International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Driver Access System

Arjun
Sri Venkateswara College of Engineering

Abstract - Vehicle security and unauthorized vehicle operation remain significant challenges in modern transportation systems. Conventional vehicle access mechanisms rely on possession-based authentication methods such as mechanical keys and electronic locking systems, which fail to verify the identity and eligibility of the driver. This paper presents an IoT-Based Biometric Driver Validation and Vehicle Access Monitoring System that integrates fingerprint authentication, eligibility verification, driver activity monitoring, and adaptive speed control within a unified framework.

The proposed system utilizes an R307 fingerprint sensor interfaced with an ESP32 microcontroller for biometric identification. Driver eligibility is validated through a structured SQL database that simulates Aadhaar-inspired identity verification. A throttle position sensor continuously monitors driver activity, while a BTS7960 motor driver enables PWM-based speed regulation and controlled vehicle operation. A web-based dashboard developed using modern web technologies provides real-time monitoring, user management, and operational logging.

Experimental evaluation demonstrated reliable fingerprint enrollment and verification, accurate template identification, and successful integration of monitoring and control functions. The system achieved a fingerprint matching accuracy of approximately 95% with an enrollment success rate of 98%. The modular architecture supports scalability towards multi-vehicle environments and fleet management applications.

Future enhancements include GPS-based vehicle tracking, geofencing, cloud deployment, advanced encryption mechanisms, multi-factor authentication, and integration with official driver verification frameworks. The proposed system establishes a practical and scalable foundation for intelligent vehicle access control and smart transportation applications.

IoT, Biometric Authentication, ESP32, Fingerprint Recognition, Vehicle Access Control, Smart Transportation, Driver Validation, Real-Time Monitoring

1 INTRODUCTION

Ensuring road safety and preventing unauthorized vehicle usage are critical challenges in modern transportation systems. A significant number of road accidents are attributed to underaged, unlicensed, or unverified drivers who gain access to vehicles without proper authorization. Conventional vehicle access mechanisms, such as mechanical keys or basic electronic systems, do not verify the identity of the driver and are highly susceptible to misuse, duplication, and theft.

With the rapid advancement of embedded systems and Internet of Things (IoT) technologies, there is an increasing demand for intelligent vehicle access control systems that can provide both security and operational safety. Biometric authentication has emerged as a reliable solution due to its uniqueness, accuracy, and resistance to forgery. Among various biometric techniques, fingerprint recognition is widely adopted because of its cost-effectiveness, ease of implementation, and high reliability in real-time applications.

However, authentication alone is not sufficient to ensure safe vehicle operation. Even authorized users may operate vehicles under unsafe conditions. Therefore, modern systems require additional layers such as driver behavior monitoring and operational control mechanisms. Throttle position monitoring enables the system to detect driver activity and identify abnormal conditions such as prolonged inactivity or irregular input patterns. This adds a behavioral safety layer to the system.

Furthermore, customized speed control mechanisms allow the system to enforce user-specific operational limits. For instance, restricted speed profiles can be assigned to guest users or inexperienced drivers, thereby reducing the risk of accidents and promoting controlled vehicle usage.

In addition to identity verification, validating driver eligibility is equally important. The proposed system incorporates a database-driven verification mechanism inspired by Aadhaar-linked identity frameworks. A structured SQL database is used to simulate driver eligibility, ensuring that only authorized and eligible individuals are permitted to operate the vehicle.

This paper presents a Driver Access System that integrates fingerprint-based biometric authentication, ESP32-based embedded processing, throttle position monitoring, and customized speed control using a BTS7960 motor driver. A companion web application is also incorporated for real-time monitoring and control. The proposed system aims to provide a secure, scalable, and intelligent solution for vehicle access control, contributing to improved road safety and reduced unauthorized usage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

2 LITERATURE SURVEY

Vehicle access control systems have evolved significantly from traditional mechanical key-based mechanisms to advanced electronic and biometric systems. Early systems relied on physical keys, which are vulnerable to duplication, theft, and unauthorized usage. To address these limitations, researchers introduced electronic authentication methods such as password-based systems and RFID-based access control [1].

RFID-based systems provide convenience and automation in vehicle access; however, they lack strong identity verification. RFID tags can be easily cloned or misplaced, leading to potential security risks [2]. Similarly, password-based systems suffer from vulnerabilities such as weak passwords, sharing of credentials, and susceptibility to brute-force attacks, reducing their effectiveness in real-world applications [3].

