Raspberry Pi-based dual authentication system for vehicle security

Ms. Komal Ananda Palande
ElectronicsandTelecommunicationEngineering,
SHIVNAGAR VIDYA PRASARAK MANDAL College of Engineering, Malegaon (BK) Malegaon, India

Mr. S. D. Kale
Electronics and Telecommunication Engineering,
SHIVNAGAR VIDYA PRASARAK MANDAL College of Engineering, Malegaon (BK)Malegaon, India

Abstract— The proposed system combines two-factor authentication using biometric fingerprint recognition and real-time image verification to establish a comprehensive security solution. The authentication process begins with the fingerprint sensor, which captures and verifies the biometric data of the user. If the fingerprint matches a registered profile, the system proceeds to the second authentication stage, where the camera module captures a real-time image of the user. This image can be further analyzed or stored for audit purposes. Only after both the fingerprint and image checks are validated does the system trigger the relay, allowing access to the vehicle. In cases of failed authentication, the system activates a buzzer to notify nearby individuals of a potential intrusion attempt, while the display provides feedback, showing an "Access Denied" message. This dual authentication approach mitigates the risks associated with single-point verification methods, significantly reducing vulnerability to unauthorized access attempts. Designed with scalability in mind, this project demonstrates a practical and effective solution for vehicle security, integrating biometric and visual verification technologies. This system can be further expanded or adapted for various security applications, providing a versatile framework for modern security needs.

Keywords—Dual Authentication; Raspberry Pi; Camera, Fingerprint,

1.1 INTRODUCTION :

With the increasing sophistication of vehicle theft methods, the need for more advanced security systems has become paramount. Traditional vehicle access controls, such as keys or remote fobs, are increasingly vulnerable to attacks like key cloning, relay attacks, and lock manipulation. To overcome these vulnerabilities, this project introduces a dual authentication security system for vehicles, incorporating both biometric fingerprint recognition and real-time image verification. The use of dual authentication elevates the security standard by ensuring that access to the vehicle is only granted to verified, authorized users, minimizing the risk of unauthorized entry. This layered approach to security addresses the limitations of single-point authentication methods, making the vehicle significantly more secure against modern threats.

The Raspberry Pi was chosen due to its computational capabilities, ease of integration with multiple sensors and modules, and support for complex software programming. This microcontroller acts as a bridge between the system's input and output devices, including a fingerprint sensor, camera module, display, buzzer, and relay. The project leverages Raspberry Pi's GPIO (General-Purpose Input/Output) pins to connect and control these components, creating a seamless and efficient security workflow.

The first layer of authentication utilizes a fingerprint sensor, which scans and verifies the user's unique biometric data. Biometric security is widely regarded as one of the most reliable forms of authentication, as fingerprints are unique to each individual and difficult to replicate. The second layer of authentication is where a camera module captures a real-time image of the user. This image verification stage adds security measures by enabling visual confirmation of the user's identity, which could be used for

further analysis or as a deterrent for unauthorized individuals.

The dual authentication process adds significant robustness to the system. Unlike traditional key-based or PIN-based systems, which can be easily compromised, this approach combines something the user *has* (their fingerprint) with something the system *sees* (their image). This makes it difficult for intruders to bypass the system, as gaining unauthorized access would require defeating both the biometric and visual verification layers. Furthermore, the system can be expanded in the future to incorporate facial recognition or remote monitoring, making it a scalable and adaptable solution for modern vehicle security needs.

In addition to the authentication modules, the system includes a display, buzzer, and relay to enhance user interaction and provide feedback on authentication attempts. The display plays a critical role by providing visual feedback to the user, indicating the status of the authentication process. For instance, messages such as "Authentication Successful" or "Access Denied" can inform users of their access status in real time. If authentication fails at any stage, the system activates a buzzer, alerting those nearby to a potential security breach. This auditory alert adds an extra layer of deterrence against unauthorized access. Finally, a relay controls the locking mechanism of the vehicle, which is only activated upon successful dual authentication. This relay setup ensures that even if one layer of security is compromised, access is only granted if both layers are verified.

