Design of Smart Vehicle Security System Using ESP32 and Zigbee for Multi-Sensor Monitoring Applications

Tangerala Pradeep Kumar[1*], Damera Venkatesh[2], Bethi Prudhvika[2], G.Mani Kumar[2], Samala Vineeth[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Electronics & Communication Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

*Correspondence: Tangerala Pradeep Kumar (johny5508@gmail.com)

To Cite this Article

Tangerala Pradeep Kumar, Damera Venkatesh, Bethi Prudhvika, G.Mani Kumar, Samala Vineeth, "Design of Smart Vehicle Security System Using ESP32 and Zigbee for Multi-Sensor Monitoring Applications", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 04, April 2026,pp: 638-645, DOI: http://doi.org/10.64771/jsetms.2026.v03.i04.pp638-645

Submitted: 03-03-2026 Accepted: 06-04-2026 Published: 13-04-2026

Abstract

The increasing number of vehicle thefts, accidents, and unsafe driving behaviors has raised serious concerns regarding transportation safety, with global vehicle theft cases exceeding millions annually and road accidents causing over 1.3 million deaths each year, while smart vehicle security systems are projected to grow at over 15% annually. Additionally, factors such as unauthorized vehicle access, fire hazards, and drunk driving significantly contribute to vehicle-related risks, highlighting the need for intelligent monitoring solutions. Traditional vehicle security systems rely on basic alarms or manual monitoring, which are often ineffective in detecting multiple threats simultaneously and lack real-time communication and remote monitoring capabilities. Furthermore, conventional systems do not integrate multi-sensor data analysis or provide location tracking, reducing their effectiveness in modern transportation environments. To address these challenges, the proposed Zigbee Vehicle Security System utilizes the ESP32 microcontroller to develop an intelligent and comprehensive vehicle monitoring solution. The system integrates a vibration sensor to detect unauthorized movement or theft attempts, a fire sensor to identify potential fire hazards, and an alcohol sensor to monitor driver sobriety. A GPS module provides real-time vehicle location tracking, while sensor data is processed and displayed locally on an LCD. Zigbee wireless communication enables data transmission to a remote monitoring station, where another ESP32 processes the information and triggers alerts through a buzzer when abnormal conditions are detected. Additionally, IoT integration allows remote monitoring and data logging through cloud platforms. This smart system enhances vehicle security, prevents accidents, enables real-time tracking, and supports the development of intelligent and connected transportation systems.

Keywords: Alcohol Detection, ESP32, GPS Tracking, Internet of Things, Smart Vehicle Security, Vibration Sensor, Vehicle Monitoring, Wireless Communication, ZigBee Technology, Fire Detection

1. Introduction

The increasing number of vehicle thefts, accidents, and unsafe driving behaviors has become a major concern in modern transportation systems [1]. Globally, millions of vehicle theft cases are reported annually, while road accidents result in over 1.3 million deaths each year, highlighting the urgent need for advanced safety and security solutions [2]. Additionally, the market for smart vehicle security systems is projected to grow at over 15% annually, driven by the integration of IoT and intelligent monitoring technologies [3]. Factors such as unauthorized vehicle access, fire hazards, and drunk driving further contribute to transportation risks. In real-world scenarios including personal vehicles, commercial fleets, logistics transport, and smart city systems [4], there is a critical need for solutions that provide continuous monitoring, real-time alerts, and enhanced safety mechanisms.

Traditional vehicle security systems primarily rely on basic alarm systems or manual supervision. These systems are limited in their ability to detect multiple threats simultaneously and often fail to provide timely alerts [5]. Conventional approaches do not include advanced sensing technologies or integrated communication systems, making them ineffective in identifying complex situations such as driver intoxication, fire hazards, or unauthorized vehicle movement [6]. Additionally, most traditional systems lack GPS tracking and remote monitoring capabilities, preventing users from accessing real-time information about vehicle status and location. This limits their effectiveness in ensuring comprehensive vehicle safety and security.