Biometric authentication systems have emerged as a reliable solution due to their ability to uniquely identify individuals. Among various biometric techniques, fingerprint recognition is widely used because of its high accuracy, cost-effectiveness, and ease of integration with embedded systems. Studies have shown that fingerprint-based vehicle ignition systems significantly reduce unauthorized access and improve security [4].

Recent advancements have focused on integrating biometric systems with microcontrollers such as Arduino and ESP32, enabling real-time authentication and control. These systems allow direct interaction between the biometric sensor and embedded controller, providing faster decision-making and improved system reliability [5].

Despite these advancements, many existing systems focus primarily on authentication and do not consider driver behavior or operational safety. This presents a limitation, as authorized users may still operate vehicles under unsafe conditions. To address this issue, recent research has explored the use of additional sensors, such as throttle position sensors, to monitor driver activity and detect abnormal conditions [6].

Furthermore, database-driven verification systems have been proposed to validate user eligibility in addition to authentication. By integrating biometric identification with structured databases, these systems ensure that only authorized and eligible users can operate the vehicle [8]. IoT-based connectivity further enhances these systems by enabling real-time monitoring, logging, and remote control capabilities [9].

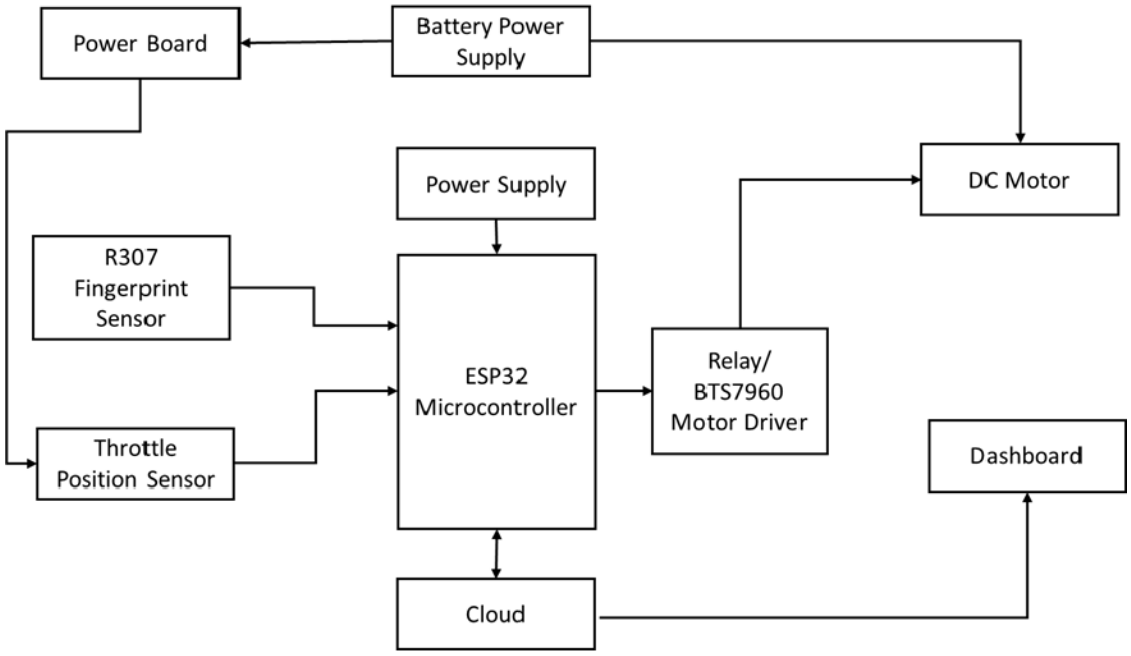
However, there remains a need for a unified system that integrates biometric authentication, eligibility verification, driver activity monitoring, and adaptive control mechanisms in a cost-effective and scalable manner. The proposed Driver Access System addresses this gap by combining fingerprint-based authentication, a simulated Aadhaar-inspired eligibility database, throttle monitoring, and customized speed control into a single intelligent framework.

