International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

Car Theft Detection Using Face Recognition

Burre Ramya[1], P Renuka Devi[2], R Dhanaswi[3], G Umamaheshwar Reddy[4], M Ramya Sri [5]
[1]Assistant professor, Dept. of CSE, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India.
[2,3,4,5]UG Students, Dept. of CSE, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India.
Emails: *burreramya5802@gmail.com[1], renuka08.polukonda@gmail.com[2], rajanaladhanaswi@gmail.com[3],* umagujjula1234*@gmail.com[4], mukarlaramyasri@gmail.com [5]*

Abstract
Vehicle theft is a growing concern due to the increasing number of unauthorized vehicle access incidents. Conventional vehicle security systems such as alarms and key-based locks are often insufficient against modern theft techniques. This paper presents a smart vehicle security system using ESP32-CAM and Telegram for real-time monitoring and owner-based authorization. When an attempt is made to start the vehicle, the system captures an image using an onboard camera and sends it to the vehicle owner through a Telegram bot along with the vehicle's live GPS location. The vehicle ignition is enabled only if the owner approves the request. If the request is rejected or suspicious activity is detected, the system activates an alarm and sends theft alerts to the owner. The proposed system is lightweight, event-driven, and does not rely on complex machine learning models, making it suitable for real-time embedded applications. Experimental implementation shows that the system effectively enhances vehicle security with fast response time and minimal hardware requirements.

Keywords: *ESP32-CAM, Vehicle Security, IoT, Telegram Bot, Theft Detection, GPS Tracking.*

1. Introduction
Vehicle theft has become a serious issue in both urban and rural areas. Traditional vehicle security mechanisms such as mechanical locks, key-based ignition systems, and basic alarm systems are vulnerable to tampering and unauthorized access. Advanced vehicle security solutions often rely on complex hardware or expensive infrastructure, making them unsuitable for low-cost and real-time deployment. Recent advancements in Internet of Things (IoT) technologies have enabled smart and connected security solutions. Microcontroller-based systems with integrated communication modules allow real-time monitoring and remote control. However, many existing systems depend heavily on cloud servers, mobile applications, or machine learning models, which increase system complexity and latency. This paper proposes a smart vehicle security system using ESP32-CAM that focuses on owner-controlled authorization rather than automated decision-making. The system captures an image whenever a vehicle start attempt is detected and sends it to the owner via Telegram. Based on the owner's response, the vehicle is either allowed to start or an alert is triggered. This approach ensures higher security, faster response, and better reliability without relying on heavy computation.

2. Related Work
Several vehicle security systems based on face recognition have been proposed in recent years. A Raspberry Pi–based vehicle anti-theft system using OpenCV and convolutional neural networks was presented, where the driver's face is captured and matched with stored images for authentication [1]. Although the system achieved high recognition accuracy, it required high computational resources, continuous model training, and controlled lighting conditions, making it less suitable for real-time, low-power embedded vehicle applications. To improve access security, hybrid authentication mechanisms combining face recognition and RFID technology have been explored [2]. These systems enhance reliability by using multiple verification factors. However, the requirement of additional hardware such as RFID readers increases system complexity, installation effort, and maintenance overhead, which limits practical deployment in compact vehicle security solutions. Lightweight IoT-based vehicle security systems using ESP32-CAM have gained

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

attention due to their compact size and low power consumption. An ESP32-CAM based anti- theft system employing the LBPH algorithm was introduced to provide real-time monitoring and alerts [3]. While this approach reduces hardware cost and power usage, its performance is affected by lighting variations and face orientation, reducing reliability in outdoor environments. Cloud-assisted intelligent vehicle access systems utilizing deep learning models and mobile networks have also been proposed [4]. These systems achieve improved accuracy by leveraging CNN architectures and cloud-based processing. However, they depend on GPU-based training, continuous internet connectivity, and cloud infrastructure, resulting in higher latency and reduced feasibility for standalone embedded implementations. Recent IoT-enabled vehicle security systems using ESP32- CAM focus on real-time alert generation and GPS-based location tracking [5]. Although these systems effectively notify owners during theft attempts, they primarily rely on automated alerts and lack direct owner-controlled authorization before vehicle ignition, which limits their ability to actively prevent unauthorized vehicle start.

3. System Architecture

The proposed Smart Vehicle Security System is designed using an ESP32-CAM–based embedded platform integrated with wireless communication, sensing units, and user authentication through Telegram. The system architecture follows a sequential and event-driven approach to ensure vehicle security and theft prevention. Initially, the system initializes all hardware and software modules, including the ESP32-CAM, Wi-Fi module, GPS module, vibration sensor, motor driver, relay, buzzer, and Telegram bot interface. Once initialization is complete, the system waits for the vehicle start request through a physical start button. When the start button is pressed, the ESP32-CAM captures the driver's image and sends it to the registered vehicle owner via Telegram for authentication. The vehicle is allowed to start only after the owner approves the request through the Telegram bot. Upon approval, the motor driver is enabled and the vehicle enters normal monitoring mode. During normal operation, the vibration sensor continuously monitors the vehicle for abnormal movements. If no suspicious activity is detected, the system continues monitoring without interruption. In case of vibration or repeated unauthorized attempts, the system identifies it as a potential theft condition. Once theft is detected, the system immediately locks the motor, activates the buzzer and warning LED, and switches to theft handling mode. The GPS module retrieves the real-time location of the vehicle, and both the location and captured image are sent to the owner via Telegram. Additionally, a shock circuit is activated through a relay to further deter theft. The system continuously monitors owner commands. If the owner sends a STOP command via Telegram, the shock circuit and buzzer are deactivated while keeping the motor locked. The system then waits for the next valid start request, ensuring continuous security and controlled vehicle access. Figure 1 shows Flow Chart

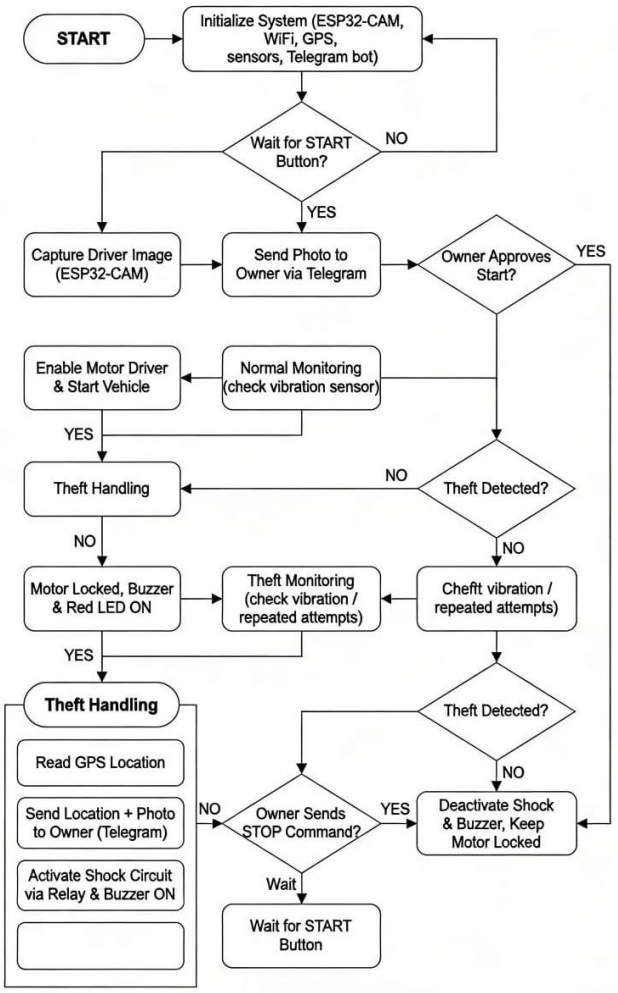

Figure 1 Flow Chart

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

4. Hardware Components

Figure 1 ESP32-CAM module

The ESP32-CAM module works by combining an ESP32 microcontroller with a camera (usually OV2640) for low-cost, Wi-Fi enabled image/video capture and streaming, using its 4MB PSRAM for buffering. Figure 1 shows ESP32-CAM module

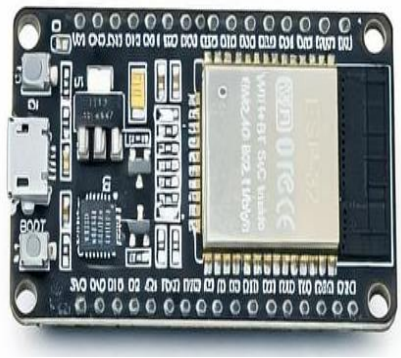

Figure 2 ESP32 Board

The ESP32 board works as a powerful, low-power microcontroller for IoT, integrating **dual-core processors (Tensilica LX6)**, **Wi-Fi**, and **Bluetooth (BLE)** on a single chip, allowing it to be a standalone system or a slave to other MCUs, handling wireless tasks while the main processor focuses on applications. It reads inputs (like sensors via analog/digital pins) and executes code (programmed via Arduino IDE or other tools), then controls outputs (like LEDs, motors) using its plentiful GPIO pins and communication protocols (I2C, SPI, UART, PWM) to connect to the internet or other devices, often stepping down 5V power to its required 3.3V. Figure 2 shows ESP32 Board

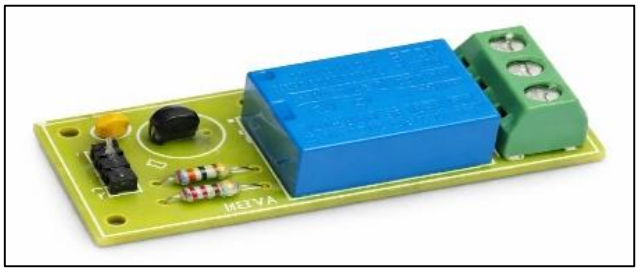

Figure 3 Relay Motor

An electromechanical switch used to control high power devices with a low power signal. Figure 3 shows Relay Motor

Figure 4 Buzzer

An IoT buzzer works by converting electrical signals from a microcontroller (like Arduino) into audible sound, using either the piezoelectric effect (vibrating crystal disc) or electromagnetism (coil attracting a diaphragm) to create vibrations that produce sound waves. Figure 4 shows Buzzer

Figure 5 DC Motor with Fan

DC motor with a fan works by converting direct electrical energy into mechanical rotation

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

via electromagnetism to spin blades, while IoT integration adds smart control using sensors (like thermistors) and microcontrollers (like Arduino) to enable remote monitoring, automated speed adjustment, and scheduling via Wi-Fi/Bluetooth, creating smart, efficient cooling systems. Figure 5 shows DC Motor with Fan

Figure 6 GPS Module

A GPS module in an IoT device works by receiving signals from orbiting satellites, calculating its distance from several (at least four) to determine its precise location (latitude, longitude, altitude) using trilateration, and then sending this location data, often with other sensor readings, over the internet (via Wi-Fi/cellular) to a cloud platform for monitoring and analysis. Figure 6 shows GPS Module

Figure 7 Red Led

A red LED works on the principle of eletro luminescence in a forward-biased P-N junction diode, where electrons and holes recombine to release energy as red photons (light). Figure 7 shows Red Led

