ISSN (Print): 2957-9325, ISSN (Online): 2957-9333

INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH TRANSACTION

(Open Access-Referred-Peer-Reviewed Journal)

Journal homepage:https://ijaer-transaction.com/

Research Article

INTEGRATED BIOMETRIC AND CREDENTIAL-BASED AUTHENTICATION FRAMEWORK FOR ENHANCED VEHICLE ACCESS SECURITY

Mr. Suraj Patil[1], Mr. Taj Ansari[2], Ms. Homeksha Hedau[3], Ms. Kanchan Kathole[4], Mrs. Ashwini Waghale [5]

[1-5] Dept. of Electronics and Telecommunicatio, Govindrao Wanjari College of Engineering, Nagpur, India.

Article History:	Received: 20.01.2025	Accepted: 24.02.2025	Published: 04.03.2025

Abstract

Biometric authentication represents an innovative technology that has been increasingly applied across various sectors. A notable area of recent interest is its application in vehicle ignition systems. This technology serves to prevent unauthorized vehicle access, ensuring that only the authorized driver can initiate the vehicle's operation. Typically, biometric authentication systems employ a combination of physiological and behavioral characteristics to identify the driver, including facial recognition, fingerprint scanning, iris recognition, voice recognition, and gait analysis. This paper seeks to provide a comprehensive overview of biometric authentication systems for vehicle ignition, examining the advantages, disadvantages, and challenges associated with their implementation. Additionally, the paper explores the various biometric modalities available for authentication, the algorithms employed for recognition, and the security considerations of the system. The findings indicate that biometric authentication for vehicle ignition has the potential to enhance vehicle security and deter theft. Nonetheless, certain technical and social challenges must be addressed before this technology can achieve widespread adoption.

Keywords: Biometric authentication, Ignition, Fingerprint Scanning, Arduino, Wi-fi Module

INTRODUCTION

Biometric authentication for vehicle ignition constitutes a security measure that employs an individual's distinct physical attributes to verify their identity before allowing vehicle operation. This technology utilizes sensors and software to analyze biometric data, including fingerprints, facial recognition, voice recognition, or iris recognition. The integration of biometric authentication for vehicle ignition is increasingly prevalent in modern vehicles due to its provision of enhanced security against theft and unauthorized use. By implementing biometric authentication, vehicle owners can ensure that only authorized drivers are permitted to start and operate their vehicles, thereby preventing theft and enhancing the safety and security of both the vehicle and its occupants.

Biometric authentication has gained prominence in recent years due to its accuracy and security in individual identification. This technology leverages unique physical characteristics, such as fingerprints, iris patterns, or facial features, to verify identity. It has been extensively employed across various industries, including finance, healthcare, and security, and is now being integrated into the automotive sector. Specifically, biometric authentication is being utilized for vehicle ignition to enhance both security and convenience in the driving experience. With this technology, drivers can unlock their vehicles, start the engine, and drive without the necessity of traditional keys or key fobs. Instead, the vehicle recognizes the driver's unique biometric information and grants access.

Biometric authentication for vehicle ignition is designed to deter car theft and bolster overall security. It offers a level of protection that traditional key-based systems cannot provide, as biometric authentication necessitates the presence of the driver's unique physical characteristics for access to be granted. Consequently, even if a thief gains entry to the vehicle, they will be unable to start the engine without the driver's biometric data. Moreover, biometric authentication offers a more convenient method of accessing and starting the vehicle. Drivers are no longer required to carry traditional keys or fobs, which are susceptible to loss or theft. Instead, they rely on their biometric data, which is unique and cannot be replicated.

A. Objectives:

- The primary objective of this project is to facilitate authentication access for vehicle ignition using the authenticated driver's fingerprint.
- It assists the owner in identifying the driver through the Live Camera Feed.
- Additionally, with the aid of GPS, the location of the vehicle can be easily determined in cases of misuse or theft.

B. Applications:

- Automotive sectors.
- Industries, factories, and high-security facilities.
- Corporate and small-scale sectors.

