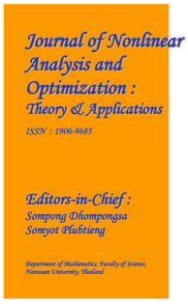
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**



A NOVEL VEHICLE SECURITY SYSTEM USING DRIVER'S LICENSE AND FINGERPRINT AUTOMATION

V. Srinivasarao, D.Mahendra, K.Lakshmi Chaitanya, B.Hemanth Sai, D.Raghava Rohan,
Department of Electronics & Communication Engineering, NRI Institute of Technology,
Pothavarappadu (V), Agiripalli (M), Eluru (Dt)-521212

Abstract:
This paper introduces a pioneering vehicle security system that combines the authentication of driver's licenses and fingerprint biometrics to significantly enhance the protection against vehicle theft. The system is built around an Arduino controller, which interfaces seamlessly with an RFID (RadioFrequency Identification) reader and a fingerprint sensor. The RFID reader constitutes the first level of security, requiring the driver's license to be equipped with an embedded RFID tag for access to the vehicle. Furthermore, the second level of security is bolstered by the fingerprint sensor, which scans the driver's fingerprint for authentication. Only when both levels of security are successfully verified does the system grant access to the vehicle. This novel approach to vehicle security offers robust protection by ensuring that only authorized individuals with both the driver's license and the registered fingerprint can start and operate the vehicle, effectively reducing the risk of theft and unauthorized use.
The Arduino controller serves as the core of the system, orchestrating the communication between the RFID reader and the fingerprint sensor. When a driver approaches the vehicle, they are first required to present their driver's license, which contains an RFID tag. The RFID reader scans the license, confirming its validity. Subsequently, the driver is prompted to place their finger on the fingerprint sensor for further authentication. Only upon the successful verification of both the driver's license and fingerprint is access granted to the vehicle. This innovative vehicle security system not only enhances protection but also offers user-friendly and efficient access control, making it a valuable addition to the automotive industry.

Keywords: Arduino, Fingerprint sensor, RFID Reader, Vehicle security

1. Introduction

In this paper [1], a smart security system for vehicles is presented, integrating IoT, sensors, and potentially biometrics to enhance security by detecting and preventing unauthorized access or theft. The paper details the system architecture, sensor integration, and communication protocols used to ensure robust security measures. In this paper [2], a safety and security system for vehicles based on smart license technology is introduced. This system aims to improve vehicle security and reduce the risk of theft or unauthorized usage by incorporating digital licenses for authentication and access control. It discusses the implementation of smart license technology, its integration with vehicle systems, and the potential benefits for both vehicle owners and authorities. In this paper [3], fingerprint recognition technology is discussed, focusing on a standardized fingerprint model for accurate and efficient identification. It covers the principles of fingerprint recognition, the development of standardized models, and applications in security systems, access control, and law enforcement.In this

paper [4], smart authentication methods tailored for smartphones are explored to enhance security and user convenience. It discusses advanced authentication techniques such as biometrics, pattern recognition, or behavioural analysis designed to secure mobile devices against unauthorized access, evaluating their effectiveness and usability in real-world scenarios. In this paper [5], an overview of emerging biometric technologies is provided, discussing modalities such as fingerprint, iris, and facial recognition. It reviews advancements in biometric technology, their applications in security systems, and challenges associated with implementation, aiming to provide insights into the current state-ofthe-art and future research directions. In this paper [6], a gesture-based control system for wheelchairs is presented, designed to improve mobility and independence for physically disabled individuals. It discusses the development of gesture recognition technology and its integration with wheelchair control systems, evaluating its usability and effectiveness in real-world settings. In this paper [7], a low-cost autonomous vehicle controlled by a PIC microcontroller-based neural network and image processing is described. The design and implementation of the vehicle's control system, including neural network algorithms and image processing techniques, are discussed, along with performance and efficiency evaluations in various scenarios. In this paper [8], comprehensive information on Automated Fingerprint Identification Systems (AFIS) is provided, covering their history, principles, algorithms, and applications in law enforcement, forensic science, and biometric authentication. It explores technological advancements and challenges in AFIS development and deployment. In this paper [9], a safety system for vehicles using Arduino microcontrollers is proposed, aiming to enhance vehicle security and safety. It discusses the integration of sensors and actuators controlled by Arduino to monitor and control vehicle operation, along with system architecture, sensor placement, and communication protocols.In this paper [11], an anti-theft vehicle locking system based on the Controller Area Network (CAN) is presented to prevent unauthorized access and theft. The design and implementation of a secure locking mechanism controlled via the CAN communication protocol are described, including features such as remote locking/unlocking, alarm systems, and tamper detection. In this paper [12], an electronic police ambush system based on a safety authentication system for vehicles and drivers is proposed to improve law enforcement efforts. It incorporates biometric authentication, vehicle tracking, and real-time communication with law enforcement agencies to detect and respond to suspicious activities effectively. In this paper [13], a comprehensive system for enhancing car security through IoT technology is proposed. It facilitates connectivity and communication between sensors and devices within the vehicle to detect unauthorized entry, movement, or tampering. IoT enables features such as remote monitoring and control of the vehicle's security status via smartphones, with insights into implementation details, benefits, and potential challenges.

