

CHAPTER 3 -RESEARCH METHODOLOGY

3.1. Research Design

This research uses a quantitative and experimental approach which focuses to design, build and test on IoT-based smart vehicle telemetry and tamper detection systems. Since the performance of the proposed system is assessed using numerical data such as vehicle speed, fuel usage, location accuracy, alert response time and data transmission success rate, a quantitative method is the most suitable approach for this study.

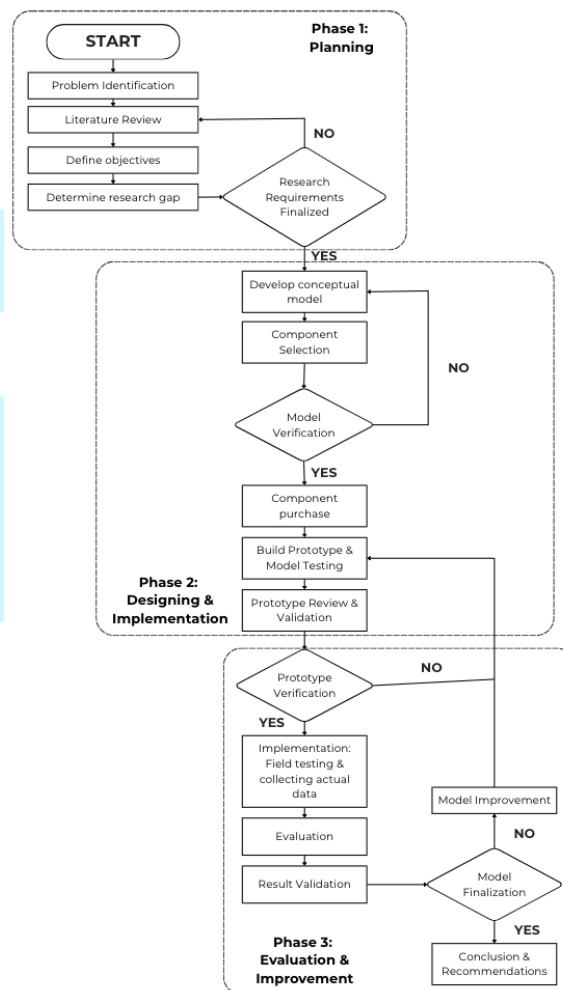


Figure 3.1: Research Framework

As shown in *Figure 3.1*, this research framework illustrates three major phases: planning, design and implementation and evaluation and improvement. During the planning phase, the research problem was identified through observations of fleet monitoring limitations in Indonesia, followed by an extensive review of related literature on IoT, vehicle telematics, IBD-II systems, tamper detection and V2X communication. Based on this review, the research objectives and existing research gaps are defined.

In the design and implementation phase, a complete system architecture was developed, which includes the hardware integration, firmware development, data flow and logic design and communication architecture. A functional prototype is then built using an ESP32 microcontroller integrated with GPS, LTE/V2X communication, OBD-II telemetry, local storage and tamper detection switches.

In the evaluation and improvement phase, the prototype was deployed on a test vehicle for real-world field testing. Telemetry performance, anomaly detection accuracy, tamper detection reliability and data transmission stability will be evaluated. The system will then be refined based on the test results and re-tested before final validation.

3.2. Data Collection Methods

This study uses experimental and hardware-based data collection methods derived from direct system testing and real-world vehicle operation. The research focuses on evaluating physical system performance, switch reliability, power continuity, and tamper detection, rather than user perception or software usability. All data is collected directly from the prototype hardware through physical tamper switches, OBD-II telemetry extraction, electrical measurements, and system logs during field testing.

3.2.1 Experimental Telemetry Data Collection

Telemetry data is collected using the ESP32-based smart vehicle monitoring device installed on a test vehicle. The collected parameters represent core hardware outputs required to evaluate system functionality and stability, including:

- Vehicle speed (from OBD-II) Engine RPM and other diagnostic parameters (from OBD-II)
- GPS location (latitude, longitude)
- Date and time stamps
- Network connectivity status (LTE available or unavailable and signal strength)
- Network Communication Metadata (Total packets generated, packets successfully received by the cloud, and exact transmission timestamps to measure system latency)

All telemetry data is:

1. Stored locally on the ESP32's internal flash memory when internet connectivity is unavailable
2. Data is transmitted wirelessly when connectivity is available for backup and validation purposes

3.2.2 Tamper and Anomaly Data Collection

Tamper and anomaly data are collected by intentionally introducing controlled physical and electrical disturbances to the system during testing. These scenarios simulate real-world tampering conditions commonly encountered in fleet operations. These simulations include:

- OBD-II disconnection detection
- GPS signal loss
- Enclosure opening or wiring interruption (tamper switches)
- Abnormal fuel usage behaviour
- Network signal loss

Each event is automatically recorded by the system with:

5. Event type
6. Time and date stamp
7. Associated sensor readings
8. Power and communication status at the time of occurrence

These records are stored on the ESP32's internal flash memory and transmitted to the cloud when connectivity is available.

