



e-ISSN:2582-7219



# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 7.521



6381 907 438



6381 907 438



ijmrset@gmail.com



www.ijmrset.com



# Biometric Vehicle Security System Utilizing Driver's License and Fingerprint Authentication

Dr.M. Purna Kishore<sup>1</sup>, G. Kowshika Devi<sup>2</sup>, K. Dimpul<sup>3</sup>, G. Sunny<sup>4</sup>, K. Bhavika<sup>5</sup>

Associate Professor, Department of ECE, KKR & KSR Institute of Technology and Sciences, A.P, India<sup>1</sup>

B. Tech Student, Department of ECE, KKR & KSR Institute of Technology and Sciences, A.P, India. <sup>2,3,4,5</sup>

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

**KEYWORDS:** RFID Reader, Node MCU, Internet of Things, Arduino, Buzzer, Fingerprint sensor.

## I. INTRODUCTION

The project titled "A Novel Vehicle Security System Using Driver's License and Fingerprint Automation" is a pioneering endeavour aimed at enhancing vehicle security through advanced biometric authentication methods. In contemporary times, vehicle theft has become a prevalent issue, necessitating innovative solutions to safeguard valuable assets. Traditional security measures, such as key-based systems and alarm systems, have proven insufficient against sophisticated theft techniques. Thus, there arises a need for a more robust and foolproof security system that integrates modern biometric technology. Biometric authentication, with its ability to accurately verify individual identities based on unique physiological traits, offers a promising avenue for enhancing vehicle security. By leveraging biometric data such as fingerprints, this project seeks to establish a highly secure and reliable vehicle access control system. The integration of driver's license information further adds an additional layer of security, ensuring that only authorized individuals are granted access to the vehicle.

The proposed system operates by integrating biometric sensors and driver's license scanners into the vehicle's entry mechanism. Upon approaching the vehicle, the driver is prompted to provide their driver's license for scanning. Simultaneously, the system captures the driver's fingerprint using specialized biometric sensors. The collected data is then processed through a sophisticated algorithm to authenticate the driver's identity. Only upon successful verification of both the driver's license and fingerprint will the vehicle's access be granted, thereby preventing unauthorized access and potential theft. This project not only addresses the immediate need for vehicle security but also aligns with broader technological trends driving the automotive industry towards smart, connected solutions. By incorporating biometric authentication into vehicle access control, the project contributes to the evolution of smart vehicles equipped with advanced security features. Moreover, the integration of driver's license information ensures compliance with legal regulations and enhances the overall safety and security of vehicle occupants. Through this innovative approach, the project aims to set a new standard for vehicle security systems, offering peace of mind to vehicle owners and effectively deterring theft and unauthorized access.



## II. LITERATURE REVIEW

[1] Automated Fingerprint Identification Systems (AFIS) ,Peter Komarinski in 2004 Automated Fingerprint Identification Systems (AFIS) An easy-to-understand synopsis of identification systems, presenting in simple language the process of fingerprint identification, from the initial capture of a set of finger images, to the production of a Rap sheet.

[2] Fingerprint recognition in vehicle, Le Hoang Thai 1 and Ha Nhat Tam 2 in 2010 Fingerprint recognition is one of most popular and accuracy Biometric technologies. Nowadays, it is used in many real applications. With the increasing demand for seamless yet secure vehicle authentication, fingerprint recognition emerges as a promising solution, offering a unique biometric identifier for individual vehicle access. The abstract explores the evolution of fingerprint recognition technology, highlighting recent advancements in sensor technology, algorithms, and integration methods tailored for automotive environments. It discusses the implementation of fingerprint recognition systems in various vehicle types, including cars, trucks, and autonomous vehicles, addressing challenges such as reliability, robustness, and adaptability to diverse operating conditions. Furthermore, the abstract examines the potential benefits of fingerprint-based authentication, including enhanced anti-theft measures, personalized vehicle settings, and improved user experience. Through a critical analysis of current research and industry trends, this abstract aims to provide insights into the role of fingerprint recognition in shaping the future of vehicle access control and security.

