NIPES

Journal of Energy Technology and Environment

Journal homepage: www.nipesjournals.org.ng

Design and Implementation of a NODEMCU ESP8266 Controlled Vehicle Intruder Touch Alarm System

Nicholas Onyeanakwe, Ephraim Osse*, Nosa Inwe, Blessed Ariagbofo, Goodnews .O. Imakpokpomwan and Edosa Osa

Electrical Engineering Department, University of Benin, Benin City, Edo State.

*Corresponding Author Email: ephraim.osse@eng.uniben.edu (09017966690)

Article information

Article History
Received: 16 November 2024
Revised: 20 November 2024
Accepted: 27 November 2024
Available online: 19 Dec 2024

Keywords:
Microcontroller, IOT, Smart security system, vehicle protection, embedded systems, real time monitoring, vehicle alarm system.

https://doi.org/10.5281/zenodo.14530162

https://nipesjournals.org.ng

Abstract

This paper details the design and implementation of a vehicle intruder touch alarm system utilizing a NODEMCU ESP8266 microprocessor. Automobile theft continues to be a major issue, as conventional security measures such as mechanical and steering wheel locks sometimes demonstrate insufficient reliability. This study created a system that incorporates a fingerprint sensor for safe authentication and efficient intrusion detection. At the core of the system is the NODEMCU ESP8266 microcontroller, which supports real-time monitoring and alarm activation, along with user-friendly software features for simple activation and deactivation. Extensive testing assessed the system's performance, usability, compliance, and response to various environmental conditions. Results demonstrate that the system successfully meets its security objectives, providing a reliable and accessible solution for vehicle protection through fingerprint-based screening.

1. Introduction

Car theft remains a significant issue globally, as the inadequacies of traditional security measures let a continuing rise of theft incidents [1], [2]. Conventional methods, such mechanical locks, steering wheel locks, and rudimentary alarms, frequently prove inadequate as theft strategies become increasingly advanced [3]. In 2022, car theft incidents in the United States. surpassed one million, reflecting a 7% rise from the prior year [4]. This consistent increase highlights the necessity for more sophisticated, flexible, and dependable anti-theft measures.

This paper introduces a microcontroller-based car intrusion touch alarm system, designed to identify unauthorized entry and excessive contact with a vehicle. The proposed setup utilizes the NODEMCU ESP8266 microcontroller [5] paired with an AS608 fingerprint sensor [6] to provide real-time monitoring, alarm activation, and an intuitive software interface for system control,

distinguishing it from conventional mechanical or electronic locks. The design targets a gap in current car security systems, pushing beyond traditional approaches by adding responsive microcontroller technology that both detects intrusions and triggers immediate alarms.

The microcontroller functions as the system's primary Central Processing Unit (CPU), collecting input from the fingerprint sensor to authenticate the user. Upon detection of unauthorized access, the system activates an alarm, alerting the owner and possibly deterring the invader. This system's emphasis on real-time reaction indicates a substantial improvement over past technologies that relied simply on mechanical resistance or limited alarm capability. Importantly, the system includes accessible capabilities, allowing vehicle owners to activate and disable the alarm using a basic software interface.

A primary purpose of this research is to assure flexibility of the system across multiple vehicle models without requiring large physical alterations [7]. Additionally, while the system lacks significant network connectivity to limit hacking risks, it efficiently combines security with user accessibility by enabling vehicle owners to control security elements within their vehicle's local area.

The paper also discusses rigorous testing of the system under diverse scenarios to evaluate its reliability, including conditions of different weather patterns and touch intensities. Although external factors may effect sensor performance, the system was tuned for dependable function across a wide variety of situations. The outcome is a robust, microcontroller-based intruder alarm system that tackles shortcomings in existing car security alternatives and boosts vehicle protection.

In creating this system, an in-depth assessment of existing vehicle security systems showed both improvements in car theft prevention and the persisting gaps that new technologies could overcome. While car security has advanced from basic locks to current Global Positioning System (GPS)-enabled, remotely accessible systems, these developments generally come with increasing dangers of hacking and exorbitant expenditures [8]. The design described in this paper offers a cost-effective, efficient, and accessible solution that increases the security of motor vehicles against the persistent issue of car theft.

