IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

Biometric Based Authentication for Vehicle Ignition System

Abhilash AS[1], Hemanth R Patil[2], Lakshman Kumara B[3],

Mohammad Rakheeb[4], MR, Praveen A[5]

Dept. of Electronics & Communication Engg. K S Institute of Technology Bangalore, India[1-4]

Assistant Professor, Dept. of Electronics and Communication KSIT, Bangalore, India[5]

Abstract: Biometric authentication is an emerging technology that has found its application in various domains. One of the domains that have recently gained attention is vehicle ignition. This technology is used to prevent unauthorized access to the vehicle and ensure that only the authorized driver can start the vehicle. The biometric authentication system typically uses a combination of physiological and behavioral traits to identify the driver, such as facial recognition, fingerprint scanning, iris recognition, voice recognition, and gait analysis. This paper aims to provide an overview of the biometric authentication system for vehicle ignition, including the advantages, disadvantages, and challenges of implementing such a system. The paper also discusses the different biometric modalities that can be used for authentication, the algorithms used for recognition, and the security aspects of the system. The results show that biometric authentication for vehicle ignition has the potential to increase the security of the vehicle and prevent theft. However, there are still some technical and social challenges that need to be addressed before this technology can be widely adopted.

Keywords: Biometric authentication, Ignition, Fingerprint Scanning, Aurdino, Wifi Module.

I. INTRODUCTION

Biometric authentication for vehicle ignition is a security measure that uses a person's unique physical characteristics to verify their identity before allowing them to start a vehicle. This technology involves the use of sensors and software to analyse a person's biometric data, such as fingerprints, facial recognition, voice recognition, or iris recognition. Biometric authentication for vehicle ignition is becoming increasingly popular in modern vehicles as it provides a high level of security against theft and unauthorized use. By using biometric authentication, vehicle owners can ensure that only authorized drivers are able to start and operate their vehicles, preventing theft, and enhancing the safety and security of both the vehicle and its occupants.

Biometric authentication is a technology that has become increasingly popular in recent years due to its accuracy and security in identifying individuals. Biometric authentication involves using unique physical characteristics, such as fingerprints, iris patterns, or facial features, to verify a person's identity. This technology has been widely used in many industries, including finance, healthcare, and security, and it is now being adopted in the automotive industry as well.

In particular, biometric authentication is being used for vehicle ignition to enhance the security and convenience of the driving experience. With biometric authentication, drivers can unlock their car, start the engine, and drive without the need for traditional keys or key fobs. Instead, the car recognizes the driver's unique biometric information and grants access to the vehicle.

Biometric authentication for vehicle ignition is designed to prevent car theft and improve overall security. It provides a level of protection that traditional key-based systems cannot offer, as biometric authentication requires the driver's unique physical characteristics to be present for access to be granted. This means that even if a thief gains access to the car, they will not be able to start the engine without the driver's biometric data.
Furthermore, biometric authentication provides a more convenient way to access and start the car. Drivers no longer have to carry traditional keys or fobs, which can be lost or stolen. Instead, all they need is their biometric data, which is unique to them and cannot be replicated.

A. Objectives:

- The main objective of this project is to provide authentication access to start the vehicle by using authenticated

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

driver's fingerprint.

- It helps the owner to identify the driver based on the Live Camera Feed.
- In addition to that with the help of GPS, one can easily find out the location of the vehicle in case of misuse or if the vehicle gets stolen.

B. Applications:

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

C. Advantages:

- Provides a high level of security compared to traditional methods.
- It eliminates the risk of stolen as the user's biometric data cannot be duplicated or replicated.
- Convenient and fast method of authentication.
- Used for driver identification and monitoring.