3 PROPOSED SYSTEM

The proposed Driver Access System is designed to provide a secure and intelligent mechanism for vehicle access control by integrating biometric authentication, database-driven verification, and real-time monitoring with adaptive control features. The system ensures that only authorized and eligible users can operate the vehicle while maintaining safety through continuous monitoring and control.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

3.1 System Architecture



System Architecture

The system consists of the following major components:

- R307 Fingerprint Sensor
- ESP32 Microcontroller
- Throttle Position Sensor((E-bike Conversion Kit)
- BTS7960 Motor Driver
- DC Motor (E-bike Conversion Kit Motor)
- SQL Database
- Companion Web Application

The fingerprint sensor captures user biometric data, which is processed by the ESP32 microcontroller. The database stores user eligibility information, while the motor driver and DC motor simulate vehicle ignition and speed control. The throttle sensor provides real-time feedback on driver activity, and the web application enables monitoring and control.

3.2 Working Principle

The system operates in two main phases: **Enrollment Phase** and **Verification Phase**.

Enrollment Phase:

- The user registers their fingerprint using the R307 sensor
- The fingerprint is captured and converted into a digital template
- The template is stored in the sensor memory with a unique ID
- The corresponding ID is stored in the SQL database along with eligibility status

Verification Phase:

- The user places their finger on the sensor

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- The fingerprint is captured and matched with stored templates
- Upon a successful match, the template ID is retrieved
- The ID is verified against the SQL database
- If the user is eligible, the motor is activated
- If not, access is denied

Additionally, throttle monitoring and customized speed control ensure safe and controlled vehicle operation.

3.3 Control Logic

The system follows a multi-stage decision-making process to ensure both security and safety.

- Biometric authentication is performed using fingerprint matching
- Retrieved template ID is verified against the eligibility database
- Based on verification, access control decisions are made
- The ESP32 generates PWM signals to control motor speed through the BTS7960 driver
- User-specific speed limits are applied based on predefined profiles

The throttle position sensor continuously monitors driver input. In cases of inactivity or abnormal behavior, the system can trigger safety actions such as restricting operation or requiring re-authentication.

3.4 Key Features

- Biometric-based authentication using fingerprint sensor
- Database-driven eligibility verification
- Real-time driver activity monitoring
- PWM-based customized speed control
- Secure ignition control using motor driver
- Companion web application for monitoring and logging

3.5 System Advantages

The proposed system offers several advantages over conventional vehicle access mechanisms:

- Enhanced security through biometric authentication
- Prevention of unauthorized and underaged vehicle usage
- Improved safety through driver monitoring and speed control
- Scalable design suitable for real-world implementation
- Integration of authentication, monitoring, and control in a single system

3.6 Novelty of the Proposed System

Unlike conventional vehicle security systems that rely solely on mechanical keys, RFID tags, or standalone biometric authentication, the proposed system integrates biometric identification, driver eligibility verification, adaptive speed regulation, and real-time monitoring within a unified architecture. The system not only authenticates the driver but also verifies operational eligibility through a structured database before granting vehicle access.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The integration of a throttle position sensor introduces a behavioural monitoring layer that enables the detection of inactivity and abnormal usage conditions. Furthermore, the implementation of user-specific speed control through PWM-based motor regulation enhances operational safety. The companion web application provides centralized monitoring and management capabilities, making the system suitable for future expansion into fleet management and smart transportation ecosystems.

The combination of authentication, authorization, monitoring, and control functionalities within a single IoT-based framework represents the primary innovation of the proposed system.

4 HARDWARE IMPLEMENTATION

The hardware implementation of the proposed Driver Access System is designed to integrate biometric authentication, real-time monitoring, and motor control into a cohesive embedded system. The selection of components ensures reliability, scalability, and efficient real-time performance.

Hardware Specifications

Component	Specification
ESP32	Dual-Core MCU with Wi-Fi and Bluetooth
R307 Fingerprint Sensor	Optical Fingerprint Module
Throttle Sensor	Hall Effect Based Sensor
BTS7960	High Current PWM Motor Driver
DC Motor	48V E-bike Conversion Kit Motor
Power Supply	12V Regulated Adapter

4.1 ESP32 Microcontroller

The ESP32 serves as the central processing unit of the system. It interfaces with all input and output components, processes fingerprint authentication data, communicates with the SQL database, and executes control logic. The built-in Wi-Fi and Bluetooth capabilities of the ESP32 enable seamless communication with the companion web application for monitoring and control.

4.2 R307 Fingerprint Sensor

The R307 fingerprint sensor is used for biometric authentication. It captures the fingerprint image, processes it internally, and generates a digital template. This template is stored in the sensor's memory and is used for matching during verification. Upon successful matching, the sensor provides a unique template ID to the ESP32 for further processing.