C. Advantages:

- Provides a superior level of security compared to traditional methods.
- Eliminates the risk of theft, as the user's biometric data cannot be duplicated or replicated.
- Offers a convenient and rapid method of authentication.
- Facilitates driver identification and monitoring.

II. LITERATURE SURVEY

Many current systems operate independently, with data collected by these individual units frequently updated in a database accessible to the vehicle owner. This provides detailed information about the driver, which can aid in verifying driver history during payment transactions. Furthermore, these systems often incorporate data security measures, such as SHA-1 and SALT algorithms, to enhance protection against unauthorized access. Such systems have the potential for further development and could support government transportation initiatives. [1]

One study presents a cost-effective and efficient embedded system designed for detecting vehicle speed. The research sought to improve results by comparing various methodologies, including FFT, DSP, and LASAR-based techniques. The system achieved greater accuracy when there were no other moving objects in close proximity. However, it's important to note that radar technology may not accurately measure a vehicle's speed when it is stationary. [2]

Another paper provides a review of various vehicle speed detection techniques. These techniques include methods like edge extraction, object tracking, motion vector analysis, the absolute centroid method, and background image subtraction. These processes are often implemented using MATLAB, and the techniques can be applied to traffic management and vehicle speed control. [3]

A separate work introduces an integrated framework for vehicle tracking that uses roadside lidar data. The process begins with the identification of vehicle clusters from raw point clouds using a three-step approach. Following this, a centroid-based tracking procedure is employed to track individual vehicles within the clusters. [4]

The accurate estimation and classification of vehicle speed present significant challenges in Vehicle Detection Systems (VDS) used for collecting traffic data in Intelligent Transportation Systems (ITS). It is generally difficult to accurately estimate per-vehicle speed using side-looking single-beam microwave detection. Moreover, obtaining reliable vehicle length data from these detectors is problematic due to the unreliable speed estimates derived from conventional data aggregation methods for single-beam detectors. [5]

One study investigated various technologies used for detecting speed violations. These technologies include radar-based technology, laser light systems, average speed computer systems, and vision-based systems. Each of these technologies can encounter limitations, such as reduced accuracy, ineffectiveness in adverse weather or light conditions, high costs, limited range, line-of-sight restrictions, or challenges in focusing on a specific vehicle. Consequently, there is a need for a system that can operate automatically with a high degree of accuracy, function effectively in various weather and light conditions, and uniquely identify vehicles by type in order to calculate average speeds for different vehicle categories. [6]

Some research focuses on video surveillance systems, which have a wide range of applications, including security for premises, accident detection, fire detection, robotics, and object recognition. Motion detection is a critical component of video surveillance systems, involving the identification of moving objects within video sequences captured by surveillance cameras. Motion detection is a well-researched area in video analysis, with numerous studies dedicated to this topic. [7]

An automobile anti-theft system that uses GSM and GPS modules offers features such as remote monitoring, high-sensitivity response, and the ability to observe a vehicle's location online. This type of system combines the security benefits of traditional vehicle alarm systems and has the potential for further development with features like Internet of Things (IoT) integration. The use of modules like NRF24L01 enables communication between vehicles, allowing other vehicles to receive warning information when one vehicle's alarm is activated, which can be useful for locating a stolen vehicle. [8]

III. HARDWARE AND SOFTWARE REQUIREMENTS

TABLE I HARDWARE COMPONENTS REQUIRED

Sr. No	Components Required	Quantity
1	Arduino Uno	3
2	R307 Fingerprint Sensor	1
3	ESP 32 cam	1
4	ESP 8266 Wi-Fi Module	2
5	U channel relay	1
6	9 Volt Battery	1
7	Neo-6m GPS Module	1
8	Jumper Wires	2 sets

