IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, July 2022

Fingerprint Based Anti-Theft Vehicle Security System

Aditi Ramprasad, P Praveen, Chirag Chengappa M D, R Rohini, S Sujay Kashyap
Department of Electronics & Instrumentation Engineering
JSS Academy of Technical Education, Bengaluru, India
aditirp2000@gmail.com

Abstract: *India has a high population rate and so is the number of automobiles. With the increase in the automobiles comes the increase in their theft and the present systems lack a few parameters which isn't being helpful in dealing with this important concern of the vehicle owner. In this time of taking off vehicle, vehicle security has turned into a question of Prime significance, especially in urban cities, where these incidents take place each and every day. Agents owe this expansion in burglaries to the lack of appropriate parking spots in neighborhood and also absence of accessibility of refined security gadgets. Advancement in technology has been proven to be effective in managing vehicle thefts. There is a need to reduce these burglaries/thefts using the required means for vehicle security. Therefore, anti-theft systems play a vital role in reduction of vehicle thefts. Implementation of biometric anti-theft security system has been operational. In this article, there are a few methods of anti-theft vehicle security systems discussed briefly.*

Keywords: Biometric finger print, anti-theft, embedded computing, arduino UNO, IoT

I. INTRODUCTION

In India, one of the most pressing problems is automobile security. One of the primary difficulties confronting emerging countries is auto theft protection. To preserve and secure the autos, several strategies have been attempted and tested. Embedded computing is a new technology that is being utilised to improve and enhance vehicle security against theft. RFID cards are used to start a car using radiofrequency identification (RFID). The approach, however, failed due to the possibility of losing or stealing the card. Fingerprint recognition is an excellent biometric technique since it allows for precise digital identification. This technology has been widely used to protect automobiles and identity fraud due to its high-speed matching algorithms and quick integration.

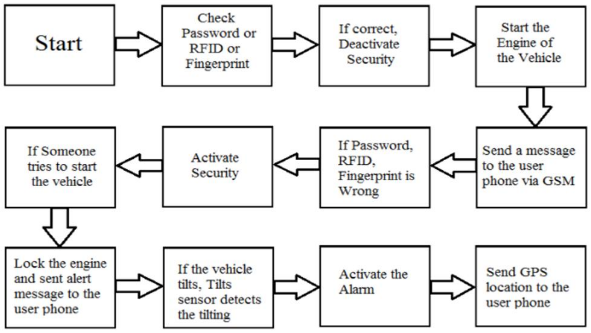

Start
Check Password or RFID or Fingerprint
If correct, Deactivate Security
Start the Engine of the Vehicle
Send a message to the user phone via GSM
If Password, RFID, Fingerprint is Wrong
Activate Security
If Someone tries to start the vehicle
Lock the engine and sent alert message to the user phone
If the vehicle tilts, Tilts sensor detects the tilting
Activate the Alarm
Send GPS location to the user phone

Figure 1: Overview of the anti-theft vehicle security system

The proposed system gives a brief explanation about the biometric security system for controlling of the vehicle theft. The proposed design includes two main cases i.e, when the authenticated input is fed and the next where the owner needs to lend the vehicle to a known individual where the passcode is sent to use the vehicle. The communication to the owner is done using the IOT technology which intimates the owner about the activation of system, matching or unmatching of the input data and aqids in sending the passcode. With the daily increase of Internet of Things (IoT) devices, which have reached tens of billions these days. The use of IoT is growing exponentially and its use can be seen across various fields. There has been a lot of theft of vehicles faced by the automobile owners. Many control methods exists in order to reduce these thefts, but they lack the efficient methodology which includes monitoring and tracking of the automobile. So,

DOI: 10.48175/IJARSCT-5840

designing a system which ensures a high security of the vehicle is a priority. Ultimately the lacking of these essential requirements in the present system has led to the idea of designing of a system which ensures the fulfillment of both of the parameters in order to increase the accuracy and effectiveness of the system. Considering an another fact of increased number in the problem of losing vehicle keys frequently by the owners, has lead to the emergence of the idea of biometric fingerprint scanning to start the vehicle.

II. LITERATURESURVEY

Sadagopan et. al. [1] has proposed a framework on an adversary of theft control system for vehicles. The proposed system uses an embedded chip that has an inductive area sensor. The vicinity sensor recognizes the key during incorporation and sends a text to the proprietor's adaptable communicating that the vehicle is endeavoring to be gotten to. The system present in the vehicle demands that the customer enter a wonderful mystery express. This mystery expression includes many characters and the vehicle key number. If the customer forgets to enter the right mystery word inside three attempts, a text is shipped off the proprietor about the unapproved use. An alert is similarly shipped off the nearby police central command with the vehicle number and the region. The region is followed using a GPS module. Now, the fuel injector of the vehicle is deactivated so the unapproved customer can't start the vehicle utilizing all possible means. This system also joins a secret lock structure that gets ordered and the unapproved customer gets found out inside the vehicle. The proprietor who is furnished with the key should deactivate the secret lock part.