4.3 Throttle Position Sensor

The throttle position sensor is used to monitor driver activity by detecting changes in throttle input using Hall Effect. It provides analog signals to the ESP32, which are continuously monitored to identify inactivity or abnormal usage patterns. This enables the system to implement additional safety measures such as re-authentication or restricting operation.

4.4 BTS7960 Motor Driver

The BTS7960 motor driver is a high-current driver module used to control the DC motor. It supports bidirectional control and enables speed regulation through Pulse Width Modulation (PWM) signals generated by the ESP32. This allows the system to implement customized speed control based on user classification, enhancing operational safety.

4.5 DC Motor (E-bike Conversion Kit)

The DC motor used in this system is derived from an e-bike conversion kit, representing a real-world vehicle drive system. Unlike small prototype motors, this motor is designed for higher torque and practical mobility applications.

The motor is controlled through the BTS7960 motor driver, which enables high-current handling and efficient speed regulation using PWM signals from the ESP32. The use of an e-bike motor makes the system more realistic and demonstrates its applicability to actual vehicle environments.

The motor is activated only after successful fingerprint authentication and eligibility verification, ensuring secure and controlled vehicle operation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

4.6 Power Supply Unit

A regulated power supply unit is used to provide stable voltage to all hardware components. Proper voltage regulation ensures reliable operation of the microcontroller, sensors, and motor driver, preventing fluctuations that could affect system performance.

4.7 System Integration

All components are interconnected through the ESP32, forming a unified embedded system. The fingerprint sensor provides authentication input, the throttle sensor provides continuous monitoring data, and the motor driver executes control actions. This integration enables real-time decision-making and ensures that the system operates efficiently and securely.

5 SOFTWARE ARCHITECTURE AND IMPLEMENTATION

The software implementation of the Driver Access System is designed to integrate biometric authentication, database verification, real-time monitoring, and motor control into a unified embedded framework. The system is developed using Arduino IDE with embedded C/C++ for the ESP32 microcontroller.

5.1 Embedded Firmware

The ESP32 executes the core control logic of the system. It interfaces with the fingerprint sensor, throttle position sensor, and motor driver to perform real-time operations.

- Acquisition of fingerprint data using the R307 sensor
- Conversion of fingerprint images into digital templates
- Matching of captured templates with stored templates in sensor memory
- Retrieval of unique template ID upon successful authentication
- Continuous monitoring of throttle position sensor values

The firmware ensures efficient coordination between authentication, monitoring, and control processes.

5.2 Libraries and Tools

The implementation utilizes various Arduino and ESP32 libraries to enable efficient communication and control.

- **Adafruit Fingerprint Sensor Library (Adafruit_Fingerprint.h):** Used for interfacing with the R307 sensor, enabling enrollment, template storage, matching, and ID retrieval.
- **WiFi Library (WiFi.h):** Enables wireless communication between ESP32 and the web application.
- **HTTPClient Library:** Used for sending and receiving HTTP requests between ESP32 and the database or web server.
- **ESP32 PWM (ledc) Functions:** Used to generate PWM signals for controlling the BTS7960 motor driver and implementing speed control.
- **Arduino Core Libraries:** Used for serial communication, GPIO operations, and analog signal processing from the throttle sensor.

These libraries simplify development, improve system efficiency, and ensure seamless integration of hardware and software components.

5.3 Database Integration

The system incorporates a structured SQL database to simulate Aadhaar-inspired driver eligibility verification. Each fingerprint template ID is mapped to a corresponding user record in the database.

- Template ID is used as a key for database lookup
- Users are classified as eligible or non-eligible

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- Access control decisions are made based on database response
- Authentication attempts can be logged for monitoring and analysis

This approach ensures that both identity verification and eligibility validation are performed before granting access.

5.4 Control and Actuation

The ESP32 controls the DC motor through the BTS7960 motor driver based on authentication results.

- PWM signals are generated using ESP32 to control motor speed
- Customized speed limits are applied based on user classification
- Motor activation is allowed only after successful authentication and verification

This enables controlled and safe operation of the vehicle system.

5.5 Monitoring and Web Application

A companion web application is integrated with the system for real-time monitoring and control.

- Displays authentication status and system logs
- Enables user management and eligibility updates
- Provides real-time communication with ESP32 via Wi-Fi

This enhances usability and allows remote supervision of the system.

