

Anti-Theft Vehicles Protection System Using ESP32

Mrs. Sushma M P¹, Punith kumar S², Rohan N³, Thippeswamy H R⁴, Pratham H A⁵

¹Assistant Professor, Department of ECE, PES College of Engineering Mandya, Karantaka, India

^{2,3,4,5}Students of ECE, PES College Of Engineering Mandya, Karnataka, India

Abstract - This project proposes an advanced anti-theft protection system for vehicles using the ESP32 microcontroller. The system prevents unauthorized motor activation by requiring a password entered through a keypad. Users have three attempts to enter the correct password. After three failed attempts, the system locks itself and sends an alert message with the GPS location to the vehicle owner via Telegram. The owner can remotely update the password through Telegram, restoring secure access. This method enhances vehicle security through IoT integration, real time alerts, location tracking, and remote password management.

Key Words: ESP32, Vehicles Protection, GPS Location, Keypad Verification, Microcontroller

1. INTRODUCTION

Vehicle theft remains a serious issue in both cities and rural regions. Conventional security methods such as locks, alarms, and immobilizers are often not enough to stop unauthorized access or provide immediate alerts to the owner. With the development of IoT technologies, microcontrollers, and real-time communication systems, it has become possible to build smarter and more automated security solutions. In this project, the ESP32, a Wi-Fi-enabled microcontroller, is used along with GPS and Telegram API integration to develop an advanced vehicle anti-theft system.

1.1 LITERATURE SURVEY

Numerous research works have been carried out in the field of smart vehicle security systems using IoT and embedded technologies. These systems typically rely on real-time data collected from sensors and microcontrollers to identify unauthorized access and enhance overall vehicle safety. The ESP32 microcontroller is widely adopted in such applications due to its integrated Wi-Fi and Bluetooth capabilities, which support efficient wireless communication and remote monitoring. In many proposed solutions, GPS modules are incorporated to enable real-time vehicle tracking, which assists in quick recovery in case of theft. Additionally, technologies such as RFID-based authentication, GSM alert systems, and mobile applications are commonly used to strengthen security and provide instant notifications to vehicle owners. Recent advancements have further explored cloud-based monitoring and mobile app integration to improve accessibility and control. Although several anti-theft systems have been proposed, integrating hardware-

based security with IoT-enabled communication offers a more reliable and practical solution.

1.2 PROPOSED METHODOLOGY

The proposed anti-theft system integrates password authentication, attempt monitoring, GPS tracking, and Telegram-based remote control to enhance vehicle security. A keypad interfaced with the ESP32 enables the user to input a password, which is verified against a value stored in the microcontroller's non-volatile memory. Each incorrect attempt increments a counter, and after three consecutive failures, the system disables the motor to prevent unauthorized access. Once the system is locked, the ESP32 obtains the current location from the Neo-6M GPS module and sends an alert message to the vehicle owner via the Telegram Bot API using a secure HTTPS connection. The alert includes real-time coordinates along with a Google Maps link for easy tracking. The system also allows remote recovery, where the owner can reset the password by sending a predefined command through the Telegram bot. The ESP32 continuously checks for such commands and, upon verifying the authorized user's chat ID, updates the stored password securely. After a successful reset, the system unlocks and resumes normal operation.

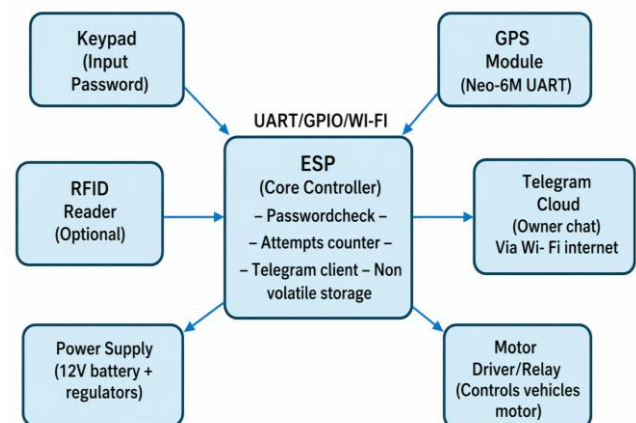


Fig-1: Block diagram of Anti-theft vehicles protection system using ESP32

2. WORKING MECHANISM

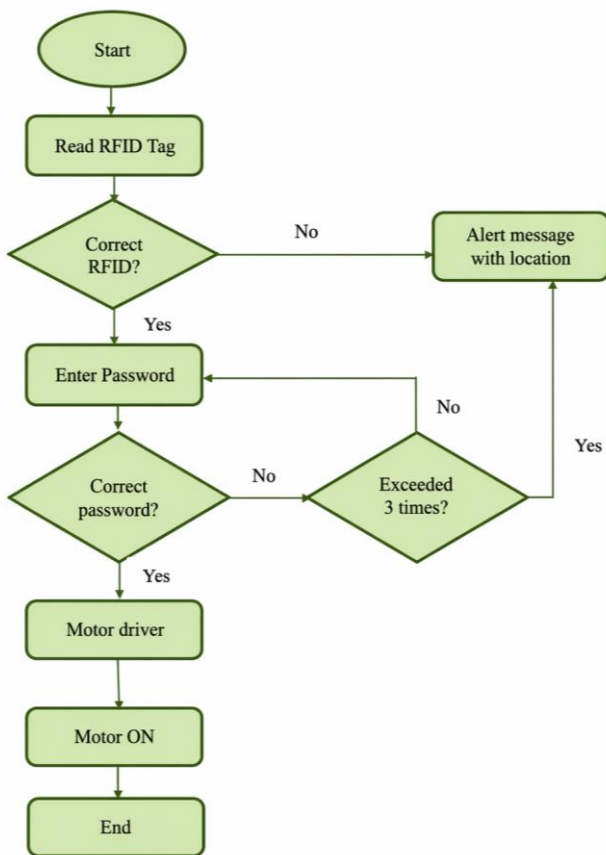


Fig-2: Flow chart for Anti-theft vehicles protection system using ESP32

The system begins by initializing and retrieving the previously stored password from the ESP32's non-volatile memory. The user then enters the password through a keypad interface, which is verified against the stored value. If the entered password is correct, the motor is activated (unlocked) and the attempt counter is reset to zero. In case of an incorrect password, the system increments the attempt counter. If the number of attempts remains below three, the user is allowed to retry password entry. However, once the attempt limit reaches three, the system enters LOCK mode and disables motor operation to prevent unauthorized access.

After locking, the ESP32 retrieves the current geographical coordinates (latitude and longitude) from the GPS module. A theft alert message, along with a Google Maps link of the vehicle location, is then sent to the owner via Telegram. The system subsequently waits for a remote command from the owner, such as "newpassword," through the Telegram bot. When a valid command is received from an authorized user, the ESP32 updates the stored password and unlocks the system. Finally, normal system operation is restored.

3. CIRCUIT EXPLANATION

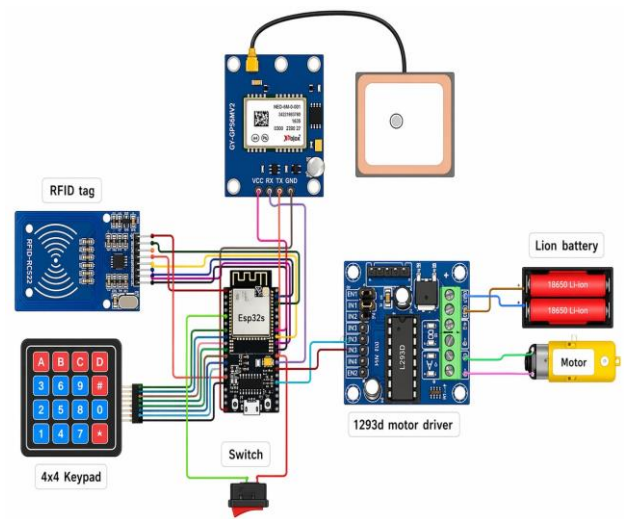


Fig 3: System circuit diagram

The circuit shown in Figure 3 consists of an ESP32 microcontroller acting as the central processing unit, interfaced with a keypad, GPS module (NEO-6M), buzzer, LED, and a Wi-Fi-based Telegram communication system. The keypad is connected to the ESP32 through digital GPIO pins and is used for entering the security PIN. The ESP32 continuously scans the keypad input and compares the entered PIN with the stored password.

If the entered password is correct, access is granted; otherwise, the system increments the count of incorrect attempts. The GPS module is interfaced with the ESP32 using UART communication, where the TX pin of the GPS module is connected to the RX pin (GPIO16) of the ESP32, and the RX pin of the GPS module is connected to the TX pin (GPIO17). The module is powered through the 5V supply to ensure stable performance.

Once a satellite fix is established, the GPS module provides real-time location data in terms of latitude and longitude. A buzzer and an LED are connected to the GPIO pins to provide audio and visual indications during incorrect password attempts or security breaches.

The ESP32 utilizes its built-in Wi-Fi capability to communicate with the Telegram Bot API. After three consecutive incorrect password entries, the system sends an alert message to the user via Telegram, including the vehicle's current location in the form of a Google Maps link. The user can then respond through Telegram to securely reset the PIN. This integration of hardware components and wireless communication ensures enhanced security and real-time monitoring in the proposed anti-theft vehicle protection system.

4. RESULTS AND DISCUSSION

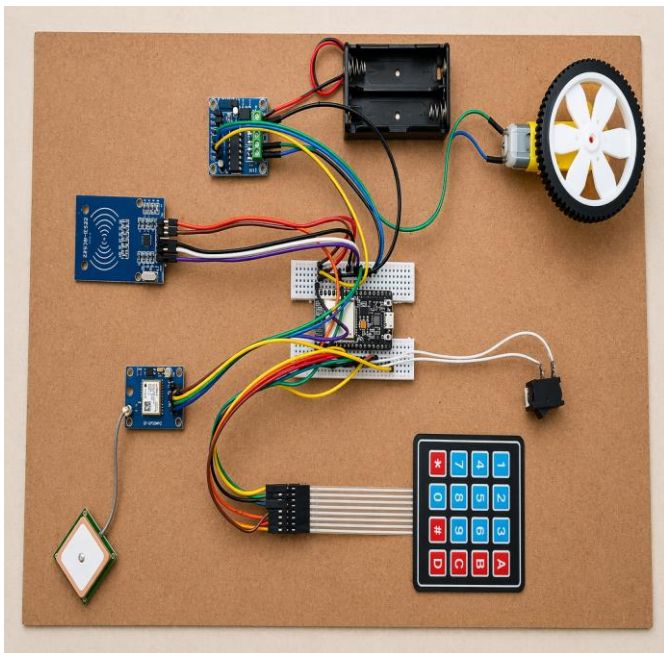


Fig 4: System model

The implemented system, as shown in Figure 4, successfully demonstrates real-time vehicle security monitoring and alert generation. During testing, the keypad accurately detected user inputs and validated the entered PIN with minimal delay. When three consecutive incorrect password attempts were made, the system reliably triggered an alert through Telegram, confirming effective intrusion detection.

The integration of the GPS module enabled the system to obtain real-time location data; however, initial satellite acquisition required outdoor conditions and a short stabilization period. The Telegram communication system, as shown in Figure 4, functioned efficiently, allowing users to receive alerts and remotely reset the PIN without delay.

The system also handled edge cases effectively, such as notifying the user when GPS signals were unavailable. Additionally, the implementation of a cooldown mechanism after reset cancellation improved security by preventing repeated unauthorized attempts.

Overall, the system proved to be robust, responsive, and suitable for real-world vehicle security applications, effectively combining embedded system design with IoT-based communication capabilities.



Fig 5: Telegram dashboard

5. OBSERVATION TABLE

Table 8.1 presents various test conditions applied to the system along with the corresponding inputs and observed responses. It illustrates the system's behavior under both normal and abnormal scenarios, including correct and incorrect password entries, GPS availability, and Telegram-based user interactions. The results confirm that the system operates as intended by granting access for valid inputs, generating warnings for incorrect attempts, and triggering alert notifications after multiple failed entries. The table also demonstrates the system's ability to function effectively under real-world conditions, such as the absence of GPS signals, while still maintaining core functionality. Additionally, it highlights the implementation of security features such as cooldown periods and controlled password reset through Telegram, which further improve the reliability and robustness of the system.

