
CHAPTER 1 - INTRODUCTION

1.1 Background

1.1.1 *Vehicle to Everything (V2X)*

The rapid development of Vehicle-to-Everything (V2X) communication technologies has significantly transformed how modern vehicles interact with their environment, surrounding infrastructure, and cloud-based management platforms (Thompson et al. 2022). As transportation systems evolve, they increasingly depend on continuous data communication, automation, and intelligent analytics rather than mechanical performance (Kaushik, 2025). Modern vehicles now generate substantial amounts of telemetry data—such as speed, fuel level, engine condition, and geolocation—which IoT-enabled systems can collect, transmit, and analyze in real time to enhance fleet management, operational efficiency, and safety (Sohail, Khattak, Khan, & Altamimi, 2025). The integration of IoT and V2X has become essential to intelligent transportation systems, offering benefits such as improved fuel efficiency, enhanced road safety, and more effective traffic management as vehicles seamlessly interact with their surroundings (Venkatasamy et al., 2024). Its impact is particularly transformative in vehicle security, where smart sensors enable real-time data processing, continuous monitoring, automated alerts, and immediate incident reporting, creating more adaptive and responsive protection mechanisms (Velasquez-Jimenez et al., 2025).

As logistics and transportation industries increasingly integrate connected vehicle technologies, the reliability and integrity of telemetry data have become critical for maintaining efficient operations (Deshpande & Aktarasayad Wallibai, 2016). Fleet managers depend on accurate real-time information related to vehicle performance, driver behavior, and location to optimize routing, reduce fuel consumption, and ensure regulatory compliance (Smart Fleet Management Report, 2023). However, the growing reliance on IoT-enabled onboard devices introduces new security vulnerabilities, as components such as OBD-II trackers, GPS modules, SIM-based communication units, and embedded microcontrollers are susceptible to physical tampering and electronic manipulation (Wen et al., 2020). Such disruptions compromise operational efficiency and undermine the trustworthiness of the data upon which logistics companies heavily rely. This increasing risk highlights the need for robust tamper-detection mechanisms capable of monitoring device integrity, identifying anomalous behavior, and issuing reliable alerts within connected fleet ecosystems (Coston et al., 2025).

1.1.2 *Internet of Things (IoT)*

IoT, broadly defined as the interaction between people, devices, and everyday objects, has expanded rapidly due to increasingly accessible and affordable broadband Internet

(Tippannavar et al., 2024). Beyond simple connectivity, IoT enables physical systems to sense, communicate, and process information autonomously through networks of embedded sensors, actuators, and microcontrollers (Asghari et al., 2023). This interconnected ecosystem allows devices to continuously collect and exchange data, supporting real-time decision-making across diverse applications such as transportation, healthcare, manufacturing, and environmental monitoring (Gubbi et al., 2013). The widespread adoption of cloud computing, edge processing, and low-cost embedded hardware has further accelerated IoT integration, enabling reliable analytics and automation in large distributed systems (Buyya & Srirama, 2022). As a result, IoT has become a foundational technology for modern intelligent infrastructure, particularly in connected vehicle environments where continuous data flow, remote communication, and system interoperability are essential for operational efficiency and safety.

1.1.3 The Indonesian Logistics Industry

The logistic industry in Indonesia plays a vital role in supporting national economic growth and has experienced significant growth in recent years, largely driven by the rapid expansion of e-commerce, the increasing volume of inter-island distribution and the rising dependence on fleet-based transportation complex networks of land, sea and air transportation routes. As noted by the OECD (2021), Indonesia's logistics sector has become one of the fastest growing in Southeast Asia, supported by strong consumer demand and ongoing digital transformation efforts. The growth of major e-commerce platforms has intensified this trend, with companies increasingly building large-scale, in-house delivery systems to accommodate fast shipping expectations and complex last-mile distribution requirements (DBS Indonesia, 2022). However, despite its scale, the sector faces persistent challenges such as high operational costs. Route inefficiencies, fuel misuse, cargo theft and limited real-time visibility across fleets (World Bank, 2023). Studies have noted that Indonesian logistics expenses account for 23-25% of GDP significantly higher than regional benchmarks due to infrastructural limitations, fragmented distribution channels and insufficient digital integration (Aritonang & Wicaksono, 2022). The rapid expansion of e-commerce has further increased demand for reliable tracking, accurate delivery times and improved security across transportation operations (Hasyim & Kurniawan, 2021). To address these issues, logistics companies have begun integrating IoT-based telemetry and monitoring systems; however, many of these remain vulnerable to device disconnection, data manipulation and hardware tampering. Research on Indonesian fleets highlights the limitations of traditional GPS trackers and OBD-II-based monitoring, which can be easily unplugged or interfered with, leading to unreliable data and undetected fuel fraud (Pamungkas et al., 2025; Iskandar et al., 2023). Although innovations such as fuel-level sensing and GSM-based fuel-theft detection prototypes (Nursalim et al., 2020; Fadjrimiratno et al.,

2015) offer partial solutions, the industry still lacks a comprehensive, tamper-resistant, and power-independent monitoring architecture capable of ensuring continuous and trustworthy telemetry across Indonesia's diverse logistics operations. In this paper, these elements are integrated into a unified, externally powered system that continues to operate even when the OBD-II device is unplugged, enabling uninterrupted tracking, fuel monitoring, and data logging despite intentional tampering.

1.1.4 Tamper Detection in Connected Vehicle Hardware

As connected fleet systems increasingly rely on onboard IoT hardware, ensuring these devices remain free from tampering has become essential for maintaining the reliability and integrity of vehicle telemetry. Components such as OBD-II diagnostic interfaces, GPS receivers, SIM-based communication modules, and embedded microcontrollers are central to collecting and transmitting operational data, yet they are also among the most frequently targeted for physical removal, obstruction, or manipulation (Wen et al., 2020). Although OBD-II devices can still be unplugged or substituted with equipment designed to falsify diagnostic or performance data (Nazari et al., 2019), this paper proposes an external ESP32-based monitoring system that continues operating independently even when the OBD-II unit is disconnected. By integrating GPS, SIM-based communication, and a fuel-flow sensor into a standalone module powered by a solar-assisted rechargeable battery, the system maintains continuous telemetry such as vehicle location, fuel consumption, and sensor status regardless of the OBD-II port's availability. This is particularly important because GPS units remain vulnerable to cable disconnection, antenna shielding, or deliberate signal manipulation that distorts positional accuracy (Humphreys, 2013), making redundant and independent sensing vital in tamper-prone environments. An onboard data saving provides reliable local data logging during periods of network loss or intentional signal interruption, ensuring that telemetry is preserved until connectivity is restored. Housing the hardware in a tamper-resistant enclosure further reduces the risk of physical interference or unauthorized access. In this paper, the design, implementation, and tamper-detection logic of this external monitoring architecture are detailed, demonstrating how independent power, redundant sensing, and secure data logging contribute to enhanced operational continuity within connected fleet environments.

1.2. Problem Statement

Fleet operators in Indonesia face escalating challenges in protecting the physical integrity and security of commercial trucks, particularly in relation to the theft of vehicles and high-value truck components. Incidents involving the removal of batteries, electronic control units (ECUs), axle components and other spare parts are increasingly reported in logistics hubs and

remote transportation corridors, often occurring when trucks are idle for extended periods or parked in unsupervised areas (Panduan Pengelolaan BBM Logistik, 2024). Police investigations in regions such as Bekasi and East Kalimantan have uncovered organised theft networks in which drivers or internal personnel collaborate with external actors to steal truck parts or, in some cases, the truck itself — demonstrating that insider participation is one of the most difficult risks to detect and mitigate using conventional monitoring systems (DetikNews, 2023). These incidents highlight a critical security weakness: most fleet-monitoring systems depend on the driver and lack mechanisms to prevent or detect tampering when the perpetrator is someone with legitimate access to the vehicle.

Beyond component and vehicle theft, fleets continue to experience operational losses caused by fuel misuse and pencurian BBM (fuel theft). Although financially significant, fuel theft represents only part of a broader pattern of losses stemming from unmonitored vehicle access and inadequate equipment protection. The problem is reinforced by findings from Indonesian fleet-logistics case studies, which show recurring concerns about uncontrolled fuel consumption, irregular refuelling activities and suspected siphoning during transit operations (Hermawan, Faris & Himawan, 2022). These losses become more difficult to detect when telemetry systems are disconnected, unplugged or intentionally obstructed to hide evidence of irregular activity.

At the technical level, current telematics solutions deployed in Indonesia remain highly vulnerable to physical tampering. On-board modules such as GPS receivers, OBD-II trackers, and SIM-based communication units can be unplugged, shielded or rewired without immediate detection, resulting in missing or falsified telemetry and a lack of real-time situational awareness for fleet operators (Sari & Prabowo, 2023). Moreover, most commercial fleet-management platforms only support location visibility and route playback, without integrated sensor-integrity monitoring, tamper alarms or data-validation mechanisms capable of identifying suspicious disconnections or component removal.

These challenges are compounded by difficult operating environments and skill-gaps in the national labour force. The adoption of advanced telematics and IoT-based fleet monitoring has been slowed by unstable network connectivity, harsh field conditions and limited availability of technicians experienced in managing remote sensors and edge-processing systems (Mordor Intelligence, 2025). As a result, operators, especially those operating outside Java, face higher maintenance costs, prolonged downtime and reduced system reliability. Collectively, these realities reveal a significant gap in Indonesia's fleet-security ecosystem: the absence of an affordable, tamper-resistant and power-independent telemetry architecture that can maintain continuous data flow.

1.3. Research Objectives

The primary aim of this research is to devise and execute an intelligent IoT-based system that amalgamates LTE and V2I communication to identify and avert fuel and equipment theft in trucks.

The following are the study's specific goals in order to accomplish this:

1. To design and implement a cost-effective, ESP32-based vehicle monitoring architecture that reliably integrates OBD-II vehicle data extraction for fuel and engine monitoring, and V2X communication into a unified, tamper-resistant system..
2. To evaluate the effectiveness of the hardware system in detecting physical tampering events, including OBD-II disconnection and external power interruption.
3. To assess the extent to which independent power and storage improve data continuity and reliability compared to standard vehicle-powered telematics.
4. To determine how solar energy harvesting and low-power hardware design enable the system to sustain continuous operation as an autonomous, self-powered unit.

1.4. Research Questions

Based on the identified problems, this research seeks to address the following questions:

1. How can a cost-effective, ESP32-based vehicle monitoring architecture be designed and implemented to reliably integrate OBD-II vehicle data extraction for fuel and engine monitoring, and V2X communication into a unified, tamper-resistant system?
2. How effective is the proposed architecture in detecting physical disconnections, maintaining data continuity during communication dropouts, and identifying abnormal data streams under real operating conditions?
3. How does the proposed independent power and storage architecture improve data continuity and reliability compared to standard vehicle-powered telematics solutions?
4. How does the integration of solar energy harvesting and low-power hardware design enable the system to sustain continuous operation as an autonomous, self-powered unit?

1.5. Significance of the Study

This study is significant because it addresses a critical and persistent vulnerability in Indonesia's fleet-management ecosystem: the inability of conventional telematics systems to maintain secure, continuous, and tamper-proof vehicle telemetry when onboard hardware is physically interfered with or disconnected. Existing commercial tracking solutions, which are typically powered through the OBD-II port and reliant on uninterrupted GSM connectivity, can

be easily compromised. Drivers or thieves can simply unplug cables, shield GPS antennas, remove SIM cards, or interrupt power sources. These limitations leave fleets exposed to incidents involving fuel theft, unauthorized component removal, and concealed vehicle misuse, especially in remote logistics routes where supervision is difficult and insider participation cannot be ruled out.

The proposed system enhances fleet-security technology by integrating an ESP32-based external monitoring module. This module is powered by a solar-assisted independent energy source, enabling uninterrupted system operation even when the OBD-II port or vehicle electrical supply is intentionally disabled. A major contribution of this research is the incorporation of redundant telemetry persistence through onboard storage. This ensures that critical parameters, such as GPS location, fuel consumption, and equipment status, continue to be logged during periods of weak signal, GSM jamming, or intentional communication interference. Once the connection is restored, all locally buffered data is synchronized to the server automatically, maintaining a complete chronological record of vehicle activity without human intervention.

The system's significance is further reinforced through active anomaly diagnostics and tamper alarms. If the communication link between the vehicle and the cloud is lost for longer than an acceptable threshold, the system generates a connectivity-loss alert to signal possible device removal, antenna damage, or interference. Additionally, the system continuously evaluates telemetry consistency over time. If the real-time data diverges significantly from calculated historical averages (for example, sudden fuel-drop patterns, improbable engine parameters, or abnormal movement), an anomaly alarm is triggered. These mechanisms allow the platform to detect suspicious behavior proactively, rather than merely recording data passively.

A realistic operational scenario underscores the value of the system: a driver or accomplice unplugs the OBD-II tracker and conceals the GPS antenna during an unauthorized fuel siphoning stop. In a traditional fleet-monitoring setup, the vehicle would disappear from the map and produce no operational evidence. By contrast, the proposed system continues recording telemetry via redundant sensors, preserves the data securely on the ESP32's internal storage, triggers a tamper and connectivity-loss alarm, and uploads all stored evidence once the device regains network access. This shifts the monitoring paradigm from simple tracking to forensic-grade telematics with active security intervention.

The practical benefits of this research include measurable reductions in fuel-theft losses, improved driver and asset accountability, enhanced transparency in vehicle operations, and faster incident investigation. The proposed solution directly supports Indonesia's logistics and transportation sector, particularly operators in tamper-prone or remote areas, by ensuring data integrity and operational continuity across the fleet. Furthermore, secure and resilient

telemetry contributes to national digital-logistics modernization by addressing safety, efficiency, and supply-chain reliability. Ultimately, the proposed modular architecture offers a critical economic advantage: by eliminating the need for expensive proprietary hardware and complex wiring, the system is projected to provide a significantly lower Total Cost of Ownership (TCO) compared to legacy fleet tracking systems.

At the scientific and technological level, this research offers a unified implementation model. It combines ESP32-based embedded systems, solar-assisted autonomous power, V2X-informed communication, tamper-diagnostic algorithms, local storage based fail-safe logging, and statistical anomaly detection in a single platform. The outcomes of this study provide a foundation for future developments in resilient Internet of Vehicles (IoV) security, scalable smart-transport deployment, and standardization of tamper-resistant telematics systems in both emerging and mature fleet ecosystems.

1.6. Hypothesis

The following theories serve as the foundation for this study, which aims to evaluate the impact and efficacy of the proposed independent vehicle monitoring system:

- H₁: The proposed independent power and storage architecture ensures near-complete data continuity (high recovery rate) during power loss events, whereas standard vehicle-powered devices experience immediate data loss.
- H₂: The hardware-based tamper detection system can reliably identify and report physical disconnection and power interruption events that are typically invisible to standard vehicle-powered OBD-II trackers.
- H₃: The proposed modular hardware architecture significantly reduces the unit production cost compared to commercially available fleet telematics solutions, making it an economically viable option for large-scale logistics deployment.
- H₄: The integration of solar energy harvesting with low-power ESP32 hardware enables the system to sustain continuous autonomous operation using exclusively renewable and stored energy, independent of the vehicle's electrical system.

Importance and Potential Contributions

It is anticipated that this study will provide theoretical and practical contributions to the domains of vehicle security systems, smart transportation, and Internet of Things applications.

- For Academics: The study broadens the knowledge of how V2X technology may be successfully implemented to improve vehicle security and telemetry. It offers a resilient hardware architecture model that may be used or improved upon by future researchers investigating data integrity and offline-capable connected vehicle systems.
- For Industry: To mitigate losses from fuel theft, equipment tampering, and data manipulation, the suggested method offers fleet operators and logistics firms a viable technical solution. Future commercial systems that combine IoT devices with cloud-based fleet management tools may use this architecture as a baseline for high-security, low-cost telematics.
- For Society: This study helps create more secure and sustainable logistics networks by enhancing the accountability, transparency, and safety of transportation operations. It contributes to reducing the financial and environmental waste generated by fuel theft and inefficient fleet management.

Contribution to Knowledge

This research advances the corpus of knowledge by:

1. Demonstrating a standalone ESP32-based telemetry architecture that leverages LTE connectivity to implement robust V2I (Vehicle-to-Infrastructure) communication without relying on the vehicle's onboard computer.
2. Introducing a hybrid tamper detection mechanism that integrates physical sensor logic with software analytics for preventive security.
3. Presenting experimental evaluation data regarding the energy autonomy, data retention, and scalability of solar-assisted fleet monitoring systems.

When taken as a whole these contributions assist the continuous shift toward intelligent, connected, and secure transportation infrastructures and bolster the scholarly basis of IoT research.

