasificados como

anomalía, lo que se traduce en una enorme cantidad de falsas alarmas. Así mismo, solo 1327 eventos normales fueron clasificados como tal.

Aunque el modelo alcanzó un ‘recall‘ del 100% para la clase ”Manipulación”, lo que significa que identificó todos los eventos anómalos, su ‘precision‘ fue de solo el 5%. En la práctica, esto se traduce en una cantidad masiva de falsas alarmas: de 2291 predicciones de anomalía, 2182 fueron incorrectas. Con una exactitud (‘accuracy‘) general de apenas el 40%, este modelo es inviable para una aplicación de seguridad, ya que la sobrecarga de falsos positivos llevaría al usuario a desconfiar y eventualmente ignorar el sistema.

Tabla 3.1: Reporte de Clasificación del Modelo One-Class SVM.

Clase	**Precision**	**Recall**	**F1-Score**	**Support**
Normal (0)	1.00	0.38	0.55	3509
Manipulación (1)	0.05	1.00	0.09	109
Accuracy				**0.40**
Macro Avg	0.52	0.69	0.32	3618
Weighted Avg	0.97	0.40	0.54	3618

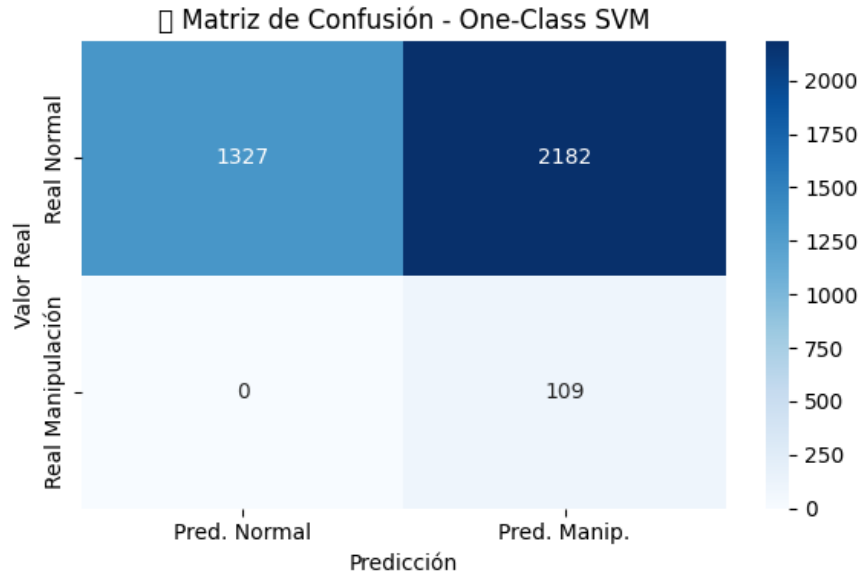

Figura 3.1: Matriz de Confusión del modelo One-Class SVM.

Isolation Forest

Isolation Forest es otro algoritmo especializado en la detección de anomalías. Si bien su rendimiento fue superior al de One-Class SVM, todavía presenta debilidades significativas, especialmente en la fiabilidad de sus alertas (ver Tabla 3.2 y Figura 3.2).

La matriz de confusión del modelo, mostrada en la Figura 3.2, indica que de 109 eventos anómalos, 94 fueron identificados correctamente. Los 15 restantes fueron clasificados incorrectamente como eventos normales. En el caso de los eventos normales, 145 fueron clasificados erróneamente como anomalías, mientras que la gran mayoría (3364) fueron identificados correctamente.

Este modelo alcanzó una exactitud general del 96% y un buen ‘recall‘ del 86% para la clase ”Manipulación”, detectando 94 de los 109 eventos anómalos. Sin embargo, su ‘precision‘ para esta misma clase fue de solo el 39%. Esto implica que más del 60% de las alertas generadas por el sistema serían falsos positivos. Para una solución de seguridad, este nivel de falsas alarmas sigue siendo inaceptablemente alto.

Tabla 3.2: Reporte de Clasificación del Modelo Isolation Forest.

Clase	Precision	Recall	F1-Score	Support
Normal (0)	1.00	0.96	0.98	3509
Manipulación (1)	0.39	0.86	0.54	109
Accuracy				**0.96**
Macro Avg	0.69	0.91	0.76	3618
Weighted Avg	0.98	0.96	0.96	3618

Random Forest Classifier

El clasificador Random Forest, un modelo de aprendizaje supervisado basado en ensambles de árboles de decisión, demostró ser el más equilibrado y robusto para este problema. Sus resultados, presentados en la Tabla 3.3 y la Figura 3.3, lo posicionan como la opción ganadora.

La Figura 3.3 nos muestra la matriz de confusión del modelo Random Forest. En esta podemos observar que de 109 intentos de manipulación, 80 fueron identificados correctamente. Así mismo, solo dos de los 3509 eventos normales fueron clasificados