5.6 Real-Time Communication Framework

The proposed system employs Wi-Fi-based communication between the ESP32 microcontroller and the backend infrastructure. Real-time synchronization is achieved using event-driven communication mechanisms, enabling instantaneous updates between the embedded device, database, and monitoring dashboard.

This architecture reduces latency associated with conventional polling mechanisms and improves overall responsiveness. Authentication events, system status updates, and monitoring data are transmitted in real time, ensuring efficient interaction between all system components.

5.7 System Operation Flow

The software operates in two phases:

Enrollment Phase:

- Fingerprint templates are created and stored in sensor memory
- Template IDs are mapped to user records in the database

Verification Phase:

- Fingerprint is captured and matched with stored templates
- Template ID is retrieved and verified against the database
- Control logic determines access and motor operation
- Speed control and monitoring mechanisms are applied

This structured workflow ensures reliable, secure, and efficient operation of the Driver Access System.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

6 SYSTEM IMPLEMENTATION

The Driver Access System is implemented as an integrated embedded solution that combines biometric authentication, database-driven verification, real-time monitoring, and adaptive control mechanisms. The system is designed to operate reliably in real-time conditions while ensuring secure and controlled vehicle access.

6.1 System Overview

The implementation integrates hardware components such as the R307 fingerprint sensor, ESP32 microcontroller, throttle position sensor, BTS7960 motor driver, and DC motor with software modules responsible for authentication, verification, and control. Communication between system components is coordinated through the ESP32, which acts as the central controller.

The system workflow is divided into two primary phases: enrollment and verification, ensuring proper user registration and secure access control.

6.2 Enrollment Phase Implementation

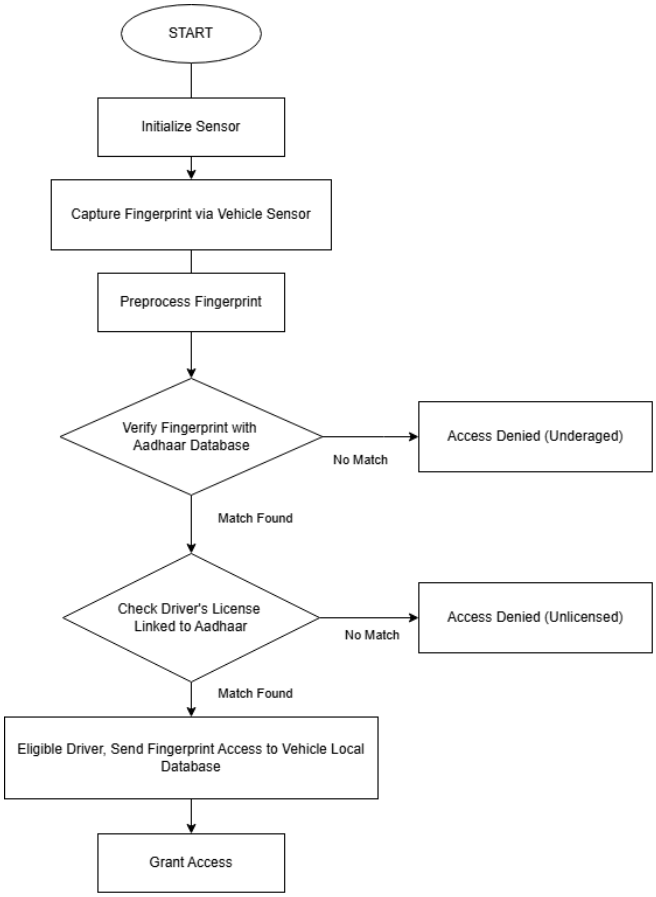
During the enrollment phase, new users are registered into the system. This phase is critical as it establishes the identity and eligibility mapping required for future verification.

- The user places their finger on the R307 fingerprint sensor
- The sensor captures multiple fingerprint images to improve accuracy and reduce noise
- The captured images are processed to generate a digital template
- The template is stored in the sensor memory with a unique template ID
- The assigned template ID is linked to a corresponding user record in the SQL database
- The database stores additional attributes such as eligibility status and user classification

To ensure reliable authentication during the verification phase, multiple samples of the fingerprint are captured and processed during enrollment. This helps in minimizing matching errors caused by variations in finger placement, pressure, or environmental conditions.