1. Arduino Uno:

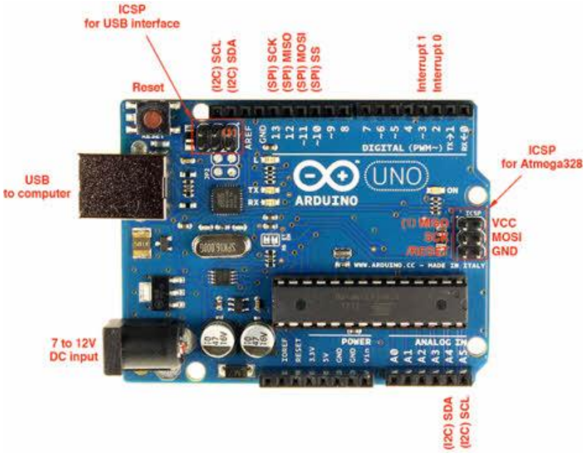

Fig.1 Arduino Uno

The Arduino Uno is one kind of microcontroller board based on ATmega328, and Uno is an Italian term which means one. Arduino Uno is named for marking the upcoming release of microcontroller board namely Arduino Uno Board 1.0. This board includes digital I/O pins-14, a power jack, analog i/ps-6, ceramic resonator-A16 MHz, a USB connection, an RST button, and an ICSP header. All these can support the microcontroller for further operation by connecting this board to the computer. The power supply of this board can be done with the help of an AC to DC adapter, a USB cable, otherwise a battery. This article discusses what is an Arduino Uno microcontroller, pin configuration, Arduino Uno specifications or features, and applications. The ATmega328 is one kind of single-chip microcontroller formed with Atmel within the megaAVR family. The architecture of this Arduino Uno is a customized Harvard architecture with 8-bit RISC processor core. Other boards of Arduino Uno include Arduino Pro Mini, Arduino Nano, Arduino Due, Arduino Mega, and Arduino Leonardo.

2. R307 Fingerprint Sensor:

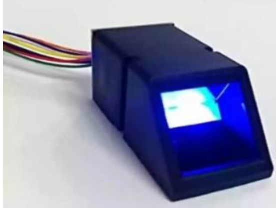

Fig 2. R307 Fingerprint Sensor

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger two times. The system will process the two-time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

3. Esp 32 Camera:

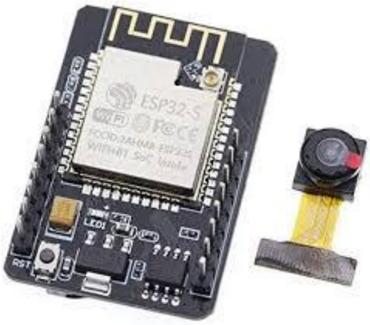

Fig 3. Esp 32 Camera

The ESP32-CAM is a budget-friendly, Wi-Fi-enabled camera module built around the ESP32 microcontroller. It's a popular choice for DIY projects like home security, surveillance systems, smart doorbells, and robots. Equipped with an OV2640 camera sensor, it can capture images up to 2 megapixels and record video at resolutions up to 1080p. The module also includes a microSD card slot for local storage and supports cloud storage.

This module is designed to be compact, measuring only 27mm x 40mm, which makes it easy to integrate into various projects. It also features several pins for connecting external components like sensors, actuators, and displays. With integrated Wi-Fi and Bluetooth, the ESP32-CAM can communicate wirelessly with other devices.

4. Esp8266 Wi-Fi Module:

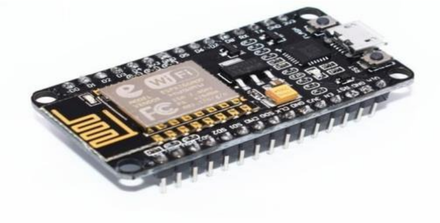

Fig 4. Esp8266 Wi-Fi Module

An ESP8266 Wi-Fi module is a SOC microchip mainly used for the development of end-point IoT (Internet of things) applications. It is referred to as a standalone wireless transceiver, available at a very low price. It is used to enable the internet connection to various applications of embedded systems. Espressif systems designed the ESP8266 Wi-Fi module to support both the TCP/IP capability and the microcontroller access to any Wi-Fi network.