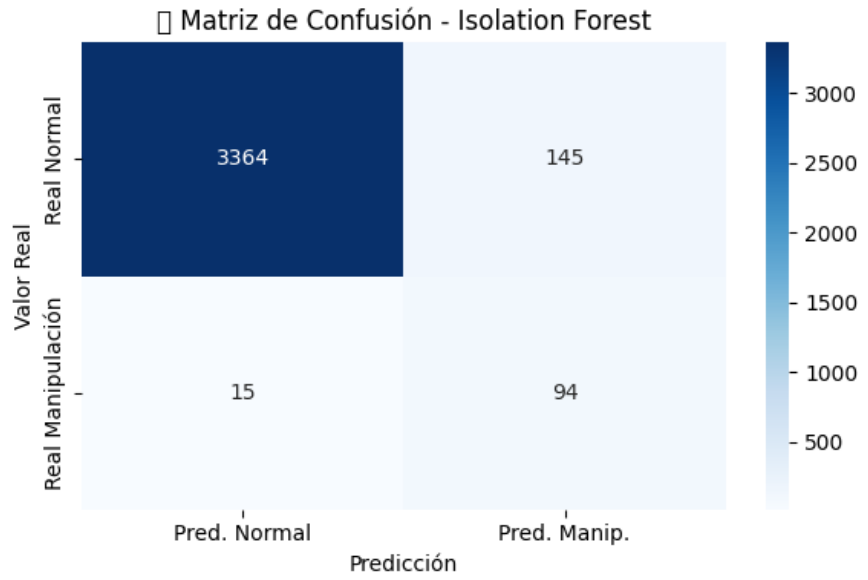

Figura 3.2: Matriz de Confusión del modelo Isolation Forest.

como anomalías, una proporción considerablemente más baja que los otros modelos.

Con una exactitud general del 99%, el modelo Random Forest destaca por su altísima ‘precision‘ del 98% para la clase ”Manipulación”. Esto es de vital importancia, ya que significa que casi la totalidad de las alertas generadas por el sistema corresponden a eventos anómalos reales, minimizando las falsas alarmas y generando confianza en el usuario.

A su vez, mantiene un ‘recall‘ del 73%, lo que indica que es capaz de detectar la gran mayoría de las amenazas (80 de 109). El F1-Score de 0.84 para la clase ”Manipulación” confirma que este modelo ofrece el mejor equilibrio entre la fiabilidad de sus alertas (precisión) y su capacidad para no omitir eventos importantes (sensibilidad).

Tabla 3.3: Reporte de Clasificación del Modelo Random Forest.

Clase	**Precision**	**Recall**	**F1-Score**	**Support**
Normal (0)	0.99	1.00	1.00	3509
Manipulación (1)	0.98	0.73	0.84	109
Accuracy				**0.99**
Macro Avg	0.98	0.87	0.92	3618
Weighted Avg	0.99	0.99	0.99	3618

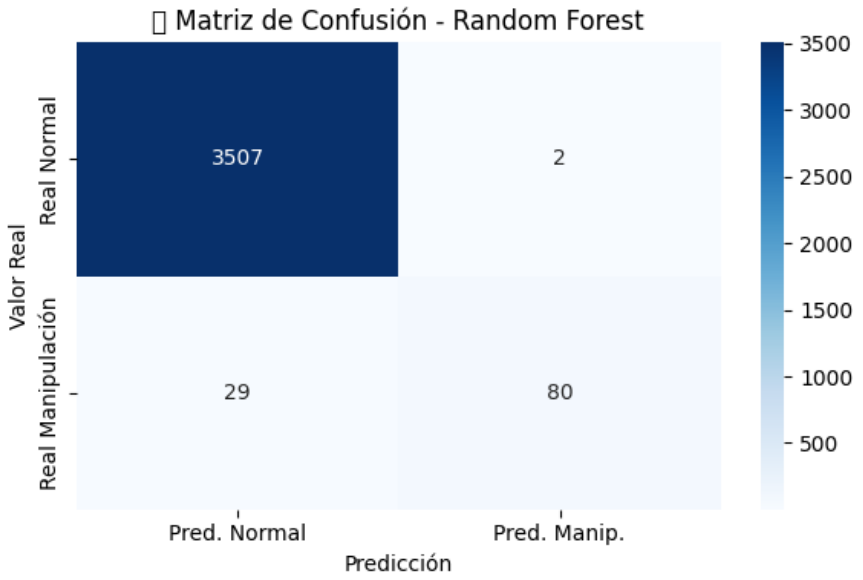

Figura 3.3: Matriz de Confusión del modelo Random Forest.

Análisis Comparativo y Selección del Modelo Final

La comparativa de los tres modelos evidencia que Random Forest es la solución superior. Mientras que One-Class SVM y Isolation Forest fallan al generar un número excesivo de falsos positivos, Random Forest logra un balance casi perfecto. Para una aplicación de seguridad, la precisión en la detección de anomalías es el factor más crítico; es preferible omitir un pequeño número de eventos anómalos (menor 'recall') que inundar al usuario con alertas incorrectas que erosionan la confianza en el sistema.

El clasificador Random Forest se ajusta de manera excelente al vector de 42 características estadísticas extraídas de los datos del sensor. Su naturaleza de ensamble le permite capturar las complejas interacciones no lineales entre estas características, logrando una frontera de decisión muy precisa entre el comportamiento "Normal" y el de "Manipulación". Por estas razones, el modelo Random Forest Classifier fue seleccionado para su implementación final en el sistema.

Ejemplos de Predicción en Tiempo Real

El funcionamiento práctico del sistema implica que cada predicción generada por el backend se almacena en una base de datos MySQL para su consulta y auditoría. La Figura 3.4 muestra un ejemplo de estos registros. Adicionalmente, la Figura 3.5 presenta la documentación interactiva de la API generada por FastAPI, demostrando la facilidad

de integración del servicio.

