# ENHANCEMENT IN IOT BASED CAR DOOR LOCK SYSTEM

**Dr. Abhijit J. Patankar**

Associate Professor, PhD. (CSE)
DY Patil College Of Engineering, Akurdi

**Aman Mulla**

DY Patil College Of Engineering, Akurdi

**Darshan Vilag**

DY Patil College Of Engineering, Akurdi

**Keshav Kumar Thakur**

DY Patil College Of Engineering, Akurdi

**Atharva Sanap**
DY Patil College Of Engineering, Akurdi

**ABSTRACT**
**Identification plays a crucial part in the production of high security in identification-based car door protection systems. Security has become incredibly crucial in today's world to protect our data from unauthorized parties. The main goal of this project is to protect the car from unwanted users by using the unique ID, or fingerprint authentication, as identification. The fingerprint scanner is used to lock and unlock the doors instead of a door security system. The other indicator system is also created by utilizing a GSM module to convey the message to the mobile device of the car owner. The Arduino UNO microcontroller manages the entire system. Arduino is a physics platform supported by simple-to-use hardware and a software package.**

## INTRODUCTION

Security is our first priority in this hectic, competitive world in order to protect our possessions like bank accounts, cars, homes, and other stuff. The general public was abusing association ID numbers and passwords as security, but there are some sneaky ways to open the accounts, for instance, when a door is mounted by the owner and left for another city, unauthorized individuals or thieves may return and unlock the door with duplicate keys. Despite the fact that more security systems were created, hackers increased in number and their collective ability to open door locks using duplicate keys. There are various protection systems designed for automobiles, including traditional and remote systems. Nevertheless, remote protection systems have the disadvantage that anyone can unlock the door.

The only way to protect our possessions is to employ a unique ID, which offers unparalleled protection. Only by abusing the finger print authentication is that extraordinary protection achievable. The finger print authentication plays the primary function for distinctive identification in all areas nowadays. Individual's finger ridges don't line up with the opposing finger ridges. Hence, there is no risk involved in picking the car's lock. And it is difficult to lock or unlock the systems collectively.

A GPS pursuit unit is an additional tool that makes use of the Global Positioning System to determine the precise location of a car, person, or other quality to which it is linked and to record the standard's position over time. The chasing unit retains the captured location data, or it will communicate it to a central location knowledge domain, an internet-connected laptop, or a mobile device (GPRS). This enables the asset's location to be displayed against a map background, either in quantity or after further analysis of the track, using a bespoke package. The primary goal of the project is to protect the car from potential theft. We have a tendency to integrate security by including bio-metrics, such as a fingerprint, in order to fully grasp this.

The car owner should initially store his or her own fingerprint in the finger print module. To send and receive messages to and from the owner, GSM equipment is used. The owner's mobile device should be configured to be mounted during the cryptography. One must input the authorized fingerprint in order to start the hackney's ignition. A notice will be sent to the owner in real time, and the native device will also be prepared to turn on, if someone inputs an unregistered fingerprint. By selecting the GSM equipment that is built into the system, we will all work together to locate the hackney for theft interference. Then a real-time chase starts, and the owner of the vehicle receives an SMS with the vehicle's GPS location. Via system notifications, the ignition of the car may also be controlled.

## OBJECTIVES

To design a lock system that is secure and safe from theft or unauthorized entry. The device is also affordable and simple to install on the vehicles.

To save costs, provide user-friendly systems, and create dependable systems
It is designed in such a way that the average person can easily use it, enjoy using it, and be reasonable to everyone.

**LITERATURE SURVEY**

**1 Paper :** Raspberry pi based biometric authentication vehicle Door locking system
**Author :** N. N. Nagamma, T. Narmada
**Description :** The high security provided by the automobile door locking system that is based on biometric authentication is significantly influenced by the biometric authentication. Today, security is essential for preserving the confidentiality of our data as well as its protection from unauthorized parties. This article's main objective is to protect the car from unwanted users by using finger print identification as a distinctive id. In the location of the car door locking system, a finger print scanner takes the place of the traditional door locking system to lock and unlock the doors.
**2 Paper :** Biometric automobile ignition locking system
**Author :** R. M. Vithlani, Sagar Shingala
**Description :** In remote areas of the city, car theft is a serious problem, and neither a key lock nor a remote keyless system provide trustworthy solutions because keys are very easy to duplicate and the encrypted data used by the remote keyless system uses radio waves that can be recorded and used to unlock the car. The only more favorable option for developing a unique key that doesn't rely on a key or radio wave is biometric solutions. Our objective is to provide biometric solutions using really cheap hardware, free hardware, and self-installable software tools.
**3 Paper :** Enhanced biometric recognition for secure authentication using iris preprocessing and hyperelliptic curve cryptography
**Author :** J. Premalatha. K. Sathya
**Description :** Combining cryptography and biometrics can prevent identity fraud in digital authentication, both theoretically and practically. Biometric traits have been demonstrated to boost security for identifying crimes because of their fascinating properties including precision, stability, and uniqueness. There are still certain limitations, such as longer processing times, poorer accuracy levels, and shorter maximum recognition durations, even though several techniques have been devised to accomplish this goal. To overcome these problems, an enhanced iris recognition method based on hyperelliptic curve cryptography has been suggested (HECC). The optimum features for iris preprocessing are extracted in the proposed study using the 2D Gabor filter approach.

**HARDWARE REQUIREMENT**

Arduino Uno
Fingerprint Scanner
Servo Motor

**SOFTWARE REQUIREMENT**

Python
Arduino software (IDE)

**EXISTING SYSTEM**

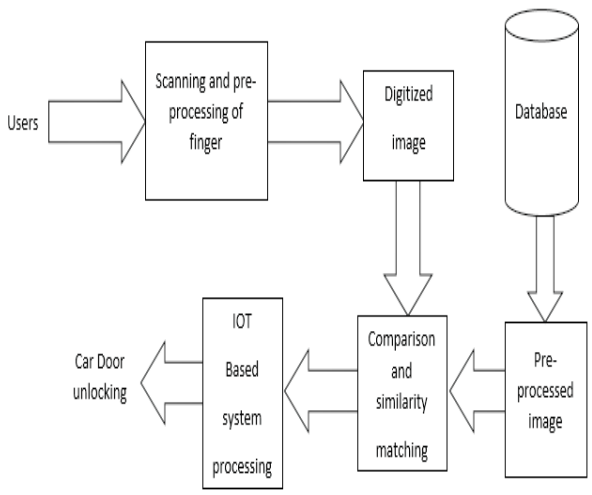
Algorithms are employed in this system for fingerprint enrolment and verification. With the exception of severe burns and profound bodily damage, a person's fingerprint never changes during their lifetime. Associate degree automated pattern recognition software can recognize fingerprints. There are three different types of fundamental phases for fingerprint recognition:
• Data collection: At this phase, the program's knowledge of fingerprints cannot be passed down. The obtained image is stored with information.
• Feature extraction: At this stage, fingerprint options are extracted, so keep an eye on the fine print.
• Matching: At this stage, a decision is made regarding who will provide identification to the World Health Organization in order to access the system.

**ALGORITHM**

The work that has been done so far in the field of fingerprint recognition is based on trivial rules. Ridge ending, bifurcation, and short ridge or dot are the three primary fingerprint ridge alternatives in a trivia-based rule. The trivial base rule relies on inherent discontinuities in the ridge flow pattern, and only a small portion of the finger picture is required for verification. While doing this, we frequently employ two rules: the minutiae-extraction method (for detecting fingerprints) and the minutiae-matching rule (for matching input and information fingerprints). Minutiae-Extraction is made up of three parts: estimation of the oriental field, ridge detection, and trivia detection. We frequently employ a purpose pattern matching rule for minutiae matching. 1. Extracting minutiae The matching of minute patterns is the foundation for fingerprint authentication. Minutiae extraction has these three parts:
• Estimating the orientation field of a fingerprint image: A fingerprint image's orientation field is a representation of its inherent characteristics.
• Ridge extraction: The important characteristic of ridges in fingerprint images is that on ridges, the grey-level values reached their local maxima in the direction from normal to a local ridge orientation. The ridges are thinned in this.
Extraction and post-processing of minutiae: The thinning ridges are depicted in this. It may pick up a lot of small details if unwanted spikes and fractures are present in thinning ridges. Prior to minutiae detection, we perform a method to eliminate spikes and join broken ridges.
Matching Minutiae Several methods, including point pattern matching, image-based matching, ridge pattern matching, graph-

based scheme, etc., can be used to match fingerprints. The basic and reliable matching algorithm is used.minutiae matching is the matching of the point pattern. A

**BLOCK DIAGRAM**




**CONCLUSION**

The IoT-based automobile door lock system is an effective, highly secure technology. Our goal is to create a secure and dependable system. After reviewing numerous research papers and its shortcomings, this system can serve as a remedy.

The technology is very effective and precise at identifying the authorized user. This paper makes a recommendation for an Internet of Things (IoT)-based car door lock system that the automotive industry and owners of vehicles can adopt. This system's major feature is its use of fingerprint biometric authentication to verify users. One of the biggest technical revolutions has been the internet of things. It is the idea behind trying to digitally transform common physical objects by connecting them to the internet.

By 2022, it is anticipated that over 18 billion gadgets will be connected to the internet. When using these gadgets and applications to connect to the internet, there are security issues that we must consider. It is challenging to standardize the security features across all devices due to the fact that each of these gadgets and programs has unique security flaws that need be taken into account. While creating a product that will interact with the immediate environment, developers must have a solid understanding of the fundamental concepts of IoT architectures.

**REFERENCES**

1. Aditya Shankar, “Finger Print Based Door Locking System”, International Journal of Engineering and Computer Science, ISSN:2319-7242 Volume 4 Issue 3 March 2015.
2. Mohamed Basheer. K. P and Dr. T. Abdul Razak, “Enhanced Biometric Based Authentication for Network Security using IRIS”. International Journal of Com- puter Engineering and Technology (IJCET), 4(6), 2014, pp. 412–422.
3. N.Nagamma, T.Narmada, Dr.M.V.Lakshmaiah, “Raspberry Pi based Biometric Authentication Vehicle Door Locking System”, ICPCSI – 2018.
4. R.M.Vithlani, “Biometric Automobile Ignition Locking System”, International Journal of Electronics and Communication Engineering and Technology (IJE- CET), Volume 7, Issue 5, September-October,2016.