

BIOMETRIC FINGER PRINT -VEHICLE ACCESS SYSTEM

Mr. A. Vinothkumar¹, Karthikeyan M², Kiruthik S³, Abibulla S⁴, Karthik V⁵

¹Assistant Professor, Department of Electrical and Electronics Engineering, P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India.

^{2,3,4,5}UG Student, Department of Electrical and Electronics Engineering, P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India.

DOI: <https://www.doi.org/10.58257/IJPREMS39133>

ABSTRACT

This technology is used to prevent unauthorized access to the vehicle and ensure that only the authorized driver can start the vehicle. Biometric authentication for vehicle ignition has the potential to increase the security of the vehicle and prevent theft. Traditional security systems such as mechanical locks and key based ignition systems are prone to breaches. Biometric fingerprint identification system integrated with a microcontroller for secure vehicle access. The proposed system enhances security by using a fingerprint sensor to authenticate the driver. The system is designed to capture, process and store fingerprint data. Which is then compared with stored templates for verification. After successful authentication the microcontroller grants access by unlocking the vehicle or enabling ignition. If an unauthorized user attempts access the system triggers an alert. The hardware implementation includes a fingerprint sensor, microcontroller, LCD display, relay module and power supply unit. The software is designed to process fingerprint and images. Extract unique features and match them against stored templates using an efficient algorithm. The system ensures high accuracy and fast response time while maintaining a user friendly interface. Then system can be enhanced by integrating IoT based remote monitoring allowing vehicle owners access logs receive security alerts in real time.

1. INTRODUCTION

Vehicle security has become a critical concern in recent years due to the increasing number of vehicle thefts and unauthorized access incidents.

To address these challenges biometric authentication has emerged as a highly secure and user friendly alternative for vehicle access control. Among various biometric techniques fingerprint recognition stands out as one of the most reliable & cost effective and widely adopted methods for identity verification. The system replaces traditional keys and passwords with a fingerprint authentication mechanism ensuring that only authorized individuals can unlock or start the vehicle. The use of fingerprint identification significantly enhances security by eliminating the risk of stolen or lost keys making it a more reliable and convenient solution for vehicle owners. Unlike passwords or key fobs which can be shared or duplicated fingerprints are unique to each individual and cannot be easily replicated thereby adding an extra layer of security. The system operates by capturing the fingerprint of the user through a biometric sensor. The unregistered fingerprint is detected the system denies access and can trigger additional security measures, such as an alarm or sending an alert to the vehicle owner by photos.

The core hardware components of the system include a fingerprint sensor, microcontroller, LCD display, relay module and power supply unit. The microcontroller acts as the central processing unit handling authentication decision making and control functions. The system is programmed to provide quick response times and high accuracy to ensure seamless user experience. The monitoring of access logs & real time notifications to vehicle owners.

2. PROBLEM DEFINITION

Vehicle security remains a major challenge due to the increasing cases of theft and unauthorized access. Traditional security mechanisms such as mechanical locks & key based ignition systems. If an even electronic key fobs are susceptible to duplication, hacking and unauthorized user.

Lost or stolen keys and forgotten passwords further compromise vehicle security making it easier for criminals to gain access. Existing security systems also lack a personalized authentication mechanism that ensures only authorized individuals can operate the vehicle. To address these issues a biometric fingerprint identification system integrated with a microcontroller based vehicle access system is proposed.

This system replaces conventional keys and passwords with fingerprint authentication ensuring that only registered users can unlock and start the vehicle. Fingerprints are unique to each individual and cannot be easily duplicated making this system a more secure reliable user friendly. It eliminates risks associated with lost keys stolen passwords or cloned access cards. It provides fast, efficient and contactless authentication reducing the chances of security breaches while offering convenience to vehicle owners. The system can also be enhanced with security alerts, alarms and remote

monitoring capabilities for real time protection. By addressing these challenges, the proposed biometric fingerprint vehicle access system provides a more effective and modern security solution, reducing theft risks and improving the overall safety of vehicles.

3. BLOCK DIAGRAM

The ESP32 microcontroller acts as the central controller, interfacing with multiple components. A fingerprint sensor is used for authentication. When a user places their finger on the sensor the ESP32 processes the input. If authentication is successful, the motor driver is activated which in turn powers the motor for the desired operation (e.g. unlocking a door). The system also includes an LCD display which provides user feedback and a buzzer. The gives auditory alerts for different system states. An ESP32 CAM module is integrated to capture images or monitor access. A separate switch is connected to ESP32 for additional manual control. Overall the circuit ensures secure access control using biometric authentication while providing real time feedback via display, buzzer and camera, making it suitable for smart security systems & automated locks or controlled motor operations.

The Joystick controlled ESP32 system, which is powered by a battery. The battery supplies energy to a power backup unit ensuring a stable power source for uninterrupted operation. A switch is included in the circuit to control power flow to the ESP32 microcontroller allowing the system to be turned on or off as needed. The joystick is directly connected to the ESP32 acting as an input device for controlling various applications. In operation, the joystick provides directional input, which is processed by the ESP32 to execute corresponding actions, such as controlling a robotic vehicle, adjusting servo motors or navigating a graphical interface. This setup is ideal for robotics, remote controlled systems or interactive projects, where a joystick serves as a simple yet effective control mechanism.

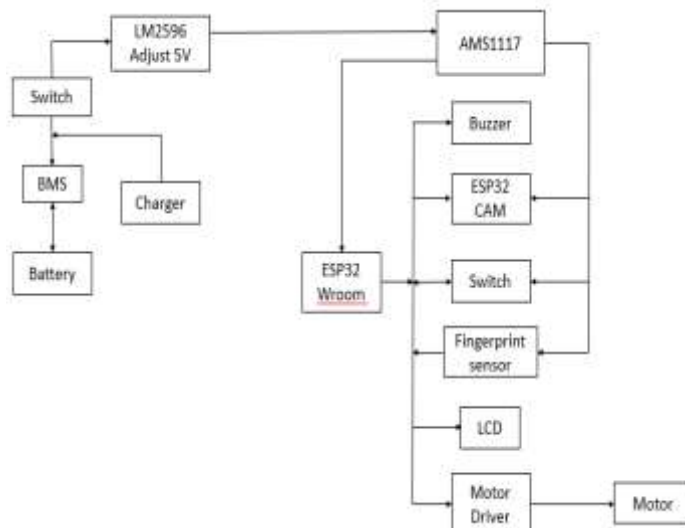


Figure.1 Block Diagram (RX)

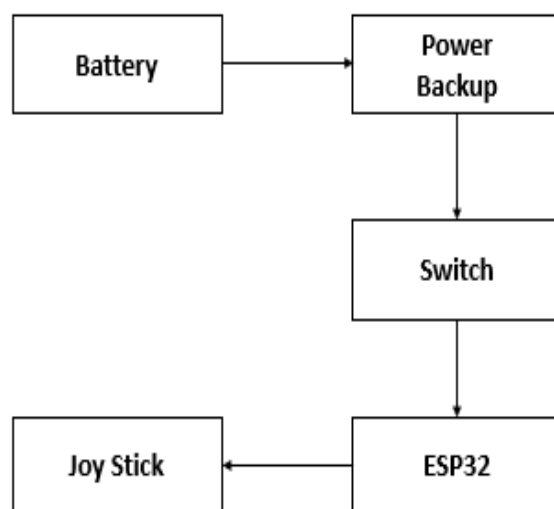


Figure 2: Block Diagram (TX)

SIMULATION DIAGRAM

MODEL 1 (RECEIVER)

Power is supplied via a 12V battery, regulated by a buck converter (LM2596) to ensure proper voltage levels. It communicates via UART (TX, RX) with the fingerprint sensor and I2C (SDA, SCL) with other peripherals such as an LCD display. The working process of the receiver begins when the fingerprint sensor scans a user's fingerprint and transmits the data to the ESP32. If verified the receiver sends a signal to the motor driver, allowing the vehicle to start. If authentication fails, access remains restricted. The receiver can also send data wirelessly via Wifi or Bluetooth to app enabling remote control and monitoring. This functionality enhances security and convenience by eliminating traditional keys, reducing theft risks and providing easy access management. The integration of wireless connectivity further enhances its usability making the fingerprint-based car system a secure and efficient solution for vehicle access.

A transmitter in a fingerprint based vehicle system functions as the input device responsible for capturing

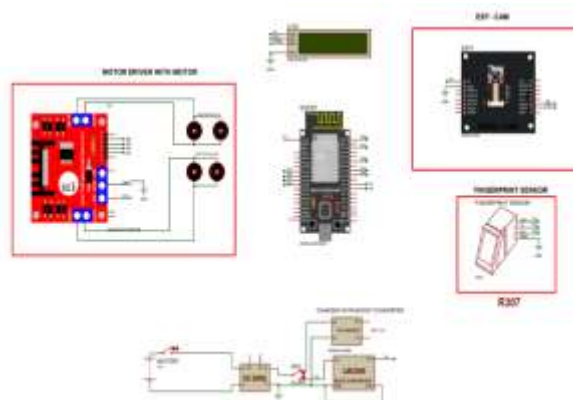


Figure.3 Block Diagram (TX)

MODEL 2 (TRANSMITTER)

authentication data and sending it to the receiver for verification. The transmitter typically an ESP32 module is connected to a fingerprint sensor that scans the user's fingerprint and transmits the data. It plays a critical role in ensuring that biometric authentication is successfully communicated to the receiver for processing. The transmitter consists of key components such as the ESP32 module that handles data transmission and the wireless communication interfaces including Wifi Bluetooth for seamless connectivity with the receiver. the system is powered by a 3.7V battery a is managed by an IP5306 power management module to ensure stable power supply. If using a wireless system the data is sent over Wifi or Bluetooth allowing remote authentication. Once the receiver processes the fingerprint data & decides to grant or deny access. The transmitter is crucial in maintaining a secure authentication process as it ensures that fingerprint data is transmitted reliably and efficiently. The integration of wireless communication allows for remote authentication adding both security and convenience. fingerprint based authentication system. the transmitter eliminates the need for traditional vehicle key reducing the risk of unauthorized access and enhancing the overall security of the vehicle.

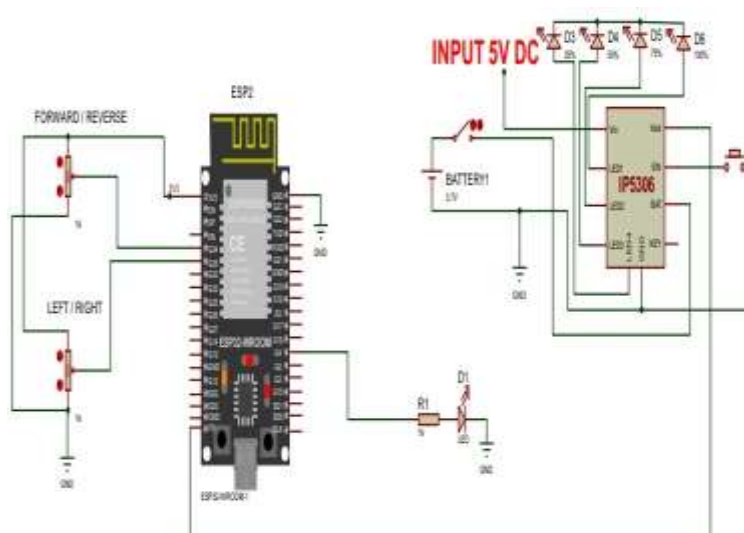


Figure.4 Block Diagram (RX)

4. RESULT AND DISCUSSION

Thus the biometric fingerprint identification system with a microcontroller based vehicle access system enhances security by allowing only authorized users to unlock and start a vehicle. The system consists of a microcontroller (ESP32) a fingerprint sensor (R307) a relay module for ignition control an LCD for feedback and optional security features like a buzzer and photos to google drive. The process involves enrolling fingerprints, storing them in EEPROM and authenticating users by matching scanned fingerprints with stored data. If a match is found then microcontroller activates the relay unlocking the vehicle was access to start. Additional features such a for alerts, Wifii for remote access and time based restrictions can be implemented. This system enhances vehicle security, prevents unauthorized access and provides a reliable, user friendly alternative to traditional keys.

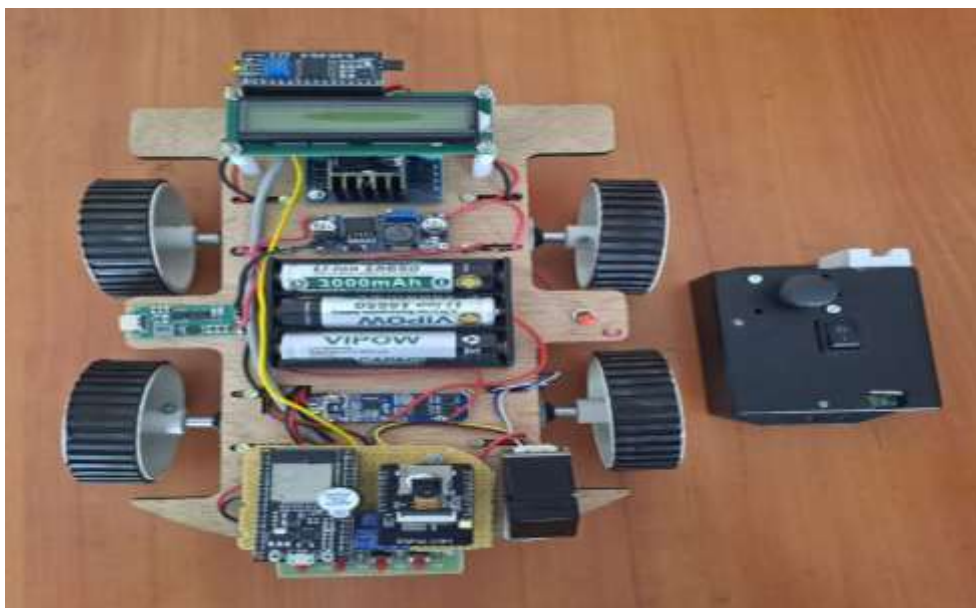


Figure.5 Hardware model of biometric finger print - vehicle access system

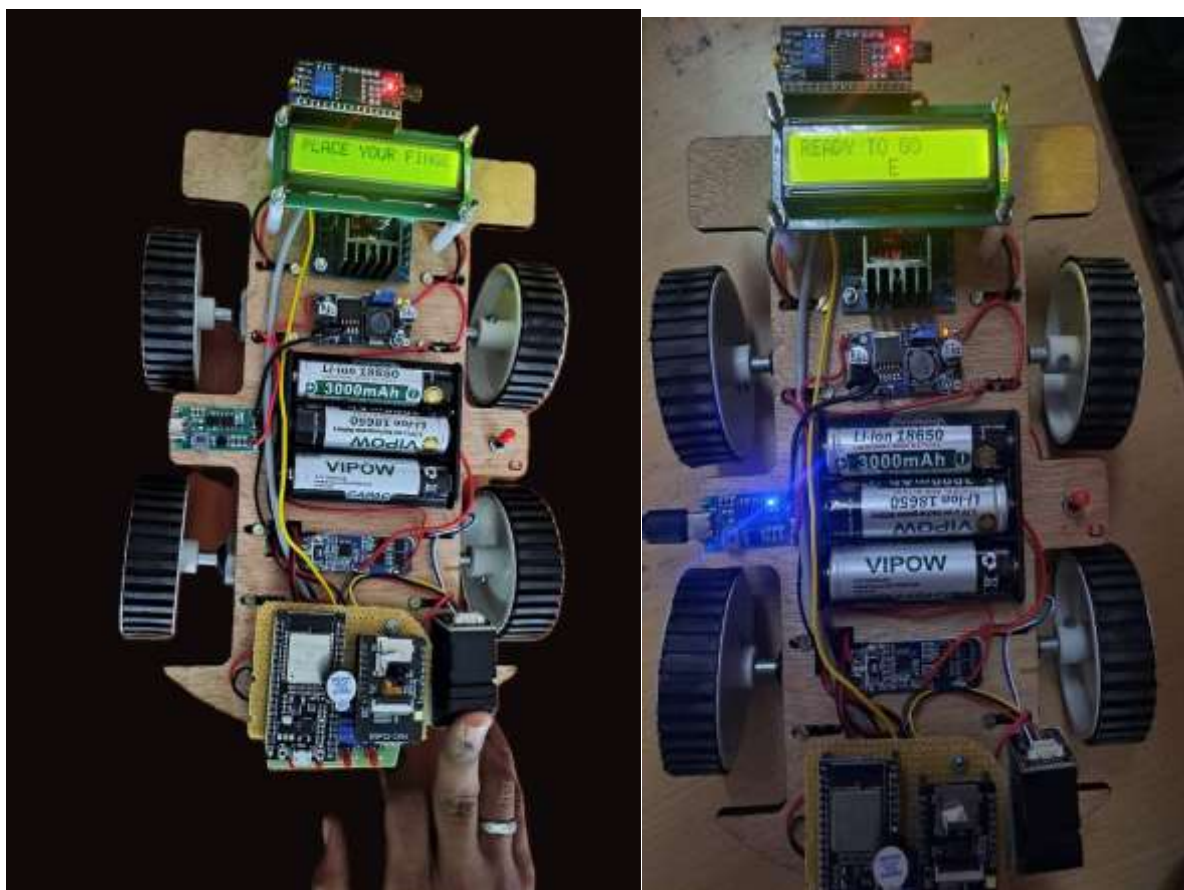


Figure 6: fingerprint enroll

Figure 7: output of drive vehicle



Figure 8: output from camera to drive

5. CONCLUSION

The thesis demonstrates the biometric fingerprint identification system with a microcontroller based vehicle access system enhances security by ensuring only authorized users can start the vehicle. By replacing traditional keys with fingerprint authentication. It eliminates risks associated with lost or stolen keys. The ESP32 microcontroller processes fingerprint data efficiently enabling quick and secure access. Additional features like a buzzer and camera improve security. As vehicle security concerns grow this system provides a reliable & modern solution that could become a standard feature in smart and secure transportation.

6. REFERENCES

- [1] Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, 31(1), 28-48.
- [2] Bhatt, B., Kalani, P., Parmar, N., & Shingala, N. (2015). Smart Vehicle Security System Using GSM & GPS. *International Journal of Engineering and Computer Science*, 4(6), 12508-12511.
- [3] Karthikeyan, A., & Sowndharya, J. (2012). Fingerprint based ignition system. *International Journal Of Computational Engineering Research*, 2(2), 236-243.
- [4] Kiruthiga, N., & Thangasamy, S. (2015). Real time biometrics based vehicle security system with GPS and GSM technology. *Procedia Computer Science*, 47, 471-479.
- [5] Kulkarni, V., & Narsimhulu, G. A low cost extendable embedded smart car security system on face detection and continuous video monitoring system. *IJCCT& IJESAT*, ISSN, 2250-3676.
- [6] Mandalapu, H., PN, A. R., Ramachandra, R., Rao, K. S., Mitra, P., Prasanna, S. M., & Busch, C. (2021). Audio-visual biometric recognition and presentation attack detection: A comprehensive survey. *IEEE Access*, 9, 37431-37455.
- [7] Manikandan, K. M. V. R. K. S. N., Manikandan, K., Vishnu, K. E., Raja, R. T., Kanthaboopathi, K., & Senthilnathan, T. (2018). Biometric vehicle security system and pollution monitoring. *FUEL*, 5(01).
- [8] Omidiora, E. O., Fakolujo, O. A., Arulogun, O. T., & Aborisade, D. O. (2011). "A Prototype of a Fingerprint Based Ignition Systems in Vehicles" Published in *European Journal of Scientific Research* ISSN 1450-216X Vol.62 No.2 (2011)
- [9] Potluri, S., & Rao, K. S. (2017). Quality of service based task scheduling algorithms in cloud computing. *International Journal of Electrical and Computer Engineering*, 7(2), 1088.
- [10] Prashantkumar, R., Sagar, V. C., Santosh, S. 2., & Nambiar, S. (2013). Two wheeler vehicle security system. *International Journal of Engineering Sciences & Emerging Technologies*, 6(3), 324-334.
- [11] Priya, P., Singh, S., Mhalan, A., & Yadav, G. S. (2013). VEHICLE THEFT ALERT SYSTEM USING GSM. *International Journal of Engineering Science and Technology*, 5(5), 1070.

-
- [12] Ramadan, M. N., Al-Khedher, M. A., & Al-Kheder, S. A. (2012). Intelligent anti-theft and tracking system for automobiles. *International Journal of Machine Learning and Computing*, 2(1), 83.
 - [13] Sehgal, V. K., Singhal, M., Mangla, B., Singh, S., & Kulshrestha, S. (2012, July). An embedded interface for GSM based car security system. In *2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks* (pp. 9-13). IEEE.
 - [14] Singh, P. K., Sangwan, O. P., Singh, A. P., & Pratap, A. (2015). A framework for assessing the software reusability using fuzzy logic approach for aspect oriented software. *International Journal of Information Technology and Computer Science*, 7(2), 12-20.
 - [15] Wang, J., Xu, H., Hou, X., Du, C., & Zhou, Q. (2021). A moment-of-inertia-driven engine start-up strategy for four-wheel-drive hybrid electric vehicles. *IEEE Transactions on Transportation Electrification*, 8(3), 3320-3335.
 - [16] Yu, S., Li, L., Dong, G., & Zhang, X. (2006, December). A study of control strategies of PFI engine during cranking and start for HEVs. In *2006 IEEE International Conference on Vehicular Electronics and Safety* (pp. 68-72). IEEE.