iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57547

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Vehicle Access Authentication and Driver Safety

Prof. Vidyashree. C[1], Prof. Spoorthi P A[2]
[1, 2]*Assistant Professors, Dept.of ECE, Dr. Ambedkar Institute of Technology, Bangalore*

Abstract: ***This paper aims with the rise in vehicle theft cases, the need for reliable anti-theft devices has become crucial. Existing vehicle lock system, including mechanical locks, car alarms, and GPS tracking, have not been able to effectively reduce theft rates. This project proposes an innovative solution using face detection technology to design and develop an advanced vehicle locking system in real time. The system allows the car module to be initiated either through face detection or by sending a status message from a cell phone. Upon receiving the message, the car module verifies user authentication. In the event of unauthorized access, a message will be forwarded to the authorized person or the owner cell phone with their photo, if the authorized person gives the permission then the ignition will be switched on. After the face detection for driver safety purpose the Alcohol content will be checked and the seat belt detection will be done. If the accident occurs while driving a car, then the message will be forwarded to the authorized people with the current location and also to the nearest police stations or to the hospitals.***
Keywords: Raspberry Pi, MEMS sensor, Camera module.

I. INTRODUCTION

In recent times, the rapid increase in the number of vehicles has led to a corresponding rise in car theft attempts, both locally and internationally. The evolution of sophisticated stealing techniques has left vehicle owners increasingly concerned about the security of their valuable assets, whether parked in common lots or outside their homes. As a result, there is a growing need to protect vehicles from theft in today's insecure environment. To address this issue, a real-time vehicle security system based on face detection has emerged as a promising solution. This proposed vehicle security system leverages image processing techniques to enable real-time user authentication using face identification and acknowledgement methods. By integrating a microprocessor-based control system on board with the vehicle, the security system becomes an integral part of car's infrastructure. The system aims to enhance vehicle security by ensuring reliable and efficient user authentication through the utilization of face identification and acknowledgement technologies. By utilizing face identification and acknowledgement algorithms, the proposed system can analyze and authenticate the individuality of the user attempting to access the vehicle. This method provides numerous benifits over traditional methods of vehicle security, such as mechanical locks or car alarms, which is easily circumvented or disabled by skilled thieves. The integration of real-time user authentication based on face detection adds an additional layer of security, making it considerably harder for unauthorized individuals to gain admittance to the vehicle. In summary, the introduction of a real-time vehicle security system based on face detection addresses the pressing need for enhanced vehicle protection in an increasingly insecure environment. By employing image processing techniques and a microprocessor-based control system, the proposed system ensures efficient and reliable user authentication, effectively mitigating the risk of car theft attempts.

II. OBJECTIVE

The objective is to implement a robust authentication system to guarantee that exclusively approved individuals can access and operate the vehicle.

Our primary objective is

1) Ensure Secure Vehicle access
2) Prevent unauthorized Use
3) Enhance Driver Identification
4) Promote Driver Safety
5) Ensure adherence to safety regulations
6) Enable Emergency Assistance
7) Continuous Monitoring and Analysis
8) Collaborate with Law Enforcement

III. PROBLEM STATEMENT

The current state of vehicle access authentication and driver safety represents several pressing concerns require attention. Firstly, the existing authentication measures lack robustness, making it relatively easy for unauthorized individuals to gain access to vehicles, leading to theft and unauthorized use. Additionally, the reliance on digital authentication methods leaves vehicles vulnerable to hacking and cyberattacks, exposing drivers to significant safety risks. Moreover, driver identification methods are often inaccurate and unreliable, resulting in access issues and potential safety concerns. Insufficient driver safety features and non-compliance with safety regulations further contribute to increased risks of accidents and compromised driver safety. Furthermore, the integration of emergency assistance services is limited, causing delays in response during accidents or emergencies. Inadequate monitoring and analysis of driver behavior prevent the identification of patterns and potential risks, hindering the advancement of targeted safety measures. Lastly, the absence of collaboration between vehicle access authentication systems and law enforcement agencies undermines effortsto track stolen vehicles, identify suspicious activity, and ensure public safety. Addressing these problems is crucial to enhance vehicleaccess authentication and driver safety, ultimately creating a secure and safe driving environment.

