SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

A MULTI-LAYERED VEHICLE AUTHENTICATION SYSTEM USING DRIVING LICENSE, FINGERPRINT, PASSWORD, AND OWNER NOTIFICATIONS

Shreyas K R
USN: 4VM22EE042
Department of Electrical and Electronics Engineering
Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka

ABSTRACT
Vehicle misuse is a significant contributor to accidents, thefts, and disputes over liability. Conventional security methods, such as ignition keys or standalone fingerprint systems, do not guarantee that a licensed and legally eligible person is driving. This paper introduces a conceptual a layered vehicle authentication framework that combines license verification, biometric fingerprint matching, password protection, and instant owner alerts. to the vehicle owner. A re-authentication delay of 20 minutes restricts repeated unauthorized trials. For rental vehicles, an additional DL verification mode is proposed to enhance accountability. Conceptual simulation demonstrates how the framework strengthens security, improves law enforcement verification, reduces accident risks, and enables identification of the driver involved in accidents through secure mobile alerts.
KEYWORDS : *Vehicle Security, Driving License Verification, Biometric Authentication, Multi-Factor Security, Owner Alerts, Rental Vehicle Protection, Driver Identification*

I. INTRODUCTION

Road safety remains a global challenge, with unauthorized vehicle use being a recurring cause of accidents and theft. Vehicle owners often lend their vehicles informally, overlooking whether the borrower holds a valid license. During traffic inspections or accident investigations, verifying the authenticity of a driver's license is often time-consuming, particularly in the presence of fake or duplicate credentials.

Existing vehicle security solutions—such as mechanical keys, RFID tags, or standalone fingerprint ignition—are insufficient. These systems fail to link vehicle usage with the legal eligibility of the driver, and they often exclude real-time owner notifications.

This study proposes a multi-layer vehicle authentication system that uniquely combines:
DL Verification – Ensures the driver has a valid license.
Fingerprint Authentication – Matches biometric data with the registered license holder.
Password Protection – Provides an additional access layer.
Owner Notifications with GPS – Keeps the owner informed of vehicle usage.
Re-authentication Delay – Prevents repeated unauthorized trials within 20 minutes.
Rental Mode – Enables additional DL re-verification for rental services.
Accident Driver Identification – Accurately identifies and notifies the owner of the driver involved in accidents..

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

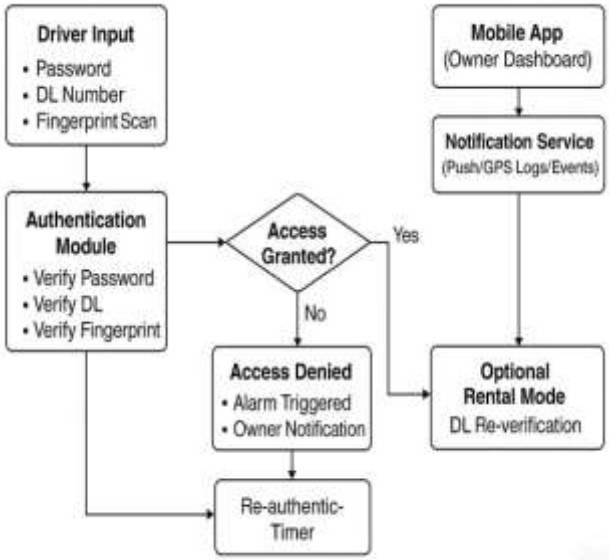


Fig. 1: Flowchart of the Multi-Layered Vehicle Authentication System

II. PROBLEM STATEMENT

Unauthorized use of vehicles leads to frequent accidents and theft. Current systems do not combine license validation, biometric verification, passwords, and alerts into a unified framework. Police face delays in verifying driver identity at checkpoints. Rental vehicle services lack robust tools to prevent misuse**.**

III. LITERATURE REVIEW

Previous research has explored:
Some studies have introduced fingerprint-based ignition methods. While these enhance vehicle security, they do not ensure that the driver holds a valid license.

RFID combined with fingerprint authentication improves access control but does not provide direct notifications to the owner or specialized features for rental vehicles.

Cloud-based biometric models offer centralized authentication, yet they lack real-time license verification and the ability to send instant alerts to vehicle owners.

There is no existing framework that integrates DL verification, fingerprint authentication, password protection, GPS-based owner alerts, a re-authentication timer, rental mode features, and accident driver identification. This gap motivates the proposed solution.

IV. PROPOSED SYSTEM

4.1 SYSTEM ARCHITECTURE

The framework includes:
Authentication Module: Validates DL, password, and fingerprint.
Notification Module: Sends usage alerts with GPS coordinates to the owner.
Re-authentication Module: Locks system for 20 minutes after shutdown or failed attempts to prevent repeated unauthorized trials.
Rental Mode: Optional feature for re-verifying DLs in rental services.
Accident Identification Module: Detects accidents and sends verified driver credentials, timestamp, and GPS location to the owner's mobile app.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

