Facial and Voice Based Vehicle Security System Using ML and IOT

CH. Swapna[1], A. Ranadheer[2], A. Pranav[3], CH. Akhil[4]
[1]*Assistant Professor, Department of Electronics and Communication Engineering, TKR College of Engineering and Technology.*
[2,3,4] *UG Scholars, Department of Electronics and communication Engineering*
TKR College of Engineering and Technology.

***Abstract*- This paper presents the design and development of a smart vehicle locking system combining facial recognition and voice commands for enhanced security and ease of use. A laptop handles image processing and machine learning to identify authorized users via the built-in camera. An ESP32 microcontroller supports Bluetooth-based voice recognition and real-time GPS tracking. The Blynk IoT platform enables remote monitoring and control. Once a face is recognized, the user can lock or unlock the vehicle through authenticated voice commands. GPS data from the ESP32 provides location tracking. This dual-authentication approach improves vehicle safety through machine learning accuracy and hands-free operation. Integrating technologies like image processing, ML, Bluetooth, and IoT, the system offers a comprehensive and practical security solution for vehicles, suitable for fleet management and smart transport systems.**

***Keywords*- Facial Recognition, Voice Authentication, ESP32, IoT, Vehicle Security, Blynk, Machine Learning, GPS**

I.INTRODUCTION

In today's world, vehicle security has become a growing concern due to the rise in thefts and system hacking. Traditional safety methods like mechanical locks and alarms are no longer sufficient against modern threats. To address this issue, an advanced vehicle security system has been developed using facial recognition, voice authentication, machine learning, and Internet of Things (IoT) technologies.

The system offers multi-layered biometric authentication, allowing only authorized users to access and start the vehicle. It uses facial recognition to capture and verify the identity of the person attempting to start the vehicle. If the individual is not recognized, an alert with their image and the vehicle's location is sent to the owner. Additionally, voice recognition acts as a second layer of security. Authorized users must speak a pre-recorded command, making it difficult for intruders to bypass the system.

IoT integration enables real-time communication between the vehicle and the owner via a mobile app. The app allows users to monitor the vehicle's location, receive alerts about unauthorized access, and remotely control actions like locking, unlocking, or even stopping the engine. This constant connectivity ensures the owner remains informed and in control at all times.

Machine learning further enhances the system by learning user behaviours and identifying unusual patterns. If the vehicle is accessed at an odd time or location, the system quickly notifies the owner, boosting security. Real-time GPS tracking and remote monitoring aid in theft prevention and recovery.

In addition to high-level security, the system supports voice commands for in-vehicle control, improving driving safety and convenience. This comprehensive approach, combining biometrics, machine learning, and IoT, delivers a smart and reliable solution to modern vehicle safety needs, ensuring both protection and user comfort.

This system merges advanced biometrics, smart connectivity, and AI-driven learning to offer comprehensive and reliable vehicle protection. With real-time monitoring, alerts, and remote management, it addresses modern security challenges effectively, giving vehicle owners peace of mind and full control over their vehicle's safety—anytime, anywhere.

II.METHODOLOGY

i . EXISTING METHODOLOGY:

Traditional vehicle security mainly depends on keys or simple biometric systems. These methods are

often outdated and easy to bypass by thieves. They usually don't offer real-time tracking to locate the vehicle instantly. Triple-factor authentication, which boosts security, is missing in most cases. Without multiple layers of verification, vehicles are more vulnerable. Basic systems also lack proper integration with IoT technologies. This means users can't remotely monitor or control their vehicle easily. In emergencies, quick remote access and control can be crucial but are unavailable. Because of these gaps, the risk of vehicle theft or misuse increases. Modern systems need smarter, connected solutions for better protection.

ii. PROPOSED METHODOLOGY:

This advanced vehicle security system incorporates facial recognition and voice command features to ensure secure and convenient access. By integrating modern technologies, the system enhances protection and usability. It employs machine learning algorithms to improve the accuracy and speed of biometric authentication, allowing the system to learn and adapt to user behaviour over time. The core hardware component used is the ESP32 microcontroller, which plays a dual role in the system. Firstly, it processes the user's voice for recognition, enabling voice-based vehicle unlocking. Secondly, it supports GPS functionality to track the vehicle's location in real time.