It provides the solutions to meet the requirements of industries of IoT such as cost, power, performance, and design. It can work as either a slave or a standalone application. If the ESP8266 Wi-Fi runs as a slave to a microcontroller host, then it can be used as a Wi-Fi adaptor to any type of microcontroller using UART or SPI. If the module is used as a standalone application, then it provides the functions of the microcontroller and Wi-Fi network. The ESP8266 Wi-Fi module is highly integrated with RF balun, power modules, RF transmitter and receiver, analog transmitter and receiver, amplifiers, filters, digital baseband, power modules, external circuitry, and other necessary components.

The ESP8266 Wi-Fi module is a microchip shown in the figure below. A set of AT commands are needed by the microcontroller to communicate with the ESP8266 Wi-Fi module.

Hence it is developed with AT commands software to allow the Arduino Wi-Fi functionalities, and also allows loading various software to design the own application on the memory and processor of the module. The processor of this module is based on the Tensilica Xtensa Diamond Standard 106 micro and operates easily at 80 MHz.

5. U Channel Relay:

Fig 5. U Channel Relay

A U channel relay is a type of electromagnetic relay designed for mounting on a printed circuit board (PCB) using a U-shaped channel or bracket. Often called a PCB relay, miniature relay, or signal relay, these small components are commonly used in electronic devices for switching or controlling signals. They work using a coil, contacts, and a frame. When current flows through the coil, it generates a magnetic field that causes the contacts to move, either completing or interrupting the circuit.

A single-channel relay is an electronic switch that can be controlled by a low-power electrical signal, such as the output from an Arduino microcontroller. By using an Arduino Uno and a 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.

6. 9v Battery:

Fig 6. 9V Battery

The nine-volt battery, or 9-volt battery, is an electric battery that supplies a nominal voltage of 9 volts. Actual voltage measures 7.2 to 9.6 volts, depending on battery chemistry. Batteries of various sizes and capacities are manufactured; a very common size is known as PP3, introduced for early transistor radios. The PP3 has a cuboid shape with rounded edges and two polarized snap connectors on the top. This type is commonly used for many applications including household uses such as smoke detectors, gas detectors, clocks, and toys.

7. GPS Module:

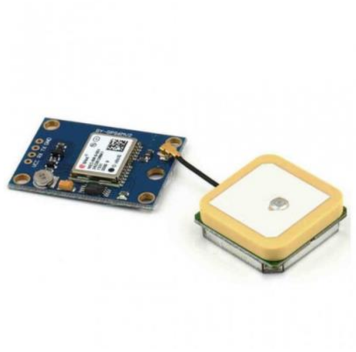

Fig 7. Neo-6m GPS Module

The module is built around the U-box NEO-6M GPS chip. Despite its small size, comparable to the size of a postage stamp, this chip is packed with features. It can simultaneously track up to 22 satellites across 50 channels and boasts a high tracking sensitivity of -161 dB while consuming only 45 mA of current. Unlike many GPS modules, it provides 5 location updates per second with a horizontal position accuracy of 2.5 meters. The Ublox 6 positioning engine also achieves a Time-To-First Fix (TTFF) in under 1 second. A notable feature is its Power Save Mode (PSM), which reduces system power consumption by selectively turning parts of the receiver on and off. This drastically lowers power consumption to just 11 mA, making it ideal for power-sensitive devices like GPS wristwatches.

IV. IMPLEMENTATION AND METHODOLOGY

A. Working Procedure:

- Authorized Fingerprint Authentication: Initially, the system is programmed with the vehicle owner's fingerprint data, which is stored in its memory. When the owner places their finger on the fingerprint sensor, the system verifies the fingerprint by comparing it to the stored data. If a match is confirmed, the system grants access, and the vehicle ignition is enabled.

- Unauthorized Fingerprint Authentication: If an unregistered fingerprint is detected by the sensor, the system denies access and prompts the owner for permission. A notification is sent to the owner's mobile application, providing them with the option to either grant or deny access.

- Granting Permission: If the owner grants permission, the system saves the unregistered fingerprint as a primary fingerprint in its memory for future use. Subsequently, the system enables vehicle ignition.

- Denying Permission: If the owner denies permission, the system maintains denied access, and the vehicle remains unable to ignite. The system does not store the unregistered fingerprint data.

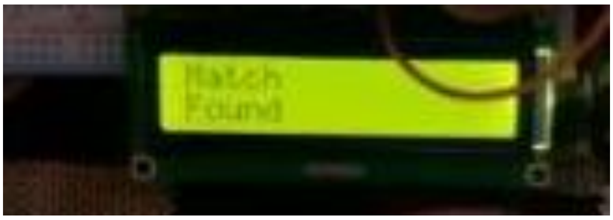

Fig 8. Case 1: Direct Access to Owner

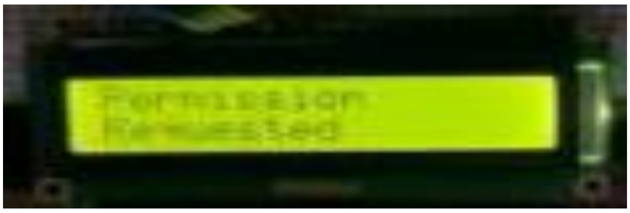

Fig 9. Case 2: Permission Required from Owner for Third Party Access.

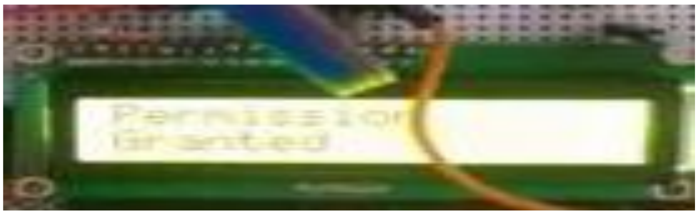

Fig 10. Case 2: Permission Granted by the Owner through Mobile Device

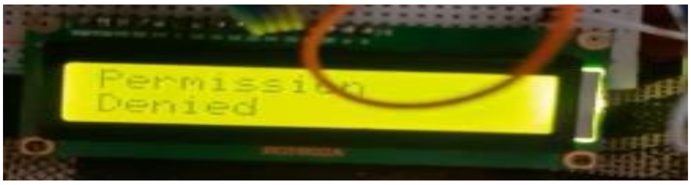

Fig 11. Case 3: Permission Denied by the Owner through Mobile Device.

B. System Hardware:
The system's hardware components include:

- Arduino UNO: This is the core microcontroller that manages the system's operation. It processes input from the fingerprint sensor and the GPS/GSM module and controls the ESP32-CAM and ESP8266 modules.
- Fingerprint Sensor: This component authenticates the user by capturing their fingerprint and comparing it to stored data to grant or deny access to the vehicle.
- ESP32-CAM: This module captures an image of the user's face for additional verification. The camera is activated when the user interacts with the fingerprint sensor.
- ESP8266: This module facilitates communication with the GPS/GSM module, enabling the transmission of location data to the user's mobile device.
- U-channel Relay: This relay controls the vehicle's ignition. It is connected to the Arduino UNO and is activated only after successful fingerprint and facial authentication, along with location verification.
- 9V Battery: This battery provides power to the entire system.
- GPS/GSM Module: This module tracks the vehicle's location and sends location data to the user's mobile device. It communicates with the Arduino UNO through the ESP8266 module.

C. Flow Chart:

The system's operational flow is as follows:

- System Initialization: When power is supplied, the system initializes all its components and enters a waiting state.
- User Authentication: When a user places their finger on the fingerprint sensor, the system captures the fingerprint and compares it to the stored fingerprint data.
- Registered User Handling: If the fingerprint matches a registered user, the system verifies the vehicle's GPS location to ensure the user is within an authorized area. If the user is authorized, the system sends a signal to the U-channel relay to start the vehicle's ignition.
- Unregistered User Handling: If the fingerprint is not recognized, the system requests permission from the owner to add the new fingerprint data. If the owner grants permission, the system stores the new fingerprint data as the primary fingerprint for future authentication.
- Ignition Process: If the user is authorized, the U-channel relay is activated, and the vehicle ignition is initiated.
- Deactivation and Reset: After the vehicle is started, the system monitors for the user to turn off the vehicle. Once the vehicle is turned off, the system resets and returns to the initial waiting state, ready for the next user.