1.2 PROBLEM STATEMENT:

In recent years, the rise in vehicle theft has exposed the limitations of conventional security mechanisms, which often rely on single-factor authentication methods such as keys, PIN codes, or remote keyless entry. These traditional methods, though widely used, have shown significant vulnerabilities. Techniques like key cloning, relay attacks, and lock picking allow criminals to bypass these systems with relative ease. As vehicles become more technologically advanced, so do the methods used by intruders to compromise them, creating a need for more sophisticated security measures. This challenge highlights a crucial gap in vehicle security: the need for an enhanced system that can effectively prevent unauthorized access.

Additionally, traditional security solutions fail to account for personalized and adaptive security. A physical key, for instance, can be used by anyone who possesses it, meaning it does not truly verify the user’s identity. PIN codes and remote fobs can be lost, stolen, or even hacked, leaving vehicles vulnerable to unauthorized individuals. This lack of identity-specific verification is a fundamental weakness, as it allows anyone with access to the key or code to bypass security without confirming their legitimacy as an authorized user. The absence of user-specific verification not only compromises vehicle security but also diminishes user trust in the system's ability to protect against unauthorized access.

1.3 MOTIVATION:

Vehicle security has become a crucial concern in recent years due to the rise in vehicle thefts and the increased sophistication of criminal methods. Traditional security mechanisms, such as physical locks, alarms, and key-based systems, are no longer sufficient to protect against these advanced threats. Criminals are often able to bypass these methods with ease, leaving vehicle owners vulnerable to theft and unauthorized access. In response, there is a growing need for more secure, technology-driven solutions that can offer enhanced protection.

Biometric authentication has proven to be a robust security measure in various applications, from smartphones to secure facilities. Fingerprint-based access control, in particular, is highly reliable, as fingerprints are unique to each individual and cannot be easily

duplicated. By incorporating a fingerprint sensor into a vehicle security system, unauthorized individuals are effectively prevented from accessing the vehicle. However, to further improve security, dual authentication systems add another layer, requiring two separate forms of verification before access is granted. In this project, a camera module is included alongside the fingerprint sensor, enabling visual verification of the user and further reducing the likelihood of unauthorized access.

The Raspberry Pi serves as the core processing unit of this dual authentication system, handling data from both the fingerprint sensor and the camera module. It is responsible for processing and validating the fingerprint, capturing images, and determining whether to activate the buzzer, display messages, or trigger the relay to lock or unlock the vehicle. The integration of multiple components, including a display and buzzer, provides immediate feedback to the user, indicating successful or failed authentication attempts. This approach not only ensures a higher level of security but also creates a user-friendly experience.

The goal of this report is to detail the design and implementation of this dual authentication vehicle security system, demonstrating its effectiveness as a deterrent to vehicle theft. This system leverages readily available components, making it a cost-effective solution without compromising security. By utilizing dual authentication methods, vehicle owners can achieve greater peace of mind, knowing that their vehicles are safeguarded by advanced, multi-layered security technology.

OBJECTIVE:

The primary objective of this project is to develop a Raspberry Pi-based dual authentication system that enhances vehicle security by integrating biometric and visual verification methods.

Specific Goals Include:

Develop a Dual Authentication Security System

Utilize Cost-Effective and Readily Available Hardware

Implement Real-Time Monitoring and Feedback Mechanisms

Securely Control Vehicle Access Using a Relay Mechanism

Strengthen the Vehicle's Security Framework Through Multi-Layered Protection

Provide a User-Friendly Interface and Experience

2. LITERATURE REVIEW

1. "**Autonomous Vehicle: Security by Design"** in IEEE Transactions on Intelligent Transportation Systems on **Date of Publication**: 30 June 2020 by Authors Mr. Anupam Chattopadhyay, Mr. Kwok-Yan Lam and Mr. Yaswanth Tavva are Senior Members, IEEE. Said it as Security of (semi)-autonomous vehicles is a growing concern, first, due to the increased exposure of the functionality to potential attackers; second, due to the reliance of functionalities on diverse (semi)-autonomous systems; third, due to the interaction of a single-vehicle with myriads of other smart systems in urban traffic infrastructure.. We attempt to identify the core issues of securing an AV. This is done methodically by developing a security-by-design framework for AV from the first principles. Subsequently, the technical challenges for AV security are identified.