2. Proposed Method

The goal of the paper is to create a sophisticated car security system that uses two-factor authentication for ignition and access. The system seeks to improve security measures to stop car theft and unauthorised access by combining RFID technology with fingerprint identification.

2.1 Proposed Design

Node MCU devices establish connectivity with the cloud server, enabling seamless data transmission and remote monitoring. This allows continuous uploading of sensor data for monitoring and management. Additionally, a motor automates bin door operations based on fill level, enhancing operational efficiency. Overall, the proposed method aims to revolutionize dust management with improved accuracy, real-time monitoring, and automated operations.

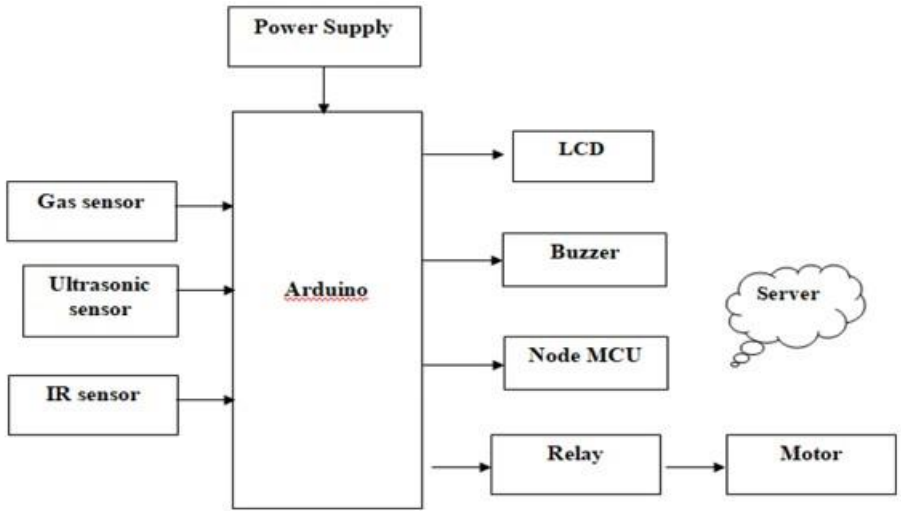


Figure.1Block diagram

2.1 Hardware description

2.1.1 Introduction to Aurdino

Arduino is an open-source electronics platform based on easy-to-use hardware and software. It consists of a microcontroller that can be programmed to sense and control objects in the physical world. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. They are used for a variety of purposes, including creating interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino boards come in various shapes and sizes, each with its own set of features and capabilities. Some of the most popular Arduino boards include:

Arduino Uno: The Uno is one of the most popular Arduino boards. It features a microcontroller, digital and analog input/output pins, USB connection, and a power jack.

Arduino Mega: The Mega is similar to the Uno but with more digital and analog input/output pins, making it suitable for larger projects that require more I/O.

Arduino Nano: The Nano is a compact board with similar features to the Uno but in a smaller form factor, making it ideal for projects with space constraints.

Arduino Due: The Due is based on a more powerful microcontroller than the Uno, making it suitable for projects that require more processing power.

Arduino Leonardo: The Leonardo is similar to the Uno but with built-in USB communication, making it easier to interface with computers.

In addition to the hardware, Arduino also provides a software development environment that allows users to write, compile, and upload code to their Arduino boards. The Arduino IDE (Integrated Development Environment) is a simple yet powerful tool that is used to write code in the Arduino programming language, which is based on Wiring, and upload it to the board.

Overall, Arduino is a versatile platform that is used by hobbyists, students, and professionals alike to create a wide range of projects, from simple blinking LED lights to complex robotics projects. Its ease of use, coupled with its affordability and flexibility, has made it one of the most popular platforms for electronics prototyping and experimentation.

2.1.2 Features of the Arduino

Arduino boards come with a variety of features that make them suitable for a wide range of projects. Some of the key features of Arduino boards include:

Microcontroller: Arduino boards are equipped with a microcontroller, which is the brain of the board. The microcontroller is responsible for executing the program and controlling the inputs and outputs of the board.

Digital Input/Output Pins: Arduino boards come with a number of digital input/output (I/O) pins that can be used to connect the board to external devices such as sensors, LEDs, and motors. These pins

can be configured as either inputs or outputs, allowing the board to read data from sensors or control external devices.

Analog Input Pins: In addition to digital I/O pins, Arduino boards also feature analog input pins that can be used to read analog signals from sensors. These pins allow the board to measure variables such as light intensity, temperature, and sound level.

PWM (Pulse Width Modulation) Pins: Some Arduino boards come with PWM pins, which can be used to generate analog-like signals. PWM is often used to control the brightness of LEDs or the speed of motors.

USB Connection: Arduino boards feature a USB connection, which allows them to be connected to a computer for programming and serial communication. The USB connection also provides power to the board, eliminating the need for an external power source.

Power Jack: Arduino boards come with a power jack that can be used to connect an external power source, such as a battery or a wall adapter. This allows the board to be powered independently of the USB connection.