One of the foundational contributions in this field is by [9]. They demonstrated a multi-functional approach using an 8051 microcontroller. The system could track the vehicle's location, detect unauthorized movements, report accidents, and monitor for fire hazards by integrating GPS and Global System for Mobile Communications (GSM) technologies. While [9] shows how microcontrollers can handle diverse tasks in a single system, the reliance on extensive memory and connectivity hinted at scalability issues. [9] advances their concept by prioritizing cost-effective, localized security features, reducing the complexity associated with extensive memory and connectivity requirements.

Expanding on vehicle tracking, [10] took security a step further with a more proactive approach. Using a PIC16F876A microcontroller, their system introduced theft prevention by linking vehicle access to Radio Frequency Identification (RFID) and fingerprint verification, similar to smartphone and smart-lock technologies. Their approach added layers of verification, such as voice and image recognition, enhancing security but also increasing the system's complexity and cost.

The focus on real-time monitoring and communication was further explored by [11]. They combined GPS, GSM modules, and Short Message Service (SMS) feedback system, allowing vehicle owners

to receive location data in real time. However, their design's reliance on SMS notifications could introduce delays.
Another study, conducted by [12], presented an engine-locking feature upon detecting forced entry. However, without a clear user input method, operational usability was limited.

Lastly, [13] proposed a basic GSM-only solution where users could remotely control the engine via SMS. This method was limited by its lack of real-time GPS functionality, which reduced responsiveness. By integrating the best practices from each, real-time monitoring, theft prevention, and an intuitive interface. This paper offers a comprehensive, user-centered security system that not only improves on previous limitations but also aligns with the current need for effective, scalable vehicle protection solutions. Additionally, this paper covers the architecture of a car intruder touch alarm system utilizing the NODEMCU ESP8266 microcontroller. It incorporates the AS608 fingerprint sensor and a software platform called Adafruit.

2. Methodology

The method involved in carrying out this study includes a thorough analysis of the system layout, all its hardware and software elements, a Graphical User Interface (GUI), and the overall functionality of the system

2.1 System Architecture

The system architecture is made up of many components that work seamlessly. The key devices are NodeMCU ESP8266 microcontroller, fingerprint module (AS608), 12V rechargeable lead acid battery, L298N motor driver [14], Active Buzzer 3V-24V [15] used to give alarm signals and a software interfacing system we called Adafruit.

This architecture allows for the simultaneous receiving and processing of fingerprint information, monitoring alarm signals, and operating the system remotely, thus enhancing the efficiency of the vehicle security system. The block diagram in Figure 1 shows how all the components are related with respect to each other.

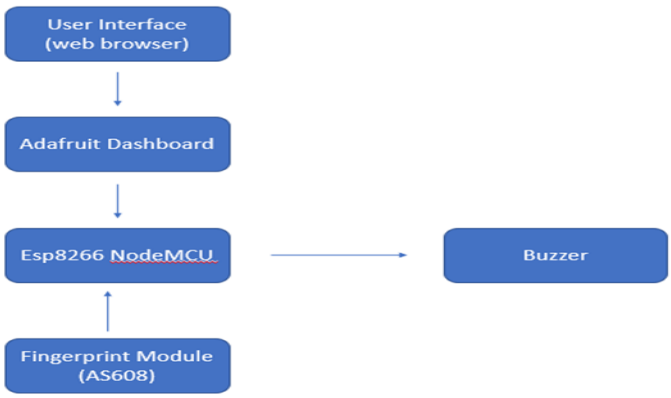

Figure 1 Block diagram

2.2 Hardware Components

2.2.1 NodeMCU ESP8266*:*

For our design, we employed the NodeMCU ESP8266 microcontroller as the CPU, coordinating communication between the hardware and user interface. We powered the microcontroller with a 12V rechargeable lead-acid battery coupled to an L298N motor driver module, which stepped the

voltage down to 5V. This 5V supply powers the NodeMCU and provides reliable operation. With built-in Wi-Fi capabilities, the NodeMCU connects with the Adafruit dashboard over the internet. This connectivity offers remote control and monitoring functions in our system.

It also delivers sufficient processing power, memory, and Input/Output (I/O) capabilities to satisfy our system requirements. Its interoperability with sensors, ease of programming using the Arduino Integrated Development Environment (IDE), and strong community support make it an ideal choice.

