

**DEVELOPMENT OF AN IOT-ENABLED, AI CHATBOT-ASSISTED SMART
VEHICLE TELEMETRY, GPS TRACKING, FUEL INTEGRITY MONITORING,
AND OBD-II TAMPER DETECTION SYSTEM USING ESP32, CELLULAR IOT,
AND V2X COMMUNICATION ARCHITECTURE**

By

Monzer Tarig Abdalla Mohamedahmed
12101025

BACHELOR'S DEGREE
in

MECHANICAL ENGINEERING – MECHATRONICS CONCENTRATION
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

23 June, 2026

STATEMENT BY THE AUTHOR

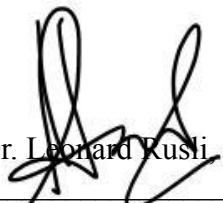
I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Monzer Tarig Abdalla Mohamedahmed

Student


23 June 2026
Date

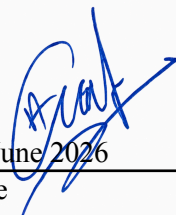
Approved by:


Dr. Leonard Rusli, Ph.D.,
Thesis Advisor

23 June 2026
Date

Hartono, S.T., M.T.

Thesis Co-Advisor


23 June 2026
Date

Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc.

Dean

Date

Monzer Tarig Abdalla Mohamedahmed

ABSTRACT

By

Monzer Tarig Abdalla Mohamedahmed

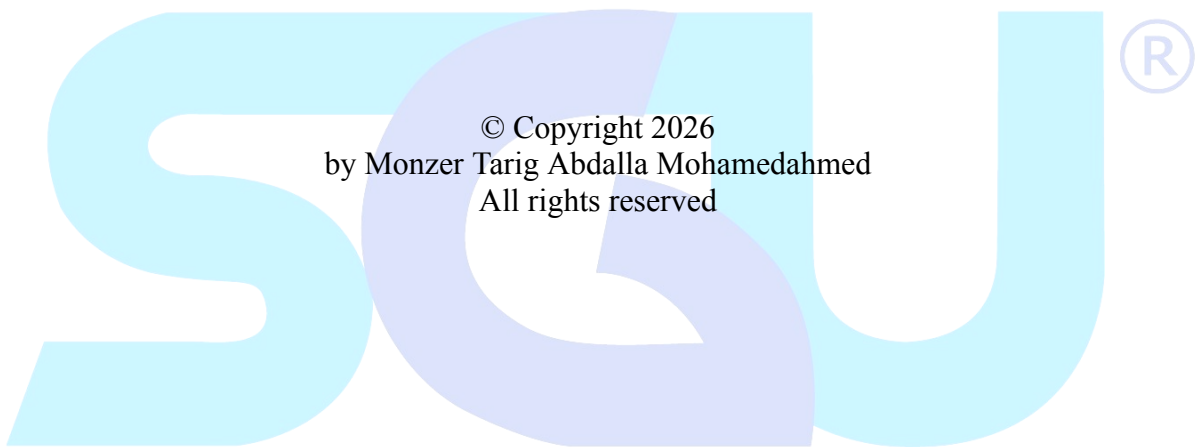
Prof. Dr. Leonard Rusli, Ph.D.

SWISS GERMAN UNIVERSITY

Indonesia's USD 67.8 billion logistics sector, operating across 17,000 islands, faces growing losses from fuel theft, equipment tampering, and unreliable vehicle telemetry, problems that conventional GPS- and OBD-II-based monitoring cannot solve because such systems are easily disconnected, manipulated, or disrupted by poor connectivity in remote corridors. This study addresses how an IoT-based system can deliver reliable tamper detection and actionable fleet intelligence under these adversarial, connectivity-constrained conditions. Following a quantitative design-build-test-refine methodology, a smart telemetry and tamper-detection system was developed and field-tested on a commercial vehicle along the Tangerang–Alam Sutera corridor, South Tangerang, Banten. The system integrates an ESP32-C3 microcontroller with OBD-II, GPS, and LTE connectivity, dual differential fuel flow sensors, multi-modal tamper detection, offline data storage, solar-assisted power, and a Gemini API-driven AI layer that runs independently of vehicle ignition, supported by real-time behavior classification, natural-language driver coaching, and dual-channel alerts via dashboard and Telegram. Testing confirmed accurate fuel theft detection, classification of 295 behavioral events with zero false positives, AI driver profiling at 97–88% confidence, telemetry ingestion at 290-microsecond latency with 99.99% cache hit rate, and AI-generated fleet reports delivered within two minutes via Telegram, showing that combining multi-modal IoT sensing, edge intelligence, and generative AI in one low-cost architecture significantly improves telemetry reliability and fleet decision-making in Indonesia's logistics sector.

Keywords: Internet of Things (IoT); Driver Behavior Monitoring, Fleet Management, Indonesian Logistics.

Monzer Tarig Abdalla Mohamedahmed



© Copyright 2026
by Monzer Tarig Abdalla Mohamedahmed
All rights reserved

DEDICATION

This thesis is dedicated to the beloved nation of Indonesia, in the hope that this work may contribute, however modestly, to its future progress and prosperity.



ACKNOWLEDGEMENTS

The author wishes to express profound gratitude to Dr. Leonard Rusli, Ph.D., for his invaluable guidance, insightful advice, and continuous support throughout the preparation and completion of this thesis. His constructive feedback and encouragement have significantly contributed to the quality and success of this work.

The author also extends sincere appreciation to the lecturers and staff of the Faculty of Engineering and Information Technology, Swiss German University, for their academic guidance, assistance, and the facilities provided during the course of this study.

Finally, the author conveys heartfelt thanks to his family and friends for their unwavering support, understanding, and motivation throughout the research and writing process.

TABLE OF CONTENTS

STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	4
ACKNOWLEDGEMENTS	6
CHAPTER 1 - INTRODUCTION	15
1.1 Background	15
1.1.1 The Connected Vehicle Imperative	15
1.1.2 Fleet Security Vulnerabilities in Connected Telemetry Systems	16
1.1.3 The Indonesian Logistics Context	17
1.1.4 Research Motivation and System Overview	18
1.1.5 Market Gap and System Uniqueness	19
1.2 Problem Statement	20
1.3 Research Objectives	21
1.4 Research Questions	22
1.5 Scope and Limitations	23
1.6 Significance of the Study	23
1.7 Hypothesis	24
CHAPTER 2 - LITERATURE REVIEW	25
2.1 Theoretical Framework	25
2.1.1 Internet of Things (IoT) Architecture Theory	26
2.1.2 Vehicle Communication Network Theory (CAN bus and OBD-II)	26
2.1.3 Cyber-Physical Systems (CPS) Model	28
2.1.4 Energy Efficiency and Sustainability Framework	28
2.2 Review of Previous Studies	29
2.3 Research Gap and Novelty	32

2.3.1 From Connected Telemetry to Stagnant Architectures	32
2.3.2 Architectural Gap: Cloud Dependence and Latency	33
2.3.3 Methodological Gap: Fuel Theft and Tamper Detection	35
2.3.4 Anomaly Detection and Cloud Integration Gap	36
2.3.5 Connectivity and Security Gap: Practical V2X and Hardening	37
2.3.6 Synthesis: From Passive Logging to Smart Edge Telemetry	38
CHAPTER 3 - RESEARCH METHODOLOGY	39
3.1 Research Design	39
3.2 Data Collection Methods	41
3.2.1 Telemetry and Navigation Data	41
3.2.2 Fuel Integrity and Tamper Data	42
3.2.3 Experimental Procedures	42
3.2.4 Driver Behavior Monitoring Data	43
3.3 Data Analysis Techniques	44
3.3.1 Pre-processing and Signal Processing	44
3.3.2 Metric Computation	47
3.3.3 AI-Assisted Behavioral Interpretation via Gemini API and Structured Prompt Engineering	47
3.3.4 Rule-Based Driver Behavior Event Classification	48
3.3.5 Latency-Optimised AI Query Routing	56
3.3.6 AI Integration Architecture Design	58
3.3.7 Dual-Channel AI Delivery Architecture	60
3.4 Required Materials and Equipment	61
3.4.1 Component Selection Justification	64
3.4.2 Client-Side WebAssembly Database Architecture	66
3.5 Timeline	69

CHAPTER 4 - SYSTEM IMPLEMENTATION, RESULTS, AND EVIDENCE	70
4.1 Overview	70
4.2 System Implementation and Component Verification	70
4.2.1 Dashboard Implementation Evidence	70
4.3 Field Experiments, Results, and Performance Evaluation	82
4.3.1 Overview of Testing Approach	82
4.3.2 Scenario A Results	82
4.3.3 Scenario B: Fuel Integrity Monitoring: System Design Validation	84
4.3.4 Scenario C Results (Tamper Detection and Communication Resilience)	85
4.3.5 AI-Assisted Analytics Results — Gemini API Performance Evidence	95
4.3.6 Driver Behavior Detection Results	97
4.3.7 Extended Field Validation: Live System Operation Evidence	99
4.3.7.1 Real-Time Driver Behavior Classification and OBD-II Monitoring	99
4.3.7.2 AI Intelligence Driver Profiling — Comparative Analysis	105
4.3.7.3 Fuel Theft Detection and Real-Time Alert Generation	115
4.3.7.4 Geofencing and Zone Boundary Monitoring	120
4.3.7.5 AI Analyst Chat Interface — Live Query Validation	123
4.3.8 Summary of Extended Validation Results	126
4.3.9 Cloud Infrastructure Performance and Backend Validation	127
4.3.9.1 Telegram Bot Fleet Report Generation	128
4.3.9.2 PostgreSQL Database Performance Validation	132
4.3.9.3 Server Resource Utilization and Network Performance	134
4.3.9.4 Summary of Cloud Infrastructure Validation	137
4.3.10 Summary of Testing Results	138
4.4 Analysis, Discussion, and Key Findings	140
4.4.1 Discussion of Results Against Research Questions	140

4.4.2 Evaluation Against Research Hypothesis	144
4.4.3 Key Findings Summary	145
4.4.4 Limitations and Recommendations for Future Work	146
4.5 Chapter Summary	147
CHAPTER 5 - CONCLUSIONS AND RECOMMENDATIONS	148
5.1 Conclusions	148
5.1.1 The System Demonstrates Operational Feasibility Under Real-World Conditions	149
5.1.2 Driver Behavior Monitoring and AI Profiling Are Validated and Operationally Effective	149
5.1.3 Fuel Theft Detection and Tamper Alerting Are Operationally Active	150
5.1.4 The Geofencing and Zone Monitoring Capability Is Validated	151
5.1.5 The Cloud Backend Is Efficient, Scalable, and Supports Advanced Reporting	151
5.1.6 The System Addresses the Research Gap Identified in Chapter 2	152
5.2 Recommendations	153
5.2.1 Recommendations for Future Research	153
5.2.2 Recommendations for Logistics Operators Considering Adoption	154
5.2.3 Recommendations for Technology Developers Pursuing Commercialization	155
5.3 Closing Statement	157
REFERENCES	158
APPENDICES	162

LIST OF FIGURES

Figure 2.1 : Theoretical Framework for Vehicle Telemetry and Tamper-Detection Architecture	25
Figure 3.1 : Research Framework: Four-Stage Design–Build–Test–Refine Methodology	40
Figure 3.2 : End-to-End Data Collection Architecture	41
Figure 3.3 : Fuel Theft Detection Algorithm Flowchart	45
Figure 3.5 : AI-Assisted Behavioral Analysis Pipeline	49
Figure 3.6 : Four-Layer Prompt Engineering Architecture for Driver Behavior Analysis	51
Figure 3.7 : Dashboard Safety Score Trend Chart Design	54
Figure 3.8 : Driver Behavior Event Frequency Breakdown Chart Design	55
Figure 3.9 : AI Integration Logic Architecture	59
Figure 3.10 : Project Timeline (Gantt Chart)	69
Figure 4.1 : SGU Dashboard GPS Tracking View — Field Testing	71
Figure 4.2 : SGU Dashboard Analytics View — Live OBD-II Readings	73
Figure 4.3 : SGU Dashboard Sensor Reports and AI Analyst Panel	74
Figure 4.4 : SGU Dashboard Offline Storage Retrieval View	77
Figure 4.5 : SGU Dashboard Orders Management View	79
Figure 4.6 : SGU Dashboard Drivers Management View	80
Figure 4.7 : Driver Details Panel — Live OBD-II and Behavior Events	81
Figure 4.8 : SGU System Alerts Panel — Door and Storage Tamper Events	85
Figure 4.9 : SGU Vehicle Telemetry Unit — Enclosure Open State and Tamper Switch	87
Figure 4.10 : SGU Analytics View — ESP-NOW to LTE Dual-Device Integration Test	89
Figure 4.11: Telegram Bot — Live Telemetry Snapshot and AI Responses	91
Figure 4.12: Telegram Bot	92
Figure 4.13 : Real-Time OBD-II Panel — High-Risk Trip (Surabaya–Malang)	100

Figure 4.14 : Real-Time OBD-II Panel — Low-Risk Trip (Jakarta–Bekasi)	101
Figure 4.15 : Driver Behavior Score Panel — Weekly Trend and Classification	102
Figure 4.16 : Behavior Events Panel — Discriminative Classification Output	103
Figure 4.17 : Complete Behavioral Event Log — Driver Daniel Cooper	104
Figure 4.18 : Alert Event Detection Frequency by Category and Severity	105
Figure 4.19 : AI Intelligence Profile — High-Risk Driver	106
Figure 4.20 : AI Intelligence Profile Continuation — High-Risk Driver	107
Figure 4.21 : AI Predictions Panel — High-Risk Driver	108
Figure 4.22: AI Intelligence Profile — Efficient Driver Benchmark	109
Figure 4.23: AI Intelligence Profile Continuation — Efficient Driver	110
Figure 4.24 : documents the maintenance and operational dimensions.	111
Figure 4.25 : AI Predictions Panel — Efficient Driver	111
Figure 4.26 : Radar Chart — High-Risk vs. Efficient Driver Behavioral Comparison	112
Figure 4.27: Grouped Bar Chart — AI Intelligence Metrics Comparison	113
Figure 4.28 : PostgreSQL Query Volume and Latency Chart	114
Figure 4.29 : Dashboard Fuel Theft Alert — Active THEFT Status	115
Figure 4.30 : Dashboard Fuel Theft Alert — Second Session	116
Figure 4.31 : Drivers Management View During Active Theft Event	118
Figure 4.32 : Behavior Events Panel During Fuel Theft Session	119
Figure 4.33 : GPS Tracking View — Vehicle Inside Geofence Zone	120
Figure 4.34 : GPS Tracking View — Vehicle Outside Geofence Zone	121
Figure 4.35 : AI Analyst Chat Interface — Natural-Language Query Responses	123
Figure 4.36 : Sensor Reports View with Parallel AI Analyst Operation	125
Figure 4.37 : Telegram Bot — Fleet Report Request and Delivery	128
Figure 4.38 : SGU Fleet Report PDF — Generated via Telegram	130
Figure 4.39 : PostgreSQL Database Statistics — Telemetry Ingestion Performance	132

Figure 4.40 : Railway Server CPU and Memory Utilization Metrics	134
Figure 4.41 : Railway Server Error Rate and Response Time Metrics	135
Figure 4.42 : Railway Server Network Traffic and Request Distribution	136
B.1. OBD-II to ESP32 CAN Bus Wiring Diagram	166
Figure B.2: Isometric render	167
Figure B.3: Exploded isometric render	168
Figure B.4: Engineering drawing1	169
Figure B.5: Engineering drawing2	170



LIST OF TABLES

Table 2.1: Literature Review	29
Table 3.1 : List of Required Hardware, Software, and Equipment	62
Table 4.3 : Extended field validation results summary	126
Table 4.2 : Summary of key quantitative and qualitative results observed during Phase 4 field testing of the SGU Telemetry System.	138
Table 4.4: Capability Comparison: SGU Telemetry System vs. Conventional Fleet Monitoring Solutions	142