Reset Button: Arduino boards feature a reset button that can be used to restart the board and re-run the program.

Integrated Development Environment (IDE): Arduino boards are programmed using the Arduino IDE, which provides a simple and intuitive interface for writing, compiling, and uploading code to the board.

Open-Source: Arduino is an open-source platform, which means that the hardware designs and software libraries are freely available for anyone to use and modify. This has led to a large community of Arduino users who share their projects and collaborate on new ideas.

Overall, Arduino boards are versatile and easy-to-use platforms that are ideal for beginners and experienced makers alike. Their combination of features, affordability, and flexibility make them a popular choice for a wide range of projects, from simple blinking LED lights to complex robotics applications.

2.1.3 Arduino Pinout

• Arduino Uno is based on an AVR microcontroller called Atmega328. This controller comes with 2KB SRAM, 32KB of flash memory, and 1KB of EEPROM. The Arduino Board comes with 14 digital pins and 6 analog pins. ON-chip ADC is used to sample these pins. A 16 MHz frequency crystal oscillator is equipped on the board. The following figure shows the pinout of the Arduino Uno Board

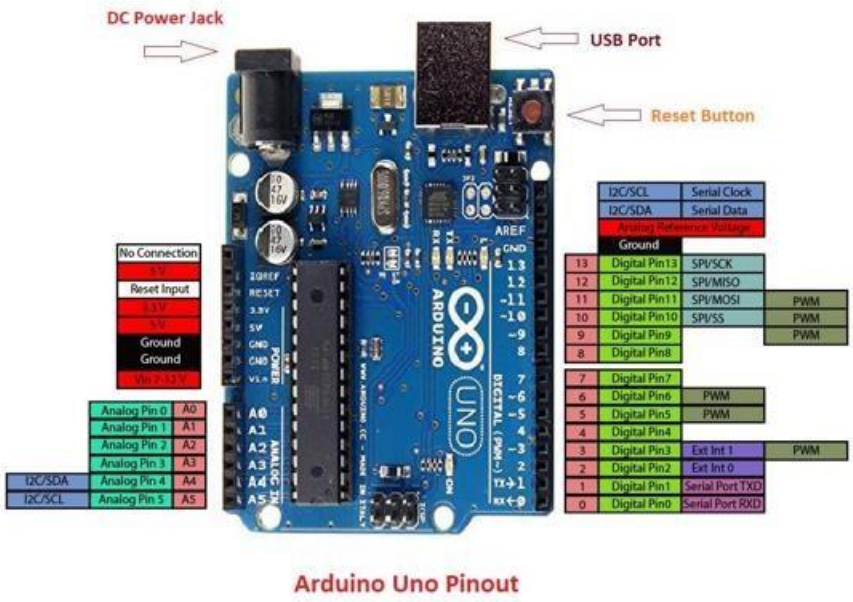


Figure.2. Arduino UNO Pinout diagram

3. Results and Discussion

3.1 Code for Arduino UNO

```
#include <Adafruit_Fingerprint.h> #include <SPI.h>
```

```
#include <MFRC522.h> #define SS_PIN 10
#define RST_PIN 9 int relay=4; int
buz=5; int a=0; int b=0;
MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance. volatile int finger_status = -1;
SoftwareSerial mySerial(2, 3); // TX/RX on fingerprint sensor Adafruit_Fingerprint finger =
Adafruit_Fingerprint(&mySerial); void setup()
{
Serial.begin(9600); pinMode(relay,OUTPUT); pinMode(buz,OUTPUT); digitalWrite(relay,HIGH);
digitalWrite(buz,LOW);
SPI.begin();              // Initiate SPI bus mfrc522.PCD_Init(); // Initiate MFRC522
// Serial.println("Approximate your card to the reader..."); Serial.println();
while (!Serial); // For Yun/Leo/Micro/Zero/... delay(100);
finger.begin(9600); if (finger.verifyPassword())
{
//          Serial.println("Found fingerprint sensor!");
} else
{
Serial.println("Did not find fingerprint sensor :("); while (1) { delay(1); }
}
finger.getTemplateCount();
// Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println("
templates"); Serial.print("#");
}
void loop()                    // run over and over again
{ finger_status = getFingerprintIDez(); if
(finger_status!=-1 and finger_status!=-2)
{
Serial.println("FINGER_MATCHED"); b=b+1;
} else

{
if (finger_status==-2)
{
for (int ii=0;ii<1;ii++) {
//                Serial.println("Not Match");          digitalWrite(buz,HIGH);          delay(3000);
digitalWrite(buz,LOW);
Serial.println("FINGER_NOT_MATCHED");
}
}
}
delay(50);              //don't ned to run this at full speed.
// Look for new cards
if ( ! mfrc522.PICC_IsNewCardPresent())
{ return;
}
if ( ! mfrc522.PICC_ReadCardSerial())
{ return;
}
String content= ""; byte letter;
for (byte i = 0; i < mfrc522.uid.size; i++)
{
```

```
content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : "
  ")); content.concat(String(mfrc522.uid.uidByte[i], HEX));
}
content.toUpperCase();

  if (content.substring(1) == "73 C5 81 2E") //change here the UID of the card/cards that you want to
give access
{
Serial.println("CARD_MATCHED"); a=a+1;
} else
{
//   Serial.println(" Access denied"); digitalWrite(buz,HIGH); delay(3000);
digitalWrite(buz,LOW);
Serial.println("CARD_NOT_MATCHED");
}
if(a==b&&a>0&&b>0)
{
Serial.println("DOOR OPENED"); digitalWrite(relay,LOW); delay(5000); digitalWrite(relay,HIGH);
} else
{
Serial.println("DOOR NOT OPENED");
}
}
// returns -1 if failed, otherwise returns ID # int getFingerprintIDez()
{
uint8_t p = finger.getImage(); if (p!=2)

{
//          Serial.println(p);
}
if (p != FINGERPRINT_OK) return -1; p = finger.image2Tz(); if
(p!=2){
//          Serial.println(p);
}
if (p != FINGERPRINT_OK) return -1; p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK) return -2; //
found a match!
// Serial.print("Found ID #"); Serial.print(finger.fingerID);
// Serial.print(" with confidence of "); Serial.println(finger.confidence); return finger.fingerID; }
```

