ISSN: 3107-6513

Auto Shield

Ms. Tanvi Kerkar[1], Ms. Vidhi Kotnis[2], Ms. Shravani Malvankar[3], Ms. Maithili Mayekar[4], Mr. P. D. Kate[5], Mrs. S. A. Palav[6]

Student, Yashwantrao Bhonsale Institute of Technology, Sawantwadi, Maharashtra, India[1,2,3,4]

Faculty, Yashwantrao Bhonsale Institute of Technology, Sawantwadi, Maharashtra, India[5,6]

vidhikotnis9@gmail.com, shravanibmalvankar282007@gmail.com, maithllimayekar94@gmail.com

Abstract:
Auto Shield is a smart vehicle anti-theft system that combines Internet of Things (IoT) and Artificial Intelligence (AI) technologies to overcome these limitations. The system is built using a Raspberry Pi along with a camera module, GPS module, and GSM communication. Facial recognition is used to verify whether the person accessing the vehicle is an authorized user. When an unknown face is detected, the system captures the image and sends it along with the real-time vehicle location to the owner using cloud services. If the owner denies access or fails to respond within a specific time, the system silently forwards the information to the nearest police authority. This approach improves security, reduces false alerts, and provides reliable evidence for faster vehicle recovery.

Keywords: Vehicle Anti-Theft System, Internet of Things, Face Recognition, Raspberry Pi, GPS, GSM

I. INTRODUCTION

The rapid growth in vehicle ownership has led to a significant increase in vehicle theft incidents across both urban and rural areas. Traditional security systems such as mechanical locks and audible alarms are no longer sufficient, as they can be easily bypassed using modern tools and techniques. Audible alarms are often ignored by people nearby, reducing their effectiveness.

GPS-based tracking systems have improved vehicle recovery rates by providing location data; however, they do not offer information about who accessed or stole the vehicle. Due to the lack of identity verification, vehicle owners often face delays in taking action, and police investigations become more complex.

Auto Shield is proposed as a smart and intelligent solution that integrates IoT devices, facial recognition technology, and cloud-based communication. By providing real-time alerts along with visual and location evidence, the system ensures faster response, improved security, and better coordination between vehicle owners and authorities.

II. PROBLEM STATEMENT

Despite advancements in vehicle security technologies, vehicle theft remains a major concern. Existing systems fail to verify the identity of unauthorized users and rely heavily on audible alarms that can be disabled or ignored. GPS systems provide only location details without visual evidence, making it difficult to confirm theft.

Additionally, owners often lack instant context, and escalation to police authorities is delayed. Frequent false alarms also reduce trust in security systems. Therefore, there is a need for a smart, silent, and evidence-based vehicle anti-theft system that can verify unauthorized access, provide real-time alerts, and assist in faster recovery.

III. OBJECTIVE OF PROJECT

The main objective of the Auto Shield project is to design and develop a smart and intelligent vehicle anti-theft system using Internet of Things (IoT) and Artificial Intelligence (AI) technologies. The system aims to enhance vehicle security by combining real-time monitoring, identity verification, and automated alert mechanisms.

Another important objective is to reduce false alarms that are common in traditional security systems by using facial recognition to verify authorized users. The project also focuses on

ISSN: 3107-6513

providing real-time vehicle location tracking using GPS technology, which helps vehicle owners monitor their vehicle at all times.

Auto Shield aims to enable quick decision-making by allowing the vehicle owner to approve or deny access through cloud-based communication. In addition, the system is designed to securely store captured images and location data on the cloud for future reference and investigation purposes. A further objective is to ensure silent operation so that the intruder is not alerted, thereby increasing the chances of successful vehicle recovery with the help of police authorities.

IV. FUTURE SCOPE

- Engine immobilization can be added to automatically stop the vehicle after theft confirmation.
- Night-vision or infrared cameras can be integrated to improve facial recognition in low-light conditions.
- Advanced AI-based behaviour analysis can be implemented to detect suspicious activities in advance.
- The system can be extended for fleet management to monitor and secure multiple vehicles simultaneously.
- Integration with smart city surveillance systems can improve theft detection and response time.
- Direct connectivity with law enforcement databases can enable faster investigation and recovery.
- Mobile application enhancements can provide better user control and real-time system monitoring.

V. EXISTING SYSTEM

Current Vehicle Security Solutions:

Mechanical Security Systems

Mechanical locks such as steering and gear locks are used to discourage theft. They are low-cost and simple to use, but experienced thieves can break them easily, making them less reliable for strong protection [1].

Electronic Immobilizers

Immobilizers stop the vehicle from starting without the correct key or code. While they help prevent basic theft, advanced methods like key cloning can still bypass these systems [2].

Audible Alarm Systems

Vehicle alarms produce sound during unauthorized access to alert people nearby. However, these alarms are often ignored or switched off, which reduces their effectiveness in real situations [3].

GPS and Telematics-Based Systems

GPS and telematics systems allow vehicle location tracking and are commonly used in fleet vehicles. Although they provide real-time location data, they do not stop theft and may fail when network signals are weak [4].

VI. LIMITATION

- Facial recognition accuracy depends on proper lighting conditions, image clarity, and correct camera placement inside the vehicle.
- In low-light or night-time conditions, face detection accuracy may reduce.
- The system requires a continuous power supply to operate effectively.
- Reliable internet connectivity is necessary for real-time alerts and cloud communication.
- Network issues may cause delay in sending notifications to the owner or police authorities.
- The initial cost of the system is higher compared to basic alarm-based security systems.
- Regular maintenance and software updates are required to ensure smooth and accurate system performance.