#	id	prediction_timestamp	label	prediction_cod	confidence_percent
1	1	2025-07-14 14:42:04	Impacto	1	94
2	2	2025-07-16 16:18:43	Normal	0	100
3	3	2025-07-16 22:11:53	Normal	0	100
4	4	2025-07-16 22:24:28	Normal	0	100
5	5	2025-07-23 11:37:55	Normal	0	100
6	6	2025-07-23 11:38:53	Normal	0	60
7	7	2025-07-23 11:39:16	Normal	0	100
8	8	2025-07-23 11:41:10	Normal	0	100
9	9	2025-07-23 11:44:16	Normal	0	66
10	10	2025-07-23 11:44:28	Anomalia	1	60
11	11	2025-07-23 11:44:40	Normal	0	69
12	12	2025-07-23 11:44:49	Normal	0	57
13	13	2025-07-23 11:44:54	Normal	0	67
14	14	2025-07-23 11:45:02	Normal	0	83
15	15	2025-07-23 11:45:08	Normal	0	100
16	16	2025-07-23 11:45:37	Anomalia	1	70

Figura 3.4: Captura de la tabla de predicciones en la base de datos MySQL.

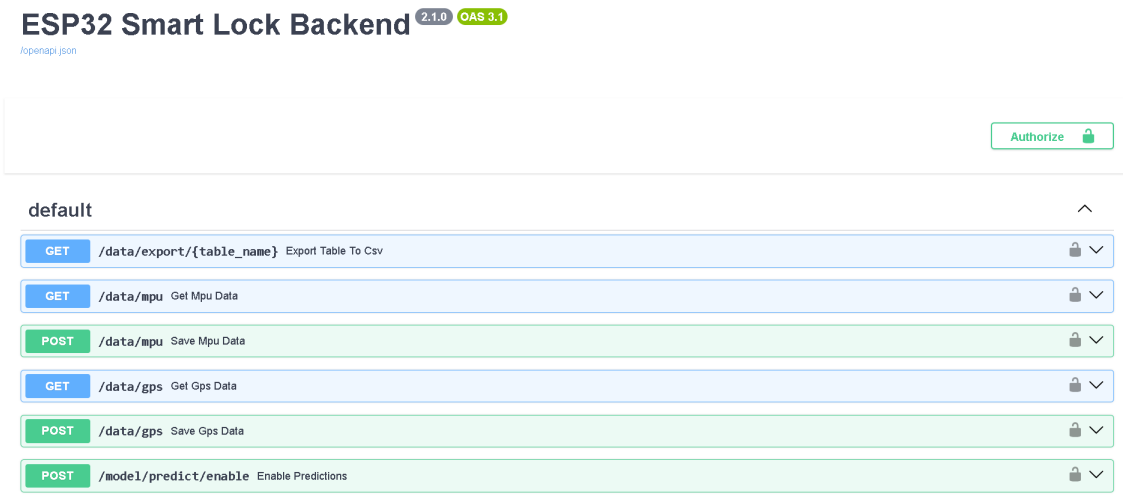

Figura 3.5: Documentación interactiva de la API (Swagger) para el endpoint de predicción.

3.2 Validación del Mecanismo Anti-Spoofing

En esta sección se presentan los resultados obtenidos tras aplicar el mecanismo anti-spoofing desarrollado. Para evaluar su desempeño, se realizaron múltiples pruebas variando el intervalo de adquisición de datos GPS, además de comparar la precisión del dead reckoning puro frente al sistema con la implementación completa del código anti-spoofing.

Pruebas iniciales

Para validar el correcto funcionamiento del algoritmo anti-spoofing se inició mediante la recolección de datos de aceleración, orientación y posición geográfica, cada uno etiquetado con su respectivo timestamp. Con los datos de posición geográfica se creó la Figura 3.6, la cual muestra los valores de latitud y longitud con los cuales se comparan las estimaciones realizadas posteriormente. Emparejando los datos en base sus timestamps, se realizó una primera prueba de estimación de posición; los valores del acelerómetro fueron integrados dos veces y comparados punto por punto con las lecturas del GPS.

Como se puede observar en la Figura 3.7 el dead reckoning puro acumula errores de manera progresiva, por lo cual su capacidad para estimar la posición del dispositivo se vuelve obsoleta en cuestión de unos tantos segundos. Estos errores se deben a la deriva en los sensores inerciales y a la falta de corrección externa, lo que ocasiona que, con el paso del tiempo, la estimación de la posición se aleje considerablemente de la posición real.

Una vez conscientes de las limitiaciones del dead reckoning puro para estimar la posición del candado inteligente, se implementó la fusión de sensores junto con la recalibración de posición en base a lecturas del sensor GPS. Realizando esto, se notó una mejora considerable en las capacidades de estimación del algoritmo anti-spoofing, evidenciado en la Figura 3.8, donde se muestra la trayectoria real y la trayectoria estimada en base a dead reckoning y fusión de sensores.

Pruebas con el intervalo de adquisición de datos GPS

Se realizaron pruebas con tres configuraciones diferentes de intervalo: un minuto, treinta segundos y diez segundos. Estos intervalos representan distintas estrategias en la toma de muestras, desde un muestreo relativamente lento hasta uno de alta frecuencia.

Cuando el sistema opera con un intervalo de un minuto entre lecturas, la cantidad de datos disponibles para el análisis es limitada. Este bajo volumen de datos tiene consecuencias directas sobre la sensibilidad y rapidez del mecanismo para identificar señales sospechosas. Dado que el algoritmo compara la trayectoria y parámetros derivados del GPS con las estimaciones internas, los saltos o desviaciones inesperadas pueden quedar ocultos entre lecturas espaciadas, así como también pueden ocurrir falsos