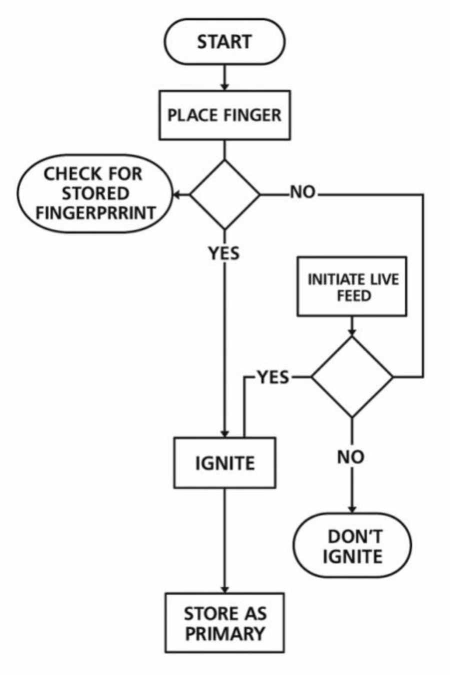

Fig 12. Flow Chart of Integrated Biometric and Credential-Based Authentication Framework for Enhanced Vehicle Access Security

V. RESULTS

A. PROPOSED DEMO MODEL:

Case 1: Owner's Direct Access

In this scenario, the system authenticates the vehicle owner by verifying their stored fingerprint data. Upon successful authentication, the vehicle's ignition system grants access to the owner. If the fingerprint does not match or if the stored fingerprint data is not found within the system, the system will identify the user as a third party. This process allows the vehicle owner to quickly and easily access the vehicle without requiring additional devices or procedures.

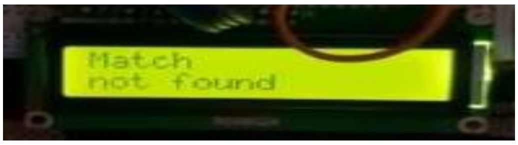

Fig 13. Fingerprint scanner continuously scanning

Fig 14. Owner placing the Finger on Fingerprint scanner

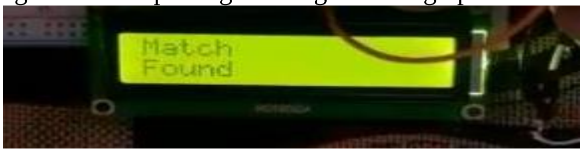

Fig 15: LCD displaying “match Found” for the Owner’s Fingerprint

Fig 16. DC motor turned ON

Case 2: Third-Party Access

When someone other than the owner attempts to access the vehicle, the system initiates a request for authentication sent to the owner's mobile device. The owner is then presented with the option to either approve or deny the access request. If the owner approves the request, the system proceeds to authenticate the third party's identity and, upon successful authentication, grants access to the vehicle. Conversely, if the owner denies the request, the system denies access to the third party. The integration of a camera enhances security by providing the owner with the ability to visually verify the third party's identity. This process ensures a more secure method for granting vehicle access, as it requires owner authorization for each third-party request and incorporates an additional layer of visual identification.

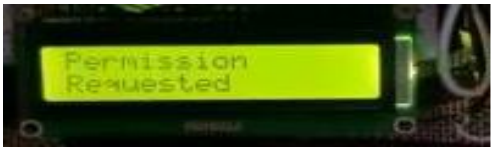

Fig 17. Request message sent when an unknown third party requires access

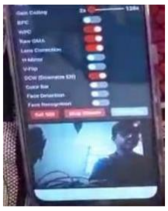

Fig 18. Live feed on owner’s mobile

Fig 19. Owner providing Access

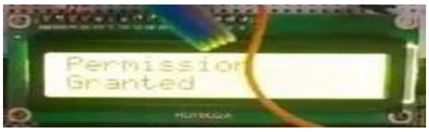

Fig 20. LCD display showing “Permission Granted” message

Fig 21. DC motor turned ON

If the owner denies the permission, then the DC motor does not turn ON. Figure 22 shows LCD displaying “Permission Denied” as the owner has not provided the access for the third party. Figure 23 shows an idle DC motor.

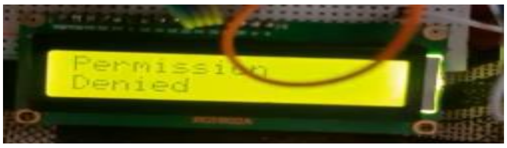

Fig 22. LCD display showing “Permission Denied” message

B. Proposed Real-Time Model

- The biometric-based authentication system for vehicle ignition was implemented on a two-wheeler motorcycle as a real-time model, and the following results were observed:
- When the owner attempted to access the motorcycle, the fingerprint sensor successfully matched the input with a fingerprint stored in its database, and the motorcycle engine was ignited.
- When a third party attempted to access the motorcycle, a notification with a live feed from the camera was sent to the owner's mobile device, allowing the owner to either grant or deny access.

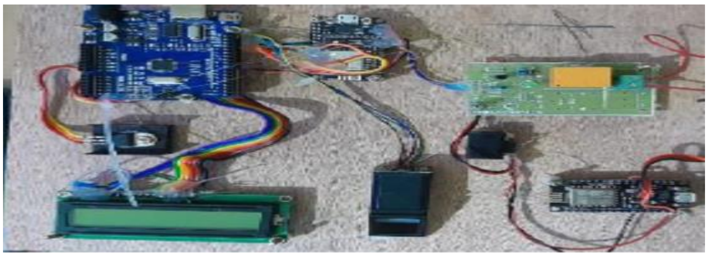

Fig 23. Proposed Real Time Implemented Model

Overall, the biometric-based authentication system for vehicle ignition enhances vehicle security by relying on unique biometric data for authentication. This system also offers vehicle owners a convenient and easy way to access their vehicles, without compromising security.

VI. CONCLUSION

In summary, biometric authentication presents a promising avenue for vehicle ignition systems, offering several notable advantages. It holds the potential to significantly enhance vehicle security, deter unauthorized access and theft, and improve the user experience by eliminating the reliance on traditional keys or passwords. Biometric authentication systems are becoming increasingly advanced and dependable, with a growing array of options such as fingerprint, facial recognition, and voice recognition available.

However, it's important to acknowledge that biometric authentication for vehicle ignition also presents certain limitations and challenges. Implementation can be costly and may necessitate substantial modifications to a vehicle's design and infrastructure. Concerns also exist regarding the accuracy and reliability of these systems, particularly in challenging environmental conditions or when users are wearing items that obscure biometric features.

Despite these challenges, biometric authentication for vehicle ignition remains a promising technology with the potential to transform how we interact with our vehicles. As the technology continues to mature and improve, we can anticipate wider adoption within the automotive industry in the years to come.

VII. FUTURE SCOPE

- Integration with Multiple Biometric Modalities: Current systems often rely on a single biometric method (e.g., fingerprint or facial recognition). Future systems could integrate multiple modalities, such as fingerprint and iris recognition, to achieve improved accuracy and security.
- Robustness to Environmental Conditions: Biometric authentication systems can be susceptible to variations in environmental factors like lighting and temperature. Future efforts should prioritize the development of systems that maintain reliable performance across diverse environmental conditions.
- Privacy and Data Security: Biometric data is inherently sensitive, making its privacy and security of paramount importance.
- Future work should emphasize the development of Secure methods for storing and transmitting biometric data. Protocols to ensure that data is used solely for its intended purpose.

- User Experience and Acceptance: Inconvenience or discomfort associated with biometric authentication systems can lead to user resistance or rejection.
- Future development should concentrate on: Enhancing the user experience. Making systems more user-friendly and accessible to a wider range of individuals.
- Interoperability: Biometric authentication systems for vehicle ignition could gain significant advantages from interoperability with other systems.

VIII. AUTHOR(S) CONTRIBUTION

The writers affirm that they have no connections to, or engagement with, any group or body that provides financial or non-financial assistance for the topics or resources covered in this manuscript.

IX. CONFLICTS OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

X. PLAGIARISM POLICY

All authors declare that any kind of violation of plagiarism, copyright and ethical matters will taken care by all authors. Journal and editors are not liable for aforesaid matters.

XI. SOURCES OF FUNDING

The authors received no financial aid to support for the research.

REFERENCES

[1] "Authenticated Access Control for Vehicle Ignition System by Driver’s License and Fingerprint Technology."Arwa M. Ali, Dr. Heisum M. Awad, Ibrahim K. Abdalgader, (2020 International Conference on Computer, Control, Electrical,and Electronics Engineering (ICCCEEE)).

[2] "FaceIgnition: An automatic anti-theft and key less solution for vehicles”, Tushar Dang, Vanshita Gupta, Diljot singh Wadia., (2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), March 17–18, 2021, Amity University Dubai)

[3] “IoT based Smart Vehicle Ignition and Monitoring System “, Dr. Fathima Jabeen, Sudhir Rao Rupanagudi, Varsha G Bhat.

[4] “Driver Authentication for Smart Car Using Wireless Sensing”, Xuejun Tan, Bir Bhanu, Yingqiang Lin.

[5] “Implementation of Vehicle Security System using GPS, GSM and Biometric”, Mridhula Ramesh, Akruthi S,
Nandhini K, Meena S, Joseph Gladwin S, and Rajavel R.

[6] “Study on Biometric Authentication Systems, Challenges and Future Trends: A Review”, Krishna Dharavath, F. A. Talukdar, R. H. Laskar

[7] “Selecting a Reference High Resolution for Fingerprint Recognition Using Minutiae and Pores”, David Zhang, E, Feng Liu, Qijun Zhao,Guangming Lu,and Nan Luo.

[8] Hu Jian-ming, Li Jie,Li Guang-hui Tianjin University of Technology and Education Tianjin, China, “Automobile
Anti-theft System Based on GSM and GPS Module”, 2012 Fifth International Conference on Intelligent Networks and Intelligent Systems.

[9] " Authenticated Access Control for Vehicle Ignition System by Smart Card and Fingerprint”: Gan Yu Han; Leong Chee Ken; Chew Kuew Wai Content 2022

[10] M. Saravnan, R. Prasanna Venkatesh, S. Poovitha, B. Thiruvarast, C. Prathepa, "Smart license-based vehicle safety and security system," International Journal on Advance research in Science and engineering, vol. no. 6, issue no. 10, pp. 1213-1220, Oct. 2017.

[11] Bonthu B, Kar A, Hilda JJ., "Optimized warning and protection system for a vehicle using RFID-based networks," Indian Journal of Science and Technology, vol. 9, issue no. 28, pp.1–5, July 2016, DOI: 10.17485/ijst/2016/v9i28/91211.

[12] Pramod Sharma, A. Shrivastav, V. Parashar, O. Kumar, R. Naresh, "Smart security system for vehicle," International Journal on Advanced Research in Computer and communication Engineering, vol. 8, issue. No. 4, pp. 279-283, April 2019.

[13] N. Kiruthinga, L. Latha, S. Thangasamy, "Real time biometrics-based vehicle safety system with GPS and GSM technology", Procedia Computer Science, (Elsevier, vol. no. 47(2015), pp. 471-479.

[14] Siyal, Karan, Gugapriya. G., "Anti-theft vehicle locking system using CAN," Indian journal of Science and Technology, vol. no. 9, issue. No. 45, 2016, DOI: 10.17485/ijst/2016/v9i45/105307.

[15] Praveen Kaur, A. Das, M. Borah, "Vehicles safety system using Arduino," ADBU Journal of Electrical and Electronics Engineering, vol. no. 3, issue no. 2, 2019.

[16] Hussain Elbehiry, "Electronic police ambush system via vehicles/drivers' safety authentication system", International Journal on Information Technology and Computer Science, vol. no. 9, pp. 32-38, 2018.