II. LITERATURE SURVEY

There are various existing models that are being implemented individually. All these models are implemented as a single unit. The data collected from these models are being updated frequently in the database, which can be viewed by the owner. Hence this system provides more information about the driver. The history of the driver can be verified during the payment times. Also, the data security added in this project is more helpful to secure the system from the hacker using SHA-1 & SALT algorithm. The proposed system can be added with more features and can be used as an assist for the government transportation. [1]

In this paper, a low cost and efficient embedded vehicular speed detecting system is presented. The work aimed at implementing the better results by comparing the existing methods such as FFT, DSP and LASAR based techniques. The output was more accurate with no other moving objects in the surrounding. In reality, the radar will not measure the actual velocity when the vehicle is not travelling [2]

This paper gives review on vehicle speed detection technique using different approaches. Different approaches are edge extraction, object tracking, motion vector technique, absolute, centroid method and background image subtraction. The processing is done in MATLAB. By using any of these methods, traffic can be controlled, and vehicle speed detection will be maintained. [3]

This work presents an integrated vehicle tracking framework using roadside lidar data. Vehicle clusters were detected from the raw point clouds using a three-step schema in the first instance. Afterward, a centroid-based tracking procedure was applied to identify clusters for each vehicle. [4]

Estimating and classifying vehicle speed are crucial problems in VDs used to gather traffic data in an ITS. However, as noted in Section I, per-vehicle speed estimation by side looking single-beam microwave detection is generally inaccurate or unsupported. In addition, collecting reliable length data from these detectors is impossible because of the noisy speed estimates provided by conventional data aggregation for single beam detectors. [5]

Studied multiple technologies used for speed violation detection like Radar Based Technology, Laser Light System, Average speed computer System, Vision Based System etc. Each of them suffers from the problem like Less Accuracy, don't work in bad weather or light condition, High Cost, Limited Range, Line of sight, problem to Focus on a particular vehicle etc. So, we need a system that can be automatically operated with good accuracy, work even in bad weather and light condition and identify the vehicle uniquely with its type to calculate the average speed for different types of vehicles. [6]

This work deals with the field of video surveillance systems. These systems can be used in many application areas: security of the premises, detection of accidents, fires, robotics, object recognition. The video is the media treated in such systems. Among the most important steps in video surveillance systems the motion detection. This step involves the detection of moving objects in video sequences captured by the surveillance camera. The motion detection stage is among the most studied problems in the field of video analysis where many research works focus on this problem.[7]

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

Automobile Anti-theft System Based on GSM and GPS Module has the functions of remote monitoring; high sensitivity responding and observation location of automobile online. The system has good properties of security integrate with traditional warning system of automobile. The system can develop deeply and add other functions such as Internet of Things. The system can achieve networking between two automobiles or among many automobiles because NRF24L01 module adopted. So other automobiles can receive the warning information if one automobile alarm. It is good to find the lost automobile. [8]

III. HARDWARE AND SOFTWARE REQUIREMENTS

TABLE I HARDWARE COMPONENTS REQUIRED

Sl.no.	Component	Quantity
1	Arduino Uno	3
2	Fingerprint sensor	1
3	ESP 32 cam	1
4	ESP 8266	2
5	U channel relay	1
6	9v battery	1
7	GPS module	1
8	Jumper Wires	1 set

A. Arduino UNO:

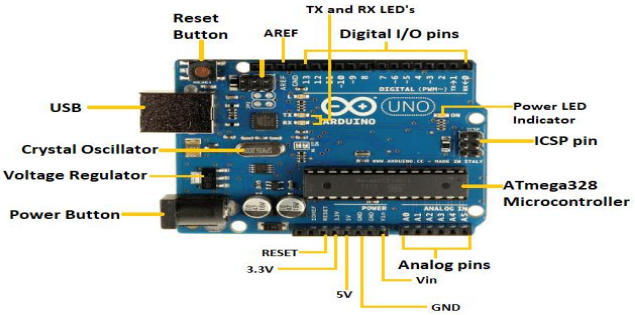

Fig 1. Arduino UNO

The Arduino Uno is a microcontroller board based on the ATmega328P chip, designed and developed by Arduino LLC. It is one of the most popular and widely used development boards in the world of electronics and programming. The board has a simple, user-friendly design that makes it ideal for beginners and advanced users alike.

The Arduino Uno board consists of a microcontroller, a USB interface, and a set of input/output pins. The microcontroller is responsible for processing the code and controlling the board's behavior, while the USB interface is used to connect the board to a computer for programming and power supply. The input/output pins allow users to connect various sensors, motors, and other electronic components to the board.

B. Fingerprint Sensor:

Fig 2. R307 Fingerprint Sensor

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

The R307 fingerprint sensor is a widely used biometric identification module that allows for secure and reliable user authentication. The sensor utilizes advanced algorithms to capture high-quality fingerprint images and accurately match them to stored templates.