Table 1: Observation Table

SL.NO	Test Condition	Input Given	System Response
1	Correct PIN	Valid PIN	Access granted
2	Wrong PIN (1st attempt)	Incorrect PIN	Warning message displayed
3	Wrong PIN (3 attempts)	Incorrect PIN	Telegram alert sent
4	GPS Fix Available	Outdoor condition	Location sent as Google Maps link
5	No GPS Fix	Indoor condition	"No GPS fix" message displayed
6	Telegram Reset YES	YES command	Allows PIN reset
7	Telegram Reset NO	NO command	Reset cancelled
8	Cooldown Active	Immediate retry	Request temporarily blocked

6. EXPECTED OUTCOMES

The primary objective of developing a smart vehicle security system using ESP32 and IoT technologies has been successfully achieved. The system ensures secure access through keypad-based password authentication, effectively preventing unauthorized usage. The integration of GPS technology enables real-time tracking of the vehicle, thereby enhancing safety and monitoring capabilities.

Furthermore, the implementation of Telegram-based communication provides instant alert notifications and supports remote control features, making the system both efficient and user-friendly. The project incorporates multiple layers of security, including password verification, alert generation after repeated incorrect attempts, and a secure password reset mechanism.

In addition, the inclusion of a cooldown mechanism further strengthens protection against repeated unauthorized access attempts. Overall, the developed system demonstrates a reliable, cost-effective, and scalable solution for modern vehicle security by effectively integrating embedded systems with IoT-based communication technologies.

7. FUTURE SCOPE

The proposed ESP32-based anti-theft vehicle protection system provides a cost-effective and reliable solution for vehicle security, with significant scope for future enhancements. A dedicated mobile application can replace or complement Telegram for improved user experience and real-time monitoring. Security can be strengthened using advanced biometrics such as face or iris recognition. Cloud storage and data analytics can enable historical tracking and intelligent alerts, while geofencing can notify users when a

vehicle exits safe zones. Integration with OBD-II systems and camera modules can further enhance functionality. Low-power optimization and AI-based threat detection can also be incorporated for better efficiency. Overall, the system can evolve into an intelligent, scalable, and fully automated vehicle security solution.

8. CONCLUSIONS

The developed ESP32-based anti-theft vehicle protection system successfully achieves its primary objective of enhancing vehicle security through real-time monitoring and intelligent control. The system integrates keypad-based password authentication, GPS tracking, and Telegram-based communication to provide a reliable and efficient security solution. It effectively prevents unauthorized access by monitoring password attempts and triggering alerts after repeated failures. The integration of GPS enables real-time location tracking, which improves the chances of quick vehicle recovery in case of theft. Additionally, Telegram-based notifications allow instant alerts and remote control features, making the system user-friendly and accessible from anywhere.

Overall, the project demonstrates a practical implementation of IoT and embedded technologies, offering a cost-effective and scalable solution for modern vehicle security. It also shows strong potential for future enhancements and real-world applications.

REFERENCES

- [1] Pawaskar M, Samant M, and Hardas A, "Microcontroller Based Anti-theft Vehicle System", International Journal of Computer Sciences and Engineering, Vol. 7, Issue: 5, pp. 765–768, 2019.
- [2] Yakubu Yakubu Musa and Jin Wang, "Vehicle Tracking and Anti-theft System using GPS-GSM", International Journal of Engineering Research & Technology, ISSN: 2278-0181, Vol. 1, Issue: 10, pp. 1–5, 2012.
- [3] Kadiri Kamoru and O. Adekoya Adegoke, "Design of a GPS/GSM Based Anti-theft Car Tracker System", Current Journal of Applied Science and Technology, Vol. 34, Issue: 3, pp. 1–8, 2019.
- [4] Vaibhav V. Gijare, Anand Sapkal, Pratik Rengade, Atharv Kulkarni, and Pratik Bangar, "Smart Vehicle Theft Detection System with Real-time Monitoring", Research & Review: Electronics and Communication Engineering, 2025.
- [5] G. N. Sandhya Devi, B. Rakesh, Ch. Naga Gopi, Ch. Anusha, and B. Lakshman Kumar, "Biometric-Based Anti-Theft Vehicle Security System with Fingerprint and Face Recognition", International Journal of Scientific Research in Science and Technology, Vol. 5, Issue: 24, 2024.