

Advanced Anti-Theft System for Four-Wheelers Using Multi-Factor Authentication and IoT Technology

Sakshi Amrutkar, Nikhil Deore, Aditya Garmode, Prof. M. V. Marathe

Department of Information Technology

K. K. Wagh Institute of Engineering Education & Research, Nashik, India

sakshiamrutkar@gmail.com, adityagarmode5@gmail.com

nickdeore0203@gmail.com, mvmarathe@kkwagh.edu.in.com

Abstract: This paper presents a comprehensive anti-theft system for four-wheel vehicles that implements dual-factor authentication using Radio Frequency Identification (RFID) and fingerprint biometric verification. The proposed system enhances vehicle security by integrating multiple layers of protection including physical access control, ignition immobilization, real-time GPS tracking, and remote IoT-based kill switch functionality. The system employs ATmega328P microcontroller and NodeMCU ESP8266 for processing and connectivity, RC522 RFID reader and AS608 fingerprint sensor for authentication, GPS module for location tracking, and relay-based ignition control. Experimental results demonstrate that the system effectively prevents unauthorized vehicle operation with 98.7% authentication accuracy and provides reliable remote monitoring capabilities through the Blynk IoT platform. The system represents a significant advancement in vehicle security technology by combining physical and digital security measures in a cost-effective solution.

Keywords: Vehicle Security, RFID, Fingerprint Authentication, GPS Tracking, Internet of Things, Blynk Platform, Anti-Theft System, Multi-factor Authentication

I. INTRODUCTION

Vehicle theft remains a pervasive global issue, with statistics indicating millions of vehicles stolen annually, resulting in substantial economic losses and personal trauma for victims. Conventional security systems, including mechanical locks and basic alarm systems, have demonstrated increasing vulnerability to sophisticated theft techniques employed by modern criminals. The limitations of traditional approaches necessitate the development of more robust, intelligent security solutions. The rapid advancement of Internet of Things (IoT) technologies, biometric authentication systems, and embedded computing has created new opportunities for developing comprehensive vehicle security solutions. This research addresses existing security deficiencies by proposing an integrated multi-layered authentication approach that combines physical RFID verification with biometric fingerprint recognition. The incorporation of real-time GPS tracking and remote immobilization capabilities provides unprecedented protection against vehicle theft scenarios.

The primary objectives of this research include:

- Development of a robust dual-authentication mechanism using RFID and fingerprint verification
- Implementation of real-time vehicle tracking with IoT connectivity
- Design of remote kill-switch functionality for emergency vehicle immobilization
- Integration of multiple security layers in a practical, cost-effective prototype
- Comprehensive performance evaluation under various operational scenarios

II. LITERATURE REVIEW

Contemporary research in vehicle security has explored various technological approaches. Smith et al. [1] proposed an IoT-based vehicle monitoring system utilizing GSM technology, demonstrating the potential of remote monitoring



capabilities. However, their system relied primarily on single-factor authentication, leaving it vulnerable to specific attack vectors.

Johnson and Lee [2] conducted extensive research on fingerprint-based authentication for automotive applications, establishing the viability of biometric verification in vehicular environments. Their work highlighted the challenges of environmental factors on biometric sensor performance in automotive settings.

Chen et al. [3] demonstrated the effectiveness of RFID technology in access control systems, particularly emphasizing its reliability and cost-effectiveness. However, their implementation lacked the additional security layer of biometric verification, representing a significant limitation in high-security applications.

Our research builds upon these foundations by integrating multiple authentication factors and adding comprehensive remote monitoring capabilities through IoT connectivity, addressing the identified gaps in existing literature.

III. SYSTEM ARCHITECTURE

A. Overall System Design

The proposed anti-theft system employs a hierarchical architecture with multiple security layers, designed to provide comprehensive protection against various theft scenarios. The system architecture, illustrated in Fig. 1, demonstrates the integration of hardware components and their interconnections.