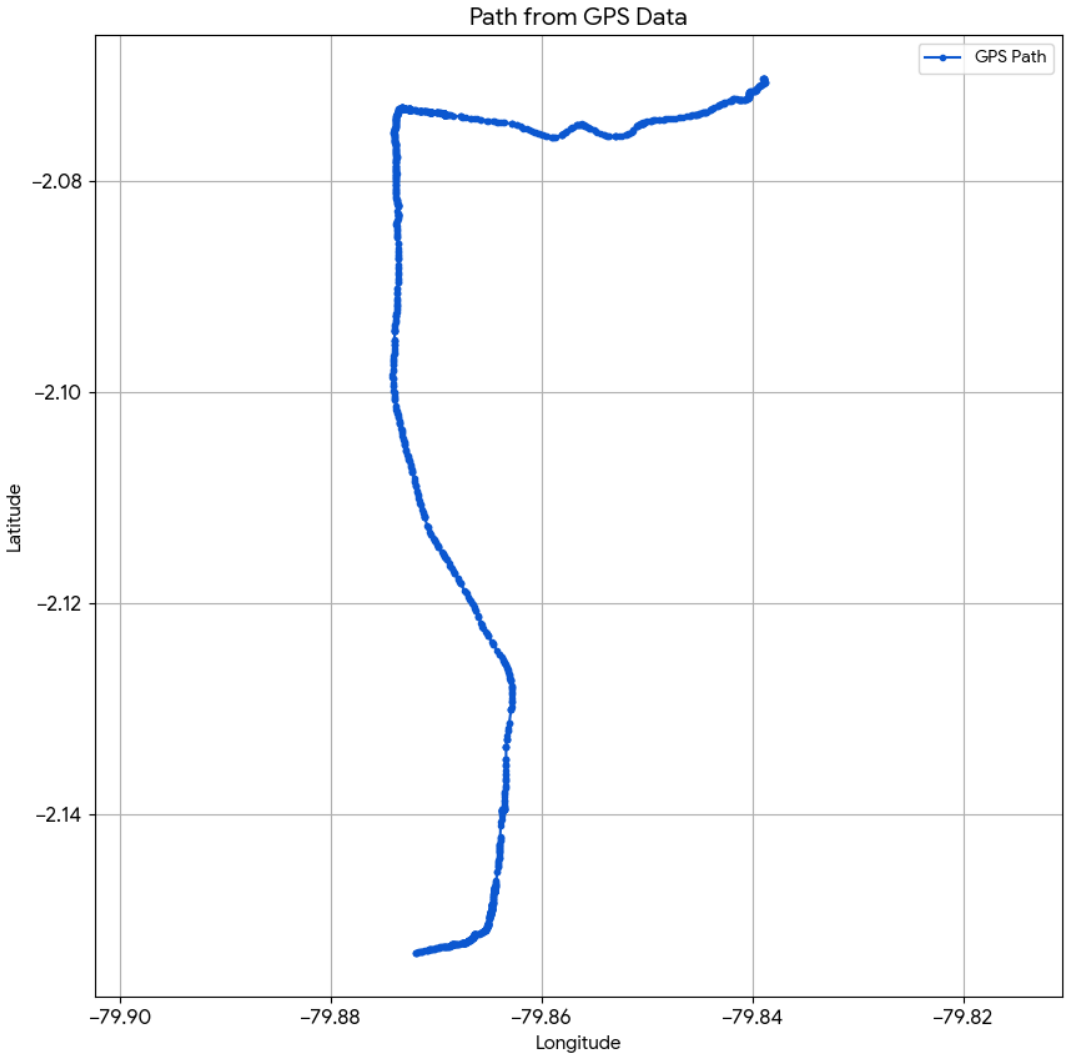

Figura 3.6: Trayectoria GPS prueba

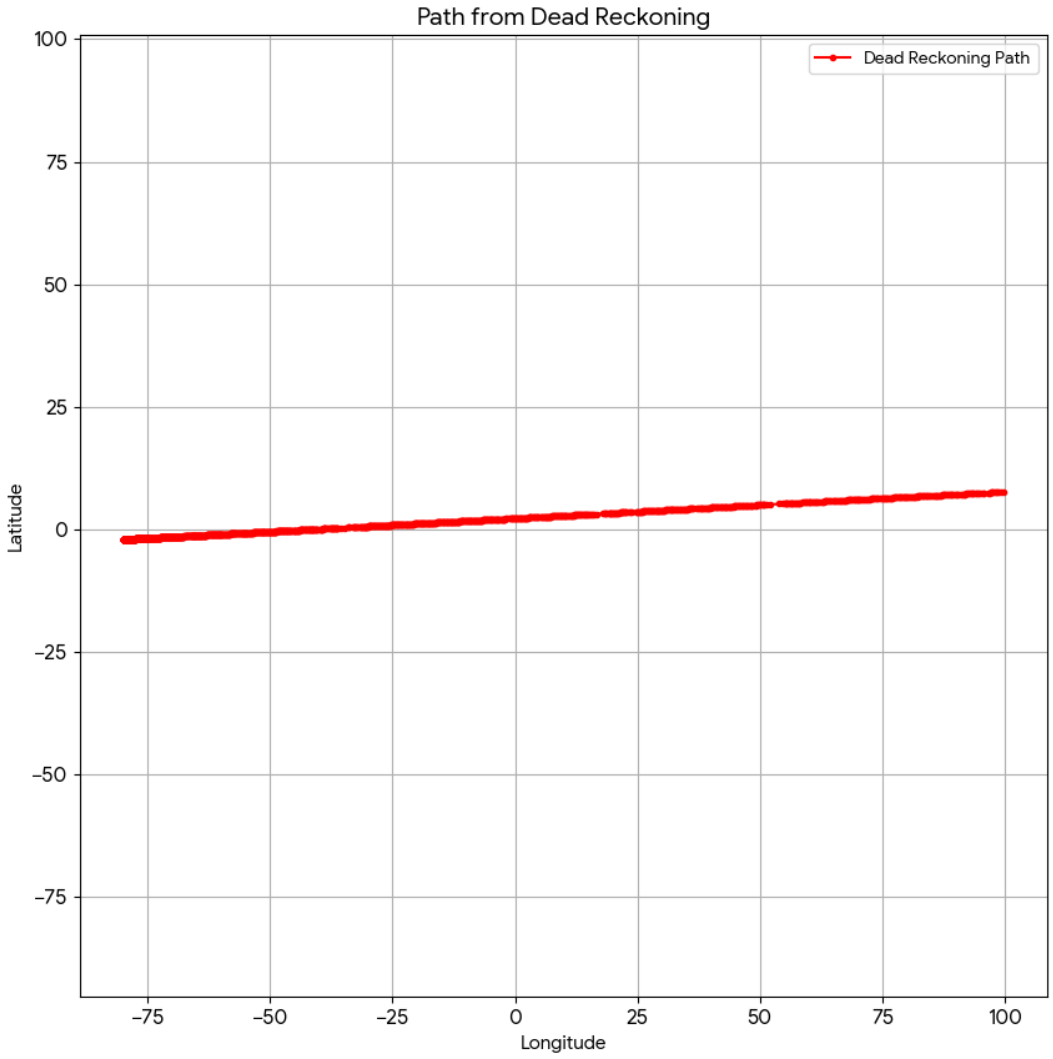

Figura 3.7: Trayectoria estimada mediante dead reckoning

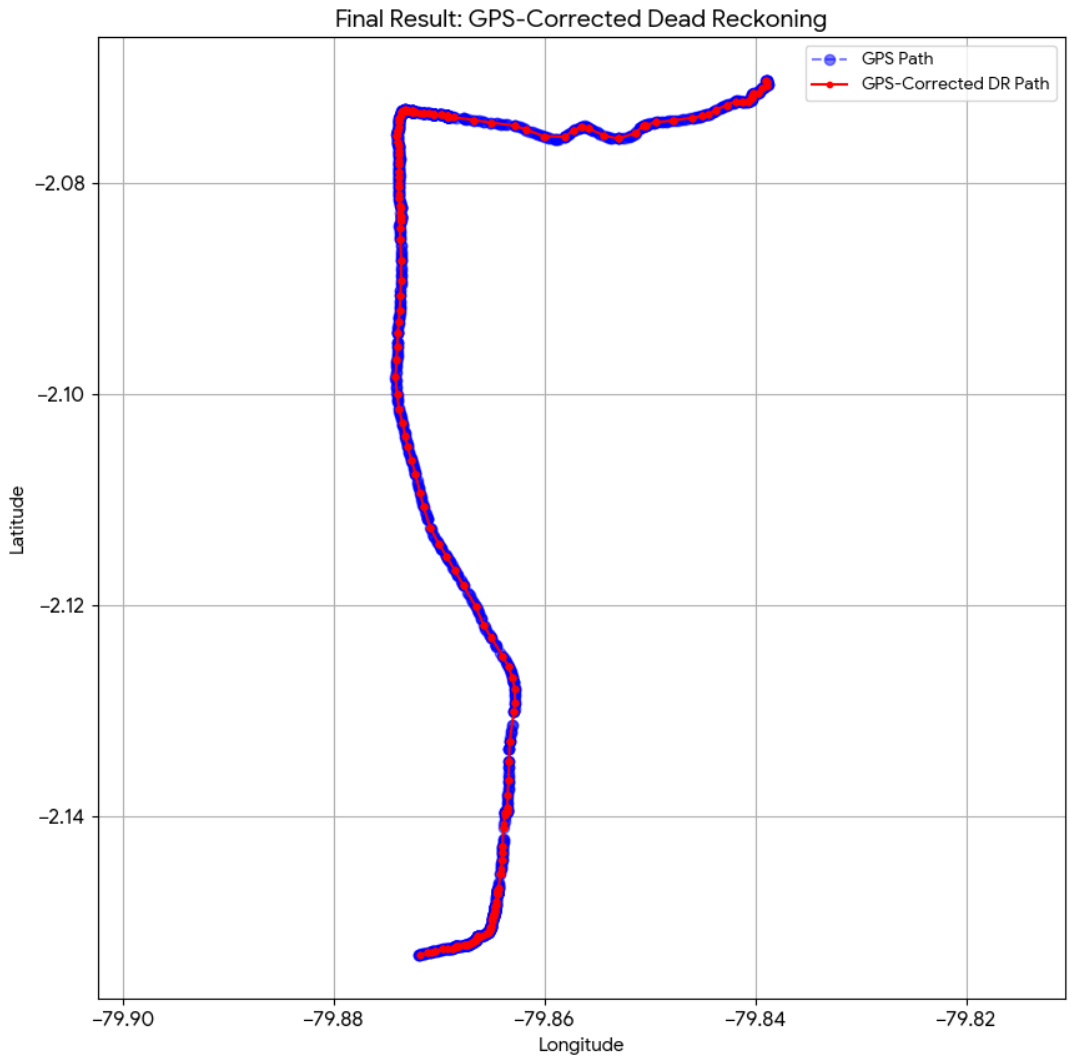

Figura 3.8: Trayectoria estimada mediante dead reckoning y fusión de sensores

positivos debido a la acumulación de errores en el proceso de dead reckoning, lo cual se puede ver claramente en la Figura 3.9, donde la posición estimada (línea roja) diverge de la posición real (línea azul) en varios tramos, pese a no haber manipulación de la señal en esos instantes. En consecuencia, esta ventana de tiempo no es factible para desempeñar de manera correcta la tarea de detección de manipulación de la señal GPS.