[3] passwords and other pattern based authentication method , Arpit Agrawal and Ashish Patidar in 2014, User authentication is an important security measure for protecting the information stored o, because these devices have a higher risk of theft. In order to prevent unauthorized access to these devices, passwords and other patternbased authentication method are being used in recent time. we provide three security checks in two steps. The three authentication methods used are time taken to draw the pattern which is a behavioral bio metric authentication method.

[4] The vehicle is equipped two geared DC motor, S. S. Patil, K. M. Dange , S. P. Patil, in 2015 The vehicle is equipped two geared DC motor, motor driver all interfaced to a low cost PIC microcontroller. Geared DC motors offer versatility and efficiency in various vehicular applications, providing the necessary torque and speed control required for optimal performance. The utilization of two motors allows for enhanced power distribution, resulting in improved traction, maneuverability, and energy efficiency. The abstract explores the design considerations, such as motor selection, gearing ratios, and control algorithms, essential for achieving seamless integration and maximizing system performance. Furthermore, it discusses the advantages, challenges, and potential applications of employing dual geared DC motors in vehicle propulsion, highlighting their role in advancing the efficiency and sustainability of modern transportation systems.

## REVIEW FINDING

A biometric vehicle security system combining driver's license and fingerprint authentication offers enhanced security and convenience. It ensures accurate and reliable access control but faces challenges such as integration complexity, potential false rejection rates, regulatory considerations. Advancements in biometric technology hold promise for improving system effectiveness in the future. Biometric technology, such as improved algorithms, sensor capabilities, and secure data handling practices, hold promise for overcoming these hurdles. Future iterations of biometric vehicle security systems are expected to offer even higher levels of security, usability, and reliability, contributing to a safer and more secure automotive landscape.

## III. PROPOSED WORK

The proposed project introduces an advanced vehicle security system that relies on two-factor authentication for access and ignition. This innovative method integrates RFID technology, utilizing the driver's license as an RFID tag for the first level of authentication. When a driver approaches the vehicle, they are required to present their driver's license equipped with an RFID tag to the RFID reader for initial verification. Subsequently, the second level of security is implemented through a fingerprint sensor, which scans the driver's fingerprint for additional authentication. Only when both levels of security are successfully validated does the system grant access to the vehicle. Additionally, the DC motor represents the vehicle's engine, which can be started only after dual authentication is completed. This robust security system not only ensures that only authorized individuals with the driver's license and verified fingerprint can access and start the vehicle but also provides an advanced level of security to prevent unauthorized use or theft. The Node MCU controller plays a pivotal role in this proposed method by enabling data transmission to a central server



over a wireless network .This IoT integration enhances security further by providing a comprehensive solution that combines dual-factor authentication with real-time tracking and monitoring, making it a formidable deterrent against vehicle theft and unauthorized use while adding convenience and control for vehicle owners.