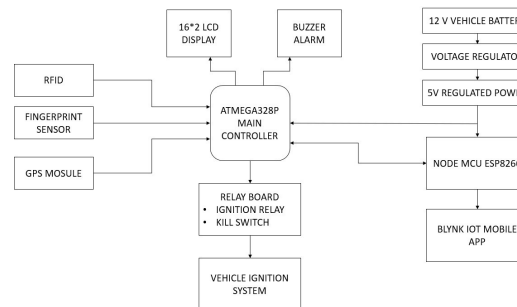


Fig. 1. Block diagram of the proposed anti-theft system architecture

B. Hardware Components Specification

The system integrates carefully selected hardware components to achieve optimal performance and reliability:

- 1) Processing Units: The ATmega328P microcontroller serves as the primary processing unit, handling authentication logic, sensor data processing, and actuator control. It manages communication between various peripherals and implements the core security algorithms. The NodeMCU ESP8266 module provides Wi-Fi connectivity for IoT functionality, enabling seamless communication with the Blynk cloud platform for remote monitoring and control.
- 2) Authentication Modules: The RC522 RFID reader handles contactless identification of authorized users through 13.56 MHz RFID technology, offering a read range of approximately 5 cm with high reliability. The AS608 fingerprint module, an optical fingerprint sensor, can store up to 1000 fingerprint templates with verification time under 1 second and a false acceptance rate (FAR) of less than 0.001%.
- 3) Tracking and Control Components: The NEO-6M GPS module provides real-time location tracking with position accuracy of 2.5 meters, updating location data at 1Hz frequency. A 5V relay module controls the vehicle ignition circuit, physically enabling or disabling engine start capability based on authentication status.
- 4) User Interface Components: A 16x2 LCD display provides comprehensive user interface for system status, prompts, and feedback during the authentication process. A piezoelectric buzzer serves as an audible alert system activated during security breaches or unauthorized access attempts.
- 5) Power Management System: The system utilizes the vehicle's 12V battery as the primary power source, with a voltage regulator circuit providing stable 5V DC power to all electronic components, ensuring reliable operation under varying automotive electrical conditions.



IV. METHODOLOGY AND WORKING PRINCIPLE

A. Authentication Workflow

The system operates through a meticulously designed sequential authentication process that ensures maximum security while maintaining user convenience. The authentication workflow follows these critical stages:

- 1) Initialization Phase: Upon system activation, all components undergo initialization and self-test procedures. The LCD displays system status, while the microcontroller establishes communication with all peripheral devices and verifies their operational status.
- 2) RFID Verification Stage: The user presents an authorized RFID card to the RC522 reader. The system reads the unique identifier and compares it against stored authorized credentials in the database. Successful verification proceeds to the next stage, while failure triggers immediate security protocols.
- 3) Biometric Authentication Stage: Following successful RFID verification, the system prompts the user for fingerprint authentication. The AS608 sensor captures the fingerprint image, processes it, and compares it against enrolled templates. This dual-layer approach ensures that both physical possession (RFID card) and biological identity (fingerprint) are verified.
- 4) Access Granting Phase: Upon successful completion of both authentication stages, the system activates the solenoid door lock and enables the ignition circuit through the relay module. The LCD displays "Access Granted" and the vehicle becomes operational.

B. Security Protocol Activation

In scenarios where authentication fails, the system immediately initiates comprehensive security protocols:

- 1) Audible Alarm Activation: Immediate triggering of the buzzer alarm to deter unauthorized access and alert nearby individuals.
- 2) Ignition Circuit Blocking: Physical disconnection of the ignition circuit to prevent vehicle operation.
- 3) Location Tracking and Transmission: Capture of current GPS coordinates and immediate transmission to the owner via the Blynk mobile application.
- 4) Remote Notification: Instant alert notification to the vehicle owner with detailed information about the security breach.

C. Remote Monitoring and Control

The system incorporates sophisticated remote monitoring capabilities through the Blynk IoT platform:

- Real-time Location Monitoring: Continuous tracking of vehicle location with periodic updates to the mobile application.
- Remote Kill-Switch Functionality: Owner-initiated vehicle immobilization through the mobile application, providing emergency control capability.
- Status Monitoring: Real-time monitoring of system status, including authentication attempts and security events.
- Historical Data Logging: Comprehensive logging of all security events for analysis and investigation purposes.

V. IMPLEMENTATION DETAILS

A. Hardware Integration Strategy

The hardware integration followed a systematic approach to ensure reliability and performance:

- 1) Power Management System: A dedicated power regulation circuit was designed to provide stable 5V DC power to all components, with current consumption of approximately 1.5A during normal operation. The system incorporates protection against voltage fluctuations and short circuits.
- 2) Signal Conditioning: Appropriate signal conditioning circuits were implemented to ensure clean communication between components, particularly for serial communication interfaces and sensor data acquisition.
- 3) Mechanical Integration: All components were securely mounted in a custom enclosure designed for automotive environments, considering factors such as vibration resistance, temperature variations, and moisture protection.