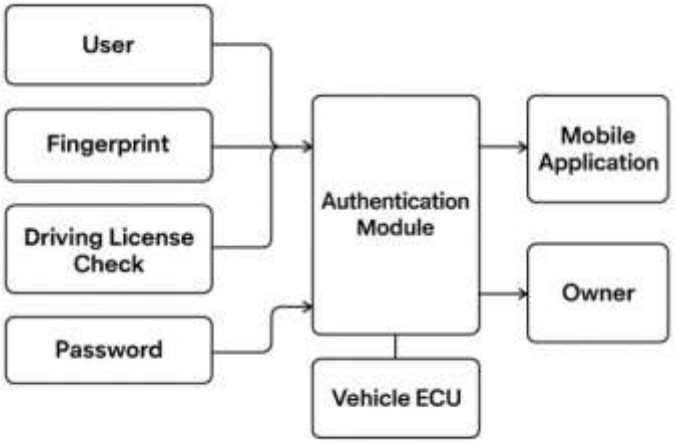


Fig 2: Block Diagram of the Authentication Framework

4.2 WORKFLOW

User enters password.
DL details are submitted and verified.
Fingerprint scan is performed.
If all credentials match, vehicle ignition is enabled and owner is notified.
If mismatch occurs, vehicle remains locked, alarm is triggered, and alert is sent to the owner.
Shutdown initiates a 20-minute lockout period.
In the event of an accident, the authenticated driver's information, along with timestamp and GPS location, is sent to the owner instantly..



Fig 3: Stepwise Workflow of the Authentication Process

V. CONCEPTUAL SIMULATION

The workflow is simulated using Python and MATLAB. Inputs are password, DL number, and fingerprint templates. Outputs include access status, notification to owner, enforcement of re-authentication lockout, and real-time accident driver identification reporting.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

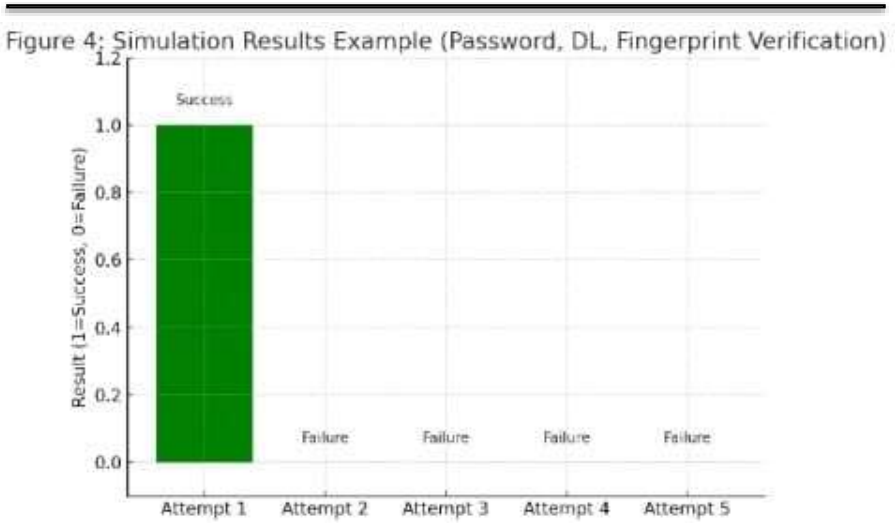


Fig 4: Simulation Results Example (Password, DL, Fingerprint Verification)

Attempt	DL Verified	Fingerprint Matched	Password Correct	Vehicle Status	Owner Notification
1	Yes	Yes	Started	Started	Sent
2	Yes	No	Yes	Off	Unsultforized Aron
3	No	Yes	Yes	Off	Unsultforized Aron

Attempt	DL Verified	Fingerprint Matched	Password Correct	Vehicle Status	Owner Notification
1	Yes	Yes	Started	Started	Sent
2	Yes	No	Yes	Off	Unsultforized Aron
3	No	Yes	Yes	Off	Unsultforized Aron

VI. APPLICATIONS

Accident Prevention: Only licensed and authenticated drivers can operate the vehicle.
Rental Services: Rental providers can activate DL re-verification to reduce misuse.
Law Enforcement: Simplifies roadside verification and post-accident inquiries.
Fleet Management: Owners can monitor driver activity to reduce unauthorized use.
Accident Driver Identification: Enables owners to instantly identify and verify the driver involved in an accident, facilitating quick investigation and liability determination.

VII. CONCLUSION

This paper presents a comprehensive a layered vehicle authentication framework that combines license verification, biometric fingerprint matching, password protection, and instant owner alerts, timed re-authentication lock, rental mode, and accident driver identification. Simulation-based validation demonstrates its effectiveness in reducing accidents, thefts, and disputes, while supporting law enforcement and commercial rental services with enhanced driver accountability and accident response capabilities.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

REFERENCES

1. *Smith, J., & Kumar, A. (2024). Biometric Approaches to Vehicle Ignition Systems. International Journal of Vehicle Security, 12(3), 45–52.*
2. *Sharma, R., & Patel, S. (2024). RFID and Fingerprint-Based Access for Smart Vehicles. Journal of Engineering Research, 15(2), 22–30.*
3. *Li, H., & Zhang, X. (2023). Cloud-Oriented Biometric Vehicle Security. IEEE Access, 11, 1150–1160.*
4. *iCarB Fingerprint Dataset. (2024). arXiv. https://arxiv.org/abs/2411.17305*