STM JOURNALS

Recent Trends in
Sensor Research & Technology

ISSN: 2393-8765
Volume 11, Issue 3, 2024
September–December
DOI (Journal): 10.37591/RTSRT

https://journals.stmjournals.com/rtsrt

Review RTSRT

Integrated Vehicle Security System: Leveraging GPS, GSM, and Fingerprint Authentication

Harsh Vijay Patil[1], Aditi Prabhakar Phatak[1], Pooja Santosh Pansare[1], Shubham Bhanu Rewale[1], Dipti Dayaram Patil[2,*]

Abstract

The vehicle security system described here is a comprehensive, robust system designed to increase vehicle security using two-factor authentication. It ensures that vehicle ignition is limited to verified users by utilizing an R307 Fingerprint Module for biometric validation and a 4x4 Matrix Keypad for command input. The system has a SIM800L module that notifies the owner via text message of the results of the authentication process, thereby informing them of the security condition of their car. Furthermore, the system incorporates Neo6M GPS technology to enable real-time tracking capabilities and remote vehicle monitoring. The core of the system is the Esp32 microcontroller, which offers a reliable and programmable control center. Together, these components create a safe and reliable car safety system that gives owners peace of mind and hands-on control. In addition to providing security, the technology is useful for evaluating car crashes to reduce the number of fatalities and property damage. It accomplishes this by providing a smart dashboard, objectively recording vehicle events, and boosting security capabilities with anti-theft, remote tracking, and surveillance tools.

Keywords: Fingerprint sensor, keypad matrix, GPS, GSM, buzzer

INTRODUCTION

Automation has become a boon in the contemporary world, with robots and programmable logic controllers (PLC) taking over the majority of industrial tasks. However, as the number of automobiles on the road increases, so does the frequency of associated crimes such as auto theft. Despite advancements in vehicle security systems and greater awareness among car owners, the rate of car theft has remained significant. The mere alteration of a vehicle's exterior can hinder traceability, leading to low recovery rates. Consequently, car owners are forced to invest heavily in insurance to safeguard their vehicles.

Goel et al. [1] introduced a GPS and GSM-based vehicle security system to track vehicles using Global Positioning System technology. Lien et al. [2] created an embedded system that combined GPS and keypad technology to deter car theft. Kalpan et al. [3] designed a system for the real-time monitoring and tracking of cargo or goods for digital logistics by utilizing both keypad and GPS technologies. This system employs a low-power 16-bit RISC microcontroller as the central processing unit, which is chosen for its compact size and high efficiency. The system automatically identifies the loaded cargo via the vehicle's terminal system, providing real-time location tracking, data and voice communication, and continuous monitoring. Integration of the keypad and GPS enhances the accuracy and efficiency of the system.

***Author for Correspondence**
Dipti Dayaram Patil
E-mail: diptipatil009@gmail.com

[1]Student, Department of Electrical Engineering, A. C. Patil College of Engineering, Navi Mumbai, Maharashtra India
[2]Assistant Professor, Department of Electrical Engineering, A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

Received Date: July 05, 2024
Accepted Date: August 17, 2024
Published Date: September 10, 2024

Citation: Harsh Vijay Patil, Aditi Prabhakar Phatak, Pooja Santosh Pansare, Shubham Bhanu Rewale, Dipti Dayaram Patil. Integrated Vehicle Security System: Leveraging GPS, GSM, and Fingerprint Authentication. Recent Trends in Sensor Research & Technology. 2024; 11(3): 11–16p.

An anti-theft security system demands rapid identification, robust door control, and a strong security framework to prevent vehicle ignition, as well as the capability to send messages to the vehicle owner in the case of unauthorized access, along with the precise location of the vehicle using GPS and GSM technologies with serial communication. To achieve this, a dependable system has been devised that utilizes fingerprints, keypads [4, 5], and password mechanisms to control access, immobilize the vehicle, and communicate with the owner, ensuring a high level of security. This paper presents an anti-theft vehicle protection system that addresses previous shortcomings and offers fully autonomous operation.