2. **"Security challenges in vehicular cloud computing"** in IEEE Transactions on Intelligent Transportation Systems on **Date of Publication:** 03 September 2012 by authors Mr. Gongjun Yan, Mr. Stephan Olariu and Ms. Michele C. Weigle are said that In a VC, underutilized vehicular resources including computing power, storage, and Internet connectivity can be shared between

drivers or rented out over the Internet to various customers. Clearly, if the VC concept is to see a wide adoption and to have significant societal impact, security and privacy issues need to be addressed. The main contribution of this work is to identify and analyze a number of security challenges and potential privacy threats in VCs.

3. **“Connected Vehicles' Security from the Perspective of the In-Vehicle Network”** in IEEE Network on 04 June 2018 by Authors Xiangxue Li and Yu Yu are said that Connected vehicles are generally equipped with many (dozens of, or even hundreds of) electronic and intelligent devices so that drivers can gain a more comfortable driving experience. Despite their numerous benefits, these technological developments have also created serious safety/security concerns.

4. **“A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)”** in IEEE Transactions on Intelligent Transportation Systems on 07 June 2021 by Authors Mr. Xiaoqiang Sun, Mr. F. Richard Yu and Ms. Peng Zhang are said that As the general development trend of the automotive industry, connected and autonomous vehicles (CAVs) can be used to increase transportation safety, promote mobility choices, reduce user costs, and create new job opportunities. However, with the increasing level of connectivity and automation, malicious users are able to easily implement different kinds of attacks, which threaten the security of CAVs. Hence, this paper provides a comprehensive survey on the cyber-security in the environment of CAVs with the aim of highlighting security problems and challenges.

5. **"Biometric and Passcode-Based Anti-Theft Vehicle Security System."** by Authors are Mr. Prashanth.S, Mr. Sachin Kumar.BU, Ms. Sahana.CE, and Mrs. Yojana Yadav are affiliated with the Department of Electronics and Communication Engineering at PES Institute of Technology and Management, located in Shivamogga, Karnataka, India. Said it as Today, vehicle owners face a significant concern regarding the potential theft of their vehicles, whether parked in communal parking areas or outside their residences. To address this issue, a real-time vehicle theft detection and prevention system based on image processing is proposed, offering an effective solution. This paper presents a cost-effective and scalable framework for a smart vehicle security system, comprising a Fingerprint Detection Subsystem (FDS), a GPS module, a GSM module, and a control platform.