3.2 Code for Node MCU

```
#include <ESP8266WiFi.h> #include "ThingSpeak.h"
const char* ssid = "project"; // your network SSID (name)
const char* password = "1234567890"; // your network password WiFiClient client; unsigned
long myChannelNumber = 2388243;
const char * myWriteAPIKey = "OSTJY1RPZUHT73EI";
// Timer variables
unsigned long lastTime = 0; unsigned long timerDelay = 30000; String String_main; String
String_1; void setup() {

Serial.begin(9600); WiFi.mode(WIFI_STA); ThingSpeak.begin(client); while (!Serial) { ;
// wait for serial port to connect. Needed for native USB port only
```

```
} }
void loop()
{
if ((millis() - lastTime) > timerDelay) {
// Connect or reconnect to WiFi if(WiFi.status() != WL_CONNECTED){ Serial.print("Attempting to
connect"); while(WiFi.status() != WL_CONNECTED){
WiFi.begin(ssid, password); delay(5000);
}
Serial.println("\nConnected.");
}
if (Serial.available())
{
String_main=Serial.readString(); Serial.println(String_main);
// String_1=String_main.substring(0,4);
// Serial.print(String_1); delay(500); ThingSpeak.setField(1,String_main);
int x = ThingSpeak.writeFields(myChannelNumber,myWriteAPIKey); if(x == 200){
Serial.println("Channel update successful.");
}

else{
Serial.println("Problem updating channel. HTTP error code " + String(x));
}
// }
// String_2=String_main.substring(2,5);
// Serial.print(String_2);
// delay(500);
// ThingSpeak.setField(2,String_2); lastTime = millis(); }
}
}
```

3.3 Results

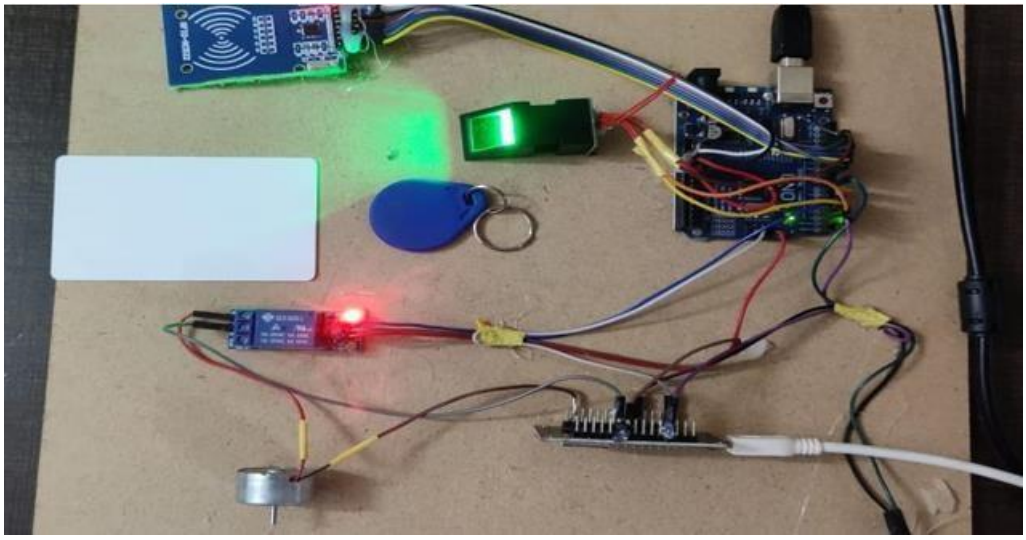
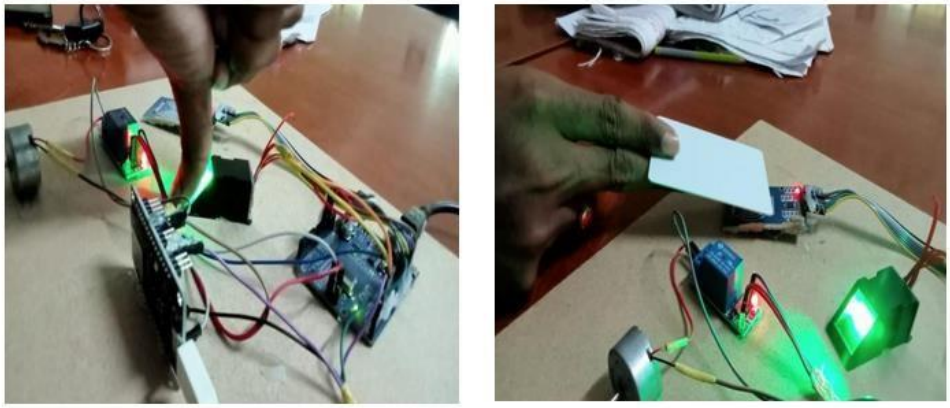