All critical data, including access attempts and location details, are communicated to the user via a mobile application. This app is developed using the Blynk IoT platform, making it user-friendly and accessible from anywhere with an internet connection. Through the app, users can actively monitor the status of their vehicle and perform remote functions such as locking or unlocking the vehicle, receiving alerts, or tracking its movement. The real-time connectivity and responsiveness of the system offer peace of mind and greater control to the user.

By combining facial recognition, voice authentication, GPS tracking, and IoT-based remote access, the system delivers a smart, secure, and practical solution for modern vehicle safety. It brings a new level of intelligence and convenience to vehicle security.

III.IMPLEMENTED DESIGN

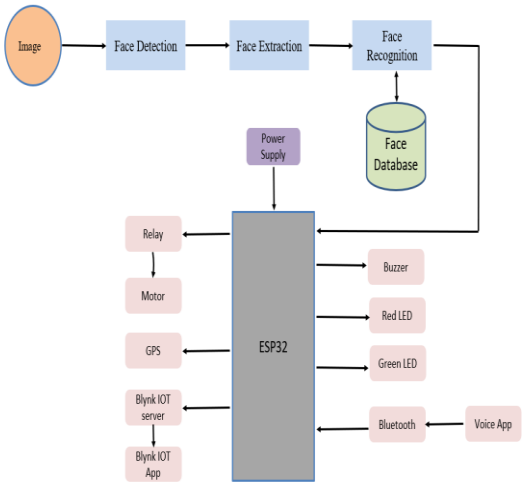

Fig1: Block Diagram

This project utilizes the ESP32 microcontroller as the central unit responsible for managing all system operations. The ESP32 is an advanced microcontroller featuring built-in Wi-Fi and Bluetooth capabilities, making it highly suitable for IoT-based vehicle security systems. It interfaces with various components such as a GPS module, Bluetooth module, relay, DC motor, buzzer, LEDs, and the Blynk IoT platform. All input and output operations are handled through the ESP32's GPIO pins, and it is powered through a 7805-voltage regulator to maintain a steady 5V supply. The HC-05 Bluetooth module is connected to the ESP32 and is used to receive voice commands from a smartphone. Commands like "start" or "lock" are processed by the ESP32 and translated into appropriate actions. The Neo-6M GPS module provides continuous real-time location data in the form of latitude and longitude, which the ESP32 forwards to the user via the Blynk IoT app over Wi-Fi.

A relay module controls the DC motor, simulating functions such as vehicle ignition or locking. When user verification is successful—such as via facial recognition or voice authentication—the relay activates the motor. A green LED indicates access is granted, while a red LED signals denial or an error. In the event of unauthorized access, a buzzer is triggered to provide an audible alert. The power system uses a barrel jack adapter connected to a 7805-voltage regulator to ensure safe voltage levels. All modules share a common ground to maintain electrical stability. The ESP32 communicates with the Blynk server via Wi-Fi, enabling the user to track GPS data and control the system remotely.

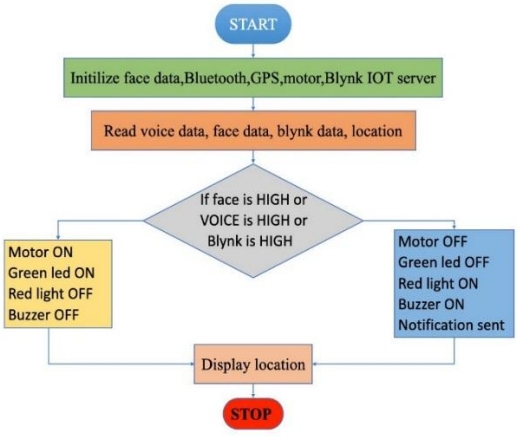

Fig2: Flow Chart

This flowchart illustrates the functioning of a smart vehicle security system. The process begins by initializing key modules: face recognition, Bluetooth, GPS, motor, and the Blynk IoT server. The system then reads data from voice input, facial recognition, Blynk app, and GPS location. It checks if any of the three conditions—face recognition, voice command, or Blynk input—is "HIGH" (true). If any input is valid, the motor is turned ON, the green LED lights up, the red LED remains OFF, and the buzzer is silent. If no input is verified, access is denied: the motor stays OFF, the red LED turns ON, the buzzer activates, and a notification is sent to the user. Regardless of the result, the system displays the real-time GPS location before stopping, completing the decision-making and response loop.

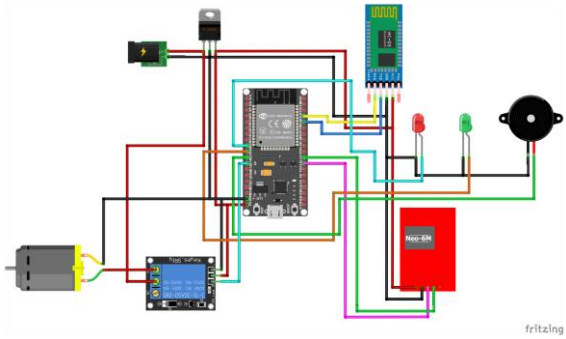

Fig3: Schematic Diagram

This schematic shows a smart vehicle control and security system built around the ESP32 microcontroller. The system integrates several components to enable remote access, real-time tracking, and theft prevention through facial recognition, voice control, and app-based monitoring.

Power is supplied via an external source regulated through a 7805-voltage regulator, ensuring a consistent 5V output for all modules. The ESP32 manages all connections and processes. A Bluetooth module (HC-05) is connected for receiving voice commands wirelessly from a mobile device. A Neo-6M GPS module is interfaced for retrieving the vehicle's location, which is crucial for real-time tracking and is sent to the user through the Blynk IoT platform.

The system includes a relay module that controls a DC motor, simulating an ignition or lock mechanism. The relay receives signals from the ESP32 to switch the motor ON or OFF based on authentication. For security indication, a red LED signals unauthorized access while a green LED confirms approval. A buzzer is triggered during intrusion attempts, providing an audible alert.

All components share a common ground, maintaining electrical consistency. GPIO pins on the ESP32 are assigned to manage inputs and outputs for LEDs, the buzzer, relay, Bluetooth, and GPS modules. The code running on the ESP32 handles data interpretation, comparing it with pre-set thresholds (like face or voice recognition) to decide system actions.

This schematic demonstrates a practical implementation of an IoT-based security solution, combining automation, user interaction, and location tracking to enhance vehicle safety and remote management capabilities.

IV.RESULT

The developed system was tested to evaluate its effectiveness in securing vehicle access through facial recognition and voice authentication. The combination of machine learning and IoT technologies enabled real-time monitoring, accurate user identification, and efficient control of vehicle functions via a mobile application. The system successfully responded to authorized users by activating the motor and granting access, while unauthorized attempts triggered alerts and notifications. GPS tracking was consistently accurate, and remote commands through the Blynk app worked reliably. Overall, the results demonstrate that the proposed system enhances vehicle security through intelligent,

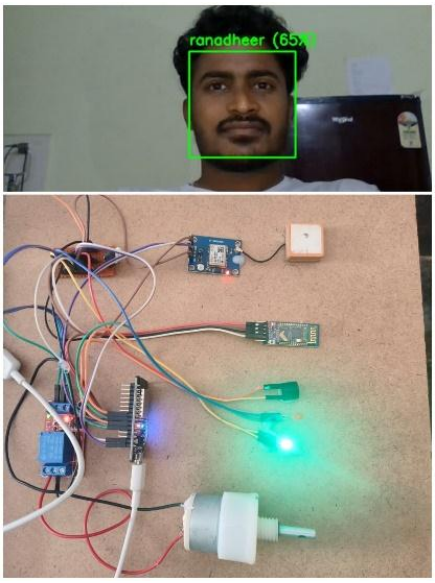

Fig4: Trained face detected and Ignition Activated

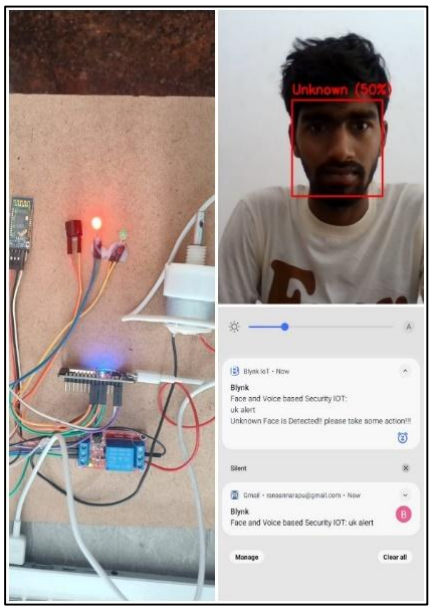

Fig5: Unknown face detected and Alert Triggered

When the system identifies a trained face—one that has already been recorded and approved it activates the ignition, thereby starting the car or device and confirming identity. This guarantees that only approved and recognized people run the system. Conversely, if an unfamiliar face is found that is, the individual is not in the database the system flags it as a possible security concern. In reaction, it activates an alert either a buzzer, a message, or a security notification—and restricted access. By differentiating between authorized and unapproved users, this two-level identification scheme aids in preserving

Fig6: Ignition Is Turned ON Through Voice Command

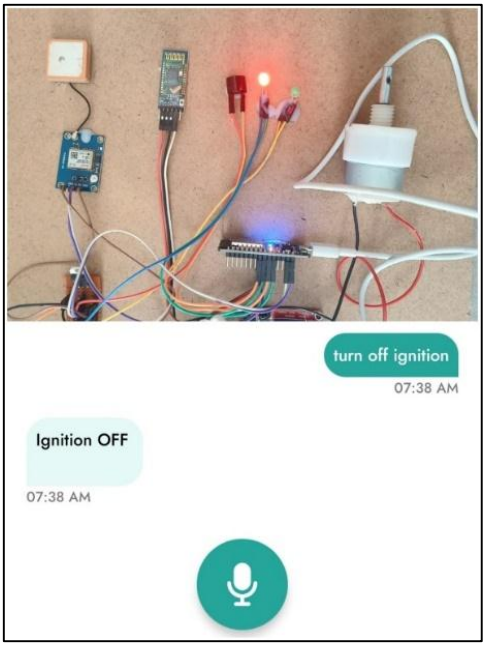

Fig7: Ignition Is Turned OFF Through Voice Command

This voice-controlled ignition system makes that dream a reality. Simply say “turn on ignition,” and the system responds with “Ignition ON,” lighting up a green LED to confirm success. When it’s time to leave, just say “turn off ignition,” and the system acknowledges with “Ignition OFF,” turning off the circuit and displaying a red LED. This innovative technology ensures only authorized voices can operate the ignition, enhancing security and ease of use.

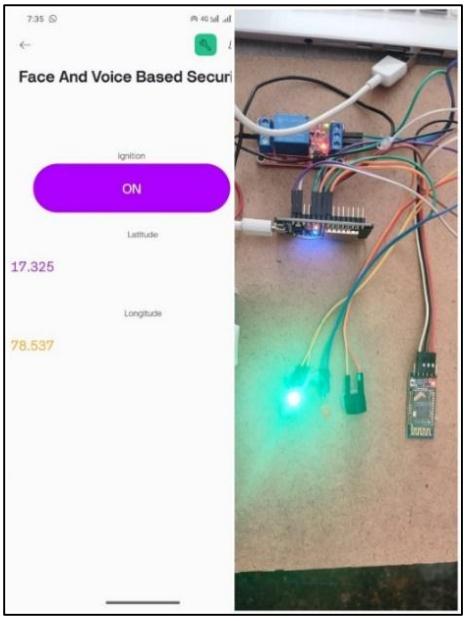

Fig8: Ignition Is Turned ON Through Blynk App

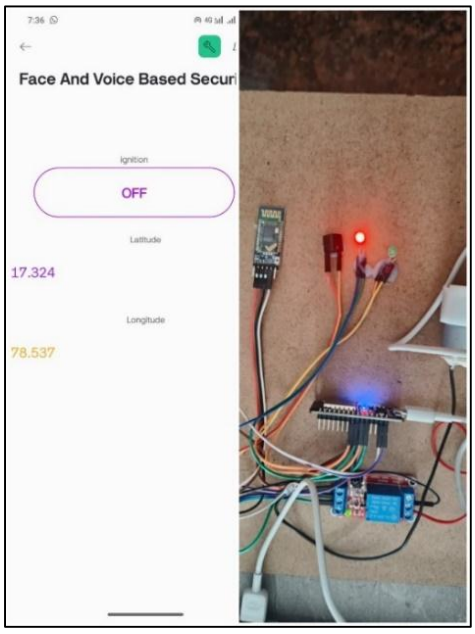

Fig9: Ignition Is Turned OFF Through Blynk App

The Blynk mobile app offers a user-friendly way to control the ignition of systems like cars or security devices. With its intuitive interface, users can easily switch the ignition state by tapping the "ON" and "OFF" buttons. When you press "ON," the app sends a command to the microcontroller, activating the circuit and lighting up a green LED to indicate the ignition is on. Conversely, pressing "OFF" deactivates the circuit, turning the LED red. This remote-control feature, enhanced with face and voice recognition, ensures secure and convenient management of the ignition system, all through intelligent IoT control.