In real-time scenarios, these limitations lead to several critical challenges affecting both vehicle protection and driver safety. Unauthorized access or theft attempts may go undetected or unreported due to the absence of continuous monitoring systems [7]. Fire hazards within vehicles can escalate quickly without early detection, posing serious risks to life and property. Drunk driving remains a major cause of accidents, and without proper monitoring, it becomes difficult to prevent such incidents. Furthermore, the lack of real-time tracking and alert mechanisms delays response actions, reducing the chances of recovery or intervention [8]. These challenges highlight the need for an intelligent, IoT-based vehicle security system capable of integrating multiple sensors, providing real-time monitoring, enabling location tracking, and generating instant alerts to ensure enhanced safety, security, and reliability in modern transportation environments.

2. Literature Survey

Tariq [9] proposed an optimized feature selection method for Distributed Denial of Service (DDoS) attack recognition and mitigation in Software Defined Vehicular Ad Hoc Networks (SD-VANETs). Setitra et al. [10] proposed a DDoS detection system in Software Defined Networking (SDN)-based VANETs using an optimized TabNet model. The system improved detection performance through deep learning-based feature representation.

Wang et al. [11] proposed a VANET edge computing model for smart city transportation using Fifth Generation (5G) networks to minimize latency and delay. Nazih et al. [12] proposed a survey on secure and trustworthy vehicular fog computing, analyzing security mechanisms and system architectures.

Peixoto et al. [13] proposed a traffic data clustering framework based on fog computing for VANETs to improve traffic analysis and management. Gaouar et al. [14] proposed a cloud-based smart traffic management protocol using an intelligent traffic light system in VANETs. Zhan et al. [15] proposed a dynamic privacy-preserving anonymous authentication scheme for fog-cloud-based VANETs that ensured secure communication and user anonymity.

Su et al. [16] proposed an efficient privacy-preserving authentication scheme that reduced dependency on trusted authorities in VANETs. Kilic [17] proposed a Transport Layer Security (TLS)-based handshake mechanism for plug-and-charge communication in vehicular networks. Amari et al. [18] proposed a comprehensive survey on trust management in

VANETs, analyzing models and techniques for ensuring reliable communication.

Mdee et al. [19] proposed a cooperative pseudonym swapping scheme for location privacy preservation in VANETs that enhanced anonymity through collaborative mechanisms. Labadie et al. [20] proposed a framework for building data management capabilities to comply with data protection regulations such as General Data Protection Regulation (GDPR).

3. Proposed System

Figure 1 illustrates the transmitter module of the Zigbee Vehicle Security System built around the ESP32. This module is installed inside the vehicle and is responsible for continuously monitoring vehicle conditions using multiple sensors such as vibration, fire, alcohol, and GPS. A regulated power supply ensures stable operation. The ESP32 processes all sensor inputs and displays system status on an LCD while transmitting the collected data wirelessly through a Zigbee transmitter module to the monitoring station. This module plays a key role in detecting abnormal events such as theft attempts, fire hazards, and drunk driving.

Step 1: Power Supply Initialization: The regulated power supply provides stable DC voltage to the ESP32, sensors, and Zigbee transmitter, ensuring reliable system operation inside the vehicle.

Step 2: Vibration-Based Theft Detection: The vibration sensor detects abnormal movements or shocks, indicating possible vehicle theft or unauthorized access.

Step 3: Fire Hazard Detection: The fire sensor continuously monitors for the presence of flames or excessive heat inside the vehicle, helping prevent accidents caused by electrical faults or fuel leakage.

Step 4: Alcohol Detection System: The alcohol sensor analyzes the driver’s breath and detects alcohol levels. If alcohol is detected beyond a safe limit, the system flags it as a violation.

Step 5: GPS-Based Location Tracking: The GPS module determines the real-time geographical location of the vehicle, which is essential for tracking during emergencies or theft.

Step 6: Data Processing by ESP32: The ESP32 collects and processes all sensor data, compares it with predefined thresholds, and determines whether conditions are normal or abnormal.

Step 7: LCD Display Output: The LCD displays real-time vehicle status, sensor readings, and alerts, allowing in-vehicle monitoring.

Step 8: Zigbee Data Transmission: The Zigbee transmitter (Tx) sends processed data wirelessly to the receiver module at the monitoring station.

