

Prototype of Dual Authentication system for Vehicle Ignition System Using Cloud

Shivani Jadhav, Pooja Kulkarni

¹Department of Computer Science, Faculty of Science and Technology, Vishwakarma University, Pune, Maharashtra, India

shivani.jadhav-434@vupune.ac.in

²Department of Computer Science, Faculty of Science and Technology, Vishwakarma University, Pune, Maharashtra, India

pooja.kulkarni@vupune.ac.in

Abstract: To start the ignition of any vehicle, two level of security is proposed in the research. Fingerprint is a more reliable tool utilized for security purposes in today's technology. Every person's fingerprint is distinctive, making it increasingly dependable to identify or approve a person. A method of identifying a person that is unique to each person is through their fingerprints. Nobody else's fingerprints will be identical to yours. There are specific patterns in fingerprints, such as ridges, valleys, arches, loops, and whorls. A fingerprint sensor, in general, offers a quicker and more secure alternative to other device-unlock security measures. As a result, in first level of security fingerprint is used for authentication of drivers with a valid license. The verifications can happen at either of two level that is at local drive data or if the data is not present at local drive, then at cloud data. When the data is verified either with local data or cloud data the driver is applicable for next level of authentication. The first level of security marks as fingerprint verification of authorized driver. Any person who does not have a valid license or do not have a license or have expired license will not be able to complete first level of security leading to unsuccessful start of the ignition of vehicle. More than 3 unsuccessful of any users will let the bulger to ring eventually leading to locking of vehicle and also notifying the owner of vehicle about the intruder. The second level of security serves as verification of vehicle with valid mandatory documents. When the first level of security is completed, that is the validation of driver is done then only the second level of security happens. You will undoubtedly encounter numerous check points and tolls on your way out of the station, each requiring you to present a different set of driving-related documents. Driving a car in India requires a specific set of documents from every driver. There will be severe consequences if you don't possess the necessary documents. To overcome these consequences, in second check, if the mandatory documents of vehicles are expired, the security fails and the driver is not allowed to start the ignition. Any mandatory document that is not valid or expired is checked in background and post failure of valid documents ignition does not start. If both the security checks are satisfied then the driver can start with ignition. The mandatory documents will be also displayed on the screen via LED. If any documents is about the expire necessary notifications will be sent to car owner regarding expiry. Through tracker, the owner of vehicle will be getting notified, about the ownership taken by driver to drive the car. The owner will be also notified with the location of the vehicle. If the very first stage of fingerprint verification fails then the second level of security check for vehicle mandatory documents are not done.

Keywords: Microcontroller, cloud, local data, Fingerprint Scanner, Dongle.

1. Introduction

Driving without a license is viewed as a highly serious offence, this leads to a fine of number of rupees as stipulated by the traffic rules. Numerous studies conducted over the past few decades have linked driving that too with a invalid license—for example, un-licensed drivers or those whose licenses have been suspended, revoked, or expired—raises your chances of causing or being involved in a traffic accident[1]. The risk of a traffic accident rises when driving without a valid license. On the world's roads, over 1.35 million people per year are killed. For people aged 5 to 29, the leading cause of death is motor vehicle accidents[2]. Driving has long been thought of as a rite of passage when a teen goes through their transition to the adult world. Driving, of course, is not a right but a privilege. If you are not careful enough and follow the rules, your right to drive can be denied and taken away by the states. To drive a vehicle, you need a license.



Unlicensed drivers include those who have never taken any driving test or individuals who had their licenses revoked or cancelled due to a gamut of possible causes or an underage human who urge to drive. 87.2% of drivers in fatal collisions between 2007 and 2009 had valid licenses, 6.7% had licenses that were suspended or revoked, 1.1% had licenses that were expired, cancelled, or denied, and 5.0% were driving without a valid license, according to the findings. 18.2% of fatal collisions, or 21,049 fatalities, involved a driver who was breaking the law or had a suspended licence. Tragically, 21,049 people lost their lives in the fatal collisions covered by the AAA report[3][Fig 1]. The age distribution of India is shown in this statistic from 2011 to 2021. According to data from 2021s, 87.2% of drivers in fatal collisions between 2007 and 2009 had valid licenses, 6.7% had licenses that were suspended or revoked, 1.1% had licenses that were expired, cancelled, or denied, and 5.0% were driving without a valid license. At the time of the fatal collisions, approximately 25.69% of Indians were under the age of 14, 67.51% were between the ages of 15 and 64, and 6.8% were over 65.[4][Fig 2].