3.2.3 Field Observation and System Log Collection

Field testing is conducted under normal driving and stationary vehicle conditions. The researcher observes system behavior such as:

- Accuracy of GPS tracking
- Stability of OBD-II readings
- System response to tamper events
- Reliability of tamper detection

All observations are supported by:

- System log files from the ESP32's internal flash memory
- Cloud database records
- Fleet dashboard alert history

3.2.4 Testing Procedure

The data collection procedure follows these steps:

- Install the prototype device on the test vehicle
- Power on the system and verify hardware module initialization
- Conduct preliminary bench testing using an OBD-II to verify hardware communication, power logic, and network stability before full vehicle deployment
- Operate the vehicle under normal conditions to collect baseline data
- Introduce controlled tamper and fault conditions
- Allow the system to detect, log, and store each event
- Restore normal operating conditions
- Retrieve stored data from local storage and communication logs for analysis

3.3. Data Analysis Techniques

This study applies quantitative hardware-oriented analysis techniques to evaluate the performance, reliability, and robustness of the proposed solar-powered vehicle telemetry and tamper detection system. The analysis focuses on electrical behavior, switch stability, power continuity, tamper detection reliability, and data retention, rather than cloud-based analytics or user-interface performance.

3.3.1 Power consumption and Energy Analysis

Power consumption is evaluated to determine system feasibility and autonomy. Voltage and current measurements are recorded during different operating states, including idle, active sensing, data logging, and communication events.

1. Daily Current and Power Consumption:

To account for the system's operational duty cycle, the total daily current drawn ($I_{Total-Daily}$) is calculated by separating the active hours from the sleep hours:

$$I_{Total} = (I_{Active} \times T_{Active}) + (I_{Sleep} \times T_{Sleep}) \quad (3.1)$$

The average current drawn over a standard 24-hour period (I_{avg}) is then calculated as:

$$I_{avg} = \frac{I_{Total}}{24h} \quad (3.2)$$

Using the nominal system voltage (V), the continuous average power consumption (P) is:

$$P = V \times I_{avg} \quad (3.3)$$

2. Energy Autonomy and Battery Capacity:

The total energy required to run the system for a complete 24-hour cycle ($E_{1\text{ day}}$) is:

$$E_{1\text{ day}} = P \times 24\text{h} \quad (3.4)$$

To ensure continuous fleet monitoring during severe weather or extended parking, the system is designed with a multi-day autonomy target ($Days$). The total autonomy energy requirement ($E_{Battery}$) is:

$$E_{autonomy} = E_{1\text{ day}} \times Days \quad (3.5)$$

A minimum operational target of two days without external charging is adopted ($Days = 2$), so that the system remains active through extended parking or prolonged low-sunlight periods during which solar recharging may be insufficient. Substituting this two-day target into the expression above, the required autonomy energy is twice the single-day demand:

$$E_{autonomy} = E_{1\text{ day}} \times 2 \quad (3.6)$$

To ensure the longevity and health of the Lithium-Ion cells, the system must not be drained to absolute zero. Factoring in a safe Depth of Discharge (DoD), the true required battery energy capacity ($E_{Battery}$) is calculated:

$$E_{Battery} = \frac{E_{autonomy}}{DoD} \quad (3.7)$$

The minimum required battery capacity ($C_{Battery}$) to sustain this target is:

$$C_{Battery} = \frac{E_{autonomy}}{V_{nominal}} \quad (3.8)$$

3. Solar Panel Sizing:

The solar charging architecture must be capable of sustaining the daily load while simultaneously recharging the total autonomy deficit within a single day. Accounting for a standard system loss factor (L) to accommodate charge controller inefficiencies and environmental variables, the target energy generation is calculated. Using regional Peak Sun Hours (PSH), the required solar panel wattage (P_{Solar}) is:

$$P_{Solar} = \frac{E_{Battery}}{PSH \times L} \quad (3.9)$$

Where:

5. V = supply voltage (V)
6. I_{Total} = total current drawn by the system over a full cycle (Ah)
7. I_{avg} = average continuous current drawn per hour (A)
8. P = average continuous power consumption (W)
9. I_{Active} = current draw during transmission/sensing (A)
10. I_{Sleep} = current draw during low-power mode (A)
11. T_{Active} = total hours spent in active mode per day (h)
12. T_{Sleep} = total hours spent in sleep mode per day (h)
13. $Days$ = target number of days for system autonomy without power input
14. $E_{1\ day}$ = total energy required to operate the system for one complete day (Wh)
15. $E_{autonomy}$ = energy required to sustain the system for the target autonomy period (Wh)
16. $C_{Battery}$ = battery capacity (Ah)
17. $V_{nominal}$ = Nominal battery voltage (V)
18. P_{Solar} = required solar panel wattage to sustain and recharge the system (W)
19. PSH = Peak Sun Hours available per day in the deployment region (h)
20. L = power loss from the solar panel due to vehicle shading and motion, soiling and dirt, high temperature, electrical loss, and flat mounting. (%)

These calculations evaluate whether the solar-assisted battery system can sustain continuous operation.

3.3.2 Tamper Detection Performance Analysis

Tamper detection reliability is evaluated by measuring how accurately and consistently the system identifies intentional interference.

Detection accuracy is calculated as:

$$Detection\ Rate\ (\%) = \frac{N_{detected}}{N_{events}} \times 100 \quad (3.10)$$

False alarms are evaluated using:

$$\text{False Alarm Rate (\%)} = \frac{N_{false}}{N_{alerts}} \times 100 \quad (3.11)$$

Response time to tamper events is calculated as:

$$T_{response} = T_{alers} - T_{event} \quad (3.12)$$

3.3.3 Data Validation and Communication Reliability

To thoroughly assess the system's ability to maintain data continuity over LTE, validation focuses on network reliability, transmission delay, and long-duration stability.

Packet Delivery Ratio (PDR):

$$PDR (\%) = \frac{N_{received}}{N_{generated}} \times 100 \quad (3.13)$$

To evaluate the reliability of the V2X communication, the PDR measures the percentage of telemetry packets successfully received by the cloud server compared to the total number of packets generated by the ESP32.

System Latency (L_{sys}):

$$L_{sys} = T_{dashboard} - T_{event} \quad (3.14)$$

To ensure tamper alerts are effective for real-time fleet security, the end-to-end latency from the moment a physical tamper event occurs (e.g., limit switch trigger) to the moment the alert appears on the dashboard is measured using synchronized UNIX epoch timestamps.

The effectiveness of local storage is measured using:

$$\text{Data Recovery Rate (\%)} = \frac{D_{uploaded}}{D_{stored}} \times 100 \quad (3.15)$$

This metric verifies that telemetry and event data are preserved even when communication is unavailable.

3.3.4 Time-Series Behavior Analysis

Time-series analysis is used to observe trends and abrupt changes in system behavior over time, including:

- Fuel usage versus time
- Power consumption versus time
- GPS signal availability versus time

3.4. Required Materials and Equipment

This research required various hardware components, power management modules, sensing devices, and supporting laboratory equipment to design, implement, and evaluate the proposed IoT-based vehicle telemetry and tamper detection system. The selected components were chosen based on their compatibility with LTE-based communication, low-power embedded operation, telemetry reliability, and suitability for deployment within the Indonesian logistics environment.

The system architecture integrates ESP32-based embedded processing, LTE cellular communication, OBD-II telemetry acquisition, local data logging storage, independent battery power, and physical tamper-detection switches into a unified monitoring platform. Supporting laboratory instruments were additionally utilized during prototyping, calibration, and electrical validation to ensure system stability and operational reliability.

The following sections describe the primary hardware components, supporting equipment, and hardware configuration utilized throughout this study.

3.4.1. Hardware Components

Table 3.1: Hardware Components

Component	Function
Main ESP32-C3 (Telemetry & Security Node)	The central microcontroller responsible for LTE communication, local data recording, power-management logic, and monitoring all physical tamper-detection switches.
SIM7600G LTE and GPS Module	Provides GPS and 4G LTE cellular communication for telemetry transmission, tamper alerts, and cloud synchronization using standard mobile-network infrastructure available throughout Indonesia.
1S3P Lithium-Ion Battery Pack	Provides independent backup power storage. Configured in a 1-series, 3-parallel (1S3P) arrangement to maximize current

	capacity and maintain continuous system operation during vehicle power loss.
Solar Charger Module (CN3791 MPPT))	Regulates charging current and voltage from the solar panel to the battery system while preventing overcharging and maintaining stable energy distribution.
Solar Panel	Supplies renewable energy to recharge the battery pack and support autonomous long-term system operation.
Battery Management System (BMS)	Protects the lithium-ion battery pack against overcharging, overcurrent, short circuit, and excessive discharge conditions.
DC-DC Step-Up Boost Converter (XL6009)	Regulates and boosts battery voltage to ensure stable power delivery to the ESP32 and LTE communication module.
TP5100 Battery Charger Module	Provides controlled charging management for lithium-ion battery cells from the OBD2 integration.
Magnetic Limit Switches (Cargo Doors)	Contactless magnetic sensors installed on rear cargo doors to continuously monitor secure closure and trigger alerts during unauthorized access.
Micro Limit Switches	Mechanical tamper-detection switches used to detect unauthorized opening or physical disconnection of monitored components such as the OBD-II interface, enclosure system, and fuel cap.

3.4.1.1 Communication Module Selection Rationale

The initial system architecture was designed using NB-IoT and Cat-M1 communication technologies using SIM7080G due to their low power consumption and suitability for IoT applications. These protocols are commonly used in lightweight telemetry systems because they offer reduced energy requirements and efficient low-bandwidth communication.

However, there were several practical limitations for implementation within the Indonesian logistics environment. NB-IoT and Cat-M1 infrastructure coverage remains limited in many regions of Indonesia, particularly outside major urban areas. Additionally, deployment often requires enterprise-level registration and direct coordination with cellular network providers, reducing practicality for scalable fleet implementation and real-world testing.

To improve the feasibility and communication reliability, the architecture was revised to utilize the SIM7600G 4G LTE communication module. Unlike NB-IoT and Cat-M1 solutions, the SIM7600G operates using standard LTE cellular infrastructure and conventional

SIM-card networks, similar to regular mobile-phone communication. This enables broader network compatibility, easier deployment, and more reliable real-time telemetry transmission across Indonesian transportation routes.

Although the LTE-based architecture introduces higher power consumption and increased hardware cost compared to low-power technologies, it significantly improves real-world usability, communication availability, and operational flexibility. Consequently, additional firmware-level power optimization techniques were implemented to maintain long-term autonomous operation.

Table 3.2: Comparison Between Initial and Final Communication Architecture

Parameter	Initial Design (SIM7080G NB-IoT/Cat-M1)	Final Design (SIM7600G LTE)
<i>Network Type</i>	NB-IoT/Cat-M1	4G LTE
<i>Infrastructure Availability in Indonesia/Fleet Scalability</i>	Limited by network support	Widely Available. Easier large-scale
<i>SIM Deployment Requirement</i>	Requires provides registration	Standard SIM
<i>Power consumption</i>	Low (~ 0.1 A)	Higher than initial design (~ 0.33 A)
<i>Data Transmission Speed</i>	Lower	Higher than initial design
<i>Hardware Cost</i>	Rp 1, 242, 940 (Cost breakdown in appendix)	Rp 1,481,750 (Cost breakdown in appendix)

The prototype hardware comparison analysis in *Table 3.2* demonstrates that the proposed system can be implemented using commercially available and relatively low-cost embedded components. Despite the inclusion of LTE communication hardware and autonomous power infrastructure, the overall prototype cost remains significantly lower than many commercial fleet telematics systems, supporting the economic feasibility of the proposed architecture for future large-scale deployment.

3.4.2. Supporting Equipment

Table 3.3: Supporting Equipment

Equipment	Purpose
Multimeter	Measures voltage and current during hardware testing.
Bench Power Supply	Provides controlled power during prototyping and debugging.
Wiring and Enclosure	Ensures secure electrical connections and tamper-resistant installation.
OBD-II / CAN Bus Node	Getting vehicle data (Speed, RPM, Fuel Level ...etc) for bench testing the ESP32 logic.
Current Sensor Module	Utilized strictly during the testing and calibration phase for high-precision logging of solar yield and system power consumption. It enabled accurate profiling of the current draw and total energy consumed (Ah) to experimentally validate the system's energy budget.
Oscilloscope	Used to display real-time graphs of the system's electrical activity, specifically monitoring the modem's power draw and the physical switch triggers.
Battery Voltage Sensor (Percentage IC)	To monitor the voltage of the battery over time (Charge and Discharge) to get accurate data specifically between 40% to 70%

3.4.3. Hardware Schematic and Pin Configuration

To ensure reliable communication and switch data acquisition, the system utilizes a distributed dual-node architecture. The hardware components are mapped to their respective microcontrollers according to the pin configuration outlined in Table 3.4.

Table 3.4: Main ESP32-C3 (Telemetry & Security Node) Pin Configuration

Component / Module	Data / Signal Pin (ESP32-C3)	Power & Ground Connections	Operational Notes
SIMCom LTE Modem	RX: Pin 19 TX: Pin 18 Power Key (K): Pin 4	VCC: + Source GND: Common Ground	The 'K' pin is utilized for hardware-level wake-up commands to exit deep sleep.
Micro Limit Switch (Fuel Cap)	Signal: Pin 3	GND: Common Ground	Physical tamper detection
Micro Limit Switch (Case Enclosure)	Signal: pin 2	GND: Common Ground	Physical tamper detection
Magnetic Limit Switch 1 (Cargo Door)	Signal: Pin 1	GND: Common Ground	Cargo-door tamper monitoring
Magnetic Limit Switch 2 (Cargo Door)	Signal: Pin 10	GND: Common Ground	Cargo-door tamper monitoring

3.4.4. Bill of Materials (BOM)

A complete Bill of Materials (BOM) for the final hardware prototype is presented in Table 3.5. The BOM enumerates every electronic component, module, and supporting part integrated into the deployed device, together with its specification, quantity, unit price, and extended cost. As detailed in Table 3.5, the total component cost of the final prototype amounts to Rp1,481,750, confirming that the proposed telemetry unit can be assembled at a small fraction of the cost of the commercial fleet-tracking solutions evaluated in Section 4.6.

Table 3.5: Bill of Materials (BOM) for the Final Hardware Prototype

No .	Component	Specification	Qty	Unit Price (Rp)	Total Price (Rp)
1	ESP32-C3	Mini DevKitM WiFi Bluetooth	1	Rp 48,500	Rp 48,500
2	Micro Limit	Micro Limit Switch	2	Rp 3,500	Rp 7,000

	Switch				
3	Magnetic Limit Switch	MC-38	2	Rp 7,500	Rp 15,000
4	Solar Charger Module	CN3791 6V	1	Rp 38,000	Rp 38,000
5	Battery Holder	3 Parallel	1	Rp 14,000	Rp 14,000
6	Solar Panel	Monocrystalline 6W 6V	1	Rp 89,000	Rp 89,000
7	18650 Batteries	3000mAh	3	Rp 75,000	Rp 225,000
8	BMS	1S 15A	2	Rp 8,000	Rp 16,000
9	SIM7600G	4G LTE	1	Rp 985,000	Rp 985,000
10	DC-DC Step Up Boost Converter	XL6009	1	Rp 26,000	Rp 26,000
11	Battery Charger	TP5100	2	Rp 9,125	Rp 18,250
TOTAL			17	Rp 1,481,750	

3.5. Firmware & System Logic Design

3.5.1 Inter-Node Communication Architecture

To maintain a secure data pipeline and isolate the vehicle's internal network from the external cellular module, the system utilizes a distributed dual-node architecture. The Secondary ESP32, located near the OBD-II port, acts as a dedicated sensor node. It continuously polls the vehicle's CAN Bus via the MCP2515 module. Once the engine telemetry (such as Speed, RPM, Fuel Level, and Engine Temperature) is parsed, it is securely transmitted to the Main ESP32-C3 Security Node using ESP NOW feature. The Main ESP32-C3 then aggregates this vehicle telemetry with the local physical tamper sensor data before executing the final data logging and LTE transmission to the cloud dashboard.

3.5.2 Dynamic Power Management and Self-Healing Logic

To achieve the target power consumption of 330mA at 5V during active states and ensure long-term autonomy, several firmware-level optimizations were implemented on the Main ESP32-C3:

- **Deep Sleep & Interrupts:** The microcontroller enters a low-power deep sleep when the vehicle is idle. It utilizes the physical limit switches as active hardware interrupts for instantaneous wake-up during tamper events, and leverages module-level interrupts

to wake the system upon detecting vehicle movement (GPS location changes) or engine activity (OBD-II speed changes).

- **Dynamic Resource Scaling:** CPU frequency is scaled down to minimize power draw, and data packets are dynamically sized to prevent the transmission of empty payloads.
- **Modem State Management:** The modem retains GNSS satellite data before entering sleep mode. This "hot-start" capability ensures an immediate connection upon waking, conserving the energy typically spent searching for a new signal, provided the satellites are still available.
- **Auto-Reboot Watchdog:** A self-healing watchdog monitors the modem's responsiveness, triggering an automatic hardware reset if it freezes.



3.6. Operational Flow of the Proposed System

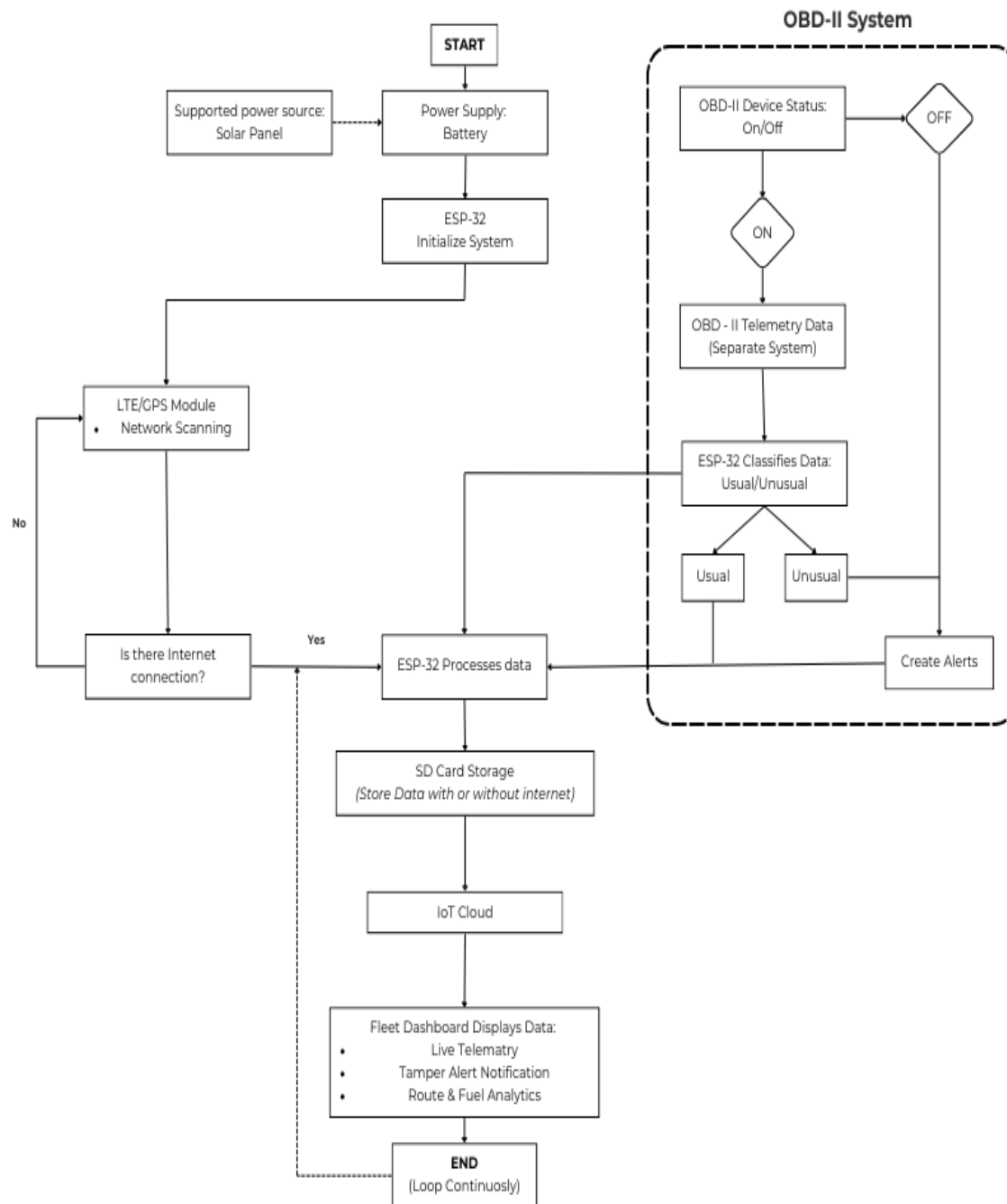


Figure 3.2: Proposed System Flowchart

Figure 3.2 presents the system operation flowchart of the proposed ESP32-based smart vehicle telemetry and tamper detection system.