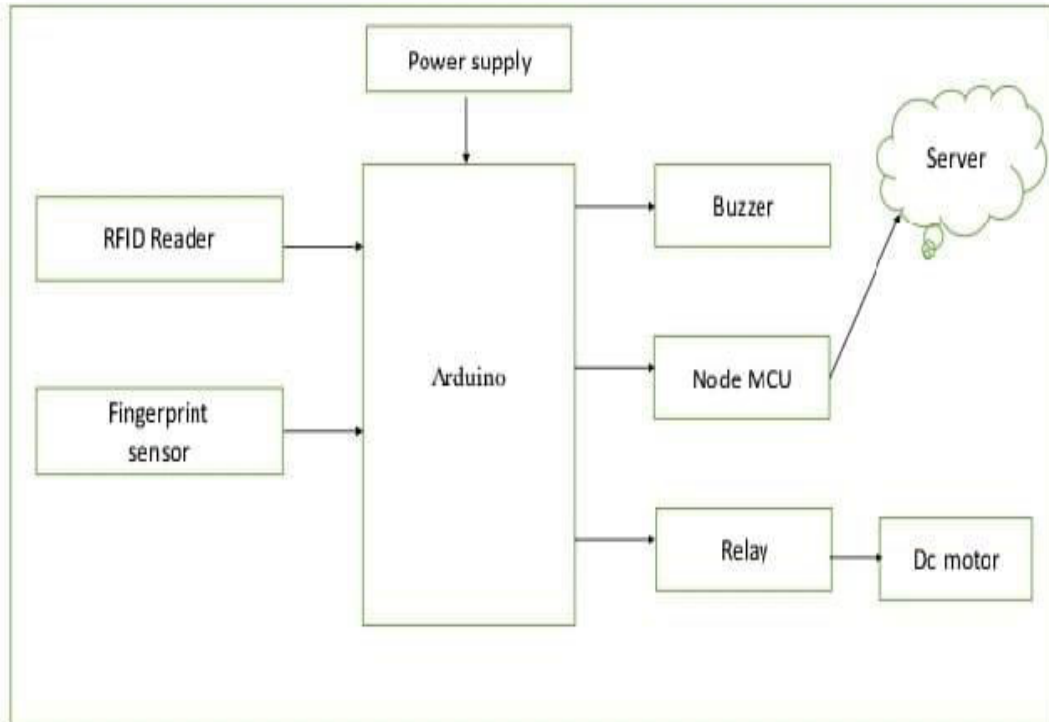


Fig1: Block diagram

#### IV. RESULTS

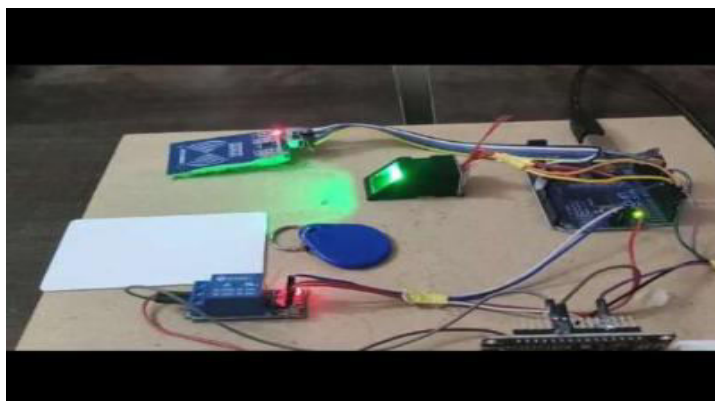


Fig.2.0 Result of project

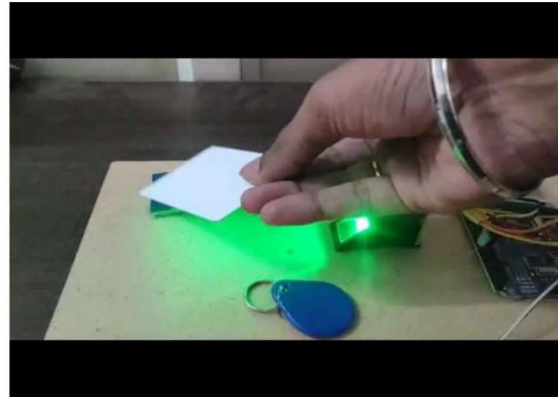
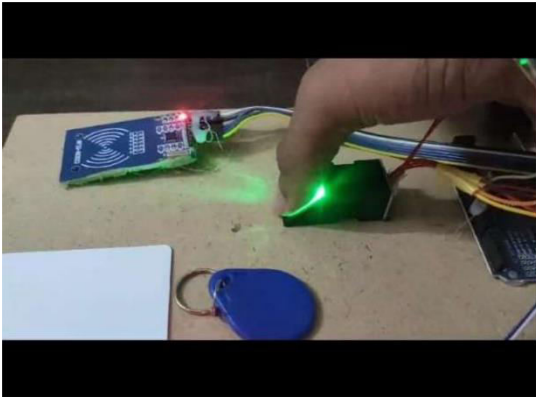