V. CONCLUSION

The Facial and Voice-Based Vehicle Security System integrates machine learning and IoT to enhance vehicle safety. It uses facial recognition and voice authentication to verify the identity of the driver before granting access. This dual biometric system significantly reduces unauthorized usage. IoT connectivity enables real-time monitoring and alerts, providing enhanced control and security. The system logs access attempts, improving traceability and response. Suitable for both personal and commercial use, it offers a modern, reliable solution against vehicle theft. Its intelligent design ensures only authorized users can operate the vehicle, aligning with the growing need for smart, secure transportation systems.

VI. FUTURE SCOPE

- Integration of advanced AI for more predictive security mechanisms.
- Expansion to multi-factor authentication, incorporating more biometric features.
- Development of a more robust IoT platform for better security and data processing.
- Enhanced security protocols for fleet and commercial vehicle management
- Driver Behaviour Monitoring
- GPS and Geo Fencing

REFERENCES

[1] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning, MIT Press, 2016
[2] Richard Szeliski, Computer Vision: Algorithms and Applications, Springer, 2010
[3] Stuart Russell and Peter Norvig, Artificial Intelligence: A Pearson, 2016 Modern Approach,
[4] Rajalingapuram Sridhar, Internet of Things (IoT) in 5G Mobile Technologies, Springer, 2021.
[5] Dey Nilanjan, Ashour Amira, and Balas Valentina Emilia, Smart Medical Data Sensing and IoT Systems Design, Academic Press, 2020.
[6] Sebastian Raschka and Vahid Mirjalili, Python Machine Publishing, 2019 Learning, Packt.
[7] Trevor Hastie, Robert Tibshirani, and Jerome Friedman, The Elements of Statistical Learning, Springer, 2009

[8] Mohamed Elhoseny and Ammar Alazab, Cybersecurity and Secure Information Systems, Springer, 2022
[9] Ajay Kumar and David Zhang, Handbook of Multibiometric, Springer, 2006
[10] Shailendra Jain, Internet of Things and Big Data Analytics, Wiley, 2019
[11] Franc Solina, Advances in Biometrics, Springer, 2007 ISSN 2456 – 5083 Page 1330 Volume 14 Issue 04 April 2025
[12] F. Javed, M. K. Afzal, M. Sharif, and B. Kim, Internet of Things (IoT) Operating Systems Support, IEEE Communications Surveys & Tutorials, 2018
[13] S. Hochreiter and J. Schmidhuber, Long Short-Term Memory, Computation, 1997 Neural
[14] R. Collobert and J. Weston, A Unified Architecture for NLP, Proceedings of ICML, 2008
[15] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, Gradient-Based Learning Applied to Document Recognition, Proceedings of the IEEE, 1998
[16] Ms.E. Devisri, N. Laharichowdary, M. Mahesh Babu, T. Naveen Kumar, E. Purushotham International Journal of Engineering Technology and Management Sciences Website: ijetms.in Special Issue: 1 Volume No.7 April – 2023 DOI:10.46647/ijetms. 2023.v07si01.020 ISSN: 2581-4621.
[17] B. Ajay Bhargav1, D. Hari Krishna2, U. Syed Abudhagir2 Mathematical Statistician and Engineering Applications ISSN: 2094-03432326- 9865 in April 2022
[18] Yogeshwar G. Landge, Vaishnavi S. Pandhare International Journal Scientific Research in Science and Technology Print ISSN: 2395-6011 |Online ISSN: 2395-602X (www.ijsrst.com) Doi: https://doi.org/10.32628/IJSRS 2022.
[19] Dr.G. Sirisha[1], K. Shivasai[2], D. Ranjith[3], K. Hitesh, J. Bharath Kumar Facial and Voice Command Based Security System ISSN: 2349- 6002. March 2022.
[20] R F Rahmat1*, M P Loi1, S Faza1, D Arisandi1 and R BudiartoUniversitas Sumatera Utara, Medan, Indonesia College of Computer Science and Information Technology, Albaha University, Albaha, Saudi
[21] Zhao, Yao, et al. Deep Learning-Based Object Detection: A Survey, IEEE Transactions on Neural Networks and Learning Systems, 2019.
[22] Raza, Shahid, et al. Security and Privacy in the Internet of Things: A Survey, IEEE Communications Surveys & Tutorials, 2017