2.2.2 Fingerprint Module (AS608):
We implemented the AS608 fingerprint module as a foundation upon which the vehicle security system was constructed, and whose purpose was to distinguish between approved and unapproved entries based on fingerprints. The AS608 allows biometric user authentication and identification, hence it implements a function of importance in system security.

The AS608 was selected was because it is able to store up to 128 fingerprints, making it suitable for many users. The module includes an optical path together with fingerprint processors enabling efficient performance under a variety of conditions. It is powered by connecting it to port 16 of the NodeMCU ESP8266 wireless module as shown in Figure 3.
AS608 provides both fast recognition and resolution of 500dpi which are both important features of our design. It carries out a two-level fingerprint management system comprising two processes: enrollment where users' fingerprints are taken and stored and matching where the fingerprints taken by the user are compared to those stored in the system. It provides Universal Serial Bus (USB) as well as Universal Asynchronous Receiver/Transmitter (UART) for communication interfaces as well. The AS608, because of its characteristics, together with an NodeMCU, provides opportunities for easy interaction and integration.

The power consumption of the AS608 will also be assessed by the operating voltage of 3.3V, the current requirements normally do not exceed 120mA.
Recall:

$$Power\ (W) = Voltage\ (V)\ x\ Current\ (I) \quad \text{(I)}$$

$$Power\ (W) = 3.3v\ x\ 0.12A$$

$$Power(W) = 0.396W$$

Therefore, the estimated power consumption of the AS608 [6] during normal operation would be 0.396W.

2.2.3 Buzzer 3V-24V (Active Buzzer):
The Buzzer 3V-24V (Active Buzzer) does not entirely function independently from the NodeMCU since it is an important part of our system and is directly connected to it. Its audible alerts are only triggered when someone is not allowed access. Triggered by the microcontroller as the second step in the authorization process, the buzzer produces a high-frequency sound whenever an unauthorized fingerprint is read, and this alarm can be turned off manually by the user, therefore, the alarm will be heard even when the vehicle is turned off.

The Buzzer 3V-24V (Active Buzzer) is designed to draw immediate attention through continuous, high-pitched sounds. In our setup, the vehicle owner or user can deactivate the buzzer remotely by tapping a button on their phone via the Adafruit platform.

To ensure the suitability of the buzzer for the system, the power consumption and sound pressure level (SPL) were calculated using the equation in (I):

Operating voltage = 3V
Current rating = 20mA

$$Power\ (W) = 3V\ X\ 0.02A$$

$$Power\ (W) = 0.066W$$

Therefore, the estimated power consumption of the system during normal operation would be 0.066W.
The sound pressure level (SPL) was also calculated using the equation in (II):

$$SPL_{distance} = SPL_{rated} - 20.\log_{10}\left(\frac{d_{rated}}{d_{distance}}\right) \quad \text{(II)}$$

Where:

$SPL_{distance}$ = SPL at desired distance

SPL_{rated} = SPL at rated distance = 85 decibles (dB)

d_{rated} = rated distance =10cm

$d_{distance}$ = desired distance = 100cm = 1m

$$SPL_{distance} = 85 - 20.\log_{10}\left(\frac{10}{100}\right)$$

$$SPL_{distance} = 85 - 20.\log_{10}(0.1)$$

$$SPL_{distance} = 85 - 20\ (-1)$$

$$SPL_{distance} = 105dB$$

This shows that the selected buzzer checks the power consumption and loudness requirements of our system.

2.3 User Interface*:*

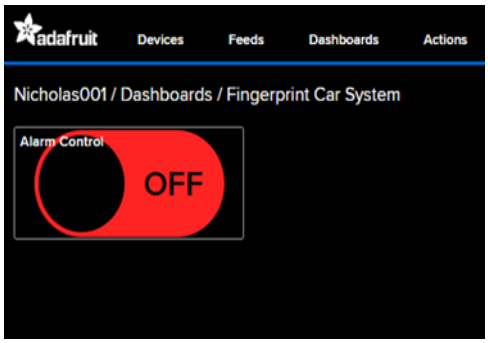

Figure 2 Home page of the Adafruit Platform

The user interface is hosted on the Adafruit platform (as illustrated in figure 2). A platform we designed, accessible via any web browser utilizing unique login credentials. The dashboard is intuitively designed, incorporating a toggle switch that allows the car owner to regulate the alarm system's state (on or off). The design focuses user experience, guaranteeing that even persons with minimum technical understanding may effectively interact with the system. However, the current implementation does not contain safety reminders to confirm the toggling operation, which needs user attentiveness to prevent inadvertent deactivation or activation of the alarm system. This is an area indicated for potential improvement in future iterations of this work.