Figure.3. Working model of the developed system

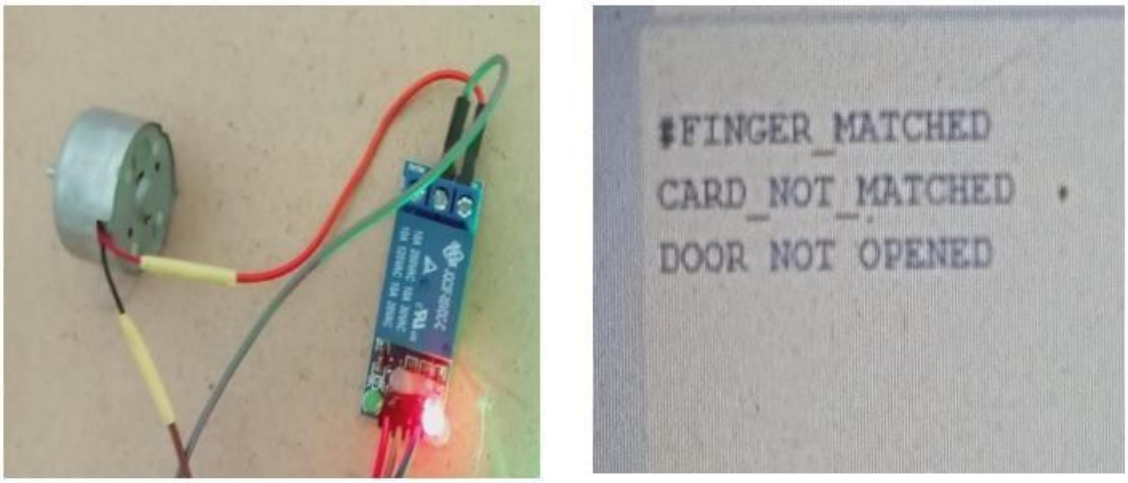
The image displays the Internet of Things integration of various components, such as an Arduino Uno, an RFID reader, a fingerprint module, a Node MCU, a relay, and a DC motor. This comprehensive solution, which combines dual-factor authentication with real-time monitoring, further improves security by acting as a strong deterrent against vehicle theft and unauthorised use while giving vehicle owners more convenience and control.



(a) (b)

Figure.4. (a)Valid Finger print (b) Valid Driver's License Card

In this case, the driver's licence card displayed in figure 4(b) is a valid licence card, and the fingerprint displayed in image 4(a) is a legitimate fingerprint. The only thing that has to be started on the car is the engine if both authentication stages pass.

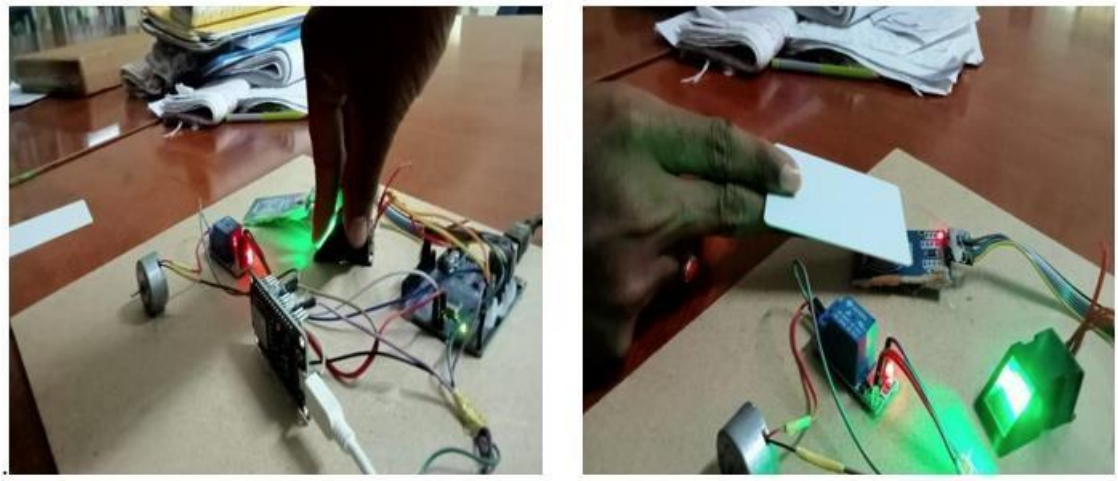


(c) (d)