IV. BLOCK DIAGRAM AND DESCRIPTION

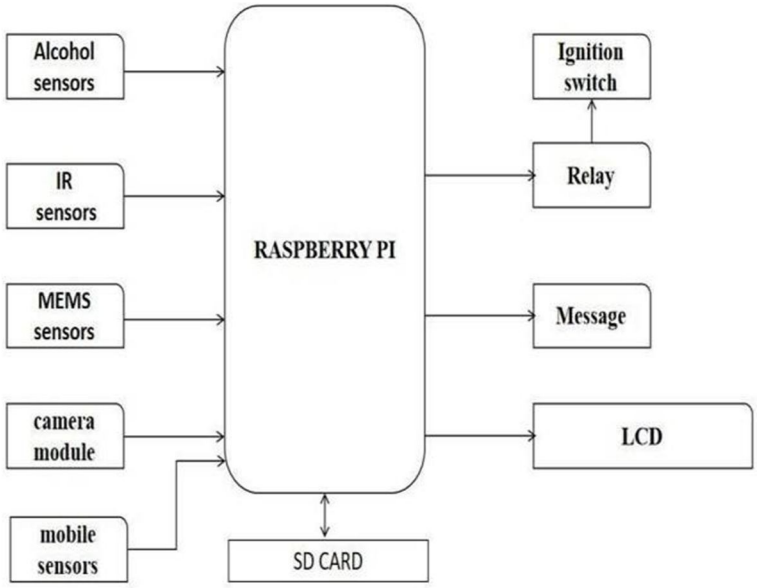


FIG : 1 - Proposed Project Block Diagram

A. Working

1) Step 1: Face Recognition

Face recognition can be utilized as a biometric authentication method to grant access to a vehicle. Instead of traditional key-based entry or keyless fobs, the system can use cameras to capture the driver's face and match it with pre-registered profiles. If the face matches, the vehicle can be unlocked and started, ensuring that only authorized individuals can gain access to the vehicle.

2) Step 2: Seat Belt Selection

IR Sensor is used to identify the seatbelt wearing. We can detect whether the driver is wearing is wearing the seatbelt or not using the IR sensor which consists of Transmitter and Receiver. The Transmitter emits the radiations when these radiations are reflected to the Receiver, it makes sense of the obstacle present in front of sensor by using this seatbelt position can be detected.

3) Step 3: Alcohol Detection

MQ-3 gas detector (alcohol sensor) is used to identify the alcohol content from the breath of the driver. It can be placed just below the face defend so that it can sense it easily. If the driver is drunken, then the resistance value drops which leads to the sudden change in voltage value, then this value transfers to the microcontroller and it prevents from the ignition of the car under this case.

4) Step 4: Accident Detection

Next is to detect the location of the driver in case of emergency using the MEMS sensor which is more stimulus to the vehicle whichwill make the detection of the location in case of accident, here it is mainly depends on the potential difference of the capacitor platespresent inside the MEMS sensor.

B. Hardware Requirements

1) Raspberry pi
2) SD card
3) Alcohol sensors
4) IR sensor
5) MEMS sensor
6) Camera module
7) Mobile sensor

C. Software Requirements

1) Python software
2) VNC viewer

V. HARDWARE AND SOFTWARE REQUIREMENTS

A. Software Analysis

1) Face recognition
2) Seat belt selection
3) Alcohol detection
4) Accident detection

