IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

SMART VEHICLE IGNITION SYSTEM

Prakash K M[1], Bhagya D B[2], Rani C O[3], Sindhu B S[4], Srushti S G[5]

Professor, E&CE, BIET, Davangere, Karnataka India[1]

Student, UG, E&CE, BIET, Davangere, Karnataka India[2,3,4,5]

Abstract: The Smart Vehicle Ignition System is a multi-layered system that integrates RFID authentication, facial recognition, and fingerprint sensing to enhance vehicle security and safety. It activates upon successful verification, providing a robust defence against unauthorized access. The system also initiates alcohol detection and tilt sensing mechanisms to ensure driver sobriety and monitor vehicle orientation for potential accidents or rollovers. The system aims to enhance vehicular security, driver responsibility, and real-time safety monitoring, making it suitable for personal vehicles, public transport, and fleet management.

Keyword: fingerprint sensing, facial recognition, vehicle.

I. INTRODUCTION

Vehicle theft is still a major problem throughout the world, causing owners to suffer severe financial losses as well as psychological anguish. Traditional car security systems, which frequently use one-off authentication techniques like physical keys or simple alarms, are becoming more and more vulnerable to theft by determined criminals. Furthermore, ordinary security packages frequently do not incorporate important driver safety features like preventing drunk driving and sending out timely alerts in the event of an accident. This raises the need for more comprehensive, reliable, and clever solutions that improve overall vehicle and driver safety in addition to preventing unwanted entry. In addition to wanting real-time updates and the capacity to communicate with their car from a distance, the modern car owner also wants more connectivity and control.

II. OBJECTIVES

The objectives of the project: To design and implement a robust multi-level authentication system for vehicle ignition, comprising-

- Level 1: Face recognition using Python (OpenCV, Haar Cascades for detection, LBPH for recognition) executed on a laptop, with results communicated to an ESP32.
- Level 2: Fingerprint verification using an optical fingerprint sensor interfaced with the ESP32.
- Level 3: RFID tag scanning for user/license validation (as a proxy for license check) using an RFID reader interfaced with the ESP32.

1. To integrate essential driver safety features:
   a) An alcohol detection system using an MQ-3 sensor to prevent engine start if the driver's breath alcohol content exceeds a predefined threshold.
   b) An accident detection system using a tilt sensor to identify potential collisions or rollovers.

2. To develop an IoT-based remote monitoring and control system using the ESP32's Wi-Fi capabilities and the Blynk platform, enabling:
   a) Real-time notifications to the vehicle owner's smartphone upon successful engine activation.
   b) The ability for the owner to remotely disable the vehicle's engine via the Blynk application.

3. To provide clear, step-by-step instructions and status feedback to the user via an LCD display.

4. To ensure that the vehicle's engine (simulated by a DC motor) can only be activated after all security layers and safety checks are successfully passed.

5. To establish reliable serial communication between the laptop (Python face recognition module) and the ESP32.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

III. METHODOLOGY

A. BLOCK DIAGRAM

The laptop computer uses a webcam to capture user faces, which are processed using Python scripts using OpenCV libraries. The ESP32 microcontroller is the core controller, receiving face recognition status, prompting for fingerprint, RFID, alcohol, and tilt sensor scanning. It then activates a relay to simulate the vehicle engine and uses Wi-Fi to connect to the Blynk server and app, acting as an intermediary for IoT communication.

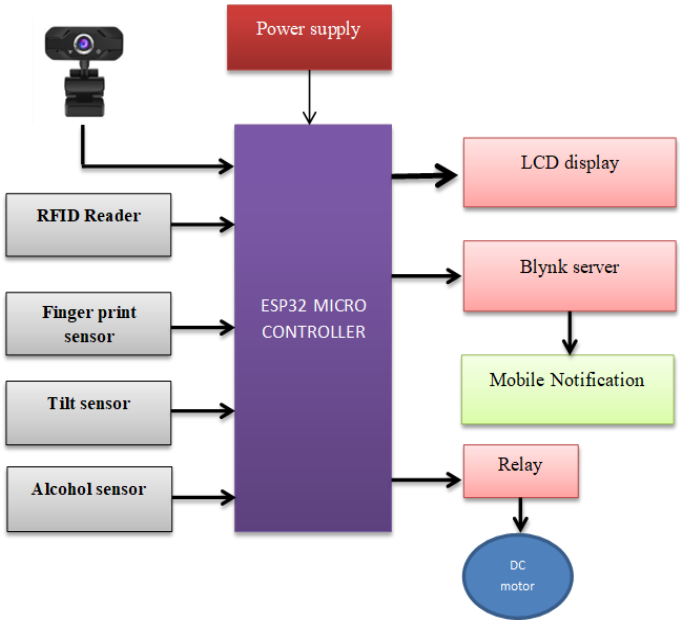

Fig 1: Block diagram

1. Laptop Computer: The laptop's webcam captures the user's face. Python scripts using OpenCV libraries (Haar Cascades for detection, LBPH for recognition) process the image. If a registered face is recognized, a success signal (e.g., "FACE_OK") is sent via serial (USB) to the ESP32.