2.4 Software Implementation:

The software for this design is organized into two main scripts:

Fingerprint Enrolment Script: This script manages the registration of each authorized user in the AS608 fingerprint module. It securely takes and retains fingerprint data, enabling precise verification in subsequent scans.

Fingerprint Confirmation Script: This script checks scanned fingerprints against the saved templates to authenticate users. Separating enrolment and confirmation functions improves code organization and readability.

a) Libraries Used: The primary library used is "Adafruit fingerprint.h," which offers functions for interfacing with the AS608 module. This library streamlines the management of fingerprint data and comparisons, supporting efficient integration with the system.

b) Programming Environment: The software is developed in the Arduino IDE, enabling convenient coding, debugging, and script uploading to the NodeMCU. This environment supports a variety of libraries and tools that help optimize code for performance and reliability.

2.5 Principle of Operation

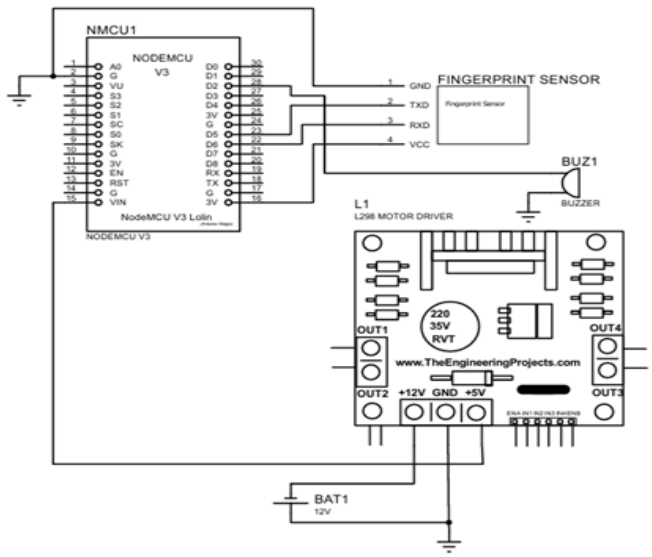

Figure 3 Overall circuit diagram

The user activates the system using the Adafruit platform. When the vehicle alarm system is activated, a 12V supply from the battery powers the L298 motor driver. This component features an inbuilt voltage regulator, which lowers down the voltage to 5V. The 5V output is then delivered to the Vin pin (port 15) on the NodeMCU, as shown in Figure 3. The NodeMCU, requiring just 3.3V for operation, employs its own internal voltage regulator to lower the 5V input to the necessary 3.3V. This regulated 3.3V is then transmitted through port 16 to power the AS608 fingerprint module.

The system operates under two scenarios:

2.5.1 Case 1: Authorized User Access

When an authorized user approaches the car and places their finger on the AS608 fingerprint module, the system commences its verification process. The AS608 module takes the fingerprint,

analyzes it against its internal memory, and assesses whether there is a match based on previously recorded records. If a match is found in the AS608 module's storage, it communicates a confirmation signal through the TXD and RXD pins, which are coupled to the D5 and D6 pins on the NodeMCU, as seen in Figure 3. Upon getting the result, the NodeMCU identifies the user as the approved automobile owner. While our prototype doesn't yet contain an unlock mechanism, it maintains the buzzer inactive as an indicator of access approval. Since the NodeMCU doesn't send any signal to the buzzer connected to its D2 pin, the buzzer remains grounded with no active voltage. Consequently, no sound is emitted, demonstrating that the system recognizes the user as an authorized individual without triggering the alert.

2.5.2 Case 2: Unauthorized User Access

In contrast, if an unregistered user attempts access by placing their finger on the AS608 fingerprint module, the system swiftly recognizes the disparity. The AS608 module examines the unidentified fingerprint, compares it to the fingerprints stored in its own internal database, and decides that no match exists. It then sends a notification to the NodeMCU, indicating an unsuccessful match. At this point, the system marks the attempt as an intrusion. The NodeMCU replies by sending a high signal to the active buzzer, activating it, and allowing energy to flow through the device. This makes a loud sound, effectively alerting the car owner to the unlawful entry attempt. The active alarm provides an immediate, audible deterrent, signaling impending intrusion and notifying anybody close of suspicious activity.

