Anti-Theft System That Sends an Intimation to the Owner to Stop the Engine Remotely
Prashanth. M¹, Rahul Raghavan. V²
Department of Electronics and Communication
CMR Institute of Technology, Bengaluru, Karnataka, India

Abstract:
Increasing rate of crimes like vehicle theft is a major concern these days. This paper aims to use the wireless technology, an end to end IOT based solution, effectively by sending an “Alert of Theft” intimation to the owner of the vehicle. The main scope is to stop the car automatically, that is done whenever a person attempts to steal the car, and an alert would be sent to the authorised user through a mobile application with the image of the person, that will be taken in the car, who is trying to access the car. The owner can send a message, acceptance or denial, back to the microprocessor that is placed in the car and correspondingly action is taken to stop the car. The image captured, of the intruder, will be sent to the database that stores the image. It is from the database where the owner’s mobile app will retrieve the image and display it on the app. The message sent by the owner through the app reaches the database and controls the access to the car.

Keywords: Facial recognition, IOT based end to end solution, Firebase, Python3, OpenCV, mobile application, Kill switch, Raspberry Pi, Pi Camera.

I. INTRODUCTION

An Anti-theft system aims to provide security to all vehicles. The existing accidental alert systems aim to rescue during accidents. The latest security systems integrated with GPS technologies, makes sure that the owner is aware of the status of the vehicle to prevent any illegal access by anyone. These new technologies create new wonders in the security of the vehicle. When the vehicle is accessed by an unauthorized person, it is firstly detected by the facial recognition technology which is implemented on the Raspberry Pi. The system triggers the kill switch and automatically sends an alert or warning signal to the owner through a mobile application which would display the image of the unauthorized person who is trying to access the car. A feature is developed in the app which allows the owner to accept or deny the unauthorized person of the access to the car.

If the owner decides not to allow the person to access the car, then the owner chooses the appropriate option in the app to deny the unauthorized access. The reply from the owner will not deactivate the kill switch and the intruder cannot access the car. If the owner decides to allow access to the person, then the owner chooses the appropriate option in the app. The reply from the owner would deactivate the kill switch and the car can be accessed. A program is developed for this purpose that is implemented on the Raspberry Pi. An effective anti-theft system, an IOT based system, is developed which uses the facial recognition technology, effective database inclusion and connection of the owner application to the database, all integrated to provide an end to end solution.

II. PROPOSED SOLUTION

Security system for vehicles is extremely essential with the alarming increase in crime rate. The aim is to use wireless technology to intimate the owner of the vehicle about any unauthorized or illegal entry. This is done by sending an auto-generated information to the owner. The owner can send back a signal which will stop the vehicle from being driven. An added advantage is that the data of the unauthorized person or intruder, trying to breach the security of the car, stored in the database will be communicated to the police for further security and action. In our system, if an unauthorized user attempts to breach the security of the car, kill switch is triggered and the Raspberry Pi sends a signal to the owner. Our system provides an IOT based end to end security thereby reducing the theft of cars considerably.

For an authorised person, the kill switch is not triggered. For an intruder, the owner receives the signal that an unauthorized person is trying to access the car. The signal received by the owner is an image of the intruder that is displayed in the app. The owner then sends back a signal to activate or deactivate the kill switch by just a click on a button provided in the app. To accomplish this result, a database is used that acts as the intermediate between the Raspberry Pi and the user application. If the owner wishes to provide access to the intruder, the button “START THE CAR” is clicked on the app.

On doing so, the kill switch is deactivated and the person can access the car. If the owner wishes to deny the access to the intruder, the button “STOP THE CAR” is clicked in the app. On doing so, the kill switch remains triggered and the intruder is unable to access the car. Thus, the owner of the vehicle can remotely stop his/her car from an intruder accessing it. This gives our project an edge over the other technologies.

A. Block Diagram-

The entire system is classified into three stages. The first stage is the part that is implemented in the vehicle where there is an interaction of the system with a person who could be an intruder. The second stage in the system is the database that connects the vehicle to the owner of the vehicle. The image
picked up by the camera is added to the database by the processor. The third stage is the part that connects the owner to the entire system. The owner is connected to the database through an application which allows him/her to view the person who is trying to access the vehicle.

The app allows the user to send a message to the database through which the vehicle can be stopped if it is an intruder, trying to access the car. The message sent by the owner happens by a click of a button.

![Figure 1. Block Diagram at the vehicle's end](image1)

![Figure 2. Database that connects the anti-theft system to the owner's app](image2)

![Figure 3. Block Diagram at the owner's end](image3)

### III. EXPERIMENT AND RESULT

Python3 software platform is used to perform the experiment. The experiment is equipped with Raspberry Pi 3 B+ model, interfaced to the firebase. An application is built to retrieve the image from the database at the user’s end.

The proposed solution is tested using the image of the owner as the authorised data. The model is trained to recognize only the owner’s image as the authorised person and unauthorized otherwise. From the test results run, we can draw the conclusion that the anti-theft system using facial recognition provides a high-level security.

### IV. CONCLUSION

The anti-theft security system developed is a reliable and functional real-world product that is used to track an unauthorized entry and improves the security of the vehicle by implementing latest technology, Facial Recognition. The system provides a multistage security involving the owner’s authentication in each entry. With facial recognition as the first stage of authentication, this system provides an edge over the other anti-theft systems. The permission to access the vehicle from an authorised user, being the second stage of authentication, assures the vehicle’s accessibility by a known user. The deexcitation of the kill switch on receiving a negative signal or response from the authorised person provides the third stage of authentication. These multistage authentications prevent the breach in security of the vehicle.

### V. REFERENCE


[5]. Kresimir Delac and Mislav Grgic "Face Recognition" Published by the I-Tech Education and Publishing, Vienna, Austria.