The R307 sensor operates on a 3.3V DC power supply and communicates with a microcontroller via UART, making it easy to integrate into a wide range of applications. The sensor features a durable, scratch-resistant glass surface that ensures consistent performance even after extended use.

C. Esp 32 Camera:

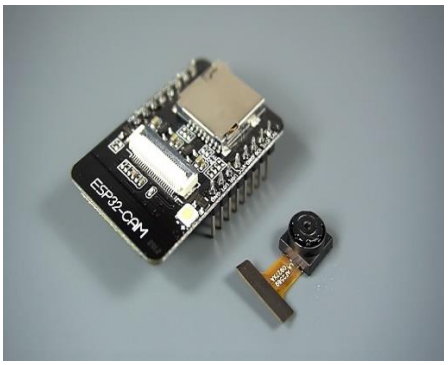

Fig 3. Esp 32 Camera.

ESP32-CAM is a low-cost Wi-Fi enabled camera module based on the ESP32 microcontroller. It is widely used in various DIY projects such as home security systems, surveillance cameras, smart doorbells, and robots. The module comes with an OV2640 camera sensor that can capture images up to 2 megapixels and record videos up to 1080p. It also has a built-in microSD card slot for local storage and supports cloud storage as well.

The ESP32-CAM module has a small form factor, measuring only 27mm x 40mm, making it easy to integrate into any project. It has various pins exposed on the module for connecting external components such as sensors, actuators, and displays. The module also has built-in Wi-Fi and Bluetooth, allowing it to communicate with other devices wirelessly.

D. Esp8266 Wifi Module:

Fig 4. Esp8266 Wifi Module

ESP8266 is a popular low-cost Wi-Fi module that is widely used in the field of Internet of Things (IoT). It is a small-sized chip that is capable of connecting to Wi-Fi networks and can be easily integrated into various IoT devices. The ESP8266 module comes in different variants and is available in the form of a standalone board or as a module that can be integrated with other microcontrollers.

The ESP8266 module is based on the ESP8266EX System on Chip (SoC) from Espressif Systems, which features a 32-bit Tensilica Xtensa LX106 RISC processor clocked at 80MHz. It has 80KB of RAM and 4MB of flash memory for program and data storage. The module supports 802.11b/g/n Wi-Fi protocols and operates in the 2.4GHz frequency range. It also supports various security protocols such as WPA/WPA2 and WEP.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

E. U Channel Relay:

Fig 5. U Channel Relay.

A U channel relay is a type of electromagnetic relay that is designed to be mounted on a printed circuit board (PCB) using a U-shaped channel or bracket. It is also known as a PCB relay, miniature relay or signal relay.

U channel relays are small in size and are commonly used in electronic devices for switching or controlling signals. They consist of a coil, contacts, and a frame that holds the coil and contacts in place. When a current is applied to the coil, it creates a magnetic field that causes the contacts to move and switch the circuit on or off.

F. 9v Battery:

Fig 6. 9V Battery.

A 9V battery is a type of power source commonly used in small electronic devices such as remote controls, smoke detectors, and toys. It is a rectangular-shaped battery that typically measures around 26mm x 48mm x 17mm and has a voltage output of 9 volts.

G. GPS Module:

Fig 7. Neo-6m GPS Module.

At the heart of the module is a GPS chip from U-blox – NEO-6M. The chip measures less than a postage stamp but packs a surprising number of features into its tiny frame.
It can track up to 22 satellites over 50 channels and achieve the industry's highest level of tracking sensitivity i.e., -161 dB, while consuming only 45 mA current.
Unlike other GPS modules, it can perform 5 location updates in a second with 2.5m horizontal position accuracy. The U-blox 6 positioning engine also has a Time-To-First Fix (TTFF) of less than 1 second. One of the best features offered by the chip is Power Save Mode (PSM). This allows a reduction in system power consumption by selectively switching certain parts of the receiver on and off. This dramatically reduces the power consumption of the module to just 11mA making it suitable for power sensitive applications such as GPS wristwatches.