3. SYSTEM IMPLEMENTATION

BLOCK DIAGRAM

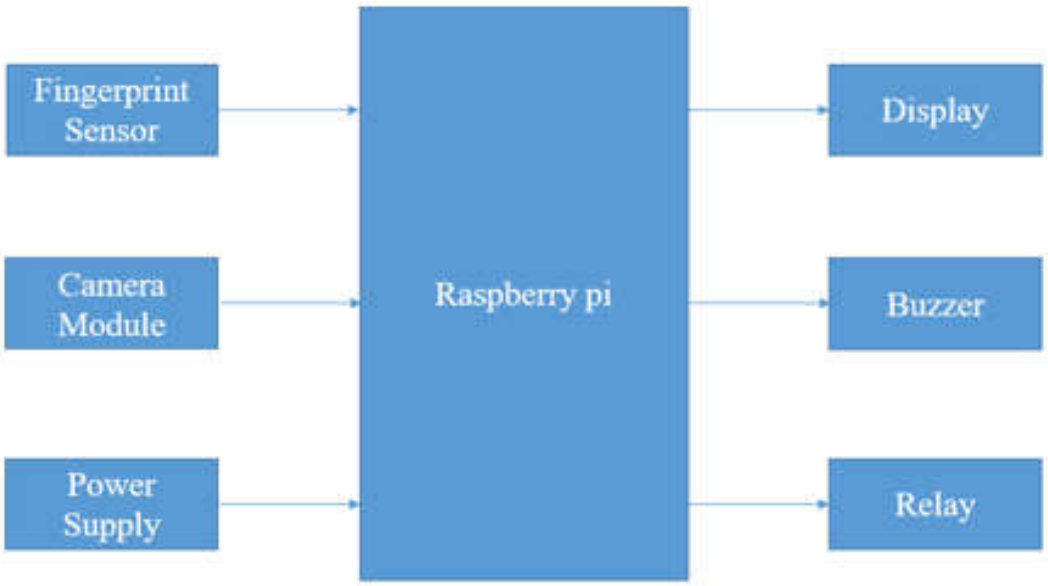

Figure 3.1 : Block Diagram

WORKING MODE:

The block diagram illustrates the components and flow of operation in a Raspberry Pi-based dual authentication system designed for vehicle security. At the center of the diagram is the **Raspberry Pi**, which acts as the core processing unit, managing inputs from various sensors and controlling outputs based on the authentication results. Each connected component plays a crucial role in ensuring the system's security and functionality.

Fingerprint Sensor: The fingerprint sensor serves as the primary layer of authentication. It scans and verifies the fingerprint of the person attempting to access the vehicle. Upon placing a finger on the sensor, the fingerprint data is captured and sent to the Raspberry Pi for analysis. If the fingerprint matches one of the pre-registered patterns stored in the system, the authentication is considered partially successful. However, without additional verification from the camera module, access is not granted. This dual-layer approach ensures that fingerprint recognition alone is not enough, adding an extra level of security.

Camera Module: The camera module provides a secondary layer of verification by capturing an image or video of the person attempting access. This allows for visual verification, which is essential in preventing unauthorized access even if the fingerprint sensor is compromised. The Raspberry Pi processes the image to confirm the identity of the user. For example, it can match the captured image against a pre-existing photo of the authorized user stored in the system. Only when both the fingerprint and the image verification are successful does the system proceed to grant access.

Power Supply: The power supply is the foundation that ensures the system operates continuously and reliably. It provides the necessary power to the Raspberry Pi, as well as to the connected sensors and modules. In real-world applications, this could be a vehicle battery or an external power source. The power supply needs to be stable to prevent sudden shutdowns, which could compromise the security and reliability of the system.

Display: The display is an important interface for user interaction, showing the status of the authentication process. When a user attempts to access the vehicle, the display may show prompts for fingerprint scanning, image capture, and authentication results (success or failure). By providing real-time feedback, the display ensures that the user is informed throughout the process, helping them understand if access has been granted or if there was a failed attempt.

Buzzer: The buzzer acts as an audio alert mechanism, providing sound feedback during the authentication process. It may emit different sounds based on the authentication status, such as a short beep for successful verification and a continuous alarm if there is a failed or unauthorized attempt. The buzzer is particularly useful in drawing attention to any unauthorized access attempts, alerting the vehicle owner or others nearby.

Relay Module: The relay is a crucial component in the system as it directly controls the vehicle’s locking and ignition mechanisms. When both fingerprint and image verifications are successful, the Raspberry Pi sends a signal to the relay, which then activates the necessary vehicle systems (such as unlocking doors or enabling the ignition). If authentication fails, the relay remains inactive, preventing the vehicle from being accessed or started. This feature acts as the final security layer, physically restricting access based on the results of the dual authentication.