5. Results

5.1.Telegram Interface

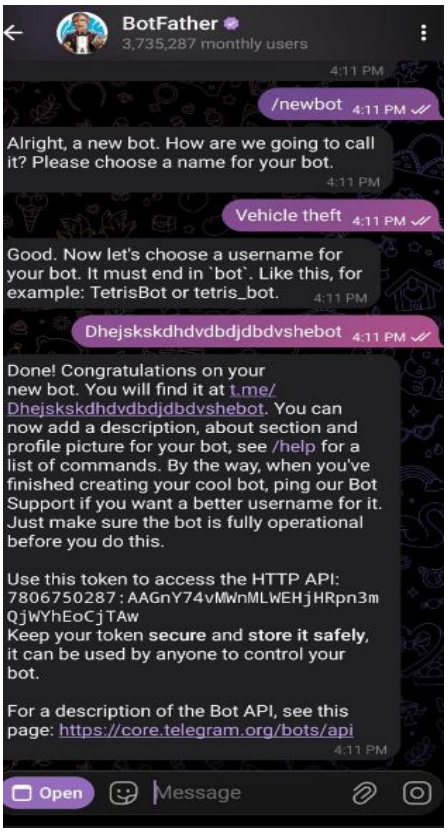

Figure 8 Owner Install Bot Father

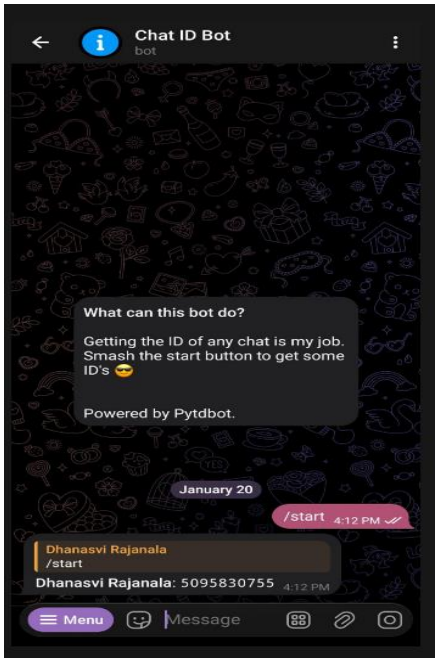

Figure 9 Owner Generate the ChatId

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

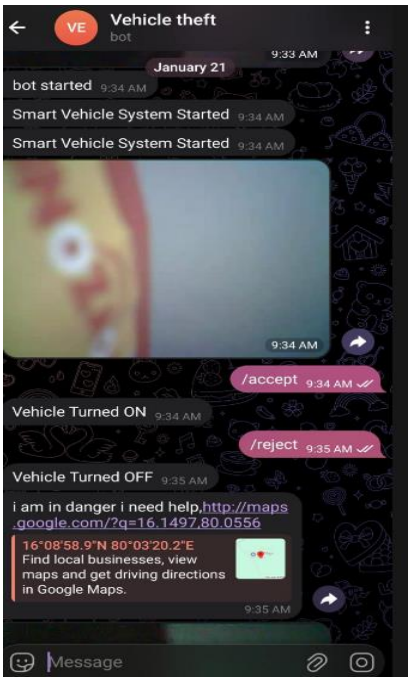

Figure 10 Accept and Reject and Image and GPS Location

5.2.Output Screens

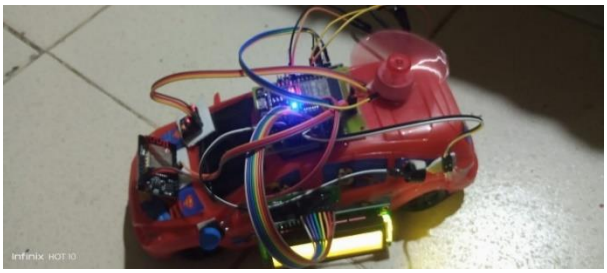

Figure 11 Owner Accept Case

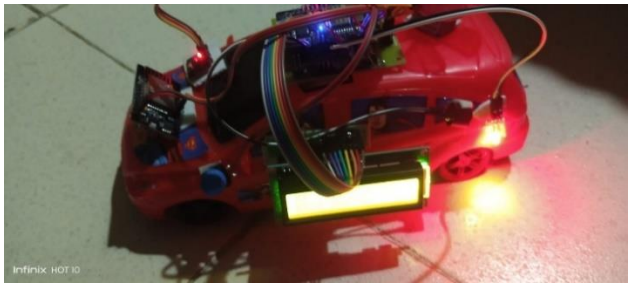

Figure 12 Owner Reject Case

The proposed vehicle anti-theft system was implemented using the ESP32-CAM, GPS module, relay, buzzer, and Telegram bot. The system was tested in real-time by simulating authorized and unauthorized vehicle start conditions. Whenever the vehicle ignition button was pressed, the ESP32-CAM successfully captured the image of the person and sent it to the vehicle owner through Telegram along with the live GPS location. This allowed the owner to clearly see who was attempting to start the vehicle and where the vehicle was located. If the owner approved the request, the ignition system was enabled and the vehicle started normally. If the owner rejected the request, the ignition remained locked and the buzzer was activated to indicate a theft attempt. In all test cases, the vehicle started only after owner approval, showing that the system effectively prevents unauthorized access. When abnormal vibrations were detected, the system immediately sent theft alert messages and GPS location details to the owner, helping in quick response. The communication between the ESP32-CAM and Telegram was fast, and notifications were received within a few seconds depending on internet availability. The system worked reliably without using complex face recognition algorithms or cloud-based processing, which reduced delay and hardware cost. Using Telegram as the user interface made the system easy to operate without the need for a separate mobile application. Overall, the results show that the proposed system provides a reliable, low-cost, and user-friendly solution for vehicle theft prevention. It improves vehicle security by combining real-time image capture, owner authorization, alert generation, and GPS tracking, making it suitable for practical and real-world applications.