2. ESP32 Microcontroller: This is the core controller.
- It receives the face recognition status from the laptop.
- Prompts the user for fingerprint scanning via the LCD and verifies the fingerprint using the connected sensor.
- Prompts for RFID tag scanning and validates the tag.
- Reads data from the alcohol sensor to check for intoxication.
- Monitors the tilt sensor for accident detection.
- Displays all prompts, status messages, and alerts on the LCD.
- If all checks pass, it activates a relay to turn ON the DC motor (simulating the vehicle engine).
- Uses its built-in Wi-Fi to connect to the Blynk server, send notifications (e.g., "Engine ON") to the owner's smartphone app, and receive remote commands (e.g., "Engine OFF").

3. Blynk Server & App: Acts as the intermediary for IoT communication. The ESP32 sends data to and receives commands from the owner's Blynk app on their smartphone through the Blynk cloud server.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

IV. FLOW DIAGRAM

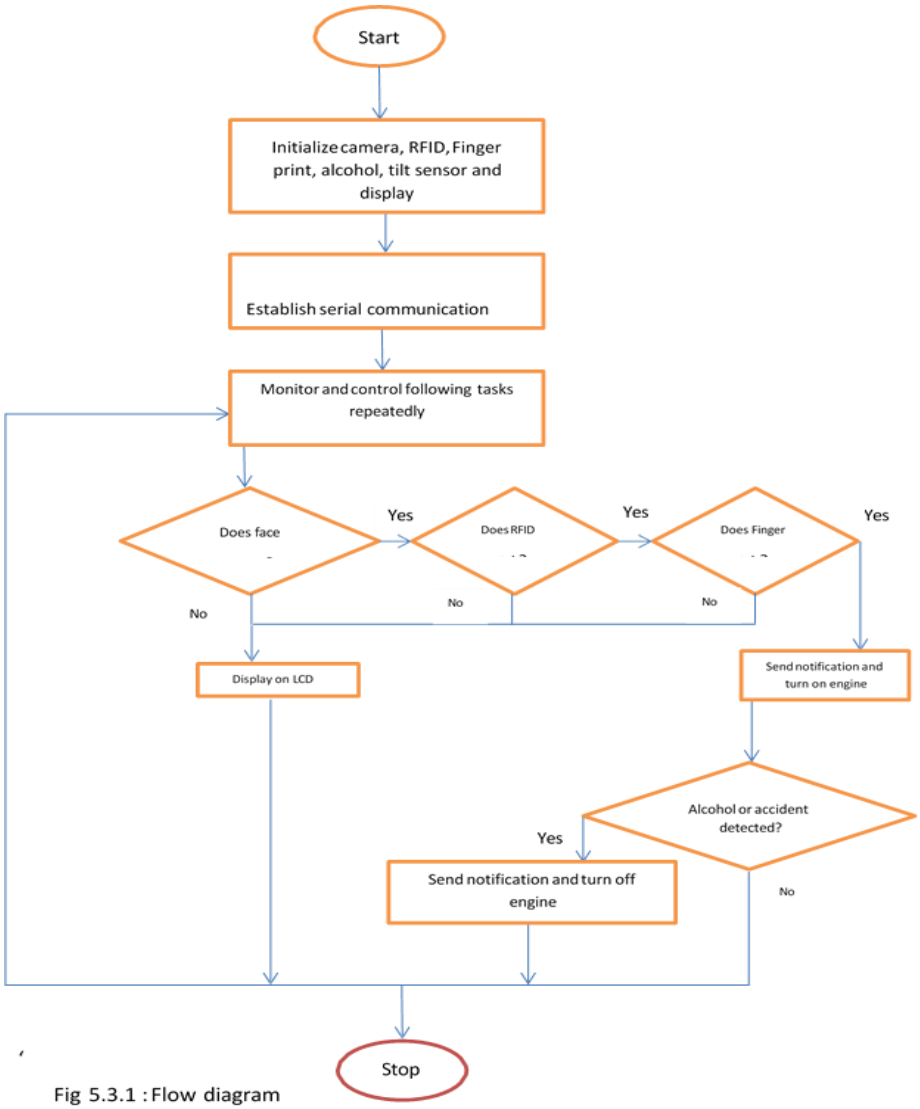

Fig 2: Flow diagram

The flowchart illustrates the vehicle security system process, where the engine is authenticated through RFID and fingerprint verification, failing which a notification is sent and the engine is turned off.

