Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 6, June : 2024

An Innovative Autonomous Vehicle Security System Employing Automated Fingerprint and Driver License

T.Naresh, Electrical and Electronics Engineering,
K.S.R.M.College of Engineering College (Autonomous) Kadapa, AP India t.naresh278@gmail.com
Dr.R. Lakshmi Narayana, *Department of Instrumentation,*
Sri Krishna Devaraya University Anathapuram, AP India lnrscience@gmail.com
B.Ravi Chandra, Mechanical Engineering,
K.S.R.M.College of Engineering College (Autonomous) Kadapa, AP India ravichandu001@gmail.com
Y.Sravanthi, Electronics and Communication Engineering,
K.S.R.M.College of Engineering College (Autonomous) Kadapa, AP India Sravanthi.sri73@gmail.com

ABSTRACT:
In order to improve convenience and security, we present an Arduino-based car ignition system that incorporates fingerprint and RFID (Radio-Frequency Identification) verification. An RFID reader, a fingerprint sensor, a buzzer, a red and green LED, a relay, a motor, and other parts are all combined into one system. The main goal is to make sure that the ignition of the car is only turned on after the successful verification of both the RFID and the fingerprint authentication. Authorized RFID tags are often assigned to vehicle owners, and the RFID reader is used to identify them. The authentication procedure begins when an approved RFID tag is positioned close to the reader. The driver's fingerprint is simultaneously captured by the fingerprint sensor for biometric authentication. To verify the user's identification, the system compares the information from the RFID tag and fingerprint to pre-registered records. only in the event that fingerprint and RFID authentication are both successful. When authentication is successful, the system activates a relay, which turns on the ignition system of the car. The status of the ignition is visually shown by the red LED. The buzzer alerts you to the possibility of unauthorised entry into the car by sounding an alarm in the event that the fingerprint or RFID identification fails. The car and its occupants are better protected thanks to this multi-layered security strategy, which also offers authorised users a seamless user experience. It is more difficult for unauthorised people to start the car thanks to the addition of an additional layer of security provided by the integration of RFID and fingerprint authentication into the ignition system. In addition, this system may be scaled and customised to satisfy varied security and access control requirements in a variety of vehicle types and applications.

INTRODUCTION:

In most countries, driving without a license is a major issue. Unlicensed drivers, intoxicated drivers, and drivers who fail to buckle up are the main causes of accidents, according to a poll. The dangerous driving conditions have led to a rise in the number of accidents. It is problematic to drive without a license for a number of reasons. It's possible that drivers who haven't received the required training and certification lack some of the skills and information necessary to operate a car safely and successfully. Additionally, unlicensed drivers can be less motivated to follow traffic laws because they are not affected by the benefits set by the licensing system [1, 2]. This defense states that drivers who do not possess valid licenses can ignore the chance of facing fines or the benefits of having their insurance rates lowered because they have not made any claims. Note that one of the following subcategories is commonly referred to as "unlicensed" when using the term:

a). drivers who are still behind the wheel but have never held a license.
b). drivers with a suspended licence who have previously held one.
c). Individuals who wish to drive alone yet only have a provisional licence.

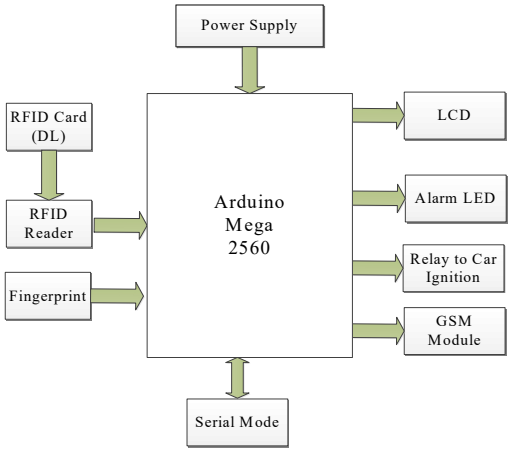
This research looks at the following problems or reasons:
1. Motorised road traffic is often the target of criminal activities, whether it is through the issuance of counterfeit licences to those who are not authorised to drive or the legalisation of stolen vehicles or parts through false registration paperwork.
2. Many unlicensed drivers are not deterred by enforcement actions or fines, and some even exploit administrative weaknesses. There seems to be a generally weak system in place for confirming the authenticity of documents and determining who owns them. Reducing the risk that unlicensed drivers pose on the highways is the main objective. This study also aims to minimise driving without a licence, reduce the risk of fraud, and improve DL functionality.
3. Permitted driver's licences and trustworthy people's fingerprints can be added to an Arduino programme. An RFID reader checks data entered by the user with data already saved in the programme when the user enters information about their driving licence. The ignition system will activate and the user will be able to control the vehicle if the data match.