Biometrics can be defined as biological measurements or physical characteristics that is used to identify person. Fingerprint based security system is the most secure system. Identification via fingerprint is the most popular form for biometric authentication in all the innovations made in biometric made. Fingerprint is used for authentication and verification because it is uniqueness which vary from person to person. It is impossible to duplicate Fingerprints or to steal. This research has two components of verification. In this paper the proposal is a prototype where any driver will be able to start the vehicle if the fingerprint matches the data on cloud. The idea is to create a clever fingerprint-based license retrieval system with the cloud on the vehicle itself for user authentication.

The project's goal is to implement a system that uses a driver's fingerprint to identify him or her, and post confirmation start of ignition. Every step of the process is completed digitally, making it simple for any driver who misplaced their documents to obtain both personal and vehicle records. Vehicle related documents will be displayed on screen in the vehicle itself. Implement the system that uses a driver's fingerprint to identify their identity so that the user won't encounter any problems if they don't have a hard copy of their license. This system makes it simple and conflict-free for the driver to verify their in-person authentication with start of ignition. Every step will be completed digitally, making it simple for any driver who misplaced his documents to obtain his personal records if any.

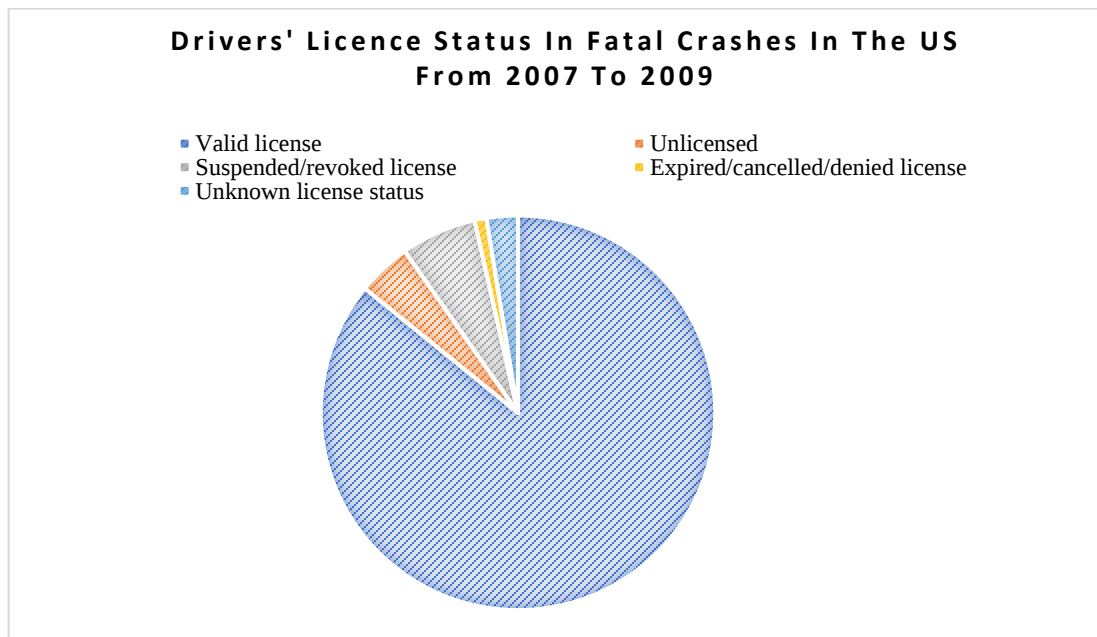


Fig. 1. Drivers' Licence Status in Fatal Crashes in the US From 2007 To 2009.

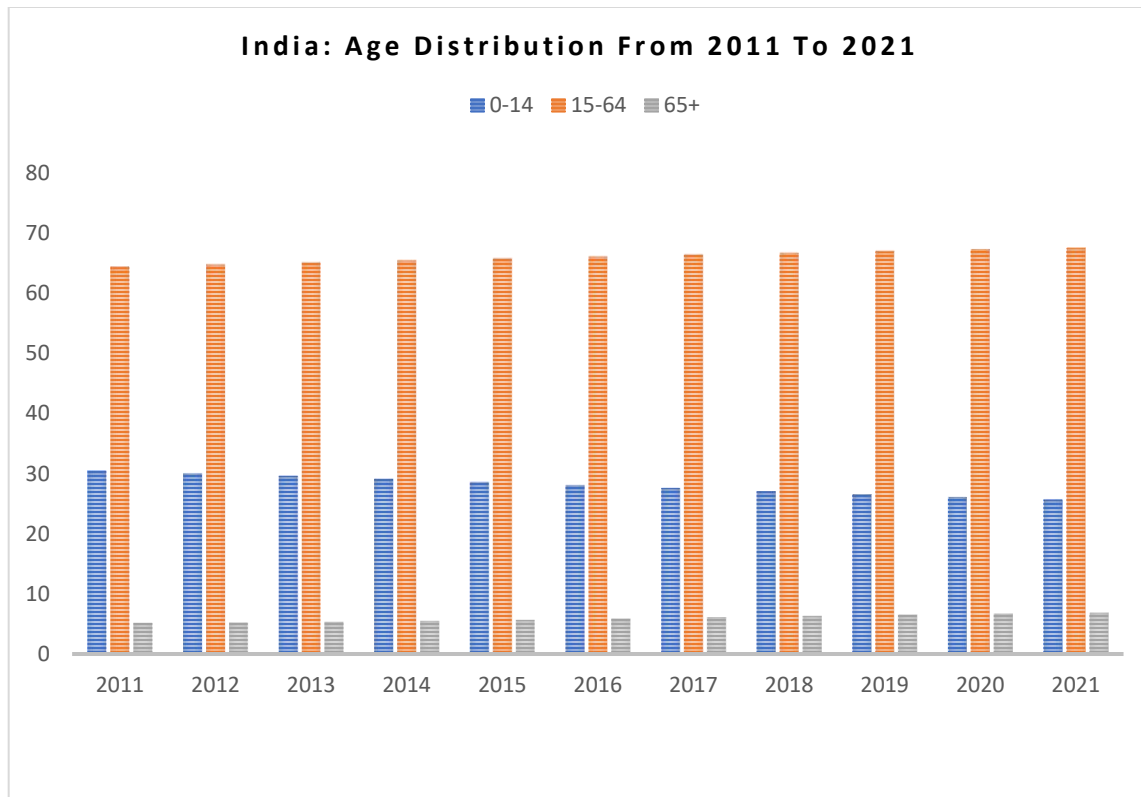


Fig. 2. India: Age Distribution From 2011 To 2021

2. Related works

Karthikeyan.a et al[5] proposed a system where model had components as microcontroller AT89c52 and fingerprint sensor FIM 3030 to provide security to ignition of vehicle. Fingerprint module is used for identification of a person to start vehicle. In this we use microcontroller to start the ignition system. If scanned fingerprint and existing local/RTO data matched then the ignition starts. LCD is used to display the authentication of the user, microcontroller is used to give the output and the Comparison is done via fingerprint module. In 2011, Omidiora E.O[6] developed a prototype which uses fingerprint to start the ignition of key. This prototype can be divided into 3 modules. Fingerprint analysis software, Hardware interface module and Ignition system module. Initially users scan his finger through the scanner, the fingerprint analysis software make a check from the database whether the user is having a valid license or not. If the user is having the valid license, then the hardware interface passes a single to Ignition system to start the vehicle and the vehicle starts. If the user is not having the valid license, then the hardware interface will not pass a single to Ignition system to start the vehicle and the vehicle will not start.

A proposed research paper by Vashist Anshul, Kansal Romanch and Nijhawan Vaibhav, Zafar Zaid et al[7] where the key components of this paper are: Biometrics, Fingerprints, Ignition, RFID, Vehicles In this paper, two ways of security is used: RFid and Fingerprint scanner. Initially in first step driving license is verified. Here RFID verification is done. The chip in license acts as RFID chip where the user scans the licence through RFID scanner. If the license is valid license it is checked in background through Dummy RTO data. If user is valid then the nest verification takes place. In Second step, User fingerprint is verified with the images in database scanner. If the data is valid then the ignition starts else now.

The data was matched by the Roopam Arora and Kapil Kumar using a sensor to read a person's fingerprint and comparing it to the authorized fingerprint image that is kept in the database. The cars will be started if a match is made. In this project, methods for digital image processing are used to determine whether an incoming fingerprint image is authentic or fake[8]. The authors of the study, Prajeesha, Rakshith B S, Nidhi Nagabhushan, and Tangirala Madhavi, seek to prohibit unauthorized drivers from accessing the vehicle, which will lower the number of careless drivers on the road and, as a result, the daily percentage of traffic accidents. The primary goal of the project is to create

a fingerprint authentication system as a requirement for car ignition together with user identification through their driver's license.[9]

Fingerprint sensor module R307 along with Arduino Uno model was proposed by Saritha Namboodiri, Palakkad, Kerala Arun P. The vehicle can be started by a human, but motion is only possible after fingerprint authentication. The valve fixed to the fuel tank outlet opens when the fingerprint is recognized, letting fuel to flow to the engine.[10] Z. Brijet¹ B. Santhosh Kumar² N. Bharathi³, proposed a AT89c52 model microcontroller and Fingerprint sensor to scan biometric. Initially whoever is the intended user who is supposed to drive, his fingerprint data is stored in system. Whenever the authorized person tries to start the vehicle, the fingerprint gets scanned with stored fingerprint data and the ignition starts. Whenever the unauthorized person tries to start the vehicle, the fingerprint gets scanned with stored fingerprint data and the ignition does not start[11].

Roopam Arora and Kapil Kumar developed model in integration of ARDUINO. A paper states about car tracking system. In this paper when any user tries to start a vehicle a message is sent to registered number about the start. If the owner finds something fishy, he sends message back to system to stop the vehicle. This mobile number is checked again in system to be authorized number and then car is stop. Similarly, through GPS users can get location details of car so he can easily track the car. Through GSM modem car owner can also connect to laptop to track the vehicle using Google map. Components used are PIC microcontroller, GSM, GPS[12].

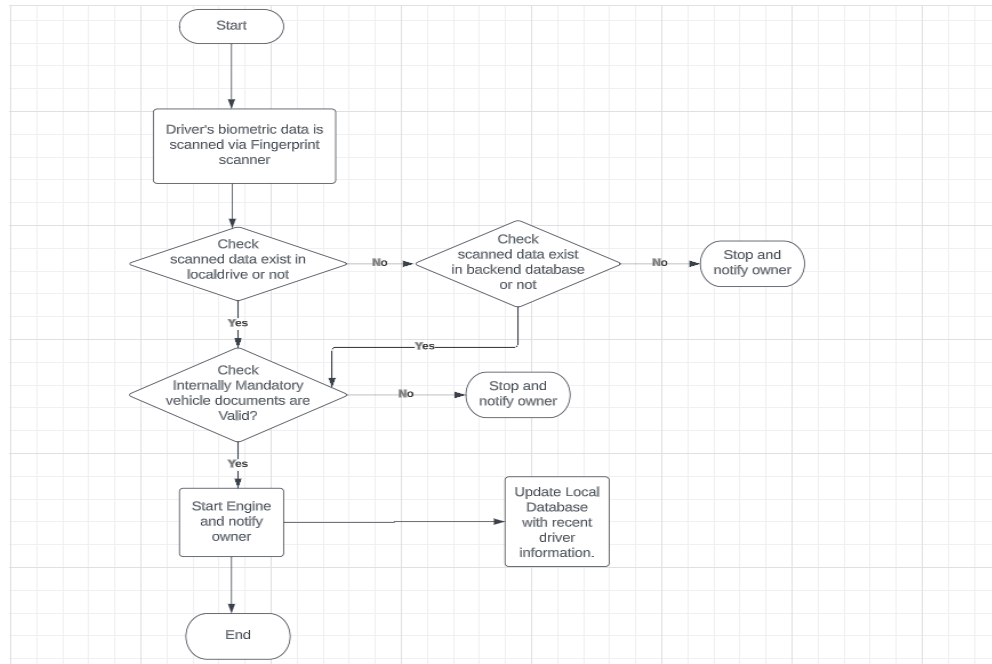
In the proposed solution, two level of security checks will be applied for ignition of vehicle. First security check will be in form of fingerprint verification. With help of embedded Microcontroller and Fingerprint user verification will be done. Initially any user who wants to drive the vehicle scans his finger via fingerprint sensor. Scanned data will be verified with Real time data on cloud via Internet. If the scanned fingerprint data is available on cloud that means user is having license and can drive the car and the car ignition starts. If the data is not available in cloud means the users is not having a valid license and cannot drive the vehicle and a message is sent to owner of vehicle that the car was accessed via person who does not have a valid license. Second security check will be in form of verification of mandatory documents of vehicle which intended person is willing to drive. Post verification of valid fingerprint, the mandatory documents of vehicle are verified in the system itself for expiry. If the documents are not expired that is the documents are valid then the user is allowed to start the ignition via key or button (as per availability in current vehicle). Failure of authentication of any one security check the key hole or button won't be visible to start the vehicle.

3. Proposed Work

There will be dual security checks which will be adapted in this paper:

A: Fingerprint Verification

Fingerprint Verification: Here fingerprint is verified through scanner used to scan biometric data. The scanned data is checked in local drive data if the data exist or not. If the data exist then the vehicle starts. If the scanned data is not available in local drive then data is checked in database. If the data exist in database then ignition starts and owner is notified that the vehicle is started by X person. If the data does not exist in database then ignition does not start and owner is notified that the vehicle is started by X unauthorized person.



Local Drive Verification: Scanned Data sent via biometric scanner is sent to local drive for verification. Local drive acts as local memory where some recently scanned data is stored which does not require internet for fingerprint verification. It works on First in last out algorithm. If the scanned data does not exist in local drive, then data verification is done at database level.

Database Cross Verification: If the fingerprint details are not available in Local Drive, then the verification is done on database side. When internet is high the scanned user data is checked in real time database. If the scanned fingerprint is available in database, then a user can start the vehicle else a notification is sent to owner of vehicle that an unauthorized user is trying to start vehicle and the history is updated.

Mobile Application Verification: Mobile application acts as a mediator between car and car owner. If any unauthorized person is driving a car, then a pop up is sent to owner of car. Post notification user can block that user from driving the car in future. If authorized person starts the vehicle, then a message is sent to owner about the details of driver.

B: Vehicle Mandatory Document Verification:

Here Documents of vehicle are used as authentication. Mandatory documents are stored internally in vehicle. If any of the mandatory documents are expired the vehicle will not open the flap where the user inserts key or push button to start the vehicle. If the documents are valid then the flap will be opened to insert the key or push button to start the ignition of vehicle. Through Mobile application user can manage the reinitialization of expired documents. The documents status will be displayed on led screen.

4. Conclusion:

This research presents a prototype of a dual authentication vehicle ignition system that integrates biometric verification and vehicle document validation through cloud-based and local data mechanisms. The proposed system enhances vehicle security by ensuring that only authorized drivers possessing a valid driving license can access and operate the vehicle. The first level of authentication uses fingerprint recognition to verify the driver's identity through local storage and cloud databases, thereby reducing the possibility of unauthorized vehicle usage. The second level of authentication validates mandatory vehicle documents such as Registration Certificate (RC), Insurance, and Pollution Under Control (PUC) certificates before permitting ignition.

The proposed framework not only improves vehicle security but also promotes compliance with transportation regulations by preventing the operation of vehicles with expired or invalid documents. Additional features such as owner notifications, vehicle tracking, document expiry alerts, and mobile application integration further strengthen

the system's practicality and effectiveness. The use of cloud technology ensures real-time verification and easy management of driver and vehicle information.

Overall, the dual authentication approach demonstrates significant potential for reducing unauthorized vehicle access, enhancing road safety, minimizing legal violations, and supporting the development of intelligent transportation systems. Future work may focus on integrating the system with official transport authority databases and deploying it in real-world automotive environments for large-scale implementation.

References

1. V. M.-R. , M. R.-I. , E. J.-M. , P. L.-C. Luis Miguel Martín-delosReyes, "Is driving without a valid license associated with an increased risk of causing a road crash?" in *Accident Analysis & Prevention*, 2021.
2. W. H. Organization, "Road traffic deaths data by Country," WHO, 2021.
3. A. Foundation, "Unlicensed to Kill," AAAFoundation, Washington, DC 20005, 2011.
4. A. O'Neill, "India: Age distribution from 2011 to 2021," Statista, 2023.
5. K. Sowndharya.j, "FINGERPRINT BASED IGNITION SYSTEM," in *International Journal Of Computational Engineering Research / ISSN: 2250-3005*, 2012.
6. F. O. A. A. O. T. A. D. O. Omidiora E. O, "A Prototype of a Fingerprint Based Ignition Systems in Vehicles," in *European Journal of Scientific Research ISSN 1450-216X Vol.62 No.2 (2011)*, pp. 164-171 , 2011.
7. R. K. V. N. Z. Z. Anshul Vashist, "A Fingerprint Based Ignition System in Vehicles," in *International Journal of Scientific & Engineering Research Volume 12, Issue 6, June-2021 ISSN 2229-5518*, 2021.
8. K. K. Roopam Arora, "START-UP THE ENGINE USING FINGERPRINTING," in *International Journal of Computer Engineering and Applications, Volume IX, Issue X, Oct. 15 ISSN 2321-3469, India*, 2015.
9. R. B. S. , N. N. T. M. Prajeesha, "Fingerprint-based Licensing for Driving," in *2021 6th International Conference for Convergence in Technology (I2CT) , India*, 2021.
10. A. P. Dr. Saritha Namboodiri, "Fingerprint based security system for vehicles," in *International Journal of Advance Research, Ideas and Innovations in Technology ISSN: 2454-132X, India*, 2018.
11. B. K. N. Z.Brijet, "Vehicle Anti-Theft System Using Fingerprint Recognition Technique," in *Open Academic Journal of Advanced Science and Technology ISSN 2577-7807*, 2017.
12. M. A. A.-K. S. A. A.-K. Montaser N. Ramadan, "Intelligent Anti-Theft and Tracking System for Automobiles," in *International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012*, 2012.