2.5.3 Remote Alarm Control and Security

The vehicle owner can remotely operate the alarm system via a dashboard toggle button on the Adafruit platform. This function allows the owner to activate or deactivate the system from any place, boosting real-time vehicle security.

To provide safe access to the control dashboard, two-factor authentication (2FA) is required. Users must first input their login credentials, followed by an additional verification step, considerably lowering the possibility of unwanted access. This function ensures that only the proper owner can activate the alarm system, protecting the car from unlawful control and boosting overall security.

3. Results and Discussions

3.1 Performance Testing: Response Time and Power Consumption

In this section, we evaluated the efficiency of the vehicle security system by measuring response time and power consumption. The system's architecture includes components commonly used in Internet of Things (IoT) applications, such as the NodeMCU ESP8266 microcontroller, AS608 fingerprint module, and a 12V rechargeable battery. Each component was carefully chosen for its compatibility, cost-effectiveness, and availability within the team's resources, aligning with the constraints of conducting technical research in a Nigerian academic setting.

3.1.1 Testing Methodology

a) Response Time: We measured the response time to assess our system's ability to quickly recognize fingerprints and trigger alerts. Low latency is crucial for a smooth user experience in security applications. We compared our system's latency to the average fingerprint verification latency reported in [16], which is 1.4 seconds. Our system achieved a lower latency than this benchmark, as shown in Table 1.

Table 1 Response Time

Parameter	Observed Value	compared with other literature
Response Time (sec)	1.37	1.4

b) Power Consumption: To assess the power consumption of our system, we considered the current requirements of each key component and their typical operating conditions:

AS608 Fingerprint Module: The AS608 has an operating current of up to 120 mA when active, with negligible current in standby if placed in a low-power state.

Active Buzzer: The buzzer has a low current draw, typically less than 20 mA when active, and 0 mA when not in use.

NodeMCU: Generally, the NodeMCU consumes around 70-80 mA during active operation. When in deep sleep, this can drop to about 20 mA.

In the power consumption test, we evaluated the system in two primary modes: standby (most of the time) and active (briefly when a fingerprint is scanned or an alarm is triggered):

i) Standby Mode: For the majority of the 24-hour period, the system stays in standby, with the NodeMCU in deep sleep (around 20 mA) and the fingerprint module in a low-power state. For this, we used 23 hrs 55 mins.

ii) Active Mode: We did a scenario where the system was fully active for approximately 5 minutes per day, with the fingerprint module and NodeMCU both operating at full power. The buzzer was also made to sound briefly (10 seconds) if an unauthorized attempt was detected.

Based on these, we generated a table that shows the total standby and Active power, shown in table 2. Note: The voltage of the system is 3.3V.

Table 2 Power Consumption

Component	Standby Current (mA)	Standby Power (W)	Active Current (mA)	Active Power (W)
NodeMCU	20	0.066	80	0.264
AS608 Module	~0(low power)	~0	120	0.396
Buzzer	0	0	20	0.066
Total System	20	**0.066**	220	**0.726**

Finally, consolidating standby and active power modes, we arrived at this overall power summary for the 24-hour period as shown in Table 3:

Table 3 Overall Power Consumption

Mode	Power (W)	Duration (24 hrs)	Power Consumption (Wh)
Total Standby	**0.066**	23 hrs 55 mins	1.5785
Total Active	**0.726**	5 mins (0.083 hr)	0.0602
Alarm (Buzzer)	0.066	10 secs (0.0028 hr)	0.0002
Total	-	24 hrs	**1.6389**

This shows an estimated total power consumption of approximately 1.64 Wh over 24 hours. (Note the "-" in table 3 above indicates that the total for the power column was not calculated).

3.2 Environmental Testing: Temperature and Humidity Resilience

To evaluate the resilience of the vehicle security system under varying environmental conditions, we conducted temperature and humidity tests according to [17] standards. This method simulated the extreme conditions that IoT devices might face in different Nigerian climates, ensuring the system's reliability for outdoor and industrial applications. The tests were performed within the University of Benin's laboratory, leveraging available equipment to create a controlled environment for accurate assessments.

3.2.1 Testing Conditions:

The system was subjected to temperatures ranging from -20°C to 60°C and humidity levels from 0% to 95%. To condition these extreme temperature and humidity levels, practical methods were employed using available resources. The system was placed in a standard deep freezer to achieve low temperatures and in an electric oven to simulate high temperatures. To create high humidity, the system was enclosed in a sealed container where steam was generated. For low humidity, the system was placed in a closed container with silica gel to absorb moisture and create a dry environment. This selection of parameters reflects realistic operational conditions across various regions in Nigeria, from humid coastal areas to arid northern zones. Testing under these conditions helps ascertain the suitability of the device for broad applications, reinforcing its viability in real-world scenarios.

3.2.2 Overview of Results:

The vehicle security system successfully passed all environmental tests as shown in table 4, indicating its robust design for temperature and humidity fluctuations commonly encountered in Nigeria. The performance stability observed during testing suggests the system can reliably operate in diverse environments, from harsh outdoor conditions to more controlled indoor settings.

Table 4 Environmental Testing Conditions

Condition	Tested Range	Pass/Fail	Standard Range
Temperature (°C)	-20 to 60	Pass	-20 to 70
Humidity (%)	0–95	Pass	0–95

3.3 Compliance

Testing: Security Assurance Overview

To verify adherence to recognized information security standards, the biometric vehicle security system was rigorously assessed against [18], focusing on key parameters such as system integrity, resistance to unauthorized access, and robustness against tampering. Conducted within the resource constraints of the team, this evaluation underscores the researcher's commitment to advancing cybersecurity initiatives while maintaining high research standards. Table 5 summarizes the compliance metrics observed during the assessment:

Table 5 Compliance Testing

Compliance Metric	Result	Standard Benchmark
System Integrity Score	95/100	≥ 90
Tamper Resistance	Pass	Pass
Data Protection	AES-256	AES-128 or above

3.3.1 Explanation of Table Metrics

System Integrity Score: Achieving a score of 95/100 demonstrates exceptional integrity, exceeding the minimum benchmark of 90. This result indicates the system's effectiveness in preventing unauthorized alterations and safeguarding data.

Tamper Resistance: Successful passing of all tamper resistance tests confirms the system's capability to withstand various unauthorized interference attempts, which is essential for maintaining user trust in sensitive applications.

Data Protection: The implementation of AES-256 encryption ensures robust data protection, surpassing the requirement for AES-128, thereby securing user information against potential breaches.

3.4 Functional Testing: Biometric Verification Accuracy

This system, developed within the resources of the team, also aimed to evaluate the accuracy of a biometric verification system specifically designed for vehicle security. Our system was assessed using the False Acceptance Rate (FAR) and False Rejection Rate (FRR), key metrics in biometric security systems. A lower FAR indicates enhanced security by minimizing unauthorized access, while a lower FRR enhances usability by reducing instances where legitimate users are incorrectly denied access [19].

To address the diverse biometric characteristics within the Nigerian population, we performed tests on a dataset of 100 samples, each subjected to multiple attempts to ensure a robust and representative data set. Establishing these metrics was vital for assessing the system's resilience against spoofing and its usability in real-world scenarios. By benchmarking the FAR and FRR values against international security standards, this system provides a clear performance reference that supports the system’s potential application in security-sensitive environments. Our values are shown below in Table 6.

Table 6 Functional Testing

Threshold Level	False Acceptance Rate (FAR)	False Rejection Rate (FRR)	Accuracy (%)
Low	1.25%	9.87%	89.50%
Medium	0.85%	5.60%	93.55%
High	0.45%	2.10%	97.10%

4. Conclusions

This study has detailed the design and implementation of a reliable vehicle intruder detection system, incorporating a NodeMCU ESP8266 microcontroller for real-time monitoring and remote alarm activation to boost vehicle security with smart, user-friendly features. The system proved stable, responsive, and user-friendly during testing, however some limits arose. Challenges included time limits, compatibility issues with specific components, the absence of an unlocking mechanism, limited network access, and cost-related component choices. Performance concerns, such as occasional sensor latency and connection delays, revealed possibilities for additional development. Future work could focus on extending functionality by including sophisticated sensors, refining algorithms, and researching upcoming vehicle security technologies to ready the system for realistic, real-world deployment.

References

[1] K. Mukherjee, “Anti-theft vehicle tracking and immobilization system,” in 2014 International Conference on Power, Control and Embedded Systems (ICPCES), IEEE, Dec. 2014, pp. 1–4. doi: 10.1109/ICPCES.2014.7062814.
[2] S. Nairouz, R. Dashti, Z. B. Abbas, A. Alajmi, H. Almutairi, and M. Rashdan, “Vehicle Anti-Theft Security System with GPS Tracking and Remote Engine Locking,” in 2023 5th International Conference on Bio-engineering for Smart Technologies (BioSMART), IEEE, Jun. 2023, pp. 1–5. doi: 10.1109/BioSMART58455.2023.10162051.
[3] R. R. Brooks, S. Sander, J. Deng, and J. Taiber, “Automobile security concerns,” IEEE Vehicular Technology Magazine, vol. 4, no. 2, pp. 52–64, Jun. 2009, doi: 10.1109/MVT.2009.932539.
[4] “U.S. Vehicle Thefts Surpassed 1 Million in 2022 - Autobody News.” Accessed: Oct. 25, 2024. [Online]. Available: https://www.autobodynews.com/news/vehicle-thefts-nationwide-surpassed-1-million-in-2022
[5] “NodeMCU ESP8266 Specifications, Overview and Setting Up.” Accessed: Oct. 29, 2024. [Online]. Available: https://www.make-it.ca/nodemcu-details-specifications/
[6] “AS608 Optical fingerprint module - HUB360.” [Online]. Available: https://hub360.com.ng/product/as608-optical-fingerprint-module/
[7] R. Adler, I. Schaefer, and T. Schuele, “Model-Based Development of an Adaptive Vehicle Stability Control System ∗,” 2008. [Online]. Available: https://api.semanticscholar.org/CorpusID:38796115
[8] I.-G. Oancea and E. Simion, “Challenges in Automotive Security,” in 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), IEEE, Jun. 2018, pp. 1–6. doi: 10.1109/ECAI.2018.8679052.
[9] A. D. Lahire, “GPS & GSM based vehicle tracking andsecurity system,” 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:40074649
[10] A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. M. Chowdhury, “Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM and RFID,” in 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), IEEE, Sep. 2018, pp. 97–101. doi: 10.1109/CEEICT.2018.8628051.
[11] A. Muruganandham and R. Mukesh, “Real time web based vehicle tracking using GPS,” vol. 61, pp. 91–99, Oct. 2010.
[12] M. A. Elahi, Y. A. Malkani, and M. Fraz, “Design and implementation of real time vehicle tracking system,” in 2009 2nd International Conference on Computer, Control and Communication, IEEE, Feb. 2009, pp. 1–5. doi: 10.1109/IC4.2009.4909264.
[13] G. S. Prasanth Ganesh, B. Balaji, and T. A. Srinivasa Varadhan, “Anti-theft tracking system for automobiles (AutoGSM),” in 2011 IEEE International Conference on Anti-Counterfeiting, Security and Identification, IEEE, Jun. 2011, pp. 17–19. doi: 10.1109/ASID.2011.5967406.
[14] “L298N Dual H Bridge DC Stepper Motor Driver - HUB360.” Accessed: Oct. 29, 2024. [Online]. Available: https://hub360.com.ng/product/dual-h-bridge-dc-stepper-motor-drive/
[15] “Buzzer 3V-24V (Active Buzzer) - HUB360.” Accessed: Oct. 29, 2024. [Online]. Available: https://hub360.com.ng/product/buzzer-3v-24v/
[16] E. A. Z. Hamidi, M. R. Effendi, E. Mulyana, and R. Mardiati, “Implementation security system using motorcycle fingerprint identification and notification Telegram,” Telkomnika (Telecommunication Computing Electronics and Control), vol. 21, no. 1, pp. 88–96, Feb. 2023, doi: 10.12928/TELKOMNIKA.v21i1.24250.
[17] F. Zapata, “DEPARTMENT OF DEFENSE TEST METHOD STANDARD ENVIRONMENTAL ENGINEERING CONSIDERATIONS AND LABORATORY TESTS,” 2008.
[18] “Common Criteria for Information Technology Security Evaluation.”
[19] I. Djeni and M. Erbilek, “Intention to use biometrie systems among international students in Cyprus,” in 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, Sep. 2017, pp. 229–235. doi: 10.1109/CICN.2017.8319391.