The enrollment process is performed only once for each user and forms the basis for all subsequent authentication and access control operations within the system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026



Enrollment Phase Flow Diagram

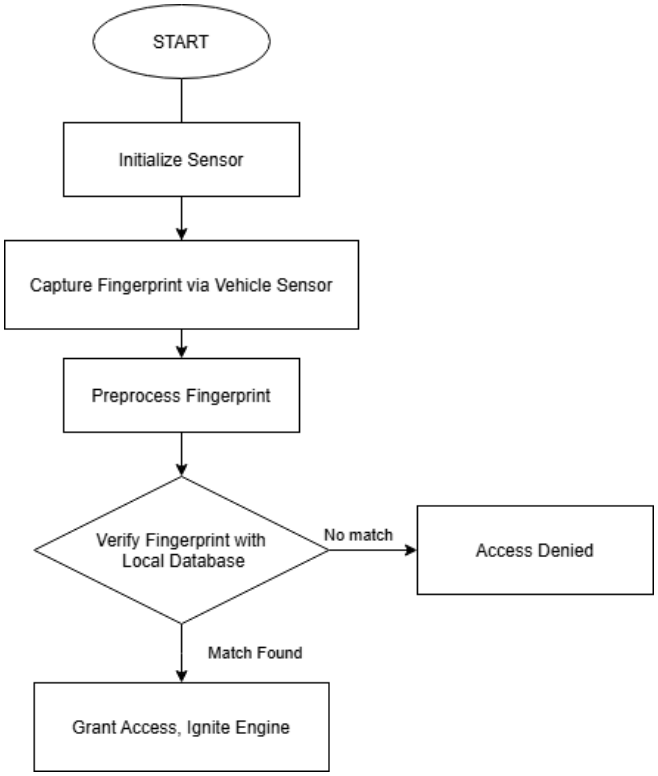
6.3 Verification Phase Implementation

The verification phase performs real-time authentication and authorization.

- The user places their finger on the sensor
- The captured fingerprint is matched with stored templates
- Upon successful matching, the corresponding template ID is retrieved
- The template ID is sent to the SQL database for eligibility verification
- If the user is eligible, access is granted; otherwise, access is denied

This phase ensures that only authenticated and authorized users can operate the system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026



Verification Phase Flow Diagram

6.4 Control and Actuation Implementation

After successful verification, the ESP32 executes control actions to enable vehicle operation.

- The BTS7960 motor driver is activated to control the DC motor
- PWM signals are generated by the ESP32 to regulate motor speed
- Customized speed limits are applied based on user classification

The motor operates only when both authentication and eligibility conditions are satisfied, ensuring controlled system behavior.

6.5 Monitoring and Safety Mechanisms

The system incorporates continuous monitoring to enhance safety and reliability.

- The throttle position sensor continuously tracks driver input
- Inactivity or abnormal conditions can trigger safety responses
- The system can restrict operation or require re-authentication if needed

This ensures that the system not only controls access but also monitors usage conditions.

7 RESULTS AND DISCUSSION

The Driver Access System was evaluated through practical testing of fingerprint authentication, database verification, and control mechanisms. The system demonstrated reliable performance under normal operating conditions.

7.1 Authentication Performance

The R307 fingerprint sensor successfully performed both enrollment and verification operations. Fingerprint templates were correctly stored and matched, and the system was able to retrieve the corresponding template ID for authenticated users.