The proposed vehicle security system integrates advanced technologies to safeguard against theft and unauthorized access. It features a sensitive motion detection mechanism that is activated upon locking and hands-free ZigBee-based remote keyless entry for convenience. The system is built on a robust in-vehicle network utilizing CAN and local interconnect network (LIN) protocols, enabling various functionalities such as alarm signals through light flashes or horns and selective disabling of ignition during an alert state. Users can arm or disarm the system remotely, and the Dynamic Car Finder feature aids in locating the vehicle in a crowded area. In addition, the system incorporates internet of things (IoT) for enhanced security, employing a low-cost Bluetooth module for communication, and GSM for message alerts. It allows engine control via a mobile device and includes safety measures, such as a password-protected keypad for locker access and seatbelt enforcement, along with an IR sensor for intrusion detection. The system also offers towing protection and utilizes radio frequency identification (RFID) for biometric recognition, ensuring that only authorized users can start the vehicle [6, 7].

As urbanization accelerates, reliance on personal transportation increases, leading to a surge in vehicle numbers, and consequently, theft. Traditional anti-theft devices, while numerous, fall short of addressing this issue comprehensively. To counteract this, a novel security system was proposed that combines IoT technology with RFID authentication to ensure vehicle safety and enable tracking in the case of theft. This system requires both RFID recognition and a physical key for engine activation to ensure double-layer security. In addition, it includes an Android application that enhances tracking and monitoring capabilities, providing a robust solution to vehicular security concerns. The advanced features of the system extend beyond simple theft prevention. In emergencies, such as accidents or driver incapacitation, a limit switch facilitates vehicle access to authorized individuals. Moreover, the system boasts a global tracking ability through GPS technology. Complementing this, a separate project introduced an RFID-based car ignition prototype, which pairs with a GSM module and an Arduino microcontroller for secure ignition control. This setup was further refined by replacing the GSM with an ESP8266 Wi-Fi module, which offers convenience and modern connectivity. Together, these innovations represent a significant leap forward in vehicle security, marrying hardware and software to protect one of our most valuable assets, respectively [8, 9].

Intelligent cars have been developed as a result of IoT integration in the automotive sector; however, this progress has also drawn criminal activity, a novel vehicle guard-and-alarm system utilizing biometric authentication has been proposed, leveraging IoT to grant access solely to authorized drivers through a Raspberry Pi 3 Model B+ interface, Pi camera, PIR sensor, and smartphone. The system alerts the owner, and potentially the police, with an intruder's image and the vehicle's location if unauthorized access is detected. Tested on the ORL and a proprietary dataset, the vehicle security system-IoT (VSS-IoT) demonstrated high accuracy (98.2% for ORL, 99.6% for the proprietary dataset) and sensitivity (97.7%), with a rapid response time of 0.152 s under varying lighting, proving its robustness and reliability for real-time face recognition on low power processors. Concurrently, securing (semi)-autonomous vehicles remains a challenge because of their complex interactions with urban traffic systems and the lack of a security-by-design framework, which is critical for mitigating the risks from potential cyber-attacks and ensuring the safe operation of these advanced vehicles [10, 11].

Problem Statement

The envisioned project was designed to bolster vehicular security via a dual-authentication mechanism. It integrates a 4 × 4 matrix keypad with an R307 Fingerprint Module to authenticate users. To initiate the

ignition of the vehicle, the user is required to input a passcode into the keypad and subsequently verify its fingerprint. If any authentication step fails, an alert is dispatched instantaneously through the SIM800L module to notify the vehicle owner. Conversely, upon successful verification, ignition was permitted to be activated. Additionally, the system was equipped with a Neo6M GPS module, enabling real-time tracking of the vehicle's location [12]. At the core of the operation is the Esp32 controller, tasked with the efficient orchestration of the authentication sequence, notification dispatch, and location monitoring. The ultimate objective is to forge an all-encompassing, dependable security apparatus that guarantees vehicle access and operation exclusively to verified users, while concurrently providing sophisticated tracking and alert functionalities for augmented security and owner reassurance [13].