Conclusion

This paper presented the design and implementation of an IoT-based smart vehicle anti-theft system using the ESP32-CAM module. The proposed system enhances vehicle security by integrating real-time image capture, owner authentication, GPS-based location tracking, and remote control through a Telegram bot. When an unauthorized access attempt is detected, the system captures the intruder's image, sends alerts to the vehicle owners, and enables the owner to remotely approve or deny vehicle ignition. In case of theft detection, the system activates security mechanisms such as motor locking, buzzer alert, while simultaneously transmitting the live location and image to the owner. The experimental results demonstrate that the proposed system

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

provides a reliable, low-latency, and user-friendly solution for vehicle theft prevention without the need for a dedicated mobile or web application. By leveraging existing communication platforms and embedded IoT hardware, the system ensures efficient monitoring and control with minimal complexity. The proposed approach is suitable for real-time deployment and can be extended in the future by incorporating cloud storage, advanced intrusion detection algorithms, and mobile application support for enhanced scalability and security.

Acknowledgements

The authors would like to express their sincere gratitude to [Project Guide Name], for their valuable guidance, continuous support, and constructive suggestions throughout the course of this project. Their expertise and encouragement played a vital role in the successful completion of this work. The authors also extend their thanks to the Head of the Department and faculty members of the Department of Computer Science and Engineering for providing the necessary resources and a conducive environment for carrying out this project. We are thankful to our friends and peers for their cooperation and assistance during the development of this project. Finally, we express our heartfelt gratitude to our family members for their constant motivation, understanding, and moral support.

References

[1]. Vehicle Anti-Theft Face Recognition System Based on IoT Using Raspberry pi (2025) S. Patel, R. Mehta, and A. Kumar, IEEE International Conference on Smart Computingand Communication, 2025. [Online] Available: https:// ieeexplore. ieee.org/ document/ 10543218

[2]. Hybrid Biometric Vehicle Security (Face + RFID) – SPIE 2025, M. Hassan, T. Rahman, and N. Islam, "Vehicle Anti-Theft System Using Hybrid Biometric Authentication and IoT," SPIE Conference on Intelligent Systems,2025.[Online]. Available: https://www.Spie digital library. org/conference-proceedings

[3]. [3] ESP32-CAM Based Face Recognition Anti-Theft System (2025) P. Reddy and S. Karthik, Low-Cost ESP32-CAM Based Vehicle Anti-Theft System Using Face Recognition," IEEE Access, vol. 13, 2025. [Online]. Available: https:// ieeexplore. ieee.org/document/ 10511890

[4]. Intelligent Facial Recognition System for Vehicles (2025) A. Verma and K. Singh, "Intelligent Facial Recognition System for Vehicle Security Using Deep Learning," IEEE International Conference on Artificial Intelligence and IoT, 2025. [Online]. Available:https://ieeexplore.ieee.org/document/10500327

[5]. Smart Anti-Theft Severity Logging System Using IoT (2024) R. Kumar and P. Jain, "Smart Vehicle Anti-Theft Severity Logging System Using IoT and Cloud," IEEE International Conference on Computing, Communication and Automation, 2024. [Online].Available:https:// ieeexplore. ieee.org/ document/ 10345621

[6]. Face Recognition Based Vehicle Starter Using ML (2022) Archana S., M. Priya, and R. Devi, "Face Recognition Based Vehicle Starter Using Machine Learning," International Journal of Engineering Research & Technology (IJERT), 2022.[Online].Available:https:// www. ijert. org/face-recognition-based-vehicle-starter

[7]. Intelligent Anti-Theft Face Recognition System (2021) K. Sharma and S. Gupta, "Intelligent Vehicle Anti-Theft System Using Face Recognition and IoT," IEEE International Conference on Smart Systems, 2021. [Online]. Available: https:// ieeexplore. ieee.org/document/9632451

[8]. Face Recognition System for Theft Prevention (2020) R. Singh and R. Raj, IoT Based Face Recognition System for Vehicle Theft Prevention," IEEE International Conference on Communication and Signal Processing, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9188743

[9]. Vehicle Anti-Theft System Using Facial Recognition and IoT (2019) S. Das and B. Prasad, "Vehicle Anti-Theft System Using Facial Recognition and IoT, IEEE

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 854-860
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0122

International Conference on Advanced Computing, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8976542

[10]. IoT-Based Biometric Automobile Theft Detection (2019) R. Kumar and S. Jain, IoT-Based Framework for Biometric Automobile Theft Detection and Driver Identification, IEEE International Conference on Internet of Things, 2019 [Online]. Available: https://ieeexplore.ieee.org/document/8893217