VI. HARDWARE AND SOFTWARE IMPLEMENTATION

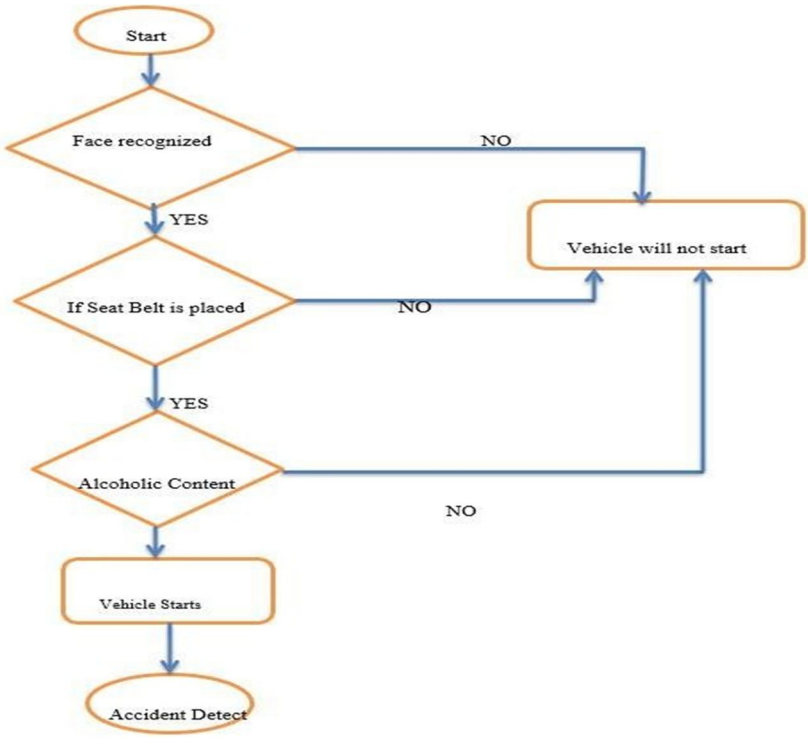


FIG :2-FLOWCHART

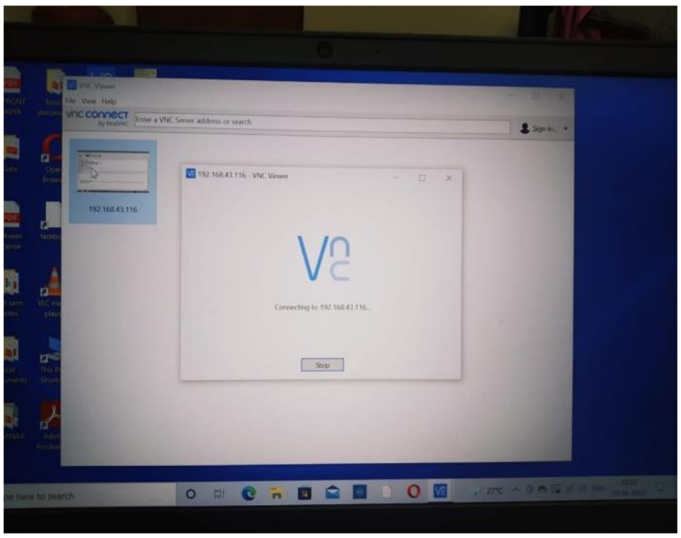


Fig:3-VNC Viewer

Aided by VNC viewer and Wi-Fi, the raspberry pi's display is displayed on the computer screen Steps for configuring a Raspberry Pi over Wi-Fi *a)* Set up the OS on your SD card.

1) Download: Ssh & WPA-Supplicant
2) Edit the Name and Password of your Wi-Fi Router in Wpa-Supplicant.
3) Then copy additional documents into your SD card.
4) Connect a 5V charger to your Raspberry Pi and insert a Micro-SD card.
5) Open your router and load a page in your browser.
6) You can find the Raspberry Pi IP address.
7) Copy this IP address and any subsequent ones in VNC viewer.
8) Press open to visit the open command window after that. Therein Type Raspberry Pi Login & Password.
9) Following that, launch Terminal Server Access from the start menu.
10) Click Connect after specifying the IP address of the Raspberry Pi.
11) On this website, kindly provide your username and password. Pi is the user name, while raspberry is the password.
12) The Raspberry Pi Screen may now be viewed on a laptop.

A. Hardware Setup

The concept of hardware architecture for machine learning based to text to speech conversion is shown in below figure.

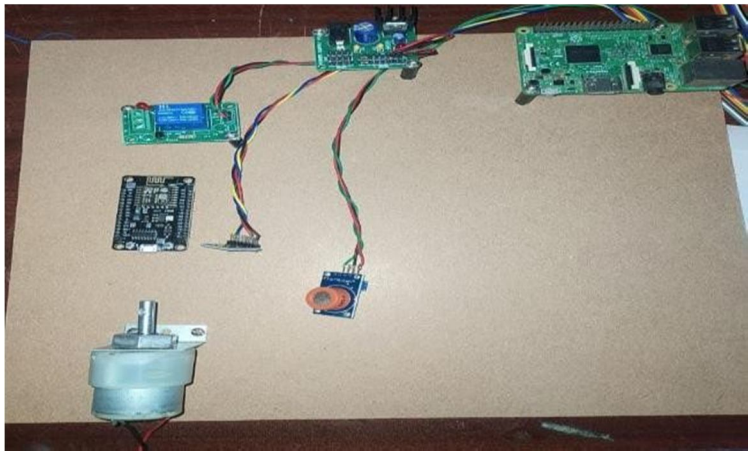


FIG:4-Hardware Setup

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

VII. ADVANTAGES AND APPLICATIONS

A. *Advantages*

1) Vehicle accessing using the face and fingerprint as aprimary factor reduces the theft of the vehicles.
2) The authorized or non-permissible driver cannot accessthe vehicle without informing the owner
3) The location of the vehicle is tracked using the accelerometer so that the accidents also detected easily using GSM.
4) The driver safety is ensured here to make use of the seat belt, without wearing the seatbelt there will be continuous alarming in thevehicle and ignition will not on.
5) The life of the person will be more secures because of the driver safety measures in the vehicle.