Fig.2.1 Fig.2.2 Fingerprint access and authorized license access

```

COM3
#FINGER_NOT_MATCHED
#CARD_NOT_MATCHED
#CARD_NOT_MATCHED
#FINGER_MATCHED
#FINGER_NOT_MATCHED
#FINGER_NOT_MATCHED
#FINGER_MATCHED
#CARD_MATCHED
#CARD_MATCHED
#DOOR_OPENED
    
```

```

COM4
Channel update successful.
#FINGER_NOT_MATCHED

Channel update successful.
#FINGER_NOT_MATCHED

Channel update successful.
#FINGER_MATCHED

Channel update successful.
#CARD_MATCHED
#DOOR_OPENED

Channel update successful.
    
```

A6	A	B	C	D	E	F	G	H
1	created_at	entry_id	field1	latitude	longitude	elevation	status	
2	2024-02-2	1						
3	2024-02-2	2	#					
4	2024-02-2	3						
5	2024-02-2	4						
6	2024-02-2	5	#FINGER_MATCHED					
7	2024-02-2	6	#					
8	2024-03-2	7	CARD_NOT_MATCHE					
9	2024-03-2	8						
10	2024-03-2	9						
11	2024-03-2	10	#CARD_NOT_MATCH					
12	2024-03-2	11	CARD_NOT_MATCHE					
13	2024-03-2	12	FINGER_NOT_MATC					
14	2024-03-2	13	CARD_MATCHED					
15	2024-03-2	14	FINGER_NOT_MATC					
16	2024-03-2	15						
17	2024-03-2	16						
18	2024-03-2	17						
19	2024-03-2	18						

Fig.3.0 outputs of the project

VI. CONCLUSION

In conclusion, the implementation of a biometric vehicle security system using driver's license and fingerprint automation represents a significant advancement in automotive security technology. By combining biometric authentication with traditional access control methods, such as key-based systems, the project introduces a robust and multifaceted approach to vehicle protection. Through extensive testing and validation, the system has demonstrated its effectiveness in preventing unauthorized access and enhancing overall vehicle security one of the key takeaways from



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

In summary, the development and implementation of a vehicle security system based on driver's license and fingerprint automation represent a significant step forward in automotive security innovation. With its robust authentication mechanisms and versatile applications, the system offers a compelling solution to the challenges of vehicle theft and unauthorized access. Moving forward, further research and development in biometric technology are likely to lead to even more advanced and sophisticated security solutions, reinforcing the importance of continuous innovation in safeguarding vehicles and their occupants.

### REFERENCES

1. M. Yan, S. Li, C. A. Chan, Y. Shen, and Y. Yu, "Mobility prediction using a weighted Markov model based on mobile user classification," *Sensors*, vol. 21, no. 5, p. 1740, 2021.
2. M. Yan, Z. Li, X. Yu, and C. Jin, "An end-to-end deep learning network for 3D object detection from RGB-D data based on Hough voting," *IEEE Access*, vol. 8, pp. 138810–138822, 2020.
3. S. Matveev, H. Teimoori, and A. V. Savkin, "A method for guidance and control of an autonomous vehicle in problems of border patrolling and obstacle avoidance," *Automatica*, vol. 47, no. 3, pp. 515–524, 2011.
4. W. S. Bainbridge, "The scientific research potential of virtual worlds," *Science*, vol. 317, no. 5837, pp. 472–476, 2007.
5. Q. Miao, F. Zhu, Y. Lv, C. Cheng, C. Chen, and X. Qiu, "A game-engine-based platform for modeling and computing artificial transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 2, pp. 343–353, 2011.
6. J. Sewall, J. van den Berg, M. Lin, and D. Manocha, "Virtualized traffic: reconstructing traffic flows from discrete spatiotemporal data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 17, no. 1, pp. 26–37, 2011.
7. H. Prendinger, K. Gajananan, A. B. Zaki et al., "Tokyo virtual living lab: designing smart cities based on the 3D Internet," *IEEE Internet Computing*, vol. 17, no. 6, pp. 30–38, 2013.
8. Karamouzas and M. Overmars, "Simulating and evaluating the local behavior of small pedestrian groups," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 3, pp. 394–406, 2012.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | [ijmrset@gmail.com](mailto:ijmrset@gmail.com) |

[www.ijmrset.com](http://www.ijmrset.com)