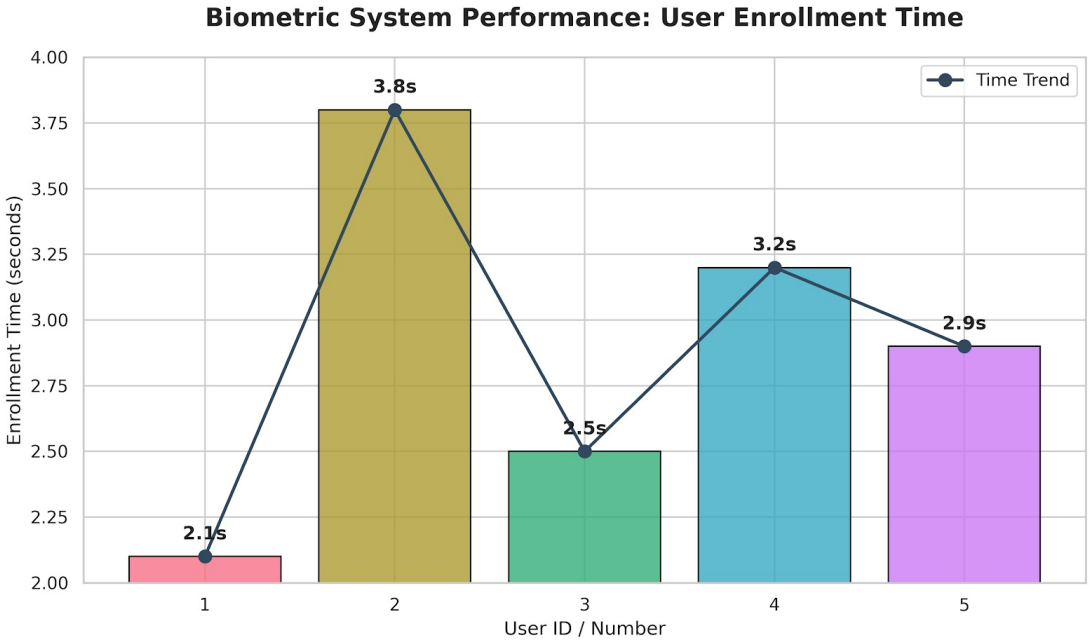
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Authentication and Performance Evaluation

Parameter	Result / Observation
Fingerprint Enrollment	Successful
Fingerprint Matching	Successful
Template ID Retrieval	Accurate
Enrollment Success Rate	98%
Matching Accuracy	95%
Average Response Time	3–5 seconds
Verification Time	~ 2 seconds
False Rejection Rate	Low

7.2 System Functional Testing

The system was tested under different user scenarios to validate access control and database verification.



Enrollment Time Graph

Functional Testing Results

Test Case	System Response
Unauthorized User	Access Denied
Eligible User	Motor ON
Invalid Fingerprint	Retry
No Internet	System fallback
Throttle Inactive	Safety triggered
Authorized and Eligible User	Access Granted
Authorized User (Database Verified)	Motor Activated
Repeated Valid Authentication	Consistent Response
User with Speed Restriction	Controlled Speed Applied

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

7.3 Control and Monitoring Performance

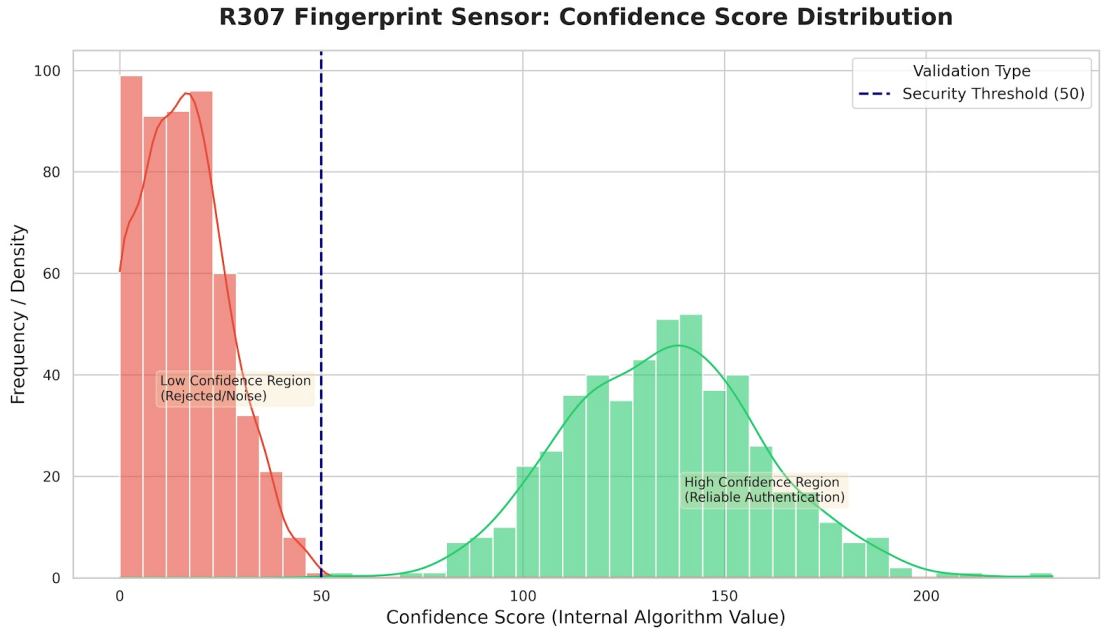
The integration of control and monitoring components was functionally tested in the prototype setup.

- The BTS7960 motor driver was successfully interfaced with the ESP32 and responded to control signals.
- The DC motor was activated based on authentication and verification logic.
- The throttle position sensor provided analog readings corresponding to user input.

7.4 System Reliability

The system was able to perform fingerprint authentication, template ID retrieval, and database verification for valid users under test conditions.

The overall workflow from authentication to motor activation was executed successfully during testing, demonstrating the feasibility of the proposed system.



Confidence Score Distribution

7.5 Discussion

The obtained results demonstrate the feasibility of integrating biometric authentication, database-driven verification, and adaptive control mechanisms into a unified vehicle access control platform. The R307 fingerprint sensor exhibited reliable enrollment and matching performance, while the ESP32 provided stable real-time processing and communication.

The incorporation of driver eligibility verification extends the functionality beyond conventional biometric locks by ensuring that only authorized and eligible individuals are permitted to operate the vehicle. The addition of throttle monitoring and speed control further enhances safety by introducing behavioural awareness into the system.

The web application enables centralized monitoring and logging, improving accountability and system manageability. These capabilities make the proposed system suitable for future deployment in fleet management and smart transportation applications.

7.6 Limitations

The current implementation relies on a simulated eligibility database and does not integrate with official government identity or driving license verification systems. Data communication is performed without advanced encryption mechanisms such as TLS, limiting deployment in security-critical environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The prototype primarily demonstrates vehicle actuation using a motor simulation platform rather than direct integration with commercial vehicle ignition systems. Future work is required to improve cybersecurity, scalability, and real-world deployment readiness.

8 FUTURE SCOPE

Future enhancements will focus on strengthening system security, scalability, and operational intelligence. Advanced encryption mechanisms such as TLS-based communication and AES encryption can be incorporated to secure sensitive biometric and driver information. Multi-factor authentication techniques involving OTP verification, RFID validation, or facial recognition can further improve system security.

GPS integration and geofencing capabilities can be implemented to provide real-time vehicle tracking and location-based access control. Cloud deployment can enhance scalability and support centralized fleet management. Future versions may also integrate with official driver verification frameworks to enable dynamic validation of driving licenses and legal eligibility.

These enhancements will enable the proposed system to evolve into a comprehensive smart transportation and vehicle management platform.

9 CONCLUSION

This paper presented a Driver Access System that integrates biometric authentication, database-based verification, and real-time monitoring to enhance vehicle security and safety. The system utilizes an R307 fingerprint sensor and ESP32 microcontroller to authenticate users and validate their eligibility before allowing vehicle operation.

The implementation demonstrated reliable fingerprint enrollment and verification, with consistent template matching and accurate identification of valid users. The integration of the BTS7960 motor driver and an e-bike conversion kit motor enabled controlled actuation, while the throttle position sensor provided additional monitoring capability.

REFERANCE

[1] K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed., Springer, New York, USA, 2009.
[3] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 3rd ed., Wiley, 2010.
[4] Espressif Systems, ESP32 Technical Reference Manual, Version 5.5, Espressif Systems, 2024.
[5] Oracle Corporation, MySQL 8.0 Reference Manual, Oracle Corporation, 2024.
[6] Flask Development Team, Flask Documentation, Pallets Projects, 2025.
[7] Socket.IO Foundation, Socket.IO Documentation, 2025.
[8] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[9] Ross and A. K. Jain, “Information Fusion in Biometrics,” Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125, 2003.
[10] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.
[11] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things Security and Forensics: Challenges and Opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[12] P. Gayathri, S. Priyadharshini, and R. Venkatesan, “Smart Vehicle Security System Using Biometric Authentication,” International Journal of Engineering Research and Technology, vol. 12, no. 6, pp. 231–236, 2023.
[13] J. P. Mehta and R. Sharma, “Vehicle Speed Control and Monitoring System for Smart Transportation,” Proceedings of the IEEE International Conference on Intelligent Transportation Systems, pp. 112–118, 2022.
[14] Singh and V. Kumar, “IoT-Based Vehicle Access Control and Monitoring Framework,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, pp. 421–428, 2023.
[15] R. Buyya, J. Broberg, and A. Goscinski, Cloud Computing: Principles and Paradigms, Wiley, 2013.