Figure.5. Relay Not Activated, Vehicle Not Started (d) Serial Monitor Output

Fingerprint: Matched, Driver's License: Not Matched, Vehicle Status: Door Not Opened

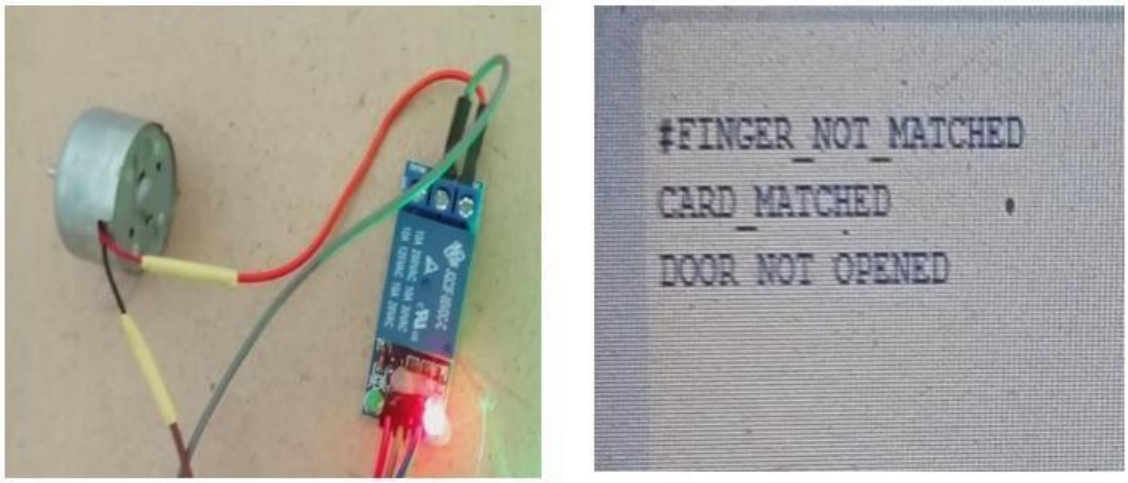
Here, first level of authentication is successful but second level of authentication i.e. valid driver's license is failed so the vehicle engine is not started and gives a beep sound.



(a) (b)

Figure. 6(a)Invalid Fingerprint (b)Valid Driver's License Card

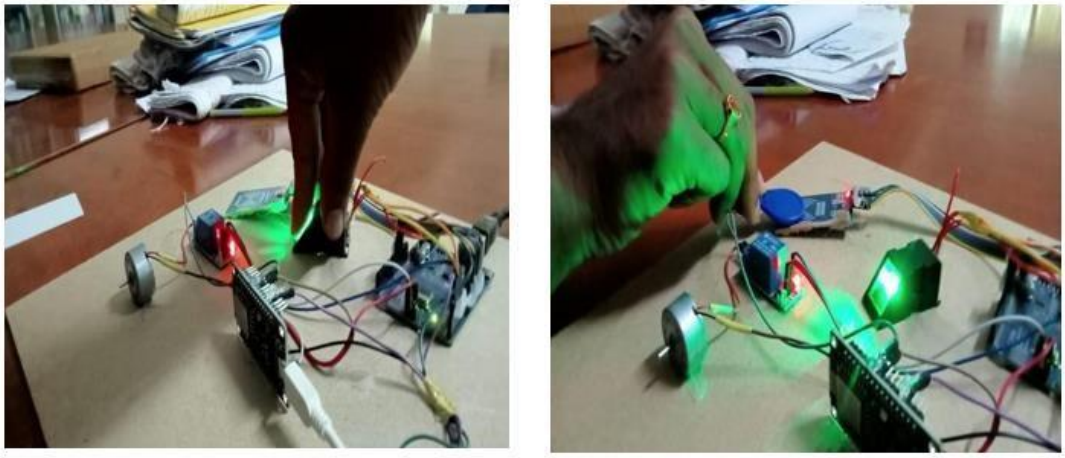
Here, the fingerprint shown in the image 6 (a) is a Invalid fingerprint and the driver's license card shown in the figure 6 (b) is a valid license card.



(c) (d)

Figure. 7 (c) Relay Not Activated, Vehicle Not Started (d) Serial Monitor Output
Fingerprint: Not Matched, Driver's License: Matched, Vehicle Status: Door Not Opened