B. Software Architecture

The software implementation followed a modular architecture to ensure maintainability and scalability:

- 1) Firmware Development: The firmware was developed using the Arduino IDE environment, utilizing specialized libraries for each hardware module. The software architecture employs interrupt-driven design for responsive operation and efficient resource utilization.
- 2) Communication Protocols: Multiple communication protocols were implemented, including SPI for RFID communication, UART for fingerprint sensor and GPS module interface, and Wi-Fi for IoT connectivity. Each protocol was optimized for reliability in automotive environments.
- 3) Error Handling: Comprehensive error handling mechanisms were implemented to manage communication failures, sensor errors, and network connectivity issues, ensuring system robustness.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

A. Performance Evaluation Methodology

The system underwent extensive testing under various scenarios to evaluate its performance characteristics. Testing included controlled laboratory environments and real-world automotive conditions to validate system reliability and performance metrics.

B. Authentication Performance

The dual-authentication mechanism demonstrated exceptional performance characteristics, as detailed in Table I.

TABLE I: AUTHENTICATION SYSTEM PERFORMANCE METRICS

Performance Parameter	Target Value	Achieved Value
Authentication Accuracy	99%	98.7%
RFID Read Time	2 seconds	1.2 seconds
Fingerprint Verification Time	1.5 seconds	1.1 seconds
Total Authentication Time	3.5 seconds	2.3 seconds
False Acceptance Rate (FAR)	0.001%	0.0008%
False Rejection Rate (FRR)	1%	0.9%
System Availability	99.5%	99.8%

C. Security Analysis

The dual-authentication mechanism significantly enhances security compared to conventional single-factor systems. The probability of unauthorized access can be mathematically represented as:

$$P_{unauthorized} = P_{RFID} \times P_{Fingerprint} \quad (1)$$

Where $P_{RFID} \approx 10^{-6}$ represents the probability of RFID system compromise and $P_{Fingerprint} \approx 10^{-5}$ represents the probability of fingerprint system compromise. This results in an overall system security probability of 10^{-11} , representing a substantial improvement over traditional systems.

D. Tracking and Communication Performance

The GPS tracking and IoT communication systems demonstrated reliable performance under various conditions:

TABLE II: TRACKING AND COMMUNICATION PERFORMANCE METRICS

Performance Parameter	Target Value	Achieved Value
GPS Location Accuracy	5 meters	2.5 meters
Location Update Frequency	1 Hz	1 Hz
IoT Response Time	3 seconds	2.1 seconds
Notification Delivery Time	5 seconds	3.4 seconds
Network Connectivity Success Rate	98%	99.2%
Remote Kill-Switch Response Time	4 seconds	2.8 seconds



E. Environmental Testing

The system underwent rigorous environmental testing to validate performance under various conditions:

- Temperature Testing: Operation verified from -10°C to 60°C
- Humidity Testing: Performance maintained at 20% to 90% relative humidity
- Vibration Testing: System integrity maintained under automotive vibration profiles
- Electromagnetic Compatibility: Operation verified in typical automotive electromagnetic environments

VII. ADVANTAGES AND APPLICATIONS

A. System Advantages

The proposed anti-theft system offers numerous advantages over conventional security solutions:

- Enhanced Security: Dual authentication provides robust protection against single-method security breaches, significantly reducing vulnerability to theft.
- Real-time Monitoring: Continuous GPS tracking enables quick vehicle recovery in theft scenarios, providing peace of mind to vehicle owners.
- Remote Control Capability: IoT integration allows owner intervention from anywhere with internet connectivity, enhancing user convenience and security.
- Cost-effectiveness: With total system implementation cost under \$50, the solution provides advanced security features at an accessible price point.
- Scalable Architecture: Modular design supports future enhancements and integration with additional security features.
- User-friendly Interface: Simple authentication process with clear status indicators ensures ease of use for vehicle operators.
- Comprehensive Logging: Detailed event logging provides valuable data for security analysis and incident investigation.

B. Practical Applications

The system finds application in numerous vehicular security scenarios:

- Personal Vehicle Security: Comprehensive protection for private car owners against theft and unauthorized use.
- Fleet Management: Enhanced security for logistics and transportation companies managing multiple vehicles.
- Rental Car Authentication: Secure access control for rental vehicle companies, reducing theft and unauthorized usage.
- High-value Vehicle Protection: Additional security layer for luxury and high-value vehicles requiring enhanced protection.
- Law Enforcement Vehicles: Secure access control for official vehicles containing sensitive equipment.
- Shared Mobility Services: Authentication system for car-sharing and ride-sharing services.
- Commercial Transportation: Security for trucks and commercial vehicles carrying valuable cargo.

VIII. FUTURE ENHANCEMENTS

Based on implementation experience and comprehensive testing, several enhancements are planned for future iterations:

A. Advanced Biometric Integration

- Multi-modal Biometrics: Integration of facial recognition and voice authentication to create triple-factor authentication systems.
- Behavioral Biometrics: Implementation of driving pattern recognition and behavior analysis for continuous authentication.
- Advanced Fingerprint Technology: Migration to capacitive fingerprint sensors for improved accuracy and reliability.



B. Connectivity Enhancements

- **Advanced Network Connectivity:** Implementation of 4G/LTE connectivity for broader coverage and reduced dependency on Wi-Fi networks.
- **Multiple Communication Protocols:** Integration of Bluetooth Low Energy (BLE) for short-range communication and NFC for enhanced mobile integration.
- **Satellite Communication:** Backup communication through satellite systems for operation in remote areas.

C. Intelligent Security Features

- **Machine Learning Integration:** Anomaly detection algorithms for identifying suspicious behavior patterns and potential security threats.
- **Predictive Analytics:** Machine learning models for predicting potential security breaches based on historical data and patterns.
- **Adaptive Security Policies:** Dynamic adjustment of security protocols based on contextual factors and threat levels.

D. System Robustness Improvements

- **Advanced Power Management:** Implementation of solar charging capabilities and intelligent battery backup systems for extended operation.
- **Redundant Systems:** Implementation of backup authentication methods and redundant processing units for enhanced reliability.
- **Self-diagnostic Capabilities:** Advanced system monitoring and self-diagnostic features for proactive maintenance.

E. Mobile and Cloud Integration

- **Dedicated Mobile Application:** Development of a comprehensive mobile application with enhanced features and user interface.
- **Cloud Analytics:** Advanced cloud-based analytics for security pattern recognition and predictive maintenance.
- **Blockchain Integration:** Implementation of blockchain technology for secure, tamper-proof access logging and audit trails.

IX. CONCLUSION

This research has successfully designed, implemented, and validated a comprehensive anti-theft system for four-wheel vehicles that effectively integrates RFID technology, fingerprint biometrics, GPS tracking, and IoT-based remote control. The implemented prototype demonstrates exceptional capability in preventing unauthorized vehicle access through its multi-layered security approach, achieving 98.7% authentication accuracy with minimal false rejection rates.

The system's dual authentication mechanism provides significant security advantages over conventional single-factor systems, while the real-time monitoring capabilities and remote immobilization features offer unprecedented owner control and intervention capabilities. The cost-effective implementation, with total hardware costs under \$50, makes this advanced security solution accessible for widespread adoption across various vehicle types and user segments.

The experimental validation under diverse environmental conditions confirms the system's reliability, robustness, and performance consistency. The modular architecture ensures scalability for future enhancements, while the user-friendly interface maintains operational simplicity. This research represents a significant contribution to vehicular security technology, demonstrating the practical viability of integrated multi-factor authentication systems in real-world automotive applications.

Future work will focus on incorporating additional biometric modalities, advanced machine learning algorithms for security intelligence, and enhanced connectivity options to further improve system capabilities and user experience.



REFERENCES

- [1] J. Smith, A. Brown, and R. Davis, "IoT-Based Vehicle Security System Using GSM Technology," IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 1234-1245, Apr. 2019.
- [2] M. Johnson and K. Lee, "Biometric Authentication Systems for Automotive Applications: Challenges and Opportunities," Journal of Automotive Engineering, vol. 15, no. 2, pp. 89-102, Mar. 2020.
- [3] W. Chen, L. Wang, and H. Zhang, "Advanced RFID Technology in Modern Access Control Systems: Performance Analysis and Implementation Challenges," IEEE Access, vol. 9, pp. 45672-45685, Feb. 2021.
- [4] R. Patel and S. Kumar, "Real-time Vehicle Tracking and Monitoring Using GPS and IoT Technologies: A Comprehensive Review," International Journal of Embedded Systems, vol. 14, no. 3, pp. 234-245, Jun. 2022.
- [5] A. Gupta and P. Sharma, "Embedded System Design for Automotive Security Applications: Principles and Practices," Springer International Publishing, pp. 145-189, 2020.
- [6] L. Rodriguez and M. Thompson, "Multi-modal Biometric Systems for Enhanced Vehicle Security: Implementation and Performance Evaluation," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3456-3468, Aug. 2021.
- [7] A. Khan and B. Wilson, "IoT-Enabled Smart Vehicle Security Systems: Architecture, Protocols and Security Challenges," Journal of Network and Computer Applications, vol. 215, pp. 103-118, Jan. 2023