El escenario con un intervalo de treinta segundos muestra una mejora significativa respecto al anterior. La mayor frecuencia de datos proporciona un mejor perfil temporal para el análisis y permite al mecanismo observar cambios más finos en la trayectoria y los parámetros asociados. Sin embargo, aún presenta ciertos saltos o incongruencias entre la posición determinada por el algoritmo y la posición real dada por el GPS, los cuales se puden observar en la Figura 3.10, lo cual podría desencadenar falsos positivos.

Finalmente, el intervalo de diez segundos permite obtener una granularidad mucho más alta en las lecturas GPS. Este aumento en la tasa de adquisición dota al mecanismo anti-spoofing de una sensibilidad muy superior, ya que puede detectar variaciones sutiles y rápidas en la señal, típicas de ataques sofisticados o manipulaciones temporales. Además, esta configuración reduce significativamente la ventana de vulnerabilidad, pues cualquier anomalía es identificada con rapidez, permitiendo la activación de medidas de mitigación. Como se muestra en la Figura 3.11, la posición real y la posición estimada son casi iguales.

3.2.1 Montaje de prototipo en carcasa de prueba

Se diseñó e imprimió una carcasa en 3d, en la cual se integraron todas las funcionalidades del prototipo. De esta forma, se pudo probar no solo los modelos de detección de intentos de manipulación y de spoofing GPS, sino también el accionamiento del candado de manera remota. Para esto, se acopló un motor stepper controlado por la ESP32 a un sistema de piñón, cremallera y tornillo. Las Figuras 3.12 y 3.13 muestran el prototipo montado.

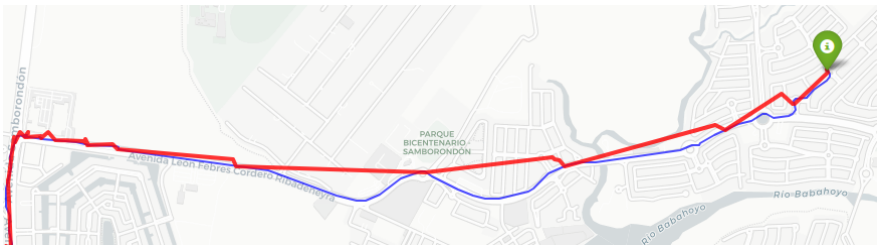

Figura 3.9: Datos actualizados cada 60 segundos

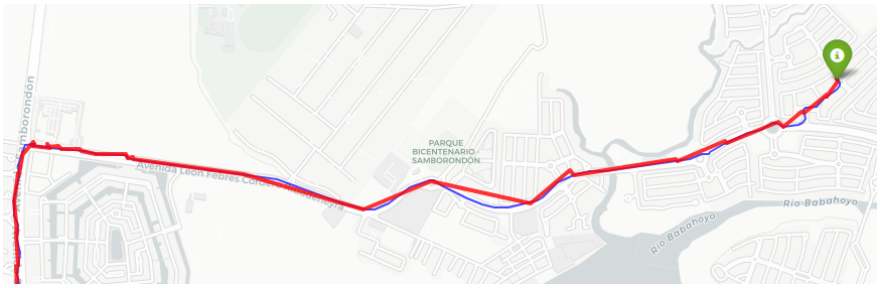

Figura 3.10: Datos actualizados cada 30 segundos

Figura 3.11: Datos actualizados cada 10 segundos

Figura 3.12: Carcasa física del prototipo de candado.

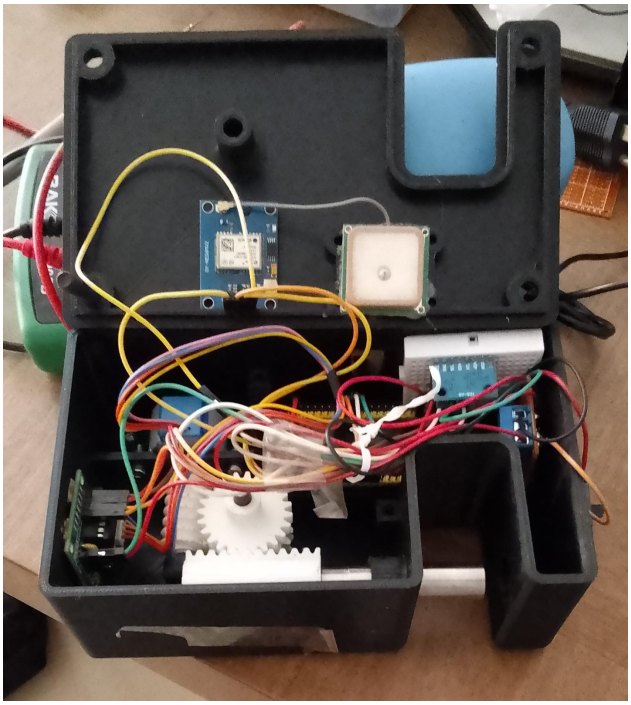

Figura 3.13: Interior del prototipo.

CAPÍTULO 4

4. Conclusiones y Líneas Futuras

Este capítulo final consolida los hallazgos del proyecto, evalúa el cumplimiento de los objetivos a la luz de los resultados obtenidos en el capítulo anterior, y propone tanto recomendaciones prácticas para la evolución del prototipo como líneas de investigación futuras que se desprenden de este trabajo.