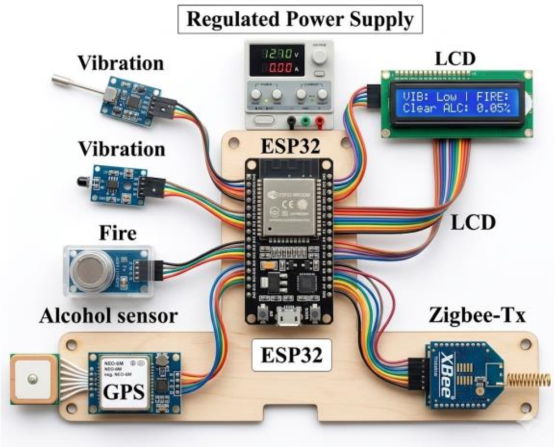

Figure 1. Zigbee Vehicle Security System – Transmitter Module.

Figure 2 illustrates the receiver module of the Zigbee Vehicle Security System, where the ESP32 acts as the central controller. The Zigbee receiver (Rx) collects the data transmitted from the vehicle’s transmitter module. The ESP32 processes this data, displays it on an LCD, and activates alerts through a buzzer when abnormal conditions are detected. Additionally, IoT connectivity enables remote monitoring of vehicle status through cloud platforms. This module ensures centralized monitoring and rapid response to vehicle-related incidents.

Step 1: Power Supply Initialization: The regulated power supply provides stable voltage to the ESP32 and all receiver components, ensuring uninterrupted monitoring.

Step 2: Data Reception via Zigbee: The Zigbee receiver (Rx) receives real-time data transmitted from the vehicle's transmitter module.

Step 3: Data Processing Using ESP32: The ESP32 processes the received data and analyzes it to detect abnormal conditions such as theft attempts, fire hazards, or alcohol detection.

Step 4: LCD Display for Monitoring: The LCD displays vehicle status, sensor readings, and alerts for monitoring by authorities or vehicle owners.

Step 5: Buzzer Alert System: When abnormal conditions are detected, the buzzer is activated to provide immediate alerts for quick action.

Step 6: IoT-Based Remote Monitoring: The ESP32 sends the processed data to a cloud platform, enabling remote tracking, monitoring, and analysis through web or mobile applications.

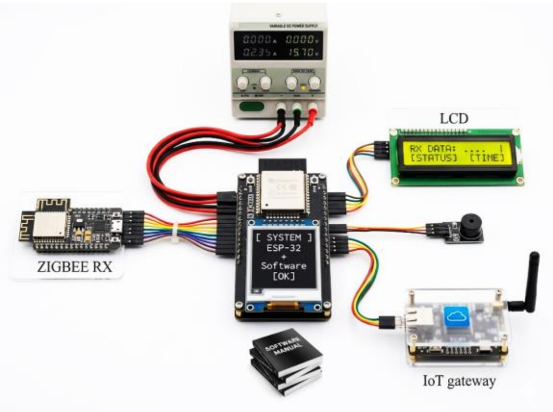

Figure 2. Zigbee Vehicle Security System – Receiver Module.

3.1 Working Procedure

The proposed Zigbee Vehicle Security System as shown in Figure 3 is designed to enhance vehicle safety and security by continuously monitoring various conditions inside the vehicle and transmitting the information to a monitoring station. The system integrates multiple sensors, wireless communication technology, and IoT connectivity to detect abnormal situations such as unauthorized vehicle movement, fire hazards, and alcohol consumption by the driver. The entire system is controlled by the ESP32 microcontroller, which acts as the central processing unit responsible for collecting sensor data and controlling the system operations.

The transmitter module is installed inside the vehicle and is responsible for monitoring different parameters using sensors. A vibration sensor detects abnormal vibrations that may occur during unauthorized vehicle movement or theft attempts. A fire sensor detects the presence of fire inside the vehicle, which may occur due to electrical faults or fuel leakage. An alcohol sensor monitors the driver's breath and detects alcohol levels to prevent drunk driving incidents. Additionally, a GPS module is used to determine the exact geographical location of the vehicle.

The ESP32 processes the sensor data and displays the vehicle status on an LCD display inside the vehicle. The collected data is then transmitted wirelessly through a Zigbee transmitter module to a receiver module located at the monitoring station. The receiver module receives the transmitted data using a Zigbee receiver and processes the information through another ESP32 microcontroller. The received information is displayed on an LCD screen, and a buzzer is activated when abnormal conditions are detected. Furthermore, the system integrates IoT technology, enabling remote monitoring of vehicle status through internet-based platforms.

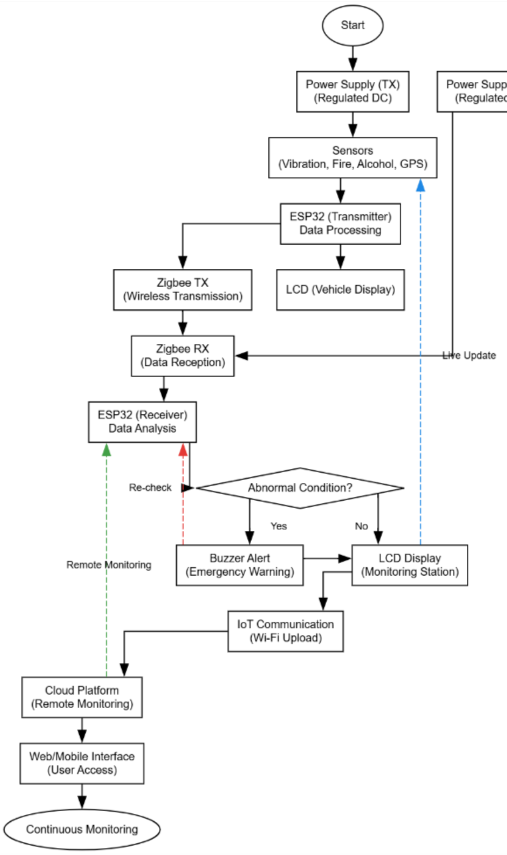

Figure 3. Proposed Flowchart.

Figure 4 illustrates the transmitter section of a ZigBee-based vehicle security system designed for real-time monitoring and theft detection. The system is powered by a regulated power supply unit comprising a step-down transformer, bridge rectifier, filter capacitors, and a 7805-voltage regulator to provide a stable +5V output.

The ESP32 microcontroller acts as the central processing unit, interfacing with a vibration sensor to detect unauthorized vehicle movement, a fire and alcohol sensor to identify hazardous conditions, and a GPS module for real-time location tracking. The collected data is transmitted wirelessly using a ZigBee transmitter module. A 16×2 LCD displays system status and sensor readings locally. This system ensures continuous monitoring and immediate detection of threats, enhancing vehicle security.

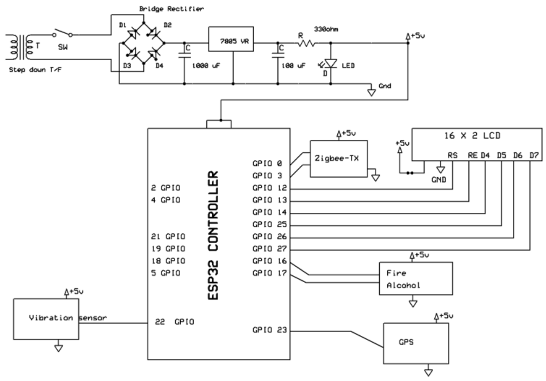

Figure 4. Transmitter Circuit Diagram of ZigBee-Based Vehicle Security System.

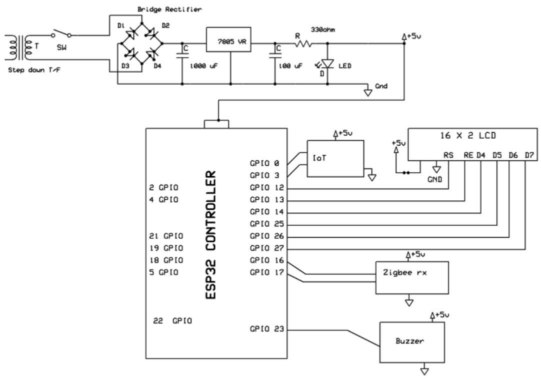

Figure 5. Receiver Circuit Diagram of ZigBee-Based Vehicle Security System.

Figure 5 presents the receiver section of the ZigBee-based vehicle security system, responsible for receiving and processing data transmitted from the vehicle. The system uses a regulated power supply like the transmitter section. The ESP32 microcontroller receives data via a ZigBee receiver module and processes it for monitoring and alert generation. An IoT module enables remote access and cloud-based monitoring of vehicle status. A 16×2 LCD displays received data such as alerts and conditions, while a buzzer provides audible warnings in case of security breaches or abnormal events. This receiver unit enhances centralized monitoring and enables quick response actions, improving overall vehicle safety and anti-theft capabilities.

4. Results and Discussion

Figure 6 shows the hardware setup of the ZigBee-Based Vehicle Security developed using the ESP32 microcontroller. The system integrates sensors and modules such as GPS, fire sensor, vibration sensor, and alcohol sensor along with an LCD display and buzzer. The ESP32 processes the sensor data and controls the system while enabling IoT-based monitoring.

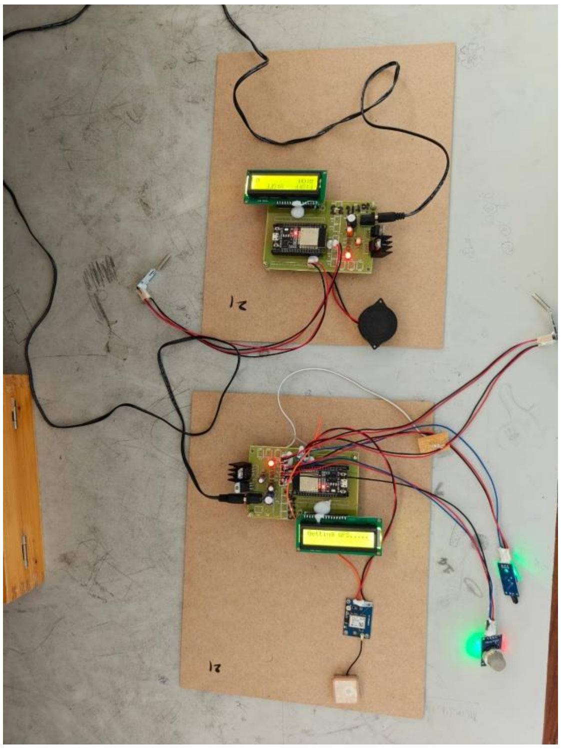

Figure 6. Hardware Implementation of ZigBee-Based Vehicle Security System.

Figure 7 shows the LCD display output of the system indicating system status. The LCD provides real-time information to users such as system initialization, authentication status, and alert messages generated by the ESP32 controller.

Figure 8 shows the IoT web server dashboard displaying the sensor data transmitted by the ESP32. The web interface records parameters such as fire detection status, vibration status, alcohol detection status, location, and time. This allows remote monitoring and management of the proposed system through the internet.

Figure 7. LCD Display Output of the ZigBee-Based Vehicle Security.

S.No	Fire	Vib	Alcohol_Status	Location	Date	
1	OFF	OFF	ON	Location	Location	2026-02-17 13:06:38
2	OFF	OFF	ON	Location	Location	2026-02-17 13:06:28
3	ON	OFF	OFF	Location	Location	2026-02-12 14:50:08
4	ON	ON	OFF	Location	Location	2026-02-12 14:49:58
5	ON	OFF	OFF	Location	Location	2026-02-12 14:49:47
6	ON	OFF	OFF	Location	Location	2026-02-12 14:49:37
7	ON	OFF	OFF	Location	Location	2026-02-12 14:40:58
8	ON	OFF	OFF	Location	Location	2026-02-12 14:40:48
9	ON	OFF	OFF	Location	Location	2026-02-12 14:40:38
10	ON	OFF	OFF	Location	Location	2026-02-12 14:40:28
11	ON	OFF	OFF	Location	Location	2026-02-12 14:40:18
12	ON	OFF	OFF	Location	Location	2026-02-12 14:40:07
13	ON	OFF	OFF	Location	Location	2026-02-12 14:39:57
14	ON	OFF	OFF	Location	Location	2026-02-12 14:39:47
15	ON	OFF	OFF	Location	Location	2026-02-12 14:39:37
16	ON	OFF	OFF	Location	Location	2026-02-12 14:39:26
17	ON	OFF	OFF	Location	Location	2026-02-12 14:39:16
18	ON	OFF	OFF	Location	Location	2026-02-12 14:39:06
19	ON	OFF	OFF	Location	Location	2026-02-12 14:38:56
20	ON	OFF	OFF	Location	Location	2026-02-12 14:38:45

Figure 8. IoT Web Server Monitoring Output

5. Conclusion

The proposed Zigbee Vehicle Security System provides a comprehensive and intelligent solution to modern transportation safety challenges by integrating multi-sensor monitoring, wireless communication, and IoT connectivity. By utilizing the ESP32 microcontroller along with vibration, fire, and alcohol sensors, the system effectively detects theft attempts, fire hazards, and unsafe driving conditions such as intoxication. The inclusion of GPS ensures accurate real-time vehicle tracking, while Zigbee communication enables reliable data transmission to a remote monitoring unit for immediate analysis and alert generation. Local feedback through the LCD display and buzzer enhances user awareness, and IoT integration supports remote monitoring, data logging, and efficient decision-making. This system overcomes the limitations of traditional security methods by providing continuous, automated, and real-time protection. Finally, it enhances vehicle safety, reduces risks associated with theft and accidents, and contributes to the development of smart, secure, and connected transportation systems.

References

[1] Yerrathi, S.; Pakala, V. Enhancing network stability in VANETs using nature inspired algorithm for intelligent transportation system. PLoS ONE 2024, 19, e0296331.

[2] S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.1403

[3] Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[4] Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines. (2025). Inaternational Journal of Communication Networks and Information Security, 16(4). https://doi.org/10.48047/ijcnis.16.4.2111

[5] Awais, S.M.; Yucheng, W.; Mahmood, K.; Badar, H.M.S.; Kharel, R.; Das, A.K. Provably secure fog-based authentication protocol for VANETs. Comput. Netw. 2024, 246, 110391.

[6] Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.

[7] Zhang, J.; Su, S.; Zhong, H.; Cui, J.; He, D. Identity-Based Broadcast Proxy Re-Encryption for Flexible Data Sharing in VANETs. IEEE Trans. Inf. Forensics Secur. 2023, 18, 4830–4842.

[8] Tariq, U. Intelligent algorithmic framework for detection and mitigation of BeiDou spoofing attacks in vehicular ad hoc networks (VANETs). PeerJ Comput. Sci. 2024, 10, e2419.

[9] Tariq, U. Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. World Electr. Veh. J. 2024, 15, 395.

[10] Setitra, M.A.; Fan, M. Detection of DDoS attacks in SDN-based VANET using optimized TabNet. Comput. Stand. Interfaces 2024, 90, 103845.

[11] Wang, M.; Mao, J.; Zhao, W.; Han, X.; Li, M.; Liao, C.; Sun, H.; Wang, K. Smart City Transportation: A VANET Edge Computing Model to Minimize Latency and Delay Utilizing 5G Network. J. Grid Comput. 2024, 22, 25.

[12] Nazih, O.; Benamar, N.; Lamaazi, H.; Chaoui, H. Toward Secure and Trustworthy Vehicular Fog Computing: A Survey. IEEE Access 2024, 12, 35154–35171.

[13] Peixoto, M.; Maia, A.; Mota, E.; Rangel, E.; Costa, D.; Turgut, D.; Villas, L. A traffic data clustering framework based on fog computing for VANETs. Veh. Commun. 2021, 31, 100370.

[14] Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.

[15] Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering

and Management Research, 10(10), 49–56.

[16] Patyrykin, K., & Vasyukova, L. (2025). Environmental Accountability or Symbolic Compliance? A Critical Review of ESG Ratings, Greenwashing, and Indirect Emissions in the Global Insurance Sector. International Journal of Energy Economics and Policy, 15(6), 917–925. https://doi.org/10.32479/ijeep.22770

[17] Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.

[18] Amari, H.; El Houda, Z.A.; Khoukhi, L.; Belguith, L.H. Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey. IEEE Access 2023, 11, 47659–47680.

[19] Cyril, H. P., & Kumara, S. Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data.

[20] Labadie, C.; Legner, C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. J. Inf. Technol. 2023, 38, 16–44