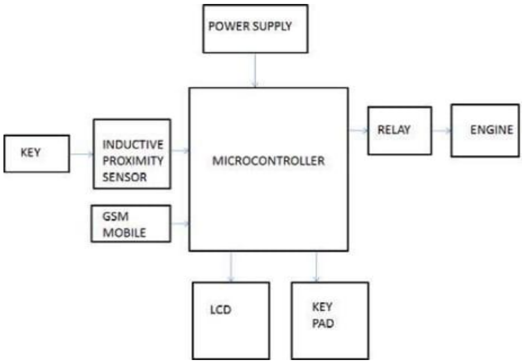


Figure 2: Block diagram explaining the principle of anti-theft control system

Pawar et. al. [2] proposed a framework those discussions about planning and advancement of hostile to robbery with a driver reconnaissance inserted framework.

The proposed framework utilizes biometric validation to get to the vehicle and it contains camera, which catches the picture of an individual attempting to get access of vehicle. The picture is then contrasted and the picture of the proprietor of the vehicle. If the picture coordinates, the admittance to the vehicle is permitted or, in all likelihood the entrance is denied. If there should arise an occurrence of disavowal of vehicle access or even a mishap, camera will catch the images. The pictures are then shipped off the proprietor or authorizer through email. This will help in the reconnaissance of driver and furthermore the vehicle. The framework is worked with the assistance of raspberry pi, high-goal camera, vibration sensor and open source programming.

Manjunath et. al. [3] Has proposed a model that uses a phone, which is introduced in the vehicle. It is spoken with Engine Control Module (ECM) through Control Area Network (CAN) Bus. The vehicle being taken can be recognized and ended by using GPS remember for the cell. The owner of the vehicle for future dealing with uses this information. The owner sends the message to the compact, which is introduced in the vehicle that has been taken. This hence controls the vehicle's engine by locking the working of the engine immediately. The made system recognizes the message and broadcasts it to the Vehicle network through CAN Bus. Yet again the owner can open the engine, by sending the message.

Mukhopadhyay et. al. [4] has proposed a unique security structure maintained with distant correspondence and an insignificant cost Bluetooth module. A GSM module is utilized for sending messages. The client can manage the motor/start and switch it off if fundamental. The construction also utilizes a secret word through keypad (with most unbelievable 3 possibilities) which controls the farewell of a security amassing entryway truly wearing a seat lash. Tolerating there is a window interloper, the IR module/sensor sees the intruder, or any obstacle and it gives a message to

DOI: 10.48175/IJARSCT-5840

the more modest than typical regulator. The regulator is connected with a Bluetooth module and to an alarm. The System sends an alert sign to the customer's convenient. The model moreover gives an answer for the matter like Towing. Thusly, the system uses Bluetooth module and controller to manage the security structure from the customer's mobile through any contraption with a potential Internet affiliation.

Ramadan et. al. [5] have proposed a technique on a proficient auto security system, implemented for against burglary, utilizing an installed framework busy with a Global Positioning System (GPS) and a Global System of Mobile (GSM). The customer works together through this method with vehicles and picks their present districts and standing using Google Earth. Utilizing GPS finder, the true's current locale is picked and sent, close by various limits got by vehicle's information port, through Short Message Service (SMS) through GSM relationship to a GSM modem that is connected with PC or PC. The GPS puts together are rectified using a discrete Kaman channel. To get the vehicle, the customer or a great deal of customers can stop for the day vehicle of the armada assuming any intruders endeavour and show it to hindering the gas dealing with line. The proposed structure is incomprehensibly ensured and successful to report emergencies, for instance, crash declaring or gear disillusionment.

Jesudoss ET. al. [6] has proposed a model whose principle point is to plan a brilliant head protector for liquor recognition and mishap aversion. The IR sensor checks in the event that the individual is wearing the cap or not. The Gas sensor detects the alcoholic substance in the rider's breath. In the event that the individual is smashed and not wearing a head protector, the bicycle won't begin. On the off chance that there's no sign of alcoholic substance present and cap is used, only the bike will start. In case of an incident, the sensor sees the condition of the motorbike and reports the disaster. Then, the GPS inside the bike will send what is happening of the accident spot to guideline server of the nearby crisis centres.