In summary, the Raspberry Pi acts as the control hub, coordinating input from the fingerprint sensor and camera module, and

managing output through the display, buzzer, and relay module. The combination of biometric and visual verification creates a robust dual authentication system that provides enhanced vehicle security, effectively deterring unauthorized access and theft. This setup ensures that access is only granted when both authentication methods confirm the user's identity, making it a reliable and advanced solution for vehicle security.

4. COMPONENTS DESCRIPTIONS

Raspberry pi :

The Raspberry Pi 4 is the latest product in the Raspberry Pi range, boasting an updated 64- bit quad core processor running at 1.4GHz with built-in metal heatsink, USB 3 ports, dual- band 2.4GHz and 5GHz wireless LAN, faster (300 mbps) Ethernet, and PoE capability via a separate PoE HAT. This version comes with 1GB of RAM, but we also have versions with 2 and 4 GB if you like. Pi 4 B is upgraded with Latest High-Performance Quad-Core 64-bit Broadcom 2711, Cortex A72 processor clocked at 1.5GHz speed. Which is designed to use 20% less power or offer 90% greater performance than its old version. Hardware upgrade on Pi4 developed for more faster performance not only the loading time with all new 1GB/2GB and 4GB LPDDR4 SDRAM variants but also in connectivity with Dual-band 2.4GHz and 5GHz, 802.11 b/g/n/ac wireless LAN and PoE capability via a separate PoE HAT. Addition to it USB 3.0, improve the transfer speed by 10x than USB 2.0 to provide you significantly faster true Gigabit internet experience. Though the Pi 4 has type C USB port for 5V 3A input power capacity, new Hardware on Pi 4 even required less power than the previous versions therefore old power adapter can provide plenty of power to the chip, Ethernet, and any USB add-ons you plug in on board.

Specifications:

Model-Raspberry Pi 4 Model-B

Processor- Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz

RAM Memory - 1 GB LPDDR4 SDRAM

Figure 4.1: Raspberry pi

Fingerprint Sensor :

R307 is a finger print sensor module with TTL UART interface. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.The FP module can directly interface with 3v3 Microcontroller. A level converter (like MAX232) is required for interfacing with PC.

The R307 fingerprint module has two interface TTL UART and USB2.0, USB2.0 interface can be connected to the computer; RS232 interface is a TTL level, the default baud rate is 57600 , can be changed, refer to a communication protocol ; can And microcontroller, such as ARM, DSP and other serial devices with a connection, 3.3V 5V microcontroller can be connected directly. Needs to connect the computer level conversion, level conversion note , embodiments such as a MAX232 circuit.

Features:-

- Supply voltage: DC 4.2 ~ 6.0V
- Supply current: Working current: 50mA (typical) Peak current: 80mA
- Fingerprint image input time: <0.3 seconds
- Window area: 14x18 mm
- Matching method: Comparison method (1: 1)
- Search method (1: N)
- Characteristic file: 256 bytes
- Template file: 512 bytes
- Storage capacity: 1000 pieces
- Storage environment: Temperature: -40 ℃ - +85 ℃ Relative humidity: <85% H (no condensation)

Figure 4.2: Fingerprint Sensor

Camera Module:

This full functionality Webcam can deliver smooth and detailed high-quality video. With bright, crystal clear footage and vibrant colors, make your video chat or online conference session, a wonderful experience. Audio quality is also immaculate. Use this camera with common Videotelephony programs such as Skype, windows Live Messenger, Google Duo, Viber and Facebook

Messenger.

Specifications:

Brand - Zebion

Model Name: Tiger Eye

Type - Web camera

Dimensions - L 5.3 x B 6.5 x H 4.3 cm

Material - Plastic

Image Sensor - CMOS

Video resolution - 640 x 480 (30 FPS)

Cable length - 1.58 Meter

Figure 4.3: L293d

Buzzer:

This is Small PCB Mountable 5V Passive Buzzer-10 Pcs. It is great to add Audio Alert to your electronic designs. It operates on 5V supply, uses a coil element to generate an audible tone.

