International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 128-133

https://doi.org/10.70917/ijcisim-2026-3427
RESEARCH PAPER

Syncing Vehicle Ignition with Legal Documentation: A Vision for Automated Road Compliance

Shivani B. Jadhav[1], Dr. Pooja Kulkarni[2]

[1] Research Scholar, Department of Computer Science, Faculty of Science and Technology, Vishwakarma University, Pune, Maharashtra, India
Email: shivani.jadhav-434@vupune.ac.in
[2] Associate Professor, Department of Computer Science, Faculty of Science and Technology, Vishwakarma University, Pune, Maharashtra, India
Email: pooja.kulkarni@vupune.ac.in

Abstract: The high development of smart transportation technologies has opened new prospects in improving road safety, legal control, and vehicle control systems. Although most of the transport related services have been digitized, the checking of most of the mandatory documents of the vehicle like the Registration Certificate (RC), Pollution Under Control (PUC) certificate, and Insurance policy is still mainly carried out by periodic check and manual checks. This tends to cause vehicles with lapsed or non-valid documents to be operated, causing legal infractions and growing environmental and safety issues. In this paper, a new car-integrated authentication system will be proposed, which will coordinate the ignition system of the vehicle with the validity of crucial legal files. The suggested framework is based on the microcontroller-based architecture and is linked with the authorized transport databases to verify the authenticity and validity of the documents in real-time. The system automatically checks the position of the RC, PUC, and Insurance records before it allows ignition. When all the documents are valid, then the microcontroller allows the ignition process. Nonetheless, in case any of the documents required has expired or is invalid, the system limits vehicle start and informs its owner of the compliance problem. The main objectives of the suggested model include the creation of responsible ownership of the vehicles, minimizing the usage of the unauthorized roads, improving the level of enforcement of the regulations, and making transportation more responsible and less harmful to the environment. This idea is a great leap towards smart, compliance-conscious mobility solutions in the future.

Keywords: Vehicle Document Verification, Registration Certificate (RC), PUC Expiry Detection, Insurance Validation, Microcontroller-based Ignition, Legal Compliance Automation, Intelligent Transportation, Real-Time Document Status

1. Introduction

The contemporary transport ecosystem is incredibly dynamic and under the influence of technological progress and the growing demand to harmonise vehicles and legal frameworks. Checking of vehicle documents including the RC, PUC certificate and insurance policy are vital to legal and safety standards adherence. Nevertheless, inefficient, error-prone, and tedious both to the vehicle owners and law enforcement agencies, the traditional manual document tracking system has demonstrated to be unproductive (Nadaf, Patil, Mundkar, and Patil, 2019).

During the recent years, other scholars have come up with automated systems that combine smart technologies in enhancing accuracy and efficiency of vehicle document verification. Sebastian (2019) discussed the application of Internet of Things (IoT) and RFID technologies to create an automated system of verification of vehicle documents in real-time. It was a system that would minimise the administrative overhead and mistakes that come with manual checks, increase road safety and legal standards. Nonetheless, these systems have been experiencing problems in the areas of regional constraints and integration with the centralized transport databases. Additional progress has been realized in the microcontroller based systems and especially in other sectors such as the health sector and security where real time access control is needed. Kim et al. (2021) showed how microcontrollers can be used to control access to sensitive areas on the basis of authentication. The technology can

have an implication on vehicle ignition systems whereby only vehicles with valid documents can start the engine of the vehicle to maintain compliance and to avoid unauthorized use.
In addition, recent literature has also emphasized that transport databases can be directly integrated with in-vehicle systems to enhance compliance and minimise unauthorised vehicle use (Reddy, Yashwanth, Nithin, and Ramya, 2024). Although such integration has potential, these systems are at risk because of issues of data privacy, security and the possibility of having smooth integration with government servers. Johnson (2022) believed that tackling such issues would greatly improve the adherence to the law, yet more research needs to be conducted to make sure that such practices are implemented safely and efficiently in other regions.
The proposed research will build upon the earlier studies by developing a viable, scalable solution to the problem of implementing real-time vehicle document validation as part of a vehicle ignition system. This solution aims to help reduce the use of vehicles illegally by installing legal compliance checks in the ignition control and promote responsibility and building a smarter transportation ecosystem. Contrary to the existing systems, the suggested structure will enable a backup system that limits vehicle ignition in case of document expiry ensuring that road safety regulations are abided with.

2. Experiment

The system proposed is designed to provide automatic checks of a vehicle, regarding the existence of legal documents required by the vehicle, before the ignition of the vehicle is allowed. The system authenticates the Registration Certificate (RC), Pollution Under Control (PUC) certificate and Insurance status based on a database based authentication system. The goal is to ensure that vehicles that have expired or invalid documents are not allowed to use the public roads and thereby encourage compliance with the regulations and improve on road safety. A prototype was developed and tried with the use of a hardware and software combination. The system imitates the behaviour of an integrated transport compliance platform that the vehicle data is compared to a centralised database before ignition process is facilitated.

2.1 System Components

1. Microcontroller (Arduino)

The RFID reader is connected to the processing unit via the Arduino microcontroller. It captures RFID tag data of a vehicle. After scanning the RFID card or tag, the Arduino interprets the unique identification number and transmits the information to the Raspberry Pi to process the information. Microcontroller is a guarantee of good communication between the central verification system and the input device.

2. Raspberry Pi

The Raspberry Pi is the processing unit of the proposed system. It gets the RFID data of the Arduino and carries out the document authentication. The Raspberry Pi retrieves the prototype RTO database stored locally and matches the identified vehicle data with the records. It verifies the expiry date and validity of the RC Book, PUC Certificate and the Insurance Policy. It uses the results of the verification to produce an authorization decision to either permit or restrict vehicle ignition.

3. Prototype RTO Database

To emulate the operation of a formal Regional Transport Office (RTO) database, a prototype database was created based on Firefox local storage. The database will hold vehicle registration, owner and document validity records such as expiry dates of RC, PUC and Insurance certificates. The Raspberry Pi uses this database during system operation to make a decision on whether all required documents are up-to-date and legally binding.

4. Ignition Control System (Relay Module)

The ignition control mechanism is realized with the help of the relay module connected with the Raspberry Pi via General Purpose Input/Output (GPIO) pins. The relay is an electronic switch used to switch the ignition circuit in the vehicle. When all required documents are proven correct, the Raspberry Pi enables the relay to be closed, with the ignition system firing the vehicle up. However, should one of the documents become expired or lost, the relay will not switch the engine on. This safety measure will provide the operation of only the vehicles that are allowed by the laws.
The experimental design is effective in proving the viability of the legal document verification and vehicle ignition control integration and building a platform on which intelligent transportation system with automatic regulation enforcement would be built in the future.

2.2 Working Procedure

The proposed system adheres to a sequential authentication process and verification to only permit legally compliant vehicles to start up. The entire process is a biometric authentication, database check, and ignition control. The sequence of operations is outlined as follows:

Step 1: Driver Authentication through Fingerprint Recognition

The steps would start with the driver tapping his finger on the fingerprint sensor that is installed in the vehicle. The sensor reads the biometric data and matches it with the registered fingerprints in the system. This measure will help to ensure that unauthorized users do not gain access to the vehicle since only registered and authorized users have access to the vehicle which will increase security and reduce the chances of unauthorized use.
Step 2: Retrieval of Vehicle Document Information

After the successful authentication of the driving person, the Raspberry Pi starts communicating with the prototype RTO database. The database also has access to the details of the vehicle Registration Certificate (RC), Pollution Under Control (PUC) certificate, Insurance policy, their validity, and expiry date. The corresponding vehicles records are pulled down to make sure that they are valid.

Step 3: Document Validation Process

The Raspberry Pi processes the data received and makes sure that all required documents are correctly verified. The system will ensure that the RC registration is valid, PUC certificate valid and that the insurance policy is not expired. The verification process is one that ensures that legal transportation is adhered to.
Step 4: Ignition Authorization

When the verification process is successful, and all the documents needed (Fig. 1) are valid, Raspberry Pi sends a control signal to the relay module. This relay then triggers the ignition circuit in the vehicle and the engine starts like normal.
Condition:
• Authorized fingerprint detected.

• RC Certificate valid.

• PUC Certificate valid• Insurance policy valid.

Result:

• Ignition Enabled

Step 5: Ignition Restriction

Once it is discovered that any of the documents have expired, has been invalidated or is missing as indicated in Fig. 1, the Raspberry Pi does not energize the relay module. This results in the ignition circuit not being connected and as a result, the vehicle is unable to start

Condition:
• Expired RC, PUC, or Insurance document.

• Unauthorized user authentication.

• Missing vehicle records.

Result:
• Ignition Disabled.

This combined authentication and verification system provides the assurance that vehicles can only be used when the driver and vehicle documentation meet the requirements of regulations. The system therefore helps in the promotion of road safety, mitigation of law breaking, improvement of accountability of owners of the vehicles used and development of smart transportation systems that can help to enforce compliance automatically.

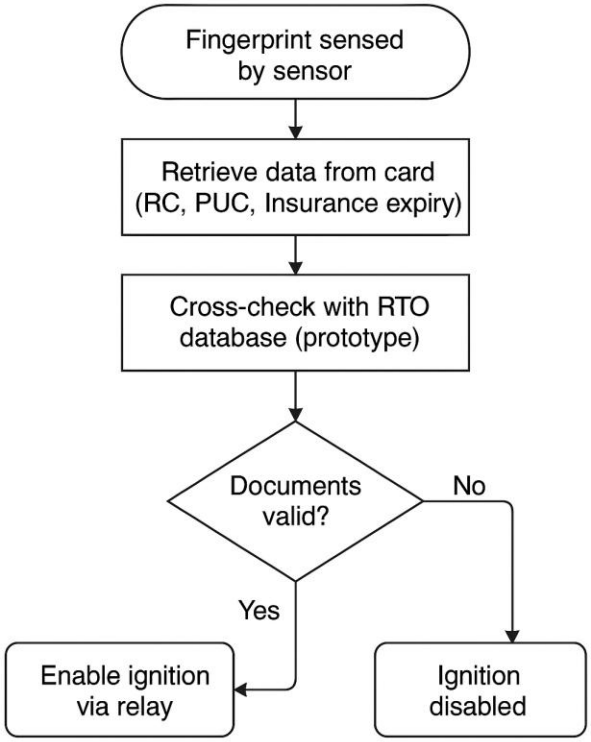


Figure 1: Discloses the flow of prototype

3. Experimental results and analysis

The proposed vehicle ignition control system was tested using the experimental study to determine its performance. There were different test cases of valid and expired vehicle documents, which were performed. These findings indicate that the system can be used to verify the status of the documents and regulate vehicle ignition accurately to comply with the transportation regulations established by law.

3.1 Pictures acquisition

According to Fig 2, the ignition will not start in case any of the documents is out of date. Fig 3 illustrates the situation in which all the documents are genuine therefore the vehicle ignition goes on. Video 1 shows us the working of vehicle when all the documents are valid.