EXISTING METHOD:
Traditional car ignition systems only provide a limited level of protection against theft or unauthorised access because they mainly rely on keys or basic keyless entry systems. These techniques leave cars open to theft and abuse since they can be used for lock picking, unauthorised key copying, or code hacking. Furthermore, there is a risk to security and inconvenience when losing or stealing keys or key fobs. Conventional systems can't guarantee the identity of the user or driver in the absence of sophisticated security measures, which leaves cars vulnerable to illegal entry.

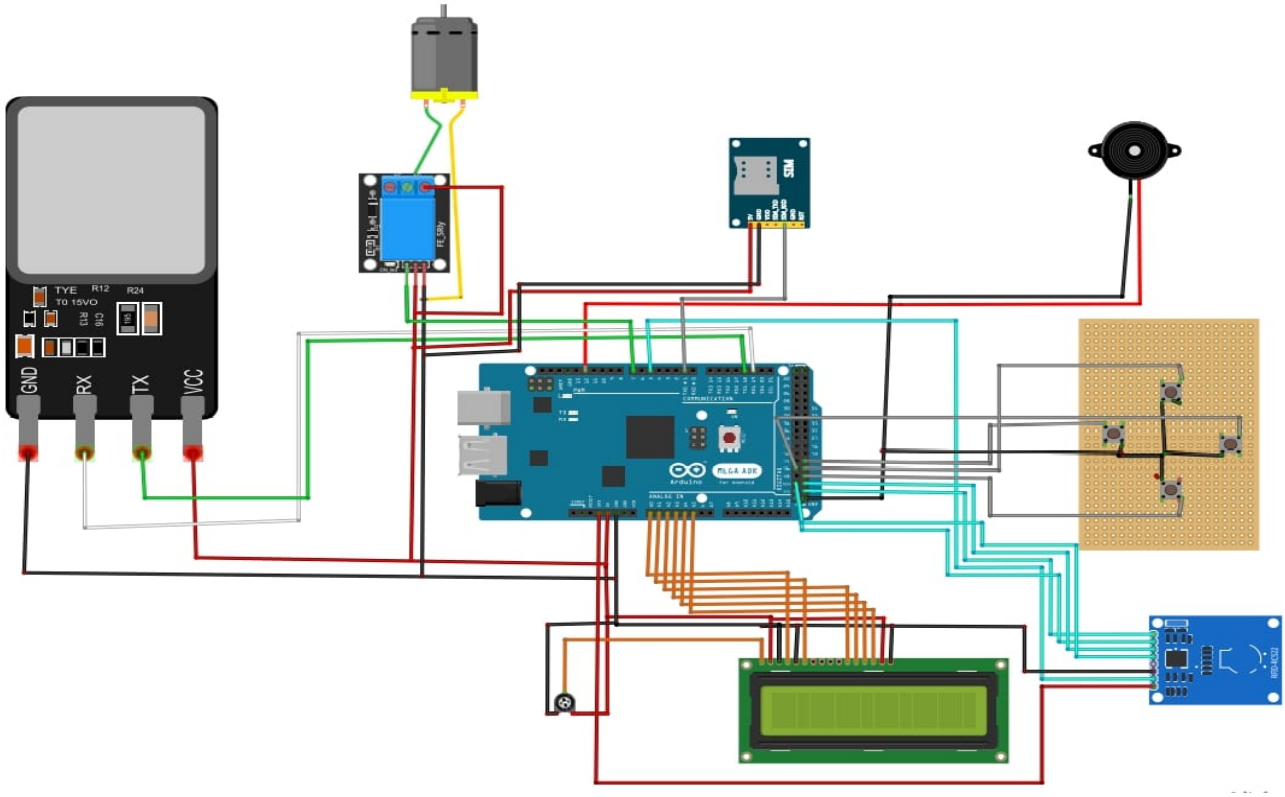
PROPOSED METHOD:
The suggested vehicle ignition system offers a reliable and secure substitute for traditional techniques. Modern technology is incorporated, such as RFID and fingerprint verification, to improve ease and security. Users must provide an approved RFID tag and their fingerprint for biometric authentication when they approach the car. The fingerprint sensor records and evaluates the user's fingerprint data, while the RFID reader reads the tag. After that, the algorithm contrasts this data with previously registered entries in the database. The system does not turn on the green LED, which indicates that the vehicle's ignition is ready for use, until both the RFID and fingerprint authentication procedures have been successfully validated.When authentication is successful, a relay is activated and the car's ignition system is given electricity. In order to make sure the user is aware of the system's response, the red LED acts as a visual indicator of the ignition state. The buzzer alerts users in the event of an authentication failure, such as an unauthorised RFID tag or mismatched fingerprint data, and the red LED stays off to deter unwanted ignition attempts. In addition to preventing theft and unauthorised access, this all-inclusive strategy improves user convenience by doing away with the need for conventional keys or key fobs.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 6, June : 2024

NETWORK TOPOLOGY:



EXPERIMENTAL SETUP:



CONCLUSION:

When compared to traditional techniques, the incorporation of RFID and fingerprint authentication into the car ignition system signifies a major improvement in security and user experience. The shortcomings of traditional systems—such as their susceptibility to theft, loss of keys, and inadequate identity verification—are addressed by this suggested approach. The technology reduces the risk of theft or unauthorised usage by requiring both RFID and fingerprint verification, ensuring that only authorised

users obtain access to the vehicle.In addition to improving car security, the deployment of this effective and safe technology has potential uses in a number of sectors where identity verification and access control are crucial. The suggested approach is proof positive that, even as technology develops, it is crucial to modify creative ideas to satisfy our daily needs for ease and security, which are becoming more and more pressing.

REFERENCES:

[1] Srinivasan, L., & Nalini, C.(2019).Abadent Object Detection & IOT Based Multi-sensor Smart Robot for Surveillance Security System.International Journal of Scientific Research in Computer Science, Engineering and Information Technology,9(4),669-677.
[2] S. P. Mohanty, U. Choppali, E. Kougianos, “Everything you wanted to know about smart cities: The Internet of things is the backbone”, IEEE Consumer Electronics Magazine, Vol. 5 (3), 2016.
[3] Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges," in IEEE Access, vol. 9, pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.
[4] B. Swathi and H. Tiwari, "Test Automation Framework using Soft Computing Techniques," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies
[5] Kumar, &KishanKumar,(2020). Charging station for EVehicles using solar with IOT. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5(8), (2040-2043).
[6] Karthiyayini, J.,(2020). Robot Assisted Emergency and Rescue System with Wireless Sensors. International Journal of Research and Scientific Innovation, 12(4)
[7] Vandana C.P., Chikkamannur A.A. Semantic Annotation of IoT Automatic Detection & Prevention of Cybercrime in Micro Blog Systems. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2(5), (1581-1584).
[8] K M Bilvika. Automotive Industry Redefined By Information Technology: Review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2019 IJSRCSEIT | Volume 4 | Issue 9 | ISSN: 2456-3307.
[9] Karthiyayini, J.,(2020). An Industrial Helmet for Air Quality and Hazardous Event Detection using Smart Band. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2(6), (1575-1578).