IV. IMPLEMENTATION AND METHODOLOGY

A. Working Procedure:

- Stored fingerprint authentication: The system is first programmed with the owner's fingerprint data, which is stored in its memory. When the owner places their finger on the fingerprint sensor, the system compares the fingerprint data with the stored data. If the fingerprints match, the system allows access, and the vehicle directly ignites.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

- Unregistered fingerprint authentication: If an unregistered fingerprint is placed on the sensor, the system does not grant access and instead asks for permission from the owner. The owner is notified through an app on their mobile device and given the option to grant or deny access.
- Owner's permission: If the owner grants permission, the system stores the unregistered fingerprint as primary in its memory for future access. The system then ignites the vehicle.
- Denial of permission: If the owner denies permission, the system does not grant access and the vehicle does not ignite. The system also 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.

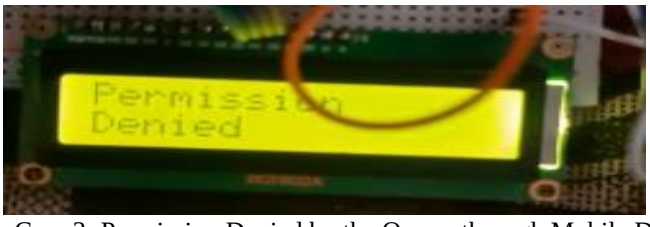

Fig 11. Case 3: Permission Denied by the Owner through Mobile Device.

B. System Hardware:

- Arduino UNO: The Arduino UNO is the main microcontroller that controls the operation of the entire system. It receives inputs from the fingerprint sensor and the GPS/GSM module and sends commands to the ESP32-CAM and ESP8266 modules.
- Fingerprint sensor: The fingerprint sensor is used to authenticate the user and allow access to the vehicle. It captures the user's fingerprint and compares it with the stored fingerprint data to grant access.
- ESP32-CAM: The ESP32-CAM module is used to capture an image of the user's face for further verification. The camera is triggered when the user places their finger on the fingerprint sensor.
- ESP8266: The ESP8266 module is used to communicate with the GPS/GSM module and send location data to the user's mobile device.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

- U-channel relay: The U-channel relay is used to control the ignition of the vehicle. It is connected to the Arduino UNO and is activated only after the user's fingerprint and face are authenticated and their location is verified.
- 9V battery: The 9V battery is used to power the entire system.
- GPS/GSM module: The GPS/GSM module is used to track the location of the vehicle and send location data to the user's mobile device. It is connected to the ESP8266 module for communication with the Arduino UNO.

C. Flow Chart:

- System initialization: Upon power up, the system initializes all components and waits for input.
- User authentication: When the user places their finger on the fingerprint sensor, the system reads the fingerprint and compares it with the stored fingerprint data.
- Registered user: If the user's fingerprint is registered, the system checks the GPS location and confirms that the user is in a designated area. If the user is authorized to access the vehicle, the system sends a signal to the U-channel relay to ignite the vehicle.
- Unregistered user: If the user's fingerprint is not registered, the system prompts the user for permission to add the new fingerprint data to the system. If the owner grants permission, the system stores the new fingerprint data as the primary fingerprint for future authentication.
- Ignition: If the user is authorized, the U-channel relay is activated, and the vehicle is ignited.
- Deactivation: Once the vehicle is started, the system waits for the user to turn off the vehicle. Once the vehicle is turned off, the system is reset and ready for the next user.