Objectives

- *Authenticate access:* Makes sure that only authorized users can operate the car by using passcode and fingerprint verification.
- *Monitor and alert:* Send instant notifications on authentication status and track the vehicle's location for security.
- *Optimize and interface:* Features low power consumption and a user-friendly interface for efficient and secure operation.

METHODOLOGY

The outlined design for the vehicle security system incorporates two-factor authentication and supplementary features to bolster vehicle protection and offer intuitive operations. The architecture utilizes a suite of components: a 4 × 4 Matrix Keypad, R307 Fingerprint Module, SIM800L module, and a Neo6M GPS module, all orchestrated by an Esp32 microcontroller. To activate a security system, users must undergo a dual-step verification process. Initially, they input personalized code via a 4 × 4 Matrix Keypad, establishing the first security layer. Subsequently, they must authenticate their identity with a fingerprint scan using the R307 Fingerprint Module, constituting the second security tier, and ignition of the car will not be allowed until both requirements have been verified. If the verification process fails at any stage, the system immediately dispatches an alert through the SIM800L module. This alert notifies the owner or an assigned contact of the attempted breach, including precise details of the time and location where the authentication is compromised, thereby reinforcing vehicle security. An additional safeguard is the integration of the Neo6M GPS module, which allows real-time tracking of the vehicle's position. This feature is invaluable for remote monitoring and is particularly beneficial in scenarios involving theft or unauthorized usage, with GPS data being relayed in alert messages. A block diagram of the vehicle security system is shown in Figure 1.

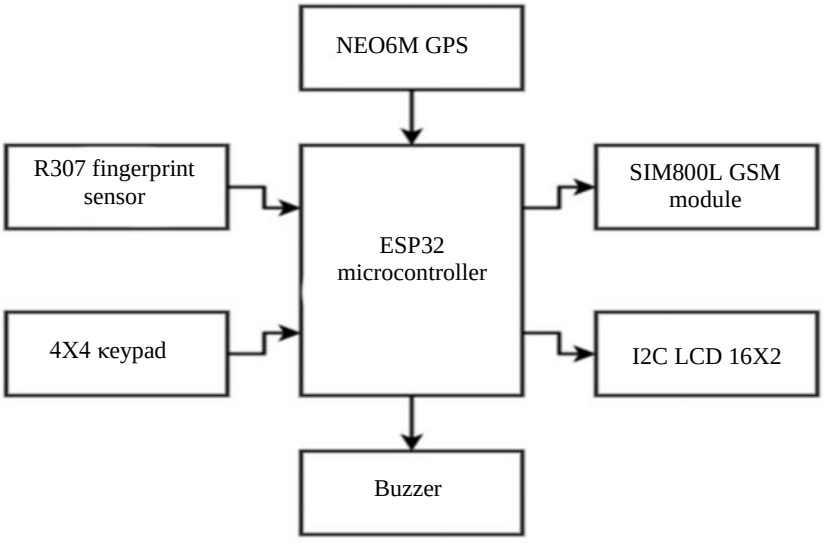

Figure 1. Block diagram of the vehicle security system.

Selecting Esp32 as the central controller guarantees a dependable and developer-friendly system. It is affordability and computational efficiency allows it to adeptly manage authentication protocols, messaging functions, and GPS tracking. This elaborates a two-factor authentication framework, coupled with its alert and tracking features, that delivers a formidable security enhancement for vehicles, ensuring tranquility for the owner or authorized operators.

SIMULATION AND RESULT

Arduino Integrated Development Environment (IDE)

The Arduino IDE is a flexible, multi-platform application that supports Windows, MacOS, and Linux and was developed using Java. Its main role is to create and upload software to the Arduino boards. The IDE code was released under the GNU General Public License, enabling C and C++ programming with established coding standards. It includes a library from the Wiring Project, which provides common methods for handling inputs and outputs. The Arduino IDE involves two essential functions: one to start the sketch, and the other for the ongoing program loop. These functions are compiled and linked with a placeholder main () function to generate a repeating executable program powered by the GNU toolchain included with the IDE. The IDE employs 'avrdude' to convert the compiled code into a hex text file, which is then transferred to the Arduino board via a bootloader in the board's firmware.

Fritzing

Fritzing is an open-source project aimed at making electronics approachable and stimulating, as a creative medium for everyone. Our offerings include a software tool, a community forum, and services that reflect the spirit of Processing and Arduino. This project fosters an environment in which users can document their prototypes, share knowledge with others, teach electronics in academic settings, and create professional-level printed circuit boards (PCBs). Fritzing also promotes creative exploration and prototyping and serves as a playground for innovators to refine their electronic ideas.

Proteus

Proteus is a comprehensive software suite for electronic design automation, which includes tools for PCB layout creation, simulation, and schematic capture. The simulation Model shown in Figure 2 serves both seasoned enthusiasts and passionate enthusiasts. Created by Lab Center Electronics Ltd., Proteus supports an extensive array of microcontrollers, including those from the Microchip, Atmel, and Advanced RISC Machine (ARM). The platform is celebrated for its intuitive interface and robust capabilities, such as mixed-mode simulation program with integrated circuit emphasis (SPICE) simulation, microcontroller simulation, and specialized IDE for simulation tasks. Proteus is also equipped with high-speed design features and 3D board visualization tools. The schematic capture module is crucial for simulating and generating PCB layouts, thus enhancing its versatility in the electronic design workflow. The simulation results are shown in Figure 3.

APPLICATIONS

- *Personal vehicle security:* This system can be installed in personal cars to enhance security. The vehicle can only be started by authorized individuals, owing to 2-factor authentication.
- *Fleet management:* This method can assist companies that own and operate a fleet of cars to keep them safe. Each driver can have a unique passcode and fingerprint access. Location tracking is essential for monitoring the routes and statuses of vehicles.
- *Car rental services:* Car rental companies can implement this system to improve vehicle security. Customers must use both passcode and fingerprint authentication to start a car, thereby reducing the risk of theft.
- *Anti-theft system:* The system can serve as an anti-theft mechanism. If someone tries to steal the vehicle and fails authentication, it can trigger an alert and send the vehicle's GPS location, allowing for a rapid response.
- *Vehicle-sharing platforms:* Companies that offer vehicle-sharing services can use this system to ensure that only authorized users can access the shared vehicles, thereby increasing security and control.

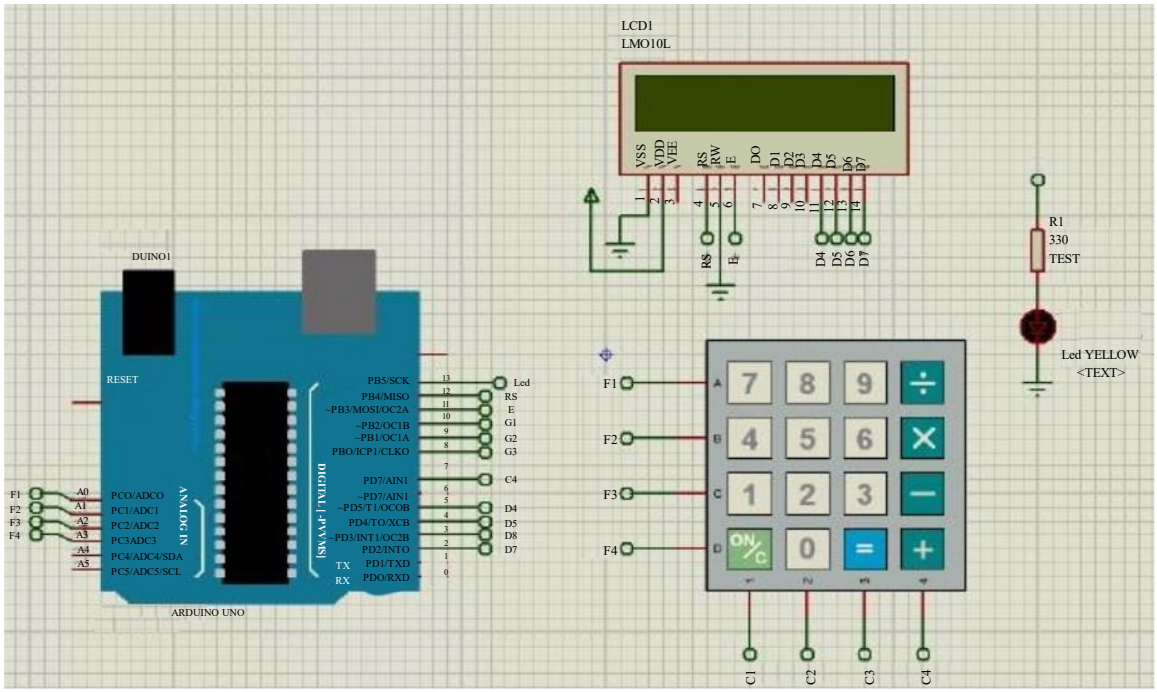

Figure 2. Simulation model.

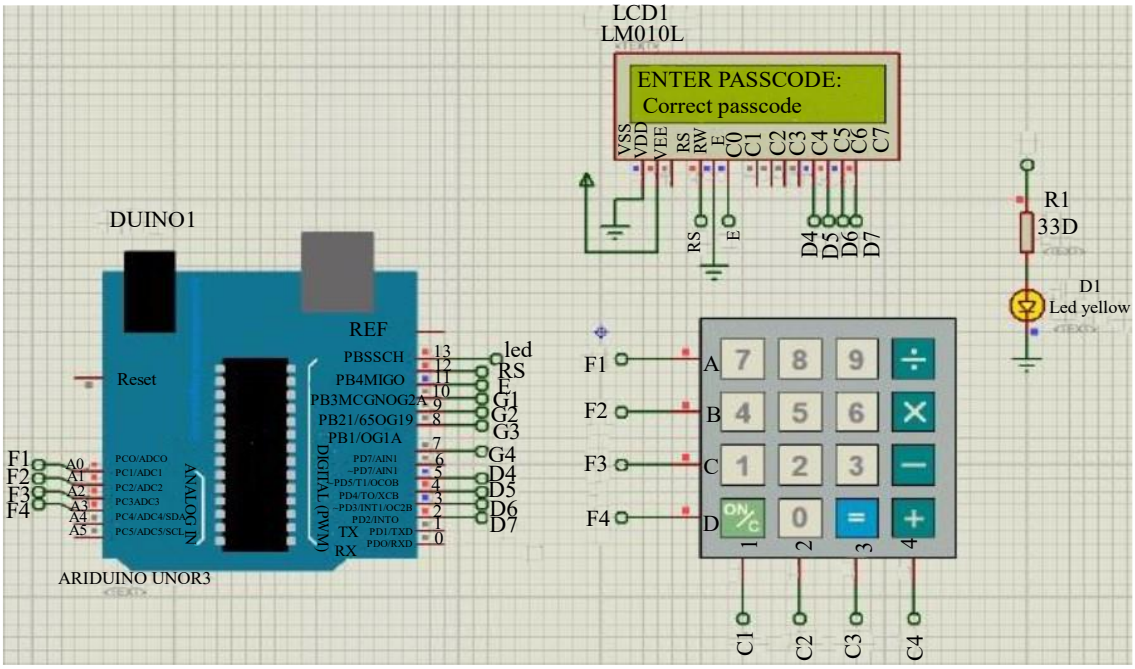

Figure 3. Simulation model result.

- *Security for high-value cargo:* For businesses involved in transporting high-value cargo, this system can add an additional layer of security and tracking.
- *Vehicle monitoring and recovery:* GPS monitoring can assist in promptly identifying and retrieving a stolen vehicle, should that tragic circumstance arise.

CONCLUSION

The integrated vehicle security system developed in this study, with two-factor authentication in association with the R307 Fingerprint Module for biometric validation, is far more efficient than the

traditional security system. In addition, the Neo6M GPS module enables anti-theft and real-time monitoring systems to avoid crashes and unwanted accidents in large vehicles by providing notifications if security breaches occur by the driver. This novelty has not yet been observed in traditional practices of digital vehicle protection systems.

Future Scope

The aim of a vehicle security system with 2-factor authentication is to increase vehicle security through a multi-layered access control system. It integrates a 4 × 4 Matrix Keypad and an R307 Fingerprint Module for user authentication, ensuring that only authorized users can initiate the vehicle. The inclusion of the SIM800L module enables the system to alert the owner via text messages about authentication outcomes, thereby providing remote awareness of the vehicle's status. Furthermore, the system offers GPS-based location tracking via the Neo6M GPS module, thereby facilitating real-time monitoring and anti-theft measures. At its core, Esp32 serves as the central controller for managing authentication, communication with the SIM800L module, and tracking functionality. This system harnesses advanced technology to fortify vehicle security, thwart unauthorized access, notify owners of security breaches, and track a vehicle's location, thereby enhancing overall safety and security.

REFERENCES

1. Goel A, Gruhn V. A Fleet monitoring system for advanced tracking of commercial vehicles. In: 2006 IEEE International Conference on Systems, Man and Cybernetics; 08/10/2006; Taipei, Taiwan. IEEE; 2006. p. 2517–22. DOI: 10.1109/ICSMC.2006.385242.
2. Lien CH, Lin CH, Bai YW, Liu MF, Ming-Bo L. Remotely controllable outlet system for home power management. In: 2006 IEEE Tenth International Symposium on Consumer Electronics (ISCE 2006); St. Petersburg, Russia. IEEE; 2006. p. 1–6. DOI: 10.1109/ISCE.2006.1689468.
3. Kalpan ED. Understanding GPS: Principles and Applications. Artech House Publishers; 1996.
4. Ali J, Nasim S, Ali T, Ahmed N, un Nabi SR. UPM Serdang. 2009. p. 33–6. DOI: 10.1109/SCORED.2009.5443760.
5. Mcdonald M, Keller H, Klijnhout J, Mauro V. Intelligent Transport Systems in Europe: Opportunity for Future Research. World Scientific Publishing; 2006.
6. Loganathan GB. Can based automated vehicle security system. Int J Mech Eng Technol. 2019;10.
7. Mukhopadhyay D, Gupta M, Attar T, Chavan P, Patel V. An attempt to develop an IOT based vehicle security system. IEEE Int Symp Smart Electron Syst (ISES); 2018. p. 195–8. DOI: 10.1109/iSES.2018.00050.
8. Nasir MAM, Mansor W. GSM based motorcycle security system. In: 2011 IEEE International Conference on System Engineering and Technology (ICSGRC). IEEE; 2011. p. 129–34. DOI: 10.1109/ICSGRC.2011.5991844.
9. Elngar AAAK, Kayed M. Vehicle security systems using face recognition based on Internet of things. Open Comput Sci. 2020;10:17–29. DOI: 10.1515/comp-2020-0003.
10. Rajput I, et al. Design and development of real-time vehicle security system. In: 3rd International Conference on Advanced Computing and Innovative Technologies in Engineering (ICACITE); 2023. IEEE.
11. Kamalakkannan MR, Dineshkumar R, Sanjay A, Sathyaganth R. Design thinking approach and implementation of anti-theft security system for vehicles using IoT. Ind Eng J. 2023;52.
12. Elngar AAAK, Kayed M. Vehicle security systems using face recognition based on Internet of things. Open Comput Sci. 2020;10:17–29. DOI: 10.1515/comp-2020-0003.
13. Chattopadhyay A, Lam KY, Tavva Y. Autonomous vehicle: Security by design. IEEE Trans Intell Transp Syst. 2021;22(Nov):7015–29. DOI: 10.1109/TITS.2020.3000797.