B. *Applications*

1) Keyless Entry System.
2) Biometric Authentication.
3) Driver Monitoring Systems.
4) Advanced Driver Assistance System.
5) Vehicle-to-Vehicle Communication.
6) Emergency Response Systems.

VIII. RESULTS AND OUTPUT ANALYSIS

Implementing vehicle access authentication and driver safety measures can lead to a range of positive outcomes. Firstly, it enhances overall vehicle security by employing methodology such as keyless entry or biometric recognition, ensuring that exclusively approved individuals can access and operate the vehicle. This effectively reduces the risk of theft or unauthorized use, giving peace of mind for vehicle owners. Additionally, these authentication mechanisms effectively prevent unauthorized access to vehicles, acting as a deterrent against theft, vandalism, and joyriding incidents. By implementing robust access authentication systems, the incidence of car theft can be significantly reduced, resulting in lower financial losses for vehicle owners and insurance companies alike.
Furthermore, driver safety is greatly improved through the implementation of driver monitoring systems and other safety technologies. These systems track driver behavior, detect signs of fatigue or distraction, and provide real-time feedback to promote safe driving practices. By increasing driver accountability, such technologies contribute to a decrease in accidents, injuries, and fatalities on the road.

IX. CONCLUSION AND FUTURE SCOPE

A. *Conclusion*

In conclusion, the importance of vehicle access authentication and driver safety cannot be overstated. The existing challenges and issues surrounding these areas pose significant risks to both vehicle owners and the general public. However, by implementing robust authentication measures, enhancing driver identification technologies, and integrating advanced safety features, we can create a safer and more secure driving environment. It is imperative to prioritize the development and implementation of comprehensive driver safety measures, including monitoring systems, compliance enforcement, and emergency assistance integration. Furthermore, collaboration between vehicle access authentication systems and law enforcement agencies is essential to combat theft, track stolen vehicles, and ensure public safety. By addressing these problems and working towards innovative solutions, we can significantly reduce the risks associated with unauthorized vehicle access and promote driver safety, leading to a more secure and protected transportation ecosystem for all.

B. *Future Scope*

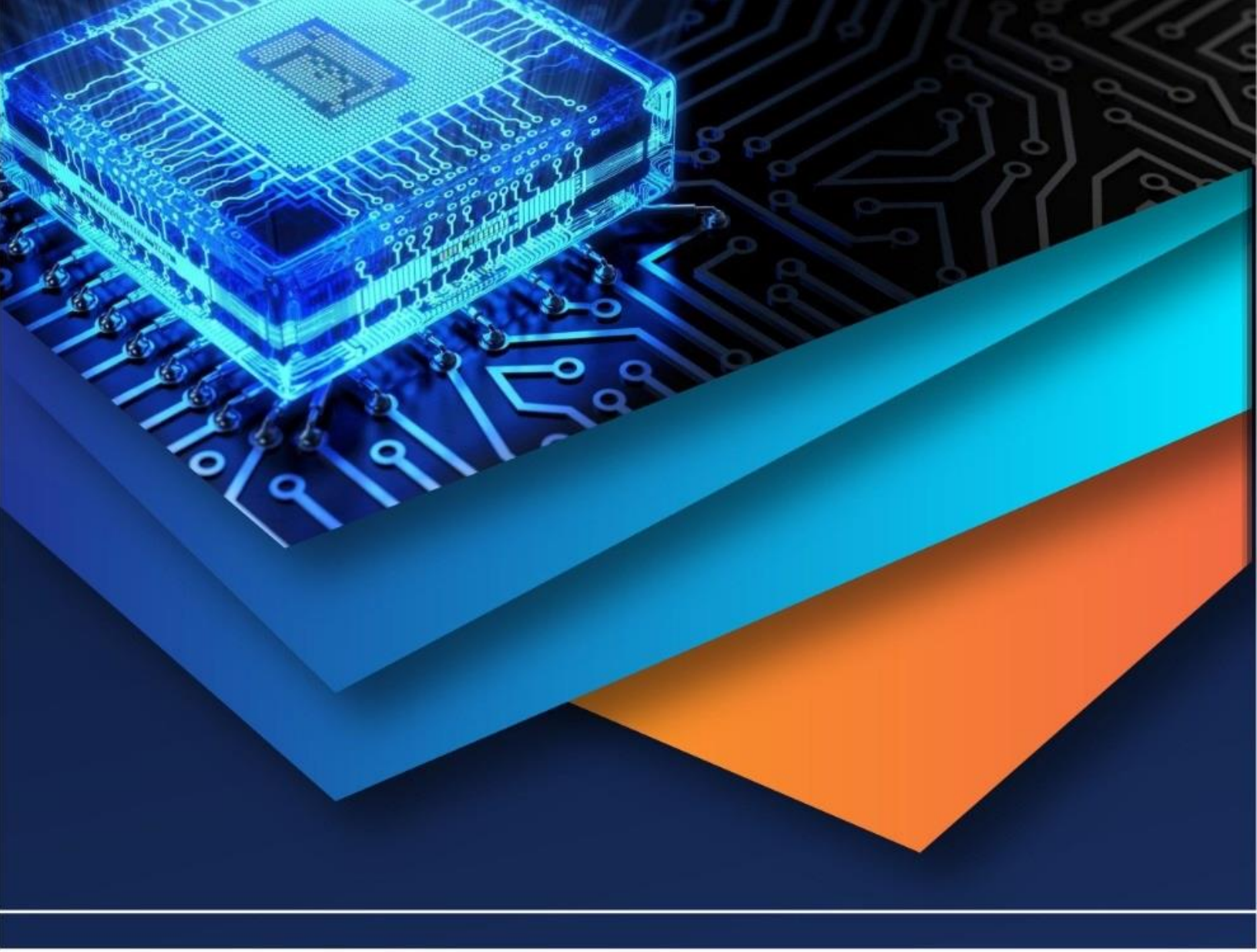
The future presents a wide range of possibilities for the evolution of vehicle access authentication and driver safety, offering innovative solutions to enhance security and protect drivers. Here are some crucial regions of future scope:

1) *Advanced Biometric Technologies:* Ongoing advancements in biometrics, such as facial recognition, fingerprint scanning, and voice recognition, will continue to improve accuracy and reliability in driver identification. These technologies will play a significant role in strengthening vehicle access authentication.
2) *Blockchain-Based Authentication:* Blockchain technology holds promise to secure and decentralized vehicle access authentication. By utilizing blockchain, access permissions can be stored in a tamper-proof and transparent manner, reducing the risk of unauthorizedaccess and enhancing overall security.

3) *Enhanced Driver Monitoring Systems:* Future developments will focus on more advanced driver monitoring systems, utilizing artificial intelligence and machine learning algorithms. These systems will be capable of detecting driver fatigue, distraction, and impaired driving, providing real-time alerts and interventions to prevent accidents.
4) *Vehicle-to-Vehicle (V2V) Communication:* Improved V2V communication will enable vehicles to share vital safety information, such as collision warnings and road hazard alerts, enhancing overall driver safety. This collaborative exchange of data between vehicles will contribute to accident prevention and safer driving practices.

REFERENCES

[1] Yan, R.; Dunnett, S.J.; Jackson, L.M. Model-Based Research for Aiding Decision-Making During the Design and Operation ofMulti-Load Automated Guided Vehicle Systems. Reliab. Eng. Syst. Saf. 2022, 219, 108264
[2] Daohua, W.; Debiao, L.; Tao, T. Qualitative and Quantitative Safety Evaluation of Train Control Systems (CTCS) with Stochastic Colored Petri Nets. IEEE Trans. Intell. Transp. Syst. 2022, 23, 10223–10238
[3] Ying, X.; Bernieri, G.; Conti, M. Covert Channel-Based Transmitter Authentication in Controller Area Networks. IEEE Trans.Dependable Secur. Comput. 2022, 19, 2665–2679.
[4] Xiao, L.; Lu, X.; Xu, T. Reinforcement Learning-Based Physical-Layer Authentication for Controller Area Networks. IEEE,Trans. Inf. Forensics Secur. 2021, 16, 2535–2547.
[5] Aliwa, E.; Rana, O.; Perera, C. Cyberattacks and Countermeasures for In-Vehicle Networks. ACM Comput. Surv. 2021, 54, 1-37
[6] Hartzell, S.; Stubel, C.; Bonaci, T. Security Analysis of an Automobile Controller Area Network Bus. IEEE Potentials 2020, 39,19–24.
[7] Hawra Al Said ;Lina Alkhatib ; Aqeela Aloraidh ; Shoaa Alhaidar , “Smart Glasses for Blind people”, Spring 2018/2019



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY