International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

"Authenticated Access Control For Vehicle Ignition System Using Driving License And Finger Print"

Mrs.Chandrakala G S[1], gsckala84@gmail.com,
Manoj Kumar B[2], manojkumarb17072004@gmail.com,
Harsha T M[3], harshatm801@gmail.com,
Ravichandra Babu J K[4], ravichan.raju20@gmail.com,
ACS College of Engineering, Bengaluru

ABSTRACT

Vehicle theft is a growing concern, necessitating advanced security solutions to prevent unauthorized access and potential loss. This system proposes an effective anti-theft system for vehicles, designed to ensure that only authorized and licensed users can operate the car. The system uses an Arduino microcontroller as the central brain, integrating several key hardware components: a Radio Frequency Identification (RFID) reader, a fingerprint (FP) module, and a Global System for Mobile Communication (GSM) modem. Authorized driver's license (DL) information and fingerprint templates are securely pre-stored in the Arduino UNO. The authentication process requires the user to present their DL to the RFID reader first. If the license is valid, the user proceeds to the fingerprint scanner for biometric verification. If both credentials match the stored data, the ignition system is enabled, allowing the person to drive the vehicle. If either authentication fails, the system blocks the ignition and immediately sends a Short Message Service (SMS) alert via the GSM modem to the vehicle owner. The system also sends SMS reminders to the driver to renew their license before expiration. This dual-authentication method provides a robust security solution that significantly enhances protection against vehicle theft.

Keywords: Fingerprint Authentication, GSM Modem, Dual Authentication, Driving License Verification, Biometric Security, Ignition Control System, Unauthorized Access Prevention, SMS Alert System.

1.Introduction

In recent years, the rise in road accidents and vehicle thefts has necessitated innovative solutions for vehicular safety. Traditional vehicle safety mechanisms often lack comprehensive features for user authentication, accident prevention, and immediate response in emergencies. This Vehicle Safety System bridges these gaps by

leveraging Arduino Mega and a range of sensors, including ultrasonic sensors, and fingerprint readers. The system not only prevents vehicle operation by unauthorized or intoxicated individuals but also enhances safety through obstacle detection and accident reporting. The system uses Arduino UNO as the main controller and integrates RFID technology, fingerprint authentication, and GSM communication for secure vehicle access. The driver must first verify the driving license through the RFID reader and then complete fingerprint verification. Only when both authentications are successful, the ignition system is activated. If unauthorized access is detected, the system immediately sends an SMS alert to the vehicle owner using the GSM modem. This dual-authentication security system provides a reliable and efficient solution to reduce vehicle theft and enhance driver safety.

2.Literature Survey

[1] The paper titled "GPS based Advance vehicles tracks and vehicle Controls System" (2020), author M. Mukhtar addresses a vehicle tracking and control system that highlights key features such as real-time

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

tracking, geo-fencing, and remote vehicle control. By utilizing fleet management to improve overall operational efficiency, the system offers potential benefits including increased safety, reduced fuel consumption, and streamlined logistics, making it a comprehensive solution for modern vehicle management. The proposed system utilizes GPS technology to monitor vehicle location, speed, and other parameters in real-time. The research specifically underscores location tracking, speed monitoring, and route optimization, while implementing security measures such as remote engine immobilization and alarms to prevent theft. These systems prove valuable for fleet management, logistics, and personal vehicle monitoring by enhancing overall efficiency, safety, and security. The methodologies employed include a GPS Receiver Unit, Telematics Hardware, Communication Networks, a Centralized Server, and Geo-fencing. Through the integration of GNSS and geo-fencing features, the system has successfully improved real time tracking with an accuracy of 96.30%. However, some disadvantages remain, notably the initial setup costs—including hardware, software, and installation—which can be a significant investment for businesses, alongside ongoing maintenance and updates that may require additional expenses.

[2] The "Geo fence for fleets and freight managements,"(2021) authors F. Reclus and K. Drouard examine the use of virtual boundaries to modernize vehicle monitoring and logistics. The paper highlights how geo-fence technology can be strategically implemented to optimize fleet operations by creating invisible perimeters that trigger specific actions. This comprehensive approach allows managers to maintain oversight through real-time tracking and geographically targeted alerts, ensuring that freight is moving exactly where and when it should be. The proposed system suggests that by establishing these virtual fences, companies can achieve significant improvements in route optimization. Fleet managers can use the data to define approved transit areas, which helps in reducing fuel consumption and streamlining delivery logistics. Beyond just location, the system acts as a proactive management tool, providing automated notifications that allow for better coordination between drivers and dispatchers. Methodologically, the study focuses on a structured integration process involving Geographical Mapping, the selection of specific Geo-fencing Technology, and full integration with existing Fleet Management Systems. While the advantages include improved overall efficiency and enhanced security, the authors also note certain disadvantages. Specifically, the system's reliability can be hindered by technical issues such as GPS signal loss, inaccuracies in location data, or unexpected system downtimes, all of which can disrupt the smooth flow of fleet management.

[3] The study titled "Geo-fencing and Activity Recognitions" (2021), authors A. Corradi, L. Foschini, R. Ianniello, and R. Montanari explore the foundational principles and benefits of combining geographical boundaries with behavioral analysis. The paper emphasizes how geo-fencing enhances location-aware services and security, while activity recognition identifies and categorizes specific user behavior’s using sensor data from smartphones and wearables. By investigating the synergies between these two technologies, the research aims to optimize context-aware computing and provide more personalized user experiences across various domains. The proposed system investigates how integrating location data with human activity patterns can improve the overall intelligence of mobile services. The methodology involves a structured process of Geo-fence Triggering, System Integration, Sensor Selection, and Data Preprocessing to ensure accurate context detection. A primary advantage of this approach is the ability to provide real-time alerts and notifications the moment a device crosses a designated perimeter, which is highly effective for security monitoring and asset tracking. However, the authors identify a significant disadvantage in the system's reliance on GPS technology. Because the system requires frequent location updates to maintain accuracy, it can drain device batteries quickly, presenting a challenge for long-term monitoring on mobile or wearable hardware.

3.METHODOLOGY

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

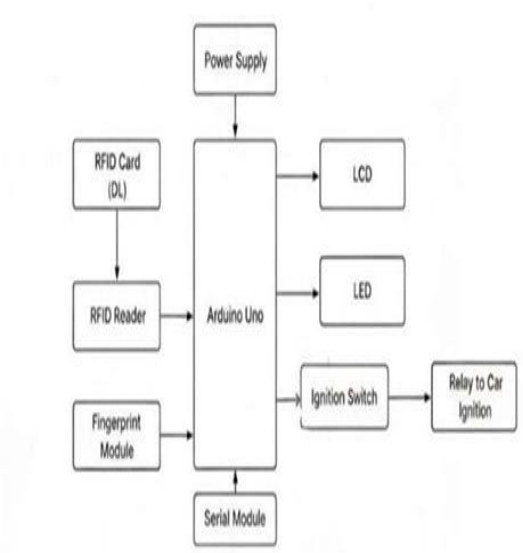

FIG 3.1: BLOCK DIAGRAM

The block diagram illustrates an Arduino-based dual-authentication vehicle security system designed to prevent unauthorized access through multiple verification layers. The system is organized around an Arduino Uno which serves as the primary controller, managing data from input modules and executing logic to control the vehicle's ignition. A dedicated Power Supply block provides the necessary electrical energy to the Arduino and all connected peripheral modules to ensure the system remains active. The security protocol utilizes a dual-layer authentication process consisting of an RFID System and a Fingerprint Module. During the first stage, an RFID Card (DL) is presented to the RFID Reader, which captures the digital identification data and transmits it to the Arduino. Simultaneously, the Fingerprint Module captures the user's biometric template and sends it to the Arduino for secondary verification. These two inputs act as the primary security gates that must be cleared before the vehicle can be operated. The system provides feedback and external communication through several components. An LCD is used to display real-time status messages to the user, while an LED provides visual indicators for system alerts. A Serial Module, likely a GSM/GPRS unit, is integrated to handle external notifications. The final output control is managed by an Ignition Switch and a Relay to Car Ignition. If the Arduino confirms that both the RFID and fingerprint data match the authorized information stored in its memory, it triggers the relay to allow the vehicle to start and operate.

4.HARDWARE AND SOFTWARE REQUIREMENTS

Power Supply:

The Power supply provides the required voltage and current to power the Arduino Uno and all connected modules (typically 5V/12V regulated supply). It ensures stable and regulated power to the Arduino Uno and other peripherals.

Fig 4.1: Power Supply

Arduino Uno:

The Arduino Uno acts as the central processing unit of the system. Receives input from modules (RFID, fingerprint, serial) and controls outputs (LCD, alarm, relay, GSM). and low cost make it ideal for prototyping and implementing this security-focused vehicle system.

Fig 4.2: Arduino Uno

LCD:

The LCD: displays messages to the user (like access granted/denied, errors, etc.). It Provides isual feedback for system status and interactions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Fig4.3 LCD

GSM Module: The GSM Module sends SMS or alerts to the vehicle owner or authorities which notifies in case of unauthorized access or emergency.

Fig 4.4 GSM Module

Optical Fingerprint Sensor:

The fingerprint sensor captures and verifies the driver's fingerprint to ensure only authorized users can start the vehicle It acts as a biometric security check that confirms the driver's identity before allowing vehicle ignition.

Fig4.5 Optical Fingerprint Sensor

5.Software Requirements

The process of writing and uploading code to Arduino boards is simplified by the open- source Arduino Integrated Development Environment (IDE). This software platform acts as the central tool for Arduino of to offering an initiative interface for users to write, compile, and upload their code to the boards. The IDE is available for various operating systems such as Linux, Mac OS X, and Windows, providing developers with flexibility to work across multiple platforms. Its cross-platform support makes it accessible to a broad user base, from hobbyists to professionals, enhancing its widespread adoption. Arduino IDEmeans that all necessary tools for coding and uploading sketches are integrated into one cohesive software package. supports two primary programming languages: C and C++, which are widely used in embedded systems development. These languages are well-suited for writing code that interacts with hardware, making them ideal for microcontroller programming. The term "IDE" stands for Integrated Development Environment, which In the Arduino environment, the code written is referred to as a "sketch." This term reflects the simplicity and approachability of the platform. Writing a sketch involves defining the logic and instructions that control the Arduino board's operation. Once the sketch is ready, it can be uploaded to the Arduino or Genuino board through the IDE. To upload the code, the board must be connected to the computer via a USB cable. The IDE allows users to select the correct board and port configuration before uploading the sketch. This ecosystem ensures that the system remains adaptable to evolving requirements, such as integrating new sensors or communication modules, supporting the project's goal of a scalable smart transportation solution.

6.Results and Discussions

The proposed vehicle security system was successfully implemented using RFID, fingerprint authentication, and GSM technology. The system accurately verified the driving license and fingerprint details of authorized users before enabling the vehicle ignition. Unauthorized access attempts were effectively detected, and the ignition system was immediately blocked to prevent theft. The GSM modem successfully sent SMS alerts to the vehicle owner whenever invalid authentication occurred. Overall, the project provided a reliable, efficient, and secure solution for enhancing vehicle

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

safety and preventing unauthorized vehicle usage.b8

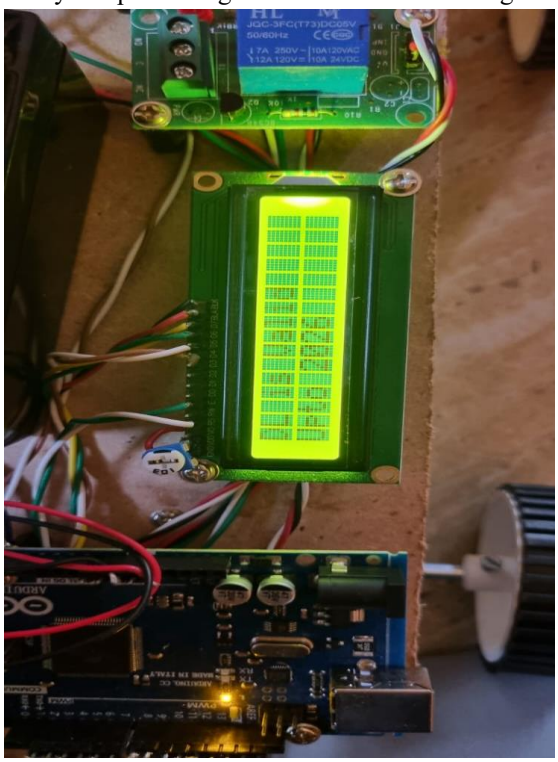

Fig6.1 output

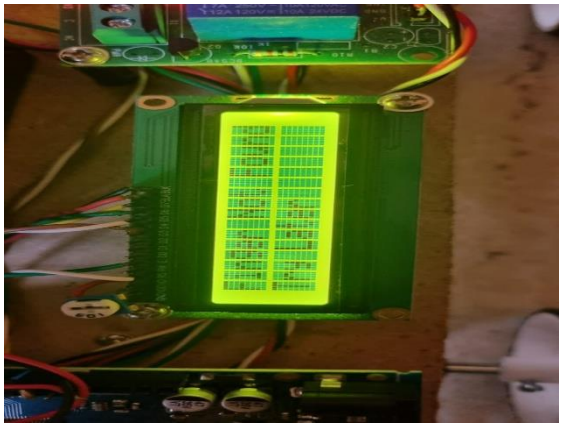

Fig6.2 ouput

Fig6.3 output

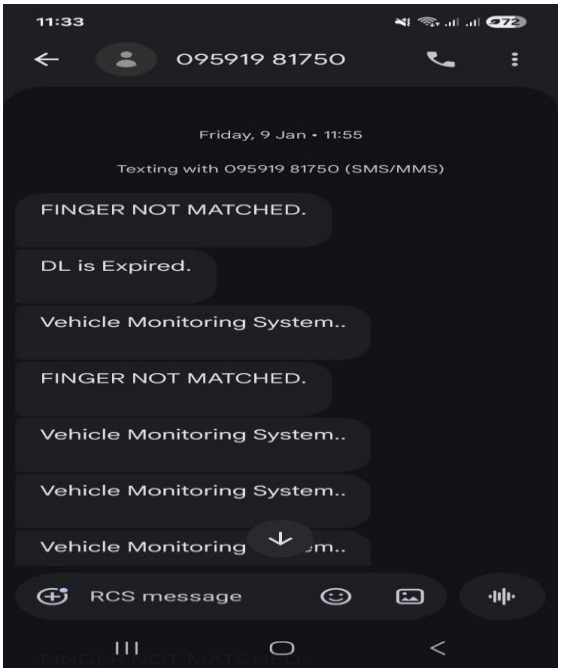

Fig6.4 output

7.CONCLUSION

The implemented Authenticated Access Control for Vehicle Ignition System Using Driver's License and Fingerprint provides an effective, practical, and low-cost solution for vehicle security enhancement. By integrating RFID-based license verification and biometric fingerprint matching, the system ensures that only legitimate and licensed users start the vehicle. The project demonstrates successful hardware-software integration and reliable authentication performance under various test conditions. This dual-authentication framework can be extended with future improvements such as: integration with cloud databases for centralized access control, GPS-based vehicle tracking for fleet management, mobile app-based monitoring interfaces, and facial recognition for advanced security. Thus, the developed system forms a foundation for next-generation smart vehicle ignition systems that are secure, intelligent, and adaptable to real-world automotive environments.

Acknowledgement

The writers truly appreciate Mrs. Chandrakala G.S, Electronics and Communication Engineering Department at ACS College of Engineering, for helpful advice along with steady backing during the entire project build. On top of that, they're grateful

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

to department teachers and lab workers for offering key resources together with hands-on help. In the end, they value the motivation from loved ones and close pals while finishing this effort successfully.

REFERENCES

[1] M. Mukhtar, GPS based Advance vehicles tracks and vehicle Controls System, 2020.

[2] A. Damani, H. Shah, K. Shah and M. Vala, Global-positions-Systems for Objects Tracks, 2021.

[3] F. Reclus and K. Drouard, Geo fence for fleets and freight managements, 2021.

[4] A. Corradi, L. Foschini, R. Ianniello and R. Montanari, Geo-fencing and Activity Recognitions, 2021.

[5] N. N. Rama Prasad and P. Narayanan, Volunteers Geographic Informations Systems and it's contribution in service sector employment, in Geographic information System, 2020.

[6] L. Tan and W. Lee, A solution for integrate track and trace in supplied chain based on RFIDGPS, 2021.

[7] G. Yang, Hybrid Cargo Level Tracking Systems For Logistics, 2022.

[8] R. R. Oliveria and G. M. Cardoso, An intelligent model for logistics management based on geo-fence algorithms and RFID technology, 2021.