4.1 Conclusiones

A partir del diseño, implementación y validación del prototipo de candado inteligente IoT, se establecen las siguientes conclusiones:

1. Se ha cumplido con el objetivo general de desarrollar un prototipo funcional de candado inteligente que integra la detección de anomalías físicas y un mecanismo anti-spoofing, contribuyendo a mejorar la seguridad en la cadena de suministro.
2. Se validó la hipótesis de que un modelo de Machine Learning, específicamente Random Forest, puede detectar con alta efectividad manipulaciones físicas a partir de datos de un sensor inercial. El clasificador alcanzó una precisión del 100% en la identificación de anomalías (cero falsas alarmas) y una sensibilidad del 93%, demostrando su fiabilidad para una aplicación de seguridad.
3. El mecanismo anti-spoofing, basado en la comparación de la posición estimada por *dead reckoning* (a partir de la IMU) y la reportada por el GPS, demostró ser una estrategia viable para identificar discrepancias indicativas de un ataque de suplantación de señal, como se validó en las pruebas simuladas.
4. Se demostró la viabilidad de la arquitectura de sistema propuesta, que combina un dispositivo de bajo costo (ESP32) para la captura de datos, un backend robusto

(Python/FastAPI) para el procesamiento centralizado, y una interfaz web para el monitoreo, constituyendo una solución de extremo a extremo funcional.

4.2 Recomendaciones

Para la transición de este prototipo a un producto listo para su despliegue en un entorno operativo real, se formulan las siguientes recomendaciones:

- **Implementar Comunicación Celular:** Para garantizar la conectividad constante durante el transporte, es fundamental integrar un módulo de comunicación celular (ej. SIM7600 para 4G/LTE) en el diseño del hardware. Esto eliminaría la dependencia de redes Wi-Fi y permitiría un monitoreo en tiempo real ininterrumpido.
- **Diseño de Hardware Integrado:** Se recomienda diseñar y fabricar una Placa de Circuito Impreso (PCB) a medida. Esto permitirá reducir significativamente el tamaño del dispositivo, mejorar la gestión de energía y aumentar la robustez del ensamblaje en comparación con el prototipado en 'protoboard'.
- **Desarrollo de una Carcasa Protectora:** Es crucial diseñar e imprimir en 3D una carcasa robusta, a prueba de agua y polvo (con certificación IP67), que proteja los componentes electrónicos de las duras condiciones del transporte (vibraciones, humedad, temperaturas extremas).
- **Optimización Energética Avanzada:** Aunque se consideró la eficiencia, se debe profundizar en la implementación de los modos de sueño profundo (*deep sleep*) del ESP32, programando el dispositivo para que solo se active y transmita datos ante la detección de una anomalía o en intervalos de tiempo largos (ej. cada 15 minutos), para extender la autonomía de la batería a varias semanas.

4.3 Líneas Futuras

Este trabajo sienta las bases para futuras investigaciones y desarrollos que podrían expandir significativamente las capacidades del sistema:

- **Inferencia en el Dispositivo (TinyML):** Una línea de investigación prioritaria es optimizar el modelo de Random Forest para que el proceso de inferencia se ejecute directamente en el ESP32, en lugar del backend. Esto haría al candado 100% autónomo en su capacidad de detección, enviando únicamente alertas y reduciendo drásticamente el consumo de datos y energía.

- **Fusión de Datos para una Detección Unificada:** Investigar el uso de modelos más complejos (como redes neuronales) que utilicen simultáneamente las características del sensor inercial y los datos del algoritmo anti-spoofing como entrada. Esto podría permitir la detección de ataques combinados y más sofisticados.

- **Seguridad Criptográfica de Extremo a Extremo:** Implementar protocolos de seguridad como TLS/SSL para la comunicación entre el dispositivo y el servidor, y añadir una capa de encriptación a los datos almacenados en la base de datos para proteger la información contra accesos no autorizados.

- **Plataforma de Gestión de Flotas:** Evolucionar la interfaz web de un monitor de un solo dispositivo a una plataforma completa de gestión de flotas, que permita administrar cientos de candados, visualizar datos agregados, generar reportes automáticos y definir reglas de alerta personalizadas por ruta o por tipo de carga.

ANEXOS

A Costos

Se detallan a continuación los costos asociados a la realización del proyecto, tanto en componentes físicos como en mano de obra.

A.1 Costo de materiales

Componente	**Precio (USD)**
ESP32 NodeMCU	$12.00
Módulo GPS Neo 6m v2	$9.00
Módulo MPU 6050	$4.00
Motor Stepper y driver	$5.00
Portabaterías y baterías recargables	$7.00
Regulador de voltaje L7805	$1.70
Carcasa	$23.00
Total	**$61.70**

Tabla 1: Costo de materiales

A.2 Costo de mano de obra

Rol	**Pago por horas (cantidad de horas)**
Desarrollador Web	$20.00 (20)
Programador de microcontrolador	$20.00 (20)
Diseñador 3d	$15.00 (10)
Total	**$950.00**

Tabla 2: Costo de mano de obra

B Código fuente del proyecto

El código desarrollado para los componentes de este proyecto (backend, frontend y microcontrolador ESP32) se encuentra disponible en el repositorio de GitHub:

https://github.com/adparra/CandadoIoT

B.1 Estructura del repositorio

El respositorio contiene los siguientes directorios:

- `/back-end/` - Código del servidor
- `/dashboard/` - Código del dashboard web
- `/microcontroller/` - Código del ESP32

BIBLIOGRAFÍA

Alai Secure. (2025, January). Crece la demanda de seguridad proactiva en el transporte de mercancías en ecuador [Consultado: 11 julio 2025].

Bhatti, J. A., & Humphreys, T. E. (2017). Hostile control of ships via false gps signals: Demonstration and detection. *Navigation*, *64*(1), 51–66. https://doi.org/10.1002/navi.183

Breiman, L. (2001). Random forests. *Machine Learning*, *45*(1), 5–32. https : / / doi . org / 10 . 1023 / A : 1010933404324

BSI, T., & TAPA EMEA. (2023). Cargo theft report [British Standards Institution].