Specifications

- Input Voltage(Max.) : 5V
- Resistance: 42 Ω
- Resonance Frequency: 2048 Hz
- Body Size : 12 x 8mm
- Pin Pitch: 6mm

Figure 4.4: Buzzer

4.5 Relay:

A single-channel relay is an electronic switch that can be controlled by a low-power electrical signal, such as the output from an raspberry pi. By using an single-channel relay module, you can control high-voltage or high-power devices, such as lights, motors, and appliances, from your computer or mobile device. In this blog, we will explore how a relay works, how to interface a single-channel relay with an Arduino Uno, and demonstrate a simple example of how to use the 5v relay module to control a lamp. This 5V Dual Channel Relay Module has a 1×4 (2.54mm pitch) pin header for connecting power (5V and 0V), and for controlling the relay.

Specifications:

Relay Type: Low Level Trigger

Logic Input: 3.3 ~ 5

Trigger Voltage (VDC): 5

Switching Voltage (VAC): 250@10A

Switching Voltage (VDC): 30@10A

Length (mm): 50.6

Width (mm): 39

Height (mm): 19.5

Weight (g): 28

Shipping Weight : 0.03 kg

Shipping Dimensions: 6 × 5 × 3 cm

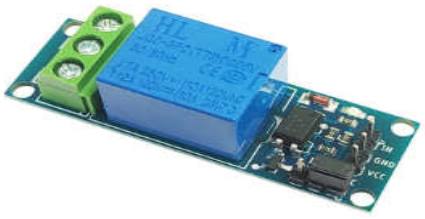

Figure 4.5: Relay

4.6 LCD :

This is LCD 1602 Parallel LCD Display that provides a simple and cost-effective solution for adding a 16×2 White on Liquid Crystal Display into your project. The display is 16 character by 2 line display has a very clear and high contrast white text upon a blue background/backlight. This is great blue backlight LCD display. It is fantastic for Arduino based project. This LCD1602 LCD

Display is very easy to interface with Arduino or Other Microcontrollers.

Specifications:

- Arduino IIC/I2C interface was developed to reduce the IO port usage on Arduino board
- I2C Reduces the overall wirings.
- 16 characters wide, 2 rows
- Single LED backlight included can be dimmed easily with a resistor or PWM.
- Interface: I2C
- Interface Address: 0x27
- Character Color: White
- Backlight: Blue
- Supply voltage: 5V

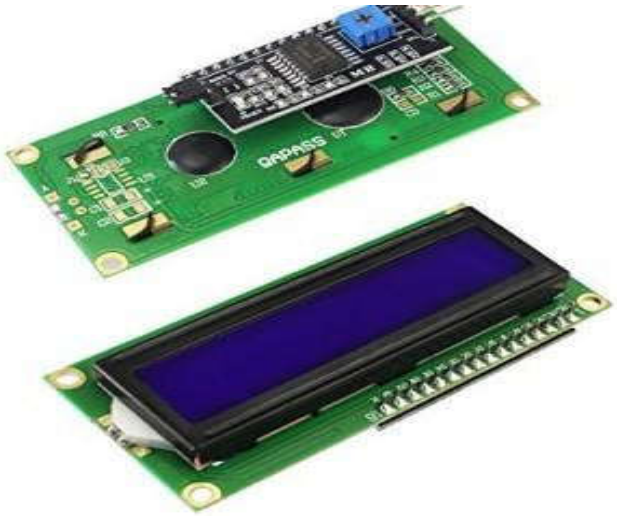

Fig 4.6 LCD

ADVANTAGES AND FUTURE SCOPE

5.1 ADVANTAGES:

- **Enhanced Security**: By using both fingerprint and face recognition, the system creates a dual-layer authentication method. This makes it significantly harder for unauthorized users to gain access, as both biometric credentials need to match. This dual approach is more secure than a single biometric method or traditional keys.
- **User-Friendly**: Biometrics are quick and convenient, allowing authorized users to unlock their vehicle without the hassle of keys or remembering a PIN. This is especially beneficial in urgent situations or when carrying items, as access can be granted with just a quick scan.
- **Scalability**: The system can register multiple users with individual biometric profiles, making it ideal for families or fleet vehicles where multiple people need access. Each user's fingerprint and facial data are stored securely, enabling easy and personalized access management.
- **Cost-Effective**: Leveraging the Raspberry Pi and readily available sensors, this solution is affordable compared to many proprietary vehicle security systems. It offers high security at a fraction of the cost, making it accessible for more users.

- **Low Power Consumption**: The Raspberry Pi and its components are designed for energy efficiency, making it practical for long-term operation in a vehicle without draining the battery. This low power demand is essential for continuous monitoring and quick activation.
- **Customizable**: This system can easily integrate additional features, such as remote alerts, GPS tracking, or even IoT connectivity. With the flexibility of the Raspberry Pi, the system can be tailored to specific needs, providing a comprehensive security solution.

5.2 DISADVANTAGES:

- **Limited Processing Power**: The Raspberry Pi, while versatile, may struggle with real-time face recognition if processing power or memory is limited, potentially causing delays in authentication.
- **Environmental Constraints**: Biometrics may not work as reliably in certain conditions, like low lighting for face recognition or dirty, wet, or damaged fingerprints, affecting performance.
- **Security Vulnerabilities**: While secure, consumer-grade biometric systems may still be susceptible to spoofing attacks, like using high-resolution photos for face recognition or fake fingerprints.
- **Privacy Concerns**: Storing biometric data raises privacy issues and requires careful handling to prevent unauthorized access or data misuse.
- **Complex Setup**: Setting up and maintaining this system requires technical expertise. Issues with software updates or component integration can lead to malfunctions if not properly managed.

5.3 APPLICATIONS:

The integration of dual biometric authentication using fingerprint and face recognition can significantly improve security and convenience in various sectors. Here are some key applications:

- **Vehicle Security**:

Private Vehicles: The system can be implemented in personal cars to prevent theft or unauthorized access. Only authorized users with pre-registered fingerprints and facial data will be able to unlock and start the vehicle.

- **Car Rental Services**: Rental companies can implement this system to streamline vehicle check-in/check-out processes, ensuring that only authorized customers can access and start rental vehicles. This minimizes risks associated with unauthorized usage or theft of rental cars.
- **Ride-sharing and Carpooling**: In car-sharing or ride-sharing scenarios, dual authentication can verify the identity of drivers, ensuring that only authorized individuals can operate the shared vehicle, thereby enhancing trust and safety for both drivers and passengers.
- **Government and Law Enforcement Vehicles**: For police, military, or emergency service vehicles, adding dual biometric authentication ensures that only authorized personnel can access and use the vehicles, protecting sensitive equipment and data inside these vehicles from unauthorized access.
- **Luxury and High-End Vehicles**: Luxury car manufacturers can incorporate this dual authentication system to offer premium security features, adding value for high-end vehicles that are often targeted by thieves due to their value.

- **Corporate and VIP Transport**: High-profile individuals and executives can benefit from this enhanced security system to ensure that only authorized drivers can access and drive their vehicles, offering peace of mind for corporate security.
- **Public Transportation Systems**: Buses, trams, or metro systems could integrate dual authentication to ensure that only certified personnel, such as drivers and conductors, can operate public transport vehicles. This could prevent unauthorized access, improving the safety of public transportation systems.
- **Valet Services**: Dual authentication can provide added security in valet services, where vehicle access is temporarily given to third parties. Only authorized valets could be granted access to move and park vehicles.
- **Automated Parking and Self-Driving Cars**: For autonomous or semi-autonomous vehicles, the system can be used to ensure that only verified users can start or control the vehicle, even when it is in self-driving mode. This can prevent unauthorized individuals from taking control of the vehicle.
- **Industrial and Commercial Vehicles**: Security for commercial or industrial vehicles such as

By integrating dual biometric systems with the Raspberry Pi, this solution provides a versatile and secure option for a wide range of vehicles, enhancing both security and operational control.

5.4 FUTURE SCOPE:

The future scope of a Raspberry Pi-based dual authentication security system for vehicles is promising, especially as biometric and embedded technologies continue to evolve. With advancements in Raspberry Pi processing power and more sophisticated machine learning algorithms, future versions of this system could achieve faster and more accurate authentication, making it feasible for broader adoption in real-world scenarios. Integrating AI-driven algorithms could also enhance biometric accuracy, improving the system's resilience against environmental factors such as lighting or fingerprint condition.

Further, this security system could integrate with IoT networks, enabling remote monitoring and control through smartphones or cloud platforms. For instance, vehicle owners could receive real-time alerts if an unauthorized access attempt is detected and potentially disable the vehicle remotely. Additionally, the system could incorporate GPS for location tracking and expand to include multi-factor authentication by integrating voice recognition or PIN entry as a backup. With these enhancements, the Raspberry Pi-based dual authentication system has the potential to become a comprehensive, accessible, and customizable security solution in the automotive industry.

CONCLUSION: In conclusion, a Raspberry Pi-based dual authentication system for vehicle security offers a robust and innovative approach to protecting vehicles through the combined use of fingerprint and face recognition. This dual-layer biometric method strengthens security, making it much harder for unauthorized individuals to gain access while providing a convenient, user-friendly experience for vehicle owners. By leveraging affordable hardware and open-source technologies, this system provides an accessible and scalable alternative to traditional security measures.

As technology advances, this system has the potential to become even more efficient and versatile. Future integration with IoT and AI capabilities can further enhance its security features and adaptability, positioning it as a viable option for secure, smart vehicles. Overall, this dual authentication system serves as a forward-thinking solution, addressing current security needs while remaining flexible for future innovations in the field of vehicle security.

References

[1]. Sadagopan, Vinoth Kumar, Upendran Rajendran, and Albert Joe Francis authored the paper titled "Design of an Anti-theft Control System Using Embedded Systems," which was presented at the 2011 IEEE International Conference on Vehicular Electronics and Safety.

[2]. Pawar, M.R., and Rizvi, I. (2018). "Development of an IoT-Based Embedded System for Vehicle Security and Driver Monitoring." In Proceedings of the Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE.

[3]. Manjunath, T. K., Andrews SamrajMaheswari, and Chidaravalli Sharmila authored a paper titled "Locking and Unlocking of Theft Vehicles Using CAN," which was presented at the 2013 International Conference on Green High Performance Computing.

[4]. Mukhopadhyay, D., et al. (2018). "Exploring the Development of an IoT-Driven Approach for Vehicle Security." In Proceedings of the 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) (pp. 1 6). IEEE.

[5]. Ramadan, M. N., Al-Khedher, M. A., and Al Kheder, S. A. published a paper titled "Intelligent vehicle security and tracking system" in the International Journal of Machine Learning and Computing in 2012 (Volume 2, Issue 1).

[6]. Jesudoss, A., Vybhavi, R., & Anusha, B. (2019). "Smart Helmet Design for Accident Avoidance." In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE.

[7]. S. Ajaz, M. Asim, M. Ozair, M. Ahmed, M. Siddiqui, and Z. Mushtaq presented a paper titled "Autonomous Vehicle Monitoring Tracking System" at SCONEST 2005, which was published in the conference proceedings spanning pages 1-4 in 2005.

[8]. Joseph A. O'Sullivan and Robert Pless contributed to the article titled "Advances in Security Technologies: Detection, and Target Imaging, and Anomaly Biometric Recognition," which was published in the International Volume of the Microwave Symposium IEEE/MTT-S in 2007.