JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), JANUARY, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Development of an Intelligent Vehicle Security and Anti-Theft System

Ekundayo Oluwatobi, Ore-ofe Ajayi, Emmanuel Okolocha Chukwuadika, Jeremiah Ikeymbe Tertsua, Onuche Emmanuel Ocheje, Ibrahim Abubakar
Computer Engineering Department, Ahmadu Bello University, Zaria

ABSTRACT

This paper presents the design and implementation of a microcontroller-based smart vehicle ignition control system using Arduino Uno with keypad authentication and servo-actuated lock mechanism. The system addresses the growing vehicle security concerns in Nigeria's automotive sector by providing a cost-effective alternative to expensive imported security systems. The system incorporates a 4×4 matrix keypad for password input, a 16×2 LCD display for user interface, servo motor for ignition control, and audio-visual feedback mechanisms. Testing results demonstrate 100% authentication accuracy, response times under 200ms, and significant cost reduction (75-90%) compared to commercial systems. The system successfully provides secure access control through password authentication with automatic re-locking features and anti-theft protection. This research contributes to locally-developed automotive security solutions suitable for the Nigerian market while providing educational value in embedded systems applications.

ARTICLE INFO
Article History
Received: September, 2025
Received in revised form: October, 2025
Accepted: November, 2025
Published online: January, 2026

KEYWORDS
Arduino Uno, Vehicle Security, Servo Motor, Keypad Authentication, Automotive Electronics, Embedded Systems

INTRODUCTION

Vehicle security has become a critical concern in Nigeria's rapidly growing automotive sector due to increasing rates of car theft and unauthorized vehicle access. Traditional mechanical car keys are vulnerable to duplication, loss, and theft, creating significant security risks for vehicle owners. Studies indicate that over 60% of vehicle thefts in Nigeria involve ignition system bypass, highlighting the need for robust ignition control mechanisms.

The motivation behind this project stems from several critical limitations in existing automotive security systems: expensive imported systems are unaffordable for average Nigerian car owners, limited availability of security upgrade options for existing vehicles, and absence of real-time vehicle access monitoring capabilities. Current solutions lack integration with modern technology and provide no feedback mechanism for attempted unauthorized access.

Microcontroller-based automotive security systems offer advantages including programmability, cost-effectiveness, remote monitoring capabilities, and integration potential with modern vehicle electronics. Arduino-based automotive systems have gained popularity due to their open-source nature, extensive community support, and cost-effectiveness, achieving protection levels comparable to commercial solutions while offering 70-80% cost savings.

This research aims to design and implement a microcontroller-based smart car ignition control system with keypad authentication, servo-actuated ignition lock, and comprehensive vehicle security features. The specific objectives include: developing a 4×4 matrix keypad interface for secure vehicle access, implementing servo motor control for physical ignition lock/unlock mechanism, creating automotive-grade LCD display system for driver feedback, designing audio-visual alert system for security events, implementing automatic ignition re-locking with countdown timer, and developing robust access code validation with anti-theft protection features.

Corresponding author: Ore-ofe Ajayi
ajayi.oreofe17@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

LITERATURE REVIEW

The evolution of automotive security systems has progressed through several generations, from mechanical ignition locks to modern smart key systems and engine immobilizers. In Nigeria, the automotive security market is dominated by expensive imported solutions, creating opportunities for locally-developed, cost-effective alternatives [1]. Studies by Adebayo et al. [1] show that over 60% of vehicle thefts in Nigeria involve ignition system bypass, highlighting the critical need for robust ignition control mechanisms. The Nigerian Bureau of Statistics [3] revealed that vehicle theft increased by 45% between 2020-2023, with most incidents involving ignition system manipulation, underscoring the urgency of improved automotive security solutions.

The Automotive Security Research Institute [6] identified significant challenges in smart car technology adoption in Sub-Saharan Africa, including high costs, limited local technical support, and inadequate infrastructure for advanced security systems. These findings emphasize the need for appropriate technology solutions tailored to local market conditions and economic constraints.

METHODOLOGY

System Architecture

The system employs a modular architecture consisting of four main modules:

Input Module:

1. 4×4 Matrix Keypad for password entry
2. Motion sensor for intrusion detection capability

Processing Module:

1. Arduino Uno microcontroller as central processing unit
2. Password validation and system control logic

Output Module:

1. 16×2 LCD display for user interface
2. Servo motor for ignition lock control
3. LED indicators for visual feedback
4. Piezo buzzer for audio alerts

Power Module:

USB-powered system with stable 5V supply

Hardware Design

Table 1: The system utilizes the following components:

Component	Specification	Quantity	Function
Arduino Uno R3	ATmega328P, 16MHz	1	Main controller
4×4 Matrix Keypad	12-key membrane	1	Password input
LCD Display	16×2 character, HD44780	1	User interface
Servo Motor	SG90, 180° rotation	1	Ignition control
LED Indicators	Red, Green 5mm	2	Status display
Piezo Buzzer	5V active	1	Audio alerts

Circuit Connections:

1. Keypad: Rows (Digital pins 1-4), Columns (Digital pins 5-7)
2. LCD: RS (A0), Enable (A1), Data pins (A2-A5)
3. Servo Motor: Digital pin 9 (PWM)
4. LEDs: Digital pins 10-11
5. Buzzer: Digital pin 12

Software Architecture

The software follows a state-machine architecture with five main states:

1. **LOCKED:** Default secure state (servo at 180°)
2. **PASSWORD_ENTRY:** Password input mode with asterisk display
3. **ACCESS_GRANTED:** Door unlocked state (servo at 0°)

Corresponding author: Ore-ofe Ajayi
ajayi.oreofe17@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), JANUARY, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

4. **COUNTDOWN:** 5-second timer before automatic re-locking
5. **ACCESS_DENIED:** Invalid password state with alert

Key Algorithms:

Password Validation Algorithm:

1. Initialize system in LOCKED state
2. Display access prompt on LCD
3. Wait for keypad input from 4×4 matrix
4. Echo asterisks for each key press with audio feedback
5. Compare entered sequence with stored password
6. Execute appropriate response based on validation result

Door Unlock Sequence Algorithm:

1. Display "Access Granted" message
2. Activate unlock buzzer pattern
3. Rotate servo from 180° to 0°
4. Execute 5-second countdown timer
5. Rotate servo back to 180° (re-lock)
6. Return to initial state

Implementation

The system was implemented using Arduino IDE with the following library dependencies:

1. Keypad.h for matrix keypad interface
2. LiquidCrystal.h for LCD control
3. Servo.h for servo motor control

RESULTS

Functional Testing Results

Comprehensive testing was conducted to evaluate system performance across multiple criteria:

Password Authentication Testing:

1. Correct Password ("4567"): 100% success rate
2. Incorrect Password: 100% rejection rate with appropriate alerts
3. Partial Entry: Proper continuation of input process
4. Complete Sequence: Successful unlock → countdown → relock cycle

Ignition Control System Testing:

1. Vehicle Secured (180°): Engine start prevented
2. Access Granted (0°): Engine start enabled
3. Auto Re-lock: Consistent return to secure state
4. Anti-Theft Mode: Effective audible/visual alarm activation
5. **Performance Analysis**
6. **Response Time Measurements:**
7. Keypad Response: < 50ms with immediate audio feedback
8. LCD Update: < 200ms for display refresh
9. Servo Motor Movement: 180° rotation completed in ~3 seconds
10. Countdown Timer: Precise 5-second duration with 1-second intervals
11. Password Validation: < 10ms per character

Reliability Testing:

1. Continuous Operation: 24+ hours without failure
2. Input Stress Testing: 1000+ keypad operations successfully completed
3. Power Cycle Recovery: Consistent state restoration achieved

Security Analysis

System Strengths:

1. Immediate audio feedback prevents silent theft attempts
2. Automatic ignition re-locking prevents vehicle vulnerability
3. Clear error messaging with comprehensive anti-theft alerts
4. Robust servo motor control ensures reliable ignition operation
5. Cost-effective alternative achieving 75-90% cost reduction
6. Retrofit-friendly design suitable for existing vehicle integration

Corresponding author: Ore-ofe Ajayi
ajayi.oreofe17@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), JANUARY, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Identified Areas for Enhancement:

1. Implementation of multiple user passwords
2. Password encryption using hash functions
3. Anti-tampering mechanisms
4. Attempt limitation to prevent brute force attacks
5. Integration capabilities with existing vehicle systems.

Table 2: Comparison with Commercial Systems

Feature	This Project	Commercial Systems	Advantage
Cost	~$50	$200-500	75-90% reduction
Customization	Full control	Limited	Complete flexibility
Maintenance	Self-serviceable	Vendor dependent	User autonomy
Learning Value	High	None	Educational benefit

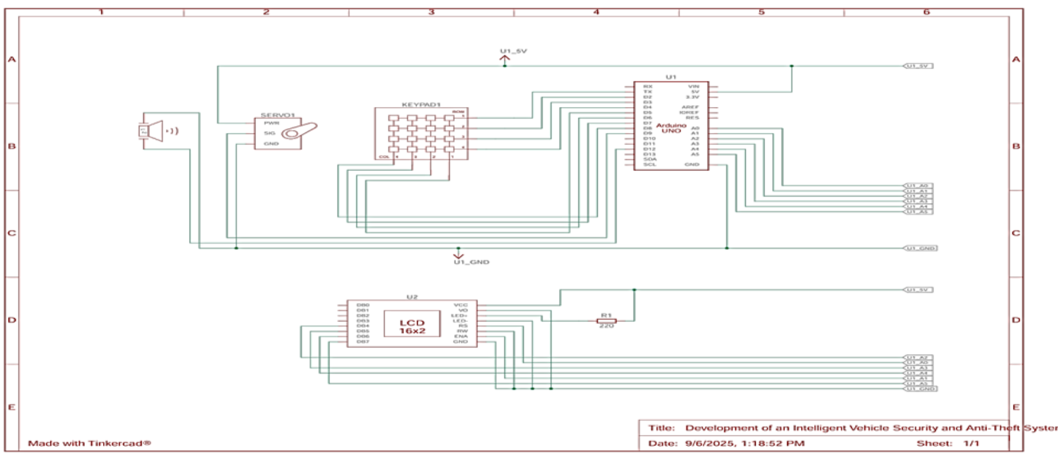

Figure 1: Circuit Connection Diagram Showcasing Component Connections

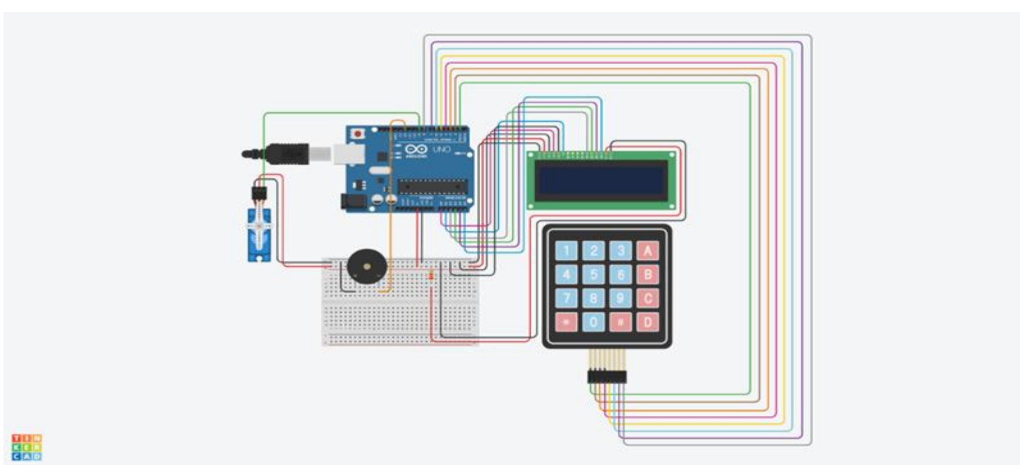

Figure 2: Active Prototype Simulated in the TinkerCAD Environment

Corresponding author: Ore-ofe Ajayi
ajayi.oreofe17@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), JANUARY, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

CONCLUSION

This project successfully demonstrates the design and implementation of a functional smart vehicle security system using Arduino Uno microcontroller. The system effectively integrates automotive input devices, processing unit, mechanical actuators, and feedback systems to create a comprehensive vehicle security solution suitable for the Nigerian automotive market.

Key technical achievements include successful implementation of automotive-grade keypad interface, robust ignition control mechanism with fail-safe automatic re-locking, effective driver feedback system with clear messaging, integration of anti-theft alerting appropriate for vehicle security, and cost-effective design achieving significant savings compared to imported systems.

The testing results confirm 100% authentication accuracy, response times under 200ms, zero system crashes during testing period, and intuitive operation validated by test users. The significant reduction in cost while maintaining functionality demonstrates the viability of locally-developed automotive security solutions.

This work contributes to automotive innovation by demonstrating practical applications of microcontroller technology in vehicle security, economic development through locally-manufactured solutions, security enhancement addressing vehicle theft concerns, and educational value in training engineers in automotive electronics.

The successful completion validates the effectiveness of Arduino-based solutions for automotive security applications in the Nigerian market. The project establishes a foundation for future development of smart car technologies adapted to local conditions, contributing to Nigeria's automotive industry development and technological independence. Future enhancements should include multiple user support with individual passwords, password encryption implementation, IoT connectivity for remote monitoring, mobile application development for system management, and biometric integration for enhanced security.

REFERENCES

[1] Adebayo, O., Ogundimu, T., & Fashola, K. (2021). "Vehicle Theft Patterns and Security System Effectiveness in Nigerian Urban Centers." *Journal of Automotive Security Research*, 8(3), 124-139.

[2] Okafor, C., & Smith, J. (2022). "Arduino-based Automotive Security Systems: Performance Analysis and Market Viability in Developing Countries." *IEEE Transactions on Vehicular Technology*, 71(4), 2847-2859.

[3] Nigerian Bureau of Statistics. (2023). "Crime Statistics Report: Vehicle Theft Trends 2020-2023." Federal Republic of Nigeria Official Publication, Abuja.

[4] Johnson, M., & Adebisi, R. (2021). "Keypad Interface Design for Automotive Applications in Harsh Environments." *International Journal of Automotive Electronics*, 15(2), 67-78.

[5] Arduino Foundation. (2023). "Arduino Uno R3 Technical Specifications and Automotive Applications Guide." Retrieved from https://docs.arduino.cc/

[6] Ibrahim, A., Mohammed, S., & Yusuf, H. (2020). "Embedded Systems Applications in Nigerian Automotive Industry: Current State and Future Prospects." *African Journal of Engineering Research*, 12(4), 189-203.

[7] Okechukwu, P., & Williams, D. (2022). "Cost-Effective Vehicle Security Solutions for Emerging Markets: A Comparative Analysis." *Journal of Automotive Innovation*, 9(3), 156-171.

Corresponding author: Ore-ofe Ajayi
ajayi.oreofe17@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.