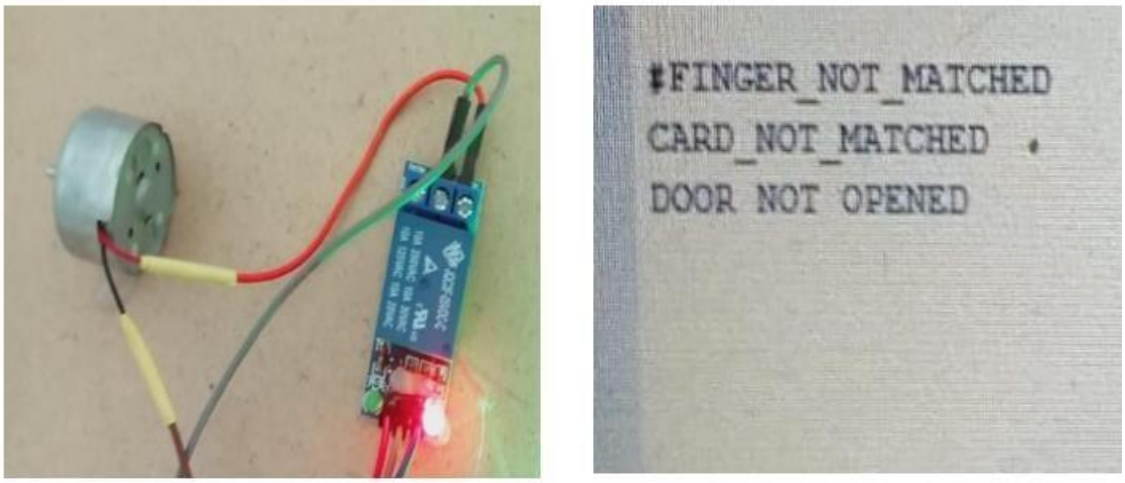
Here, the vehicle's engine does not start and emits a beep sound after the initial fingerprint authentication fails, yet the subsequent authentication succeeds.



(a) (b)

Figure. 8 (a)Invalid Fingerprint (b)Invalid Driver's License Card

Here, the fingerprint shown in the image 8 (a) is a Invalid fingerprint and the driver's license card shown in the figure 8 (b) is a valid license card.



(c) (d)

Figure.9 (c) Relay Not Activated, Vehicle Not Started (d) Serial Monitor Output

Fingerprint: Not Matched, Driver's License: Not Matched, Vehicle Status: Door Not Opened. Here both levels of authentication are failed, so the vehicle engine is not started and gives a beep sound.

2024-01-20T07:12:44+00:00	54 FINGER_MATCHED
2024-01-20T07:14:40+00:00	55
2024-01-20T07:15:12+00:00	56 CARD_MATCHED
2024-01-20T07:15:50+00:00	57
2024-01-20T07:16:23+00:00	58 FINGER_MATCHED
2024-01-20T07:16:56+00:00	59 FINGER_MATCHED
2024-01-20T07:17:37+00:00	60
2024-01-20T07:18:10+00:00	61 #FINGER_MATCHED
2024-01-20T07:18:43+00:00	62
2024-01-20T07:19:16+00:00	63 CARD_NOT_MATCHED
2024-01-20T07:20:23+00:00	64
2024-01-20T07:20:56+00:00	65 #CARD_NOT_MATCHED
2024-01-20T07:31:14+00:00	66
2024-01-20T07:31:47+00:00	67 CARD_MATCHED
2024-01-20T07:32:20+00:00	68
2024-01-20T07:32:53+00:00	69 CARD_NOT_MATCHED
2024-01-20T07:33:25+00:00	70
2024-01-20T08:45:55+00:00	71 FINGER_MATCHED

Figure.10. Dual Authentication Analysis & Real-Time Data Visualization

The efficacy of dual-factor authentication (fingerprint and RFID) is demonstrated in image 10. It shows both successful and unsuccessful attempts graphically, with "card matched" and "fingerprint matched" entries clearly labelled alongside their "not matched" counterparts. Users are able to obtain insights into the authentication performance over a given period of time by examining this visual representation.

Additionally, this project sends data to Thing Speak, a potent real-time data visualisation and analysis tool, via NodeMCU. By enabling wireless connection between cars and a central computer, this integration improves our system and makes monitoring and control easier. Users can view real-time car data visualisation with Thing Speak, which offers insightful information about how vehicles operate and perform. This all-encompassing strategy guarantees the highest levels of safety and operational effectiveness while giving owners and authorities remote monitoring and management capabilities.

3.4 ADVANTAGES

- Enhanced Two-Factor Authentication:
- Robust Vehicle Security:
- Real-Time Vehicle Monitoring:
- Remote Control and Tracking:
- Convenience for Vehicle Owners