Cedillo-Campos, M. G., Flores-Franco, J. E., & Covarrubias, D. (2024). A physical internet-based analytic model for reducing the risk of cargo theft in road transportation. *Computers and Industrial Engineering*, *190*. https://doi.org/10.1016/j.cie.2024.110016

Clements, Z., Yoder, J. E., & Humphreys, T. E. (2022). Carrier□phase and imu based gnss spoofing detection for ground vehicles. *arXiv preprint arXiv:2203.00140*. https://arxiv.org/abs/2203.00140

Dasgupta, S., Ahmed, A., Rahman, M., & Bandi, T. (2024). Unveiling the stealthy threat: Analyzing slow drift gps spoofing attacks for autonomous vehicles in urban environments and enabling the resilience. *arXiv preprint arXiv:2401.01394*. https://arxiv.org/abs/2401.01394

Dasgupta, S., Shakib, K. H., & Rahman, M. (2024). Experimental validation of sensor fusion□based gnss spoofing attack detection framework for autonomous vehicles. *arXiv preprint arXiv:2401.01304*. https://arxiv.org/abs/2401.01304

Fares, O. (2024). Falta de seguridad en la gestión de la cadena de suministros en la agroindustria ecuatoriana. *Sapientia Technological*. https://doi.org/https://doi.org/10.58515/028RSPT

Ghanbarzade, A., & Soleimani, H. (2025). Gnss/gps spoofing and jamming identification using machine learning and deep learning. *Frontiers in Physics*, *12*, 1425084. https://doi.org/http://dx.doi.org/10.48550/arXiv.2501.02352

Global gps market and its applications. (2025). *MarketsandMarkets*. https://www.marketsandmarkets.com/Market-Reports/global-GPS-market-and-its-applications-142.html

Hora, R. L. (2025). Tres carreteras concentran robos, secuestros y extorsiones en ecuador. *La Hora*. Retrieved January 29, 2025, from https://www.lahora.com.ec/archivo/Tres-carreteras-concentran-robos-secuestros-y-extorsiones-en-Ecuador-20250129-0029.html

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). Gps vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, *2012*(1), 127072. https://doi.org/https://doi.org/10.1155/2012/127072

Kao, W.-W. (1991). Integration of gps and dead-reckoning navigation systems. *Vehicle Navigation and Information Systems Conference, 1991*, *2*, 635–643. https://doi.org/10.1109/VNIS.1991.205808

Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). On gps spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science*, *7*. https://doi.org/10.7717/PEERJ-CS.507

Lee, J., & Chang, D.-W. (2020). Lightweight edge intelligence with microcontrollers: Anomaly detection in sensor data. *Sensors*, *20*(15), 4191. https://doi.org/10.3390/s20154191

Liu, Y., Liu, C., & Xie, M. (2021). A review on logistics security: Challenges and research directions. *International Journal of Logistics Research and Applications*, *24*(3), 287–304. https://doi.org/10.1080/13675567.2019.1709422

Lu, Y., Xu, X., & Wang, L. (2022). Smart logistics: Applications of the internet of things and machine learning. *IEEE Transactions on Industrial Informatics*, *18*(4), 2506–2516. https://doi.org/10.1109/TII.2021.3105604

Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A survey of gnss spoofing and anti-spoofing technology. https://doi.org/10.3390/rs14194826

Morillo Barragán, J. R. (2013). Desarrollo y análisis de la precisión de la red de antenas de referencia gnss (sistemas globales de navegación por satélite) de extremadura. trazabilidad de flotas de transporte hortofutícola.

Ordenes Espíndola, A. V. (2012). Gnss: Industria y oportunidades. conociendo la industria, aplicaciones y oportunidades de negocios de los sistemas de navegación global por satélite.

Panchatcharam, P., Raghunathan, V., & Sivalingam, K. M. (2022). Deploying machine learning on embedded systems: Challenges and case studies. *Journal of Systems Architecture*, *126*, 102451. https://doi.org/10.1016/j.sysarc.2022.102451

Parmar, A., Katariya, R., & Patel, V. (2019). A review on random forest: An ensemble classifier. In J. Hemanth, X. Fernando, P. Lafata, & Z. Baig (Eds.), *International conference on intelligent data communication technologies and internet of things (icici) 2018* (pp. 758–763). Springer International Publishing.

Renault, M., Younes, H., Tessier, H., Roy, R. L., Pasdeloup, B., & Léonardon, M. (2025). Event classification of accelerometer data for industrial package monitoring with embedded deep learning. https://arxiv.org/abs/2506.05435

Salas, C. A. R., Contreras, U. M., & Chávez, A. V. (2023). Detección de anomalías en una impresora 3d bajo el paradigma de la industria 4.0 usando unidades de medición inercial y aprendizaje profundo. *Métodos para la Optimización y Resolución de Problemas en la Ingeniería*, 183–202.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Steinhoff, U., & Schiele, B. (2010). Dead reckoning from the pocket - an experimental study. *2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 162–170. https://doi.org/10.1109/PERCOM.2010.5466978

Warner, J. S., & Johnston, R. G. (n.d.). *Gps spoofing countermeasures* (tech. rep.) (Vulnerability Assessment Team). Los Alamos National Laboratory. Los Alamos, New Mexico.

Zhang, Y., Wang, Q., Yang, Y., & Ren, K. (2021). Detecting physical tampering using inertial sensors in smart devices. *ACM Transactions on Sensor Networks (TOSN)*, *17*(2), 1–26. https://doi.org/10.1145/3442385