

---

## CHAPTER 2 - LITERATURE REVIEW

### 2.1. Theoretical Framework

The goal of this research is to develop an intelligent, safe, and energy-efficient vehicle telemetry and tamper-detection system by combining the ideas of the Internet of Things (IoT), Vehicle-to-Infrastructure (V2I) communication and Cyber-Physical Systems (CPS). The suggested framework creates a basis for real-time monitoring, safety, and decision-making by integrating OBD-II telemetry (leveraging the CAN bus protocol), GPS positioning, and LTE communication technologies into a unified architecture controlled by an ESP32 microcontroller.

#### 2.1.1 Internet of Things (IoT) Architecture Theory

The fundamental framework for linking embedded devices, switches, and communication modules is provided by the Internet of Things (IoT) architecture. This study adopts the standard three-layer model comprising the Perception, Network, and Application layers, but enhances it with Edge Computing principles to ensure local decision-making capabilities.

- **Perception Layer (Edge Layer):** This layer consists of the physical hardware, including the OBD-II interface, tamper switches, and the ESP32 microcontroller. Crucially, this research implements Edge Processing at this level, allowing the device to validate the data (e.g., Geofence logic) locally before transmission, reducing latency and false alarms.
- **Network Layer:** Real-time data transmission is handled exclusively via the LTE (4G) cellular interface. This layer utilizes lightweight protocols such as MQTT to ensure reliable message delivery even in low-bandwidth environments, bridging the gap between the vehicle and the cloud server.
- **Application Layer:** The final output is presented to fleet managers via cloud-based dashboards. This layer transforms raw telemetry into actionable insights, such as theft alerts, fuel consumption graphs, and historical tracking logs.

Similar to those outlined by Rahman & Singh (2020) and Chowdhury et al. (2023), this layered strategy guarantees scalability, interoperability, and modular integration; however, it is improved here with LTE-based continuous communication and cross-layer data validation.

#### 2.1.2 Vehicle Communication Network Theory (CANBUS and OBD-II)

Modern vehicle data interchange between Electronic Control Units (ECUs) relies on the Controller Area Network (CAN) protocol. This serial communication standard allows

microcontrollers and devices to communicate with each other in applications without a host computer. The OBD-II (On-Board Diagnostics) standard provides the necessary access interface to retrieve crucial real-time parameters from this network, such as engine RPM, vehicle speed, and fuel level.

This study utilizes the integrated CANBUS and OBD-II framework to implement multi-source validation. By cross-checking internal vehicle data against direct physical hardware interrupts—specifically a micro limit switch on the fuel cap, magnetic limit switches monitoring the two rear cargo doors, and a general limit switch securing the main device enclosure—the system significantly improves reliability and eliminates false alerts. This approach contrasts with previous systems examined in the literature, which frequently depended on single-source measurements that were prone to manipulation.

### ***2.1.3 Tamper Detection and Anomaly Theory***

Anomaly detection theory, which entails spotting departures from anticipated sensor or communication patterns, serves as the foundation for tamper detection in automotive systems. This study expands on the idea by including both physical tamper (fuel tank entry) and logical tamper (suspicious OBD data inconsistency). Conventional systems, such as those suggested by Kumar et al. (2019), only detected physical gasoline level reductions.

The system can effectively distinguish between theft and natural fuel usage thanks to the integration of cross-domain information.

### ***2.1.4 Cyber–Physical Systems (CPS) Model***

The proposed architecture functions as a Cyber-Physical System (CPS), characterized by the deep integration of computation, networking, and physical processes. In this model, the physical layer (vehicle dynamics, and fuel levels by the CANBUS network) is continuously monitored and interpreted by the cyber layer (the ESP32 microcontroller and cloud analytics algorithms). Unlike passive tracking devices, this CPS framework establishes a closed feedback loop. This ensures that secure data flow enables real-time monitoring and immediate local decision-making. By bridging the physical and digital domains, the model supports the system's capacity to autonomously respond to manipulation attempts or operational irregularities without waiting for human intervention.