III. METHODOLOGY

A method is proposed for putting the vehicle in motion using a fingerprint control. All past work relating to fingerprint biometric security acts on the ignition system. This security mechanism, however, is easily circumvented. Direct manipulation of the ignition wires kept behind the wheel takes less effort to start the car. Rather of protecting ignition, we've implemented a security feature that allows only fingerprint-authenticated individuals to start the vehicle. Fingerprint authentication is performed using the R307 sensor module. Fingerprint Enrolment/Addition and Fingerprint Recognition are the two sub modules of the Fingerprint Sensor Module. The fingerprint enrolment/addition module enrolls and stores all users who are permitted to operate the vehicle. This sub-module allows legitimate users' fingerprints to be enrolled in the database. The Fingerprint Module R307 sensor contains a micro switch with three buttons to help with enrolling. The first button is used to collect the fingerprint's 3D image. The other two options are for adding and removing fingerprints from the database. The input fingerprint is compared to one or more templates in the database by the fingerprint matching sub-module. Pattern matching and minutiae-based matching are the fingerprint matching approaches employed. Before a user can operate a vehicle, his or her fingerprint is compared to one in the database. The signals from the fingerprint sensor Module R307 are sent to the Arduino Uno board's microprocessor ATtmega328. The microcontroller sends the desired signal to start the car once the scanned fingerprint matches the one stored in the database. The state of the system is displayed on an LCD display. It also shows when fingerprints are being added, erased, or when authentication is successful.

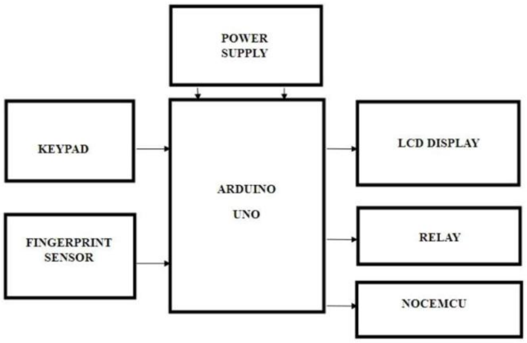


Figure 3: Block diagram of the proposed system

DOI: 10.48175/IJARSCT-5840

- The Arduino is used as the microcontroller board for processing the input signal. It reads the state of input, which can be 0 or 1.
- Input is fed to the system with the help of fingerprint sensor.
- When the input fingerprint is given the Arduino reads the state of input.
- If the fingerprint matches with the preset one then the ignition will be turned on.
- In case of mismatch of the fingerprint, the system asks for an authentication from the owner(pin).
- Once the authentication is given Arduino sends a signal to the relay which in turn initiates the ignition to start the vehicle.

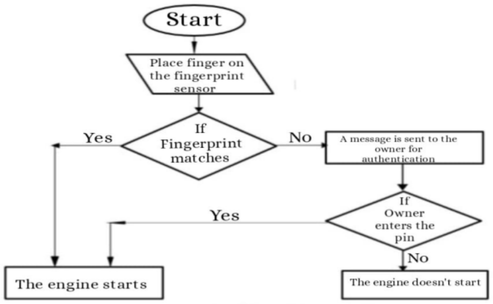


Figure 4: Flowchart of the proposed system

IV. TESTS AND RESULTS

Step 1: When the Fingerprint-based Anti-Theft Vehicle Security System is activated there is a message sent to the owner of the vehicle the following are the pictures of the activated system.

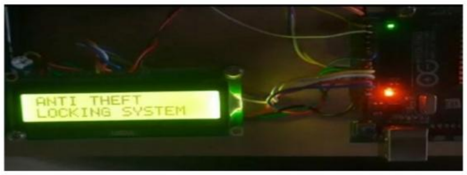


Fig.A: Activation of system

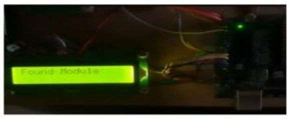


Fig.B: WiFi module connected

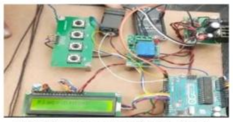
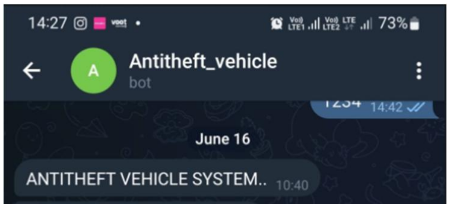


Fig.C: System asking for an input Fingerprint

Here figure A shows the activation of system message, whereas figure B shows the wifi module connected. Figure C is where the system asks for an input fingerprint by displaying “place a finger”.



14:27 73%

Antitheft_vehicle
bot

14:42

June 16

ANTITHEFT VEHICLE SYSTEM.. 10:40

Fig. D: Message from the circuit system to the phone regarding the activation of the system

A message is also sent to the owner’s mobile regarding the activation of the system.

DOI: 10.48175/IJARSCT-5840

Step 2: Using the fingerprint sensor module, the input is given to the circuit. The resulting test cases that have been satisfied.
Case 1: For when the Fingerprint matches to the one that is stored in the system.
Case 2: For when the Fingerprint do not match.

Test Case Results:
Case 1: When the Fingerprint matches.
When there is a finger placed on the fingerprint module and then if the fingerprint matches the following results are seen.

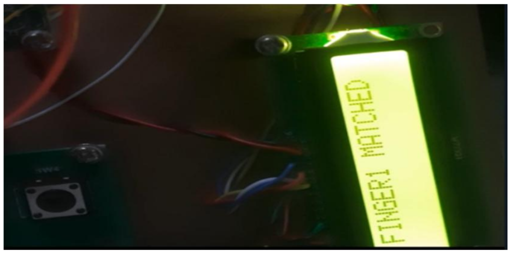


Fig. E: Fingerprint1 matched

Case 2: When the Fingerprint do not match.
When the fingerprint placed on the module is not stored in the system the vehicle asks for the permission from the owner the following results of a finger not match test case.

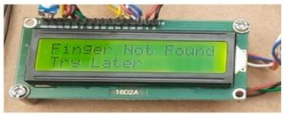
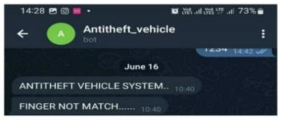


Fig.F: when unregistered finger placed on the module

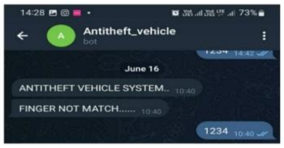


June 16

ANTITHEFT VEHICLE SYSTEM.. 10:40

FINGER NOT MATCH...... 10:40

Fig.G: message from system to the owner



June 16

ANTITHEFT VEHICLE SYSTEM.. 10:40

FINGER NOT MATCH...... 10:40

1234 10:40

Fig.H: passcode sent by the owner to initiate the ignition of vehicle

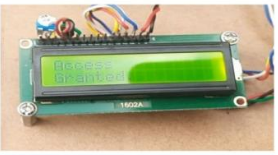


Fig.I: "Access granted" message display as soon as the passcode is sent

If the owner knows the person trying to unlock the vehicle, then the vehicle ignition is initiated by the owner using a passcode from their phone. The above images are the results of the vehicle starting when the ignition is initiated by the owner using their phone.

V. CONCLUSION

The proposed system is pointed towards working fair and square of safety in automobiles. It can be concluded that the theft of the automobiles can be reduced/controlled by making use of methodologies based on IOT and biometric fingerprint technology. The major advantage being the high security and quick intimation to the owners.
Using the fingerprint sensor module the input is given to the circuit. The next step is based on the result of the two cases: if the given input fingerprint matches, the relay in the circuit ignites the spark plug to power up the engine. If the fingerprint doesn't match, a message is sent to the owner indicating that the given input fingerprint doesn't match with the pre-fed input data. Later if the owner wants to grant permission for the usage of vehicle by a third person, he is supposed to send back a password which in-turn starts the engine. The system also consists of LCD display in the circuitry to indicate whether the fingerprint is matched or not.

DOI: 10.48175/IJARSCT-5840

The major application of the project is to reduce the thefts of the automobiles by the advancement of the security system using biometrics. Recent advancements in the field of biometrics for security purpose makes this design commercially possible to implement for real-time usage.

The system accuracy is more due to the biometric (which is unique for an individual and can't be hacked) criteria used for security purpose.

The proposed system is cost effective compared to other systems that are available in the market.

The proposed system can be interfaced with any existing vehicle.

ACKNOWLEDGEMENT

We would like to thank the Principal, Head of the Department, faculty, friends, and parents for their continuous co-operation and support.

REFERENCES

[1]. Sadagopan, Vinoth Kumar, UpendranRajendran, and Albert Joe Francis. "Anti-theft control system design using embedded system." Proceedings of International Conference on Vehicular Electronics and Safety, 2011 IEEE.

[2]. Pawar, Mahesh R., and Imdad Rizvi. "IoT based embedded system for vehicle security and driver surveillance." 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018.

[3]. Manjunath, T. K., Andrews SamrajMaheswari, and Chidaravalli Sharmila. "Locking and Unlocking of Theft Vehicles Using CAN." Proceedings of 2013 International Conference on Green High Performance Computing. 2013.

[4]. Mukhopadhyay, Debajyoti, et al. "An attempt to develop an iot based vehicle security system." 2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS). IEEE, 2018.

[5]. Ramadan, Montaser N., Mohammad A. Al-Khedher, and Sharaf A. Al-Kheder. "Intelligent anti-theft and tracking system for automobiles." International Journal of Machine Learning and Computing 2.1 (2012).

[6]. Jesudoss, A., R. Vybhavi, and B. Anusha. "Design of smart helmet for accident avoidance." 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2019.