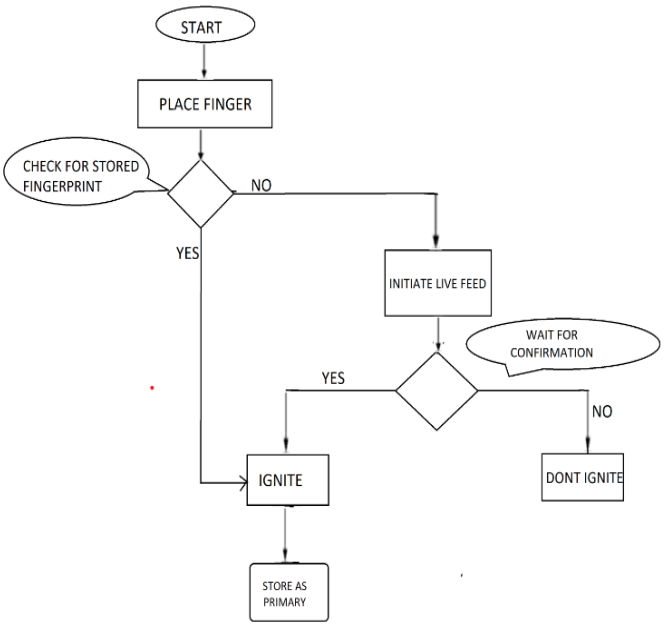

Fig 12. Flow Chart of BIOMETRIC BASED AUTHENTICTAION FOR VEHICLE IGNITION SYSTEM

V. RESULTS

The results of Demo model as well as Real time Implemented Model, including different cases of working are briefly described in this section.

A. DEMO MODEL:

Case 1: Direct access for Owner.

In this case, the system will authenticate the vehicle owner's identity through the stored fingerprint, and if the authentication is successful, the vehicle's ignition system will grant access to the owner. The system will consider as Third Party if the fingerprint does not match or if the stored fingerprint is not available in the system. This case provides a fast and convenient way for the vehicle owner to access the vehicle, without the need for any additional devices or processes. Figure 13 depicts the fingerprint module which is continuously scanning for a finger. Figure 14 shows the owner placing his finger on the fingerprint sensor. Figure 15 shows that the Fingerprint "Match Found" message indicating the authenticity of owner. Figure 16 shows the DC motor (replacement for Vehicle), turning ON.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

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.

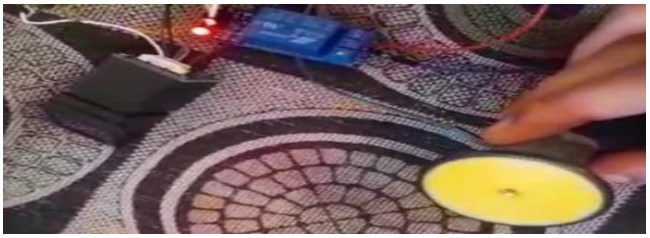

Fig 16. DC motor turned ON.

Case 2: Third Party access.

In this case, when a third party wants to access the vehicle, the system will send a request to the owner's mobile device to authenticate the request. The owner will then have the option to approve or deny the request. If the owner approves the request, the system will authenticate the third party's identity and grant access to the vehicle. If the owner denies the request, the system will deny access to the third party. The implementation of a camera adds an additional layer of security by allowing the owner to visually confirm the identity of the third party. This case provides a more secure way of granting access to the vehicle, by requiring the owner's approval for every third-party request, and by adding an additional layer of visual identification. Figure 17 depicts request sent to owner’s mobile whenever an unknown third party requires access to the vehicle. Figure 18 shows the live feed of the camera. Figure 19 shows the mobile application (Home Automation By Arduino) on the owners device where the owner provides access by sending “Yes” as a confirmation message to the Arduino. Figure 20 depicts the LCD displaying “Access Granted” message. Figure 21 shows the DC motor (replacement for Vehicle), turning ON.

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

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

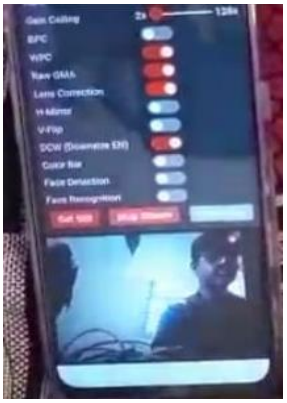

Fig 18. Live feed on owner's mobile.

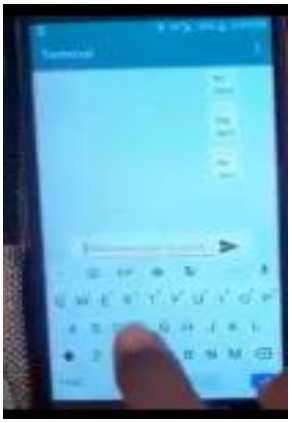

Fig 19. Owner providing Access.

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.

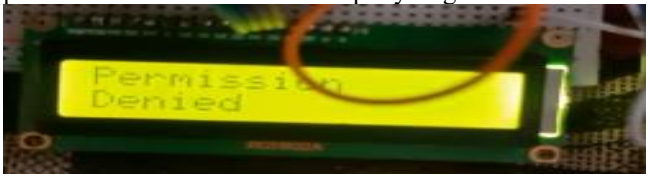

Fig 22. LCD display showing "Permission Denied" message.

Fig 23. Idle DC motor.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10434

B. Real Time Model.

The biometric based authentication for vehicle ignition system model was implemented on a 2-wheeler motorcycle as a real time implementation and the following results were observed:

- When the owner wanted to access the motorcycle, the fingerprint sensor found a match in its stored fingerprints database and the motorcycle engine was ignited.
- When a third party wanted to access the motorcycle, a notification with live feed from the camera was sent to owner's mobile through which the owner was able to either Grant or Deny access.

Figure 24 is the model implemented in the motorcycle.

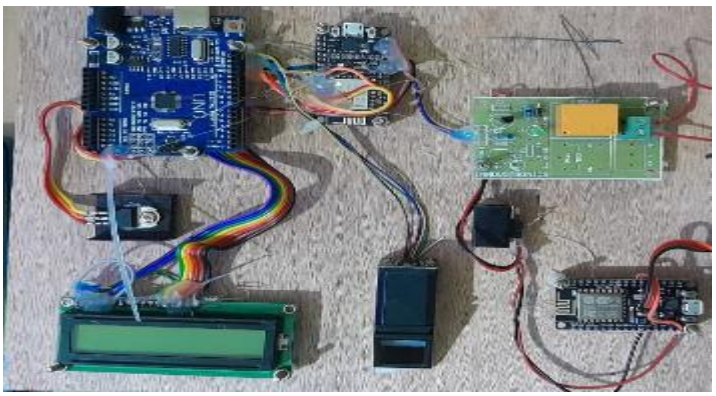

Fig 24. Real Time Implemented Model.

Overall, the biometric-based authentication system for vehicle ignition provides a more secure way of accessing the vehicle, as it relies on unique biometric data to authenticate the identity of the user. It also provides convenience and ease of access to the vehicle owner while maintaining a high level of security.

VI. CONCLUSION

In conclusion, biometric authentication for vehicle ignition is a promising technology that offers several benefits. It can significantly enhance the security of the vehicle, prevent unauthorized access and theft, and improve the user experience by eliminating the need for physical keys or passwords. Biometric authentication systems are becoming increasingly sophisticated and reliable, with many options available, including fingerprint, facial recognition, and voice recognition.

However, it is important to note that biometric authentication for vehicle ignition is not without its limitations and challenges. The technology can be expensive to implement and may require significant changes to the vehicle's design and infrastructure. There are also concerns about the accuracy and reliability of biometric authentication systems, particularly in adverse weather conditions or when users are wearing masks or other facial coverings.

Despite these challenges, biometric authentication for vehicle ignition is a promising technology that has the potential to revolutionize the way we interact with our vehicles. As the technology continues to evolve and improve, we can expect to see more widespread adoption in the automotive industry in the coming years.

A. FUTURE WORK

- Integration with multiple biometric modalities: Currently, most biometric authentication systems for vehicle ignition rely on a single modality, such as fingerprint or facial recognition. However, integrating multiple modalities, such as fingerprint and iris recognition, can improve the accuracy and security of the system.
- Robustness to environmental conditions: Biometric authentication systems can be affected by various environmental conditions, such as changes in lighting or temperature. Future work could focus on developing systems that are robust to these conditions, ensuring that they work reliably in all circumstances.
- Privacy and data security: Biometric data is highly sensitive, and ensuring its privacy and security is crucial. Future work could focus on developing secure storage and transmission methods for biometric data, as well as developing protocols for ensuring that the data is only used for the intended purpose.
- User experience and acceptance: Biometric authentication systems can be inconvenient or uncomfortable for

DOI: 10.17148/IARJSET.2023.10434

users, which can lead to resistance or non-adoption. Future work could focus on improving the user experience and making the systems more user-friendly and accessible.

- Interoperability: Biometric authentication systems for vehicle ignition could benefit from interoperability with other systems, such as those used for access control or payment systems. Future work could focus on developing standards and protocols that enable interoperability between different biometric authentication systems.

REFERENCES

[1] "Authenticated Access Control for Vehicle Ignition System by Drivers 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.