### ***2.1.5 Energy Efficiency and Sustainability Framework***

The architecture integrates the idea of sustainable IoT deployment, utilizing solar energy and a backup battery system, since constant monitoring necessitates consistent power. This addresses a constraint observed in Ahmed et al. (2022), where systems failed during idle or parked states, and is consistent with current research in low-power IoT architecture.

---

This framework increases the dependability of vehicle surveillance systems by continuing to function when the engine is off.

## 2.2. Review of Previous Studies

Several studies have proposed IoT-based vehicle monitoring systems, but most of them address only a single function and do not combine the full set of hardware features needed for fleet-grade monitoring and fraud detection. For example, Singh et al. (2025) developed an ESP32-based crash forensics node that focuses on secure event logging and tamper-proof storage for accident analysis. While the design strengthens data integrity, it is not intended for continuous fleet telemetry and the authors note that GPS integration should be added in future work, which limits location-based validation during real operations.

Other work emphasizes communication and safety rather than hardware resilience. Tippannavar et al. (2023) proposed an IoT-enabled smart car system with V2X-enhanced communication and safety alerts. Their system demonstrates that vehicle events can be detected and alerts can be transmitted, but it does not focus on practical fleet threats such as device unplugging, switch disconnection, or maintaining operation when vehicle power is removed.

Vehicle security has also been studied through theft detection and tracking prototypes. Pushpa et al. (2025) implemented an IoT theft detection system using GPS and cellular communication to track unauthorized movement and send alerts. Although effective for theft tracking, this type of system typically does not include OBD-II telemetry, fuel monitoring, or hardware integrity checks that detect attempts to disable monitoring by unplugging or blocking modules.

Finally, several studies have integrated OBD-II with embedded controllers to support vehicle diagnostics and fleet monitoring. Smart Vehicle Diagnostics (FDRP Journals) and related OBD-II telematics approaches (Malekian et al., 2017; Anusuya & Anusuya, 2023) show that vehicle parameters can be collected and transmitted for remote monitoring. However, these systems commonly rely on continuous vehicle power and network availability, and they rarely include hardware-based tamper detection or local data saving to preserve data during internet outages. These limitations motivate the need for an integrated, power-independent hardware architecture that combines OBD-II, GPS, tamper detection, and offline storage—capabilities that are addressed in this thesis. *Table 2.1* summarizes these studies and highlights the remaining gaps.

**Table 2.1: Comparison of Previous Studies**

| Author(s)                                      | Paper Title                                                                                    | Problem Identified                                                                                                                       | Objective                                                                                                      | Methodology                                                                                                                                                                                                                 | Results & Conclusion                                                                                   | Recommendation / Research Gap                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Singh, Insa, Sharma, & Bhadani (2025)          | Vehicle Crash Forensics Node Using ESP32: A Tamper-Proof Embedded System for Accident Analysis | Post-crash evidence can be incomplete and vulnerable to alteration; traditional “black box” devices lack secure sharing and diagnostics. | Develop a tamper-resistant embedded node for crash event logging and integrity protection.                     | ESP32-based forensics node; logs crash parameters; uses SHA-256 hashing for tamper-proof storage and ESP-MESH for decentralized log validation; supports OTA log recovery; designed to operate without continuous internet. | Demonstrates feasibility of tamper-proof event logging and local/offline operation for vehicle events. | Focus is crash forensics, not continuous fleet telemetry (OBD/fuel). No solar power architecture for long-duration deployment, and no operational fraud/tamper alarms (OBD unplug, GPS block, network loss) aimed at fleet security. (This thesis adapts the “tamper-proof + offline logging” concept for fleet telemetry and tamper detection.) |
| Tippannavar, Yashwanth, Murthy, & Kumar (2023) | IoT enabled Smart Car with V2X Enhanced Communication and Safety Alert system                  | Emergency response is delayed because incidents are not detected/reported quickly.                                                       | Detect accident events and transmit alerts with location information.                                          | Hardware concept using vibration sensing + Raspberry Pi processing + GPS extraction; sends alerts to contacts (V2X/communication emphasized).                                                                               | Shows that sensor-triggered alerting with GPS location is practical for safety notification.           | Does not address fleet fraud or telemetry integrity. No device-integrity monitoring (tamper), no OBD-II/fuel telemetry, no local data saving fallback logging, and no power-independent (solar + battery) design for continuous operation.                                                                                                       |
| Pushpa et al. (2025)                           | Design and Implementation of an IoT-Enabled Smart Vehicle Theft Detection and Tracking System  | Vehicle theft requires real-time tracking and fast owner notification.                                                                   | Detect theft attempts and send immediate alerts with vehicle location; enable local alarm and remote response. | Arduino UNO + GPS (NEO-6M) + GSM (SIM800L) with vibration sensor, ignition status detection, and accelerometer; SMS alerts include coordinates; buzzer alarm; tested under simulated theft conditions.                      | Reports high detection performance and average alert latency below ~4 seconds in simulations.          | Strong theft alerting, but not designed for fleet telemetry integrity: no OBD-II data validation, no fuel monitoring, no solar-powered backup, and no local storage for internet outages. Limited emphasis on detecting “monitoring-device tampering” (e.g., unplugging OBD/GPS to hide fraud).                                                  |
| Fifth Dimension Research Publication           | Smart Vehicle Diagnostics: Integrating OBD-II and                                              | Maintenance is often reactive; vehicle health                                                                                            | Promote real-time health monitoring by combining                                                               | Describes cloud-based monitoring and logging of vehicle parameters                                                                                                                                                          | Supports the value of real-time monitoring                                                             | Weak on hardware security and resilience: no tamper detection (OBD                                                                                                                                                                                                                                                                               |

|                        |                                                                        |                                                                                    |                                                                                                               |                                                                                                                                                                                            |                                                                                              |                                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (2024)                 | Cloud Technology for Enhanced Health Monitoring                        | data is not continuously available for decision-making.                            | OBD-II data with cloud-based monitoring.                                                                      | with API and integration and dashboards; emphasizes continuous monitoring and historical logging (cloud).                                                                                  | and logging for fleet operations and diagnostics.                                            | unplug, wiring cut), no offline logging during network loss, and no independent power strategy for continuous telemetry when vehicle power is unavailable.                                                                                                                                         |
| Malekian et al. (2017) | Design and Implementation of a Wireless OBD II Fleet Management System | Fleets need speed/distance/fuel estimation with tracking and remote visualization. | Design an OBD-II fleet system that reads ECU data, computes fuel usage, and transmits to a server with a GUI. | OBD-II reader collects speed + MAF; computes distance and fuel consumption; adds GPS; transmits via Wi-Fi to remote server/database; GUI for visualization; qualification tests performed. | Demonstrates successful parameter acquisition, computation, transmission, and visualization. | System depends on connectivity and does not address physical tampering/disconnection or adversarial manipulation. No solar/battery continuity, and no local data saving logging. This thesis extends the fleet-telemetry idea with tamper alarms, anomaly detection, and power/network resilience. |

### 2.3. Research Gap and Novelty

Based on the reviewed studies, several critical limitations were identified. Most existing systems depend entirely on vehicle power, meaning they cease operation immediately if unplugged. Furthermore, many solutions lack hardware-level tamper detection and rely heavily on continuous cloud connectivity, resulting in significant data loss when the network is unavailable.

The novelty of this research lies in the integration of these missing features into a single, unified system. The proposed architecture combines ESP32-based telemetry with a solar-powered independent energy source, hardware tamper detection, and local data storage. Unlike previous studies, this system ensures continuous operation even when vehicle power is cut or network connection is lost, making it a significantly more resilient solution for real-world fleet logistics.