ISSN: 3107-6513

VII. IMPLEMENTATION

Working of Auto Shield System (Step-by-Step)

Step 1: Start
The Auto Shield system starts when the vehicle is powered on and the security system becomes active.

Step 2: System Initialization
All components such as the Raspberry Pi, camera, GPS, GSM, and network connection are initialized and checked to ensure proper functioning.

Step 3: Monitoring Mode
After initialization, the system enters monitoring mode. The camera continuously monitors the vehicle area to detect any human presence.

Step 4: Face Recognition
When a person is detected, the camera captures the image and the system compares the face with stored authorized user images.

Step 5: Alert Owner
The captured image is sent to the vehicle owner with a message asking, do you know this person? The owner can easily answer with **Yes** or **No**.

Step 6: Authorized Access (Yes)
If the owner selects **Yes**, the person is treated as authorized. The system resets and continues monitoring.

Step 7: Tracking and Logging (No)
If the owner selects **No**, the system treats it as unauthorized access. The intruder's image is stored, event data is logged, and continuous GPS location updates are sent to the owner.

Step 8: Alert Police
After confirming theft, the system sends the intruder's details and live GPS location to the police authorities.

Step 9: Reset System
Once the alert process is completed, the system resets itself and prepares for the next operation cycle.

Step 10: Stop
The system stops the current process and remains ready for future monitoring.

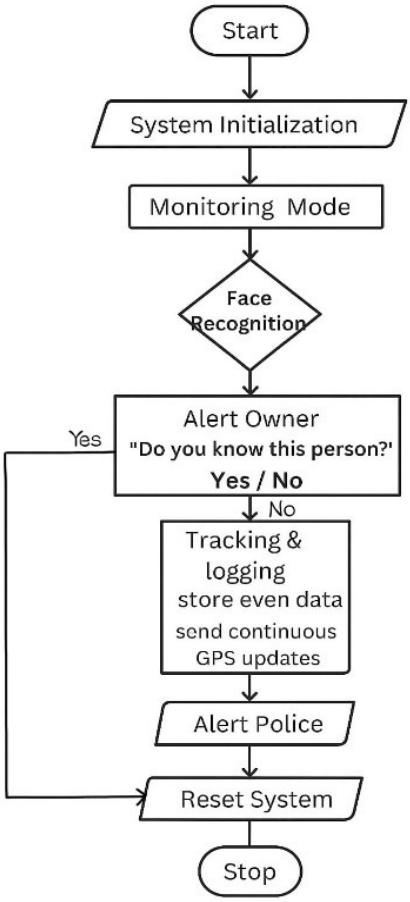

Fig.1 Flow Chart

VIII. CIRCUIT OF AUTO SHIELD

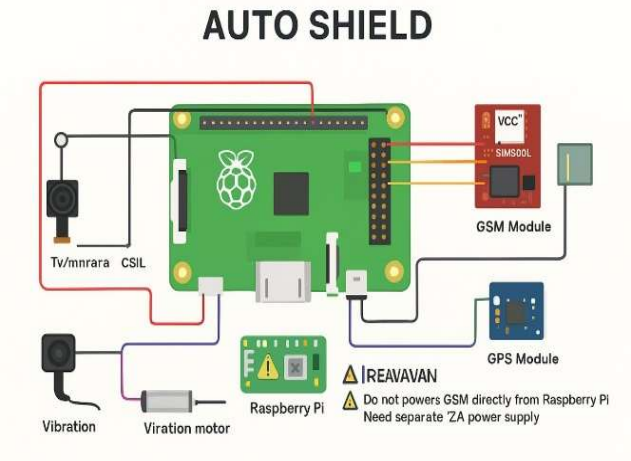

Fig.2 Circuit Diagram

IX. CONCLUSION

Auto Shield provides a smart and reliable solution to vehicle theft by integrating IoT, AI, and cloud technologies. The system not only detects unauthorized access but also verifies identity,

ISSN: **3107-6513**

tracks vehicle location in real time, and enables owner-controlled escalation to authorities. Its silent operation and evidence-based approach make it suitable for modern vehicle security applications and demonstrate the effectiveness of intelligent anti-theft systems.

ACKNOWLEDGEMENT

The authors sincerely express their gratitude to **Mr. P. D. Kate** and **Mrs. S. A. Palav** for their valuable guidance, continuous encouragement, and technical support throughout the development of this project. Their suggestions and insights played an important role in the successful completion of this work. We also thank the Head of the Department and faculty members of the Department of Computer Engineering, Yashwantrao Bhonsale Institute of Technology, for providing the necessary facilities and a supportive academic environment. Finally, we are thankful to our friends and family members for their motivation and support during the project work.

REFERENCES

[1] M. R. Pawar and I. Rizvi,
"Development of an IoT-based embedded system for vehicle security"
in Proc. Second Int. Conf. Inventive Communication and Computational Technologies (ICICCT),
IEEE, 2018.

[2] T. K. Manjunath, A. Samraj Maheswari, and C. Sharmila,
"Locking and unlocking of theft vehicles using CAN,"
in Proc. Int. Conf. Green High Performance Computing,
2013.

[3] S. Shivananda, D. M. Darshan, G. Harish, M. Vinay Kumar, and N. Madhu Kumar,
"Vehicle security system for accident detection, theft prevention and engine locking mechanism,"
Int. J. Creative Res. Thoughts, vol. 12, no. 5, pp. 1136–1140, May 2024.

[4] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan, and V. Patel,
"Exploring the development of an IoT-driven method for vehicle security,"
in Proc. IEEE Int. Symp. Smart Electronic Systems (iSES),
pp. 1–6, 2018.