V. RESULTS AND DISCUSSION

A. Face Recognition Module (Laptop):

1. Expected Result: The system should correctly recognize trained individuals with an accuracy of >90% under varying lighting conditions (though LBPH is somewhat robust to this) and minor variations in pose/expression. Recognition time per frame should be within 200-500ms on a moderately powered laptop.
2. Testing: Test with multiple images of registered users, images of unregistered users, and registered users under different conditions (glasses, hat, different lighting).
3. Discussion: False Positive Rate (FPR) and False Negative Rate (FNR) would be key metrics. Factors affecting performance (lighting, distance from camera, training dataset quality) would be discussed.

B. Fingerprint Authentication Module (ESP32):

1. Expected Result: Successful enrollment of fingerprints and >95% accuracy in verifying registered users. Verification time should be < 2 seconds.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

2. Testing: Enroll multiple fingers from different users. Test verification with correct fingers, incorrect registered fingers, and unregistered fingers. Test with varying finger pressure and condition (dry, slightly moist).
3. Discussion: Discuss reliability, ease of use, and any issues encountered with sensor sensitivity.

C. RFID Validation Module (ESP32):
1. Expected Result: 100% accuracy in reading and validating registered RFID tags within the specified read range (typically a few cm for MFRC522). Read time should be almost instantaneous.
2. Testing: Test with registered tags, unregistered tags, and at varying distances/orientations.
3. Discussion: Confirm reliability and discuss practical read range.

D. Alcohol Detection Module (ESP32):
1. Expected Result: The MQ-3 sensor should show a noticeable increase in analog output when exposed to alcohol vapor (e.g., from a test solution or breath after consuming alcohol, if ethically permissible and safe for testing). A clear threshold should be determinable to distinguish between sober and potentially intoxicated states.
2. Testing: Calibrate sensor with known non-alcohol air, then expose to controlled alcohol vapor. Observe ADC readings.
3. Discussion: Sensor warm-up time, sensitivity, stability, and the challenge of setting an accurate and reliable threshold for "intoxication" without professional calibration equipment would be discussed. Cross-sensitivity to other fumes could also be noted.
E. Accident Detection (Tilt Sensor) Module (ESP32):
1. Expected Result: The tilt sensor should reliably change its digital state when the system is tilted beyond a predefined angle (e.g., >45 degrees).
2. Testing: Manually tilt the breadboard/prototype assembly to simulate an accident.
3. Discussion: Simplicity of the SW-520D vs. the potential for false positives (e.g., steep incline parking). An MPU6050 would offer more sophisticated detection but adds complexity.

F. Blynk IoT Integration (ESP32 & App):
1. Expected Result: Real-time notifications for engine status ("Engine ON," "Accident," "Alcohol Detected") should be received on the Blynk app within a few seconds of the event. Remote engine OFF command from the app should promptly disable the DC motor.
2. Testing: Perform full system run-throughs, trigger events, and observe app notifications. Use the app to send commands.
3. Discussion: Reliability of Wi-Fi connection, latency of notifications/commands.

G. Overall System Integration and Performance:
1. Expected Result: Smooth transition between authentication layers. Total time from initiating face recognition to engine start (for a successful run) should be acceptable (e.g., 10-20 seconds).
2. Testing: Multiple end-to-end test runs with various success/failure scenarios at each stage.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

F. Test Cases

Test Case ID	Test Scenario	Input	Expected Output	Pass/Fail Criteria
TC001	Face Recognition - Authorized User	Valid registered face	Authentication successful; proceed to fingerprint scan	System moves to next step (fingerprint)
TC002	Face Recognition - Unauthorized User	Unrecognized face	Authentication failed; access denied	Access is blocked
TC003	Fingerprint Scan - Valid	Valid registered fingerprint	Authentication successful; proceed to RFID check	System moves to next step (RFID)
TC004	Fingerprint Scan - Invalid	Invalid or unregistered fingerprint	Authentication failed; access denied	Access is blocked
TC005	RFID Check - Valid License Card	Valid RFID tag	Authentication successful; system ready to start engine	Access is granted
TC006	RFID Check - Invalid Tag	Unauthorized or unrecognized RFID tag	Authentication failed; access denied	Access is blocked
TC007	Alcohol Detection - No Alcohol	Breath sample = 0% BAC	Engine start allowed	System proceeds to ignition
TC008	Alcohol Detection - Alcohol Detected	Breath sample > threshold (e.g., 0.03% BAC)	Engine start blocked; alert triggered	Ignition prevented
TC009	Accident Detection	Tilt sensor detects sudden change (e.g., > threshold angle)	Accident alert sent via Blynk; system notifies owner	Notification received on Blynk app
TC010	Engine ON Notification	Successful 3-layer authentication	Real-time notification sent to owner via Blynk	Notification appears on smartphone
TC011	Remote Engine Disable via Blynk	Owner presses "Engine OFF" button on Blynk	Engine operation disabled	Engine stops remotel y
TC012	LCD Display Feedback	Each security stage triggered	LCD shows real-time messages like "Scan Face", "Scan Finger", etc.	Appropriate message displayed at each stage
TC013	Power Interruption Recovery	System is restarted after power failure	System resumes and re- initiates authentication sequence	System functions as expected after reboot
TC014	Multiple Failed Attempts	Three consecutive failed login attempts	Lockout mechanism triggered or alert sent	System prevents further access temporarily
TC015	All Systems Go (Happy Path)	Valid face, fingerprint, RFID, no alcohol	Vehicle starts normally; all stages passed	Engine starts, user authenticated

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2025

DOI: 10.17148/IJIREEICE.2025.13826

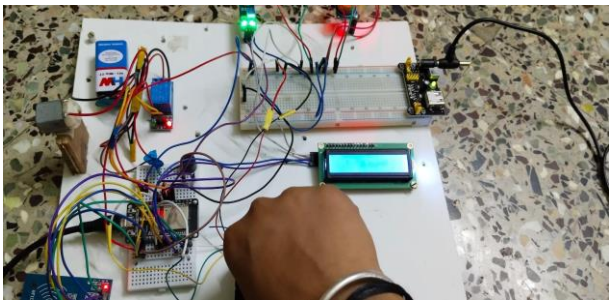

Fig 3: Waiting for Fingerprint

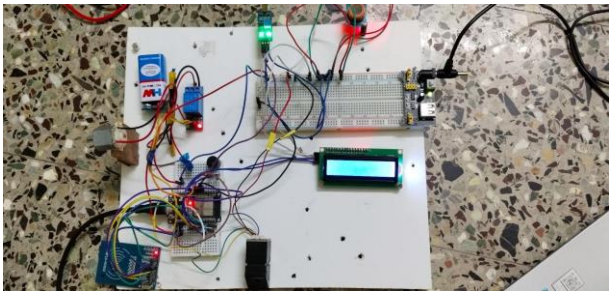

Fig 4: DC Motor Ignited

VI. CONCLUSION

This project successfully demonstrated the design and implementation of a "Multi-Level Security System for Vehicles" incorporating face recognition, fingerprint scanning, RFID validation, alcohol detection, accident sensing, and IoT-based remote monitoring and control. The system effectively integrates Python for face recognition on a laptop with an ESP32 microcontroller managing subsequent security layers, sensors, and user interaction via an LCD and the Blynk platform. The layered authentication approach significantly enhances vehicle security compared to traditional systems. The inclusion of safety features like alcohol and accident detection contributes positively to driver and vehicle safety. The IoT capabilities provide valuable real-time awareness and control to the vehicle owner.

While the prototype has certain limitations, primarily related to the practical deployment of laptop-based face recognition in a vehicle and sensor accuracies, it serves as a strong proof-of-concept for a comprehensive and intelligent vehicle security and safety solution. The project successfully met its core objectives by creating a functional system that validates users through multiple checks before granting access and allowing engine operation.

REFERENCES

[1]. S. Ahmed and M. K. Hasan, "Face Recognition Based Car Ignition System with Anti-Theft Security using GSM Technology," International Journal of Computer Applications, vol. 167, no. 8, pp. 12-16, Jun. 2017. DOI: 10.5120/ijca2017914404.

[2]. P. Kumar and R. Singh, "A Multi-Layered Vehicle Security System using Fingerprint and RFID Technology," in Proceedings of the 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, Mar. 2019, pp. 865-869. DOI: 10.1109/ICCMC.2019.8819774.

[3]. R. Patel, M. Shah, and R. Makwana, "IoT Based Smart Vehicle Alcohol Detection and Accident Alert System," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 3, pp. 2345-2349, Feb. 2020. DOI: 10.35940/ijeat.C6239.029320.

[4]. P. Viola and M. J. Jones, "Robust Real-Time Face Detection," International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154, May 2004. DOI: 10.1023/B:VISI.0000013087.49260.fb.

[5]. T. Ahonen, A. Hadid, and M. Pietikäinen, "Face Description with Local Binary Patterns: Application to Face Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037-2041, Dec. 2006. DOI: 10.1109/TPAMI.2006.244.

[6]. S. Manivannan, K. S. Kumar, P. S. Pradeep, S. Rajesh, and R. S. Kumar, "ESP32 Based Smart Security System with Blynk App Integration," Journal of Physics: Conference Series, vol. 1916, no. 1,p. 012113, Jun. 2021. DOI: 10.1088/1742-6596/1916/1/012113.