3.5 APPLICATIONS

- Vehicle Security Enhancement: The primary application of this project is to bolster vehicle security by implementing a sophisticated access control system. By integrating driver's license and fingerprint authentication, the system ensures that only authorized individuals can access the vehicle, significantly reducing the risk of theft or unauthorized use.
- Fleet Management Solutions: Fleet management companies can utilize this technology to manage and monitor their vehicle fleets more effectively. With enhanced security measures in place, they can prevent unauthorized access to fleet vehicles and track driver activities, promoting accountability and ensuring compliance with operational protocols.
- Rental Car Industry: Rental car companies can benefit from this system by improving the security and integrity of their vehicle rental services. By implementing biometric authentication, they can streamline the rental process, eliminate the risk of fraudulent rentals, and enhance customer confidence in the safety of their vehicles.
- Commercial Vehicle Security: Businesses operating commercial vehicles, such as delivery trucks and service vans, can deploy this technology to safeguard their assets and ensure the security of valuable cargo. By restricting access to authorized drivers only, they can mitigate the risk of theft, tampering, or misuse of company vehicles.
- Government and Law Enforcement Vehicles: Government agencies and law enforcement organizations can integrate this system into their vehicle fleets to enhance security and access control. By incorporating biometric authentication, they can ensure that only authorized personnel can operate government vehicles, minimizing the risk of misuse or unauthorized access.
- Executive Protection Vehicles: High-profile individuals, such as corporate executives or government officials, often require enhanced security measures for their vehicles. This system can be deployed in executive protection vehicles to enforce strict access control protocols, safeguarding VIPs and their valuable assets from potential threats or security breaches.
- Transportation Network Companies (TNCs): TNCs like Uber and Lyft can integrate this system into their ride-sharing platforms to enhance driver authentication and passenger safety. By ensuring that only verified drivers can access the TNC vehicles, and passengers can confirm the identity of their drivers, the system enhances trust and security within the ride-sharing ecosystem.
- Military and Defense Applications: Military and defense organizations can deploy this technology in military vehicles and armored vehicles to enforce strict access control measures and prevent unauthorized access by adversaries. By integrating biometric authentication with vehicle security systems, they can enhance operational security and protect sensitive equipment and personnel in high-risk environments.

4. Conclusion

The novel vehicle security system implementation, which incorporates driver's license and fingerprint automation, signifies a substantial advancement in automotive security technology. This project combines biometric authentication with traditional access control methods, such as key-based systems, to introduce a robust and multifaceted approach to vehicle protection. Extensive testing and validation have demonstrated the system's effectiveness in preventing unauthorized access and enhancing overall vehicle security.

A key takeaway from this project is the importance of integrating multiple layers of security to create a comprehensive defence mechanism against theft and unauthorized use. By utilizing biometric data, such as fingerprints, along with driver's license verification, the system establishes a highly secure authentication process that significantly reduces the risk of unauthorized access. This layered approach not only enhances vehicle security but also provides peace of mind to vehicle owners and operators.

References

[1] Pramod Sharma, A. Shrivastav, V. Parashar, O. Kumar, R. Naresh, “Smart security system for vehicle,” International Journal on Advanced Research in Computer and communication Engineering, vol. 8, issue. No. 4, pp. 279-283, April 2019.

[2] M. Saravnan, R. Prasannavenkatesh, S. Poovitha, B. Thiruvarast, C. Prathepa, “Smart license based vehicle safety and security system,” International Journal on Advance research in Science and engineering, vol. no. 6, issue no. 10, pp. 1213-1220, Oct. 2017.

[3] Fingerprint recognition using standardized fingerprintmodel Le Hoang Thai 1 and Ha Nhat Tam 2 1 Faculty ofInformation Technology, University of Science Ho ChiMinh City, 70000, Viet Nam 2 University of Science Ho ChiMinh City, 70000, Viet Nam, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010

[4] Arpit Agrawal and Ashish Patidar, “Smart Authentication for Smart Phones”, International Journal of Computer Science and Information Technologies, Vol. 5, No4 , pp.4839-4843,2014. [5] Adeoye, O. S. “A survey of emerging biometric technologies”, International Journal of Computer Applications,2010

[6] S. S. Patil, K. N. Patil , S. P. Patil “Gesture based wheel chair for physically disabled person” International Journal of Engineering and sciences and research technology (IJESRT) (ISSN:22779655), pp-245-252,Publicatio Impact Factor:3.785,December 2015.

[7] S. S. Patil, K. M. Dange , S. P. Patil “PIC Microcontroller based Neural network and image processing controlled low cost autonomous vehicle” International Research Journal of Engineering and Technology (IRJET) Volume 2 Issue 9, (I20R),pp-504- 507,Publication Impact Factor:4.45, December 2015.

[8] Automated Fingerprint Identification Systems (AFIS) Book by Peter Komarinski Originally published: 17th December 2004.

[9] Praveen Kaur, A. Das, M. Borah, “Vehicles safety system using Arduino,” ADBU Jounal of Electrical and Electronics Engineering, vol. no. 3, issue no. 2, 2019.

[10] Elngar, Ahmed A. and Kayed, Mohammed. "Vehicle Security Systems using Face Recognition based on Internet of Things" Open Computer Science, vol. 10, no. 1, 2020, pp. 17-29. https://doi.org/10.1515/comp2020-0003.

[11] Siyal, Karan, Gugapriya. G., “Anti-theft vehicle locking system using CAN,” Indian journal of Science and Technology, vol. no. 9, issue. No. 45, 2016, DOI: 10.17485/ijst/2016/v9i45/105307.

[12] Hussain Elbehiry, “Electronic police ambush system via vehicles/drivers safety authentication system”, International Journal on Information Technology and Computer Science, vol. no. 9, pp. 32- 38, 2018.

[13] Vivek K. S., Soumitra M., and Harshit M.,” Car Security using Internet of Things”, 1st IEEE International Conference on Power Electronics Intelligent Control and Energy Systems (ICPEICES2016), 978-1-4673-8587-9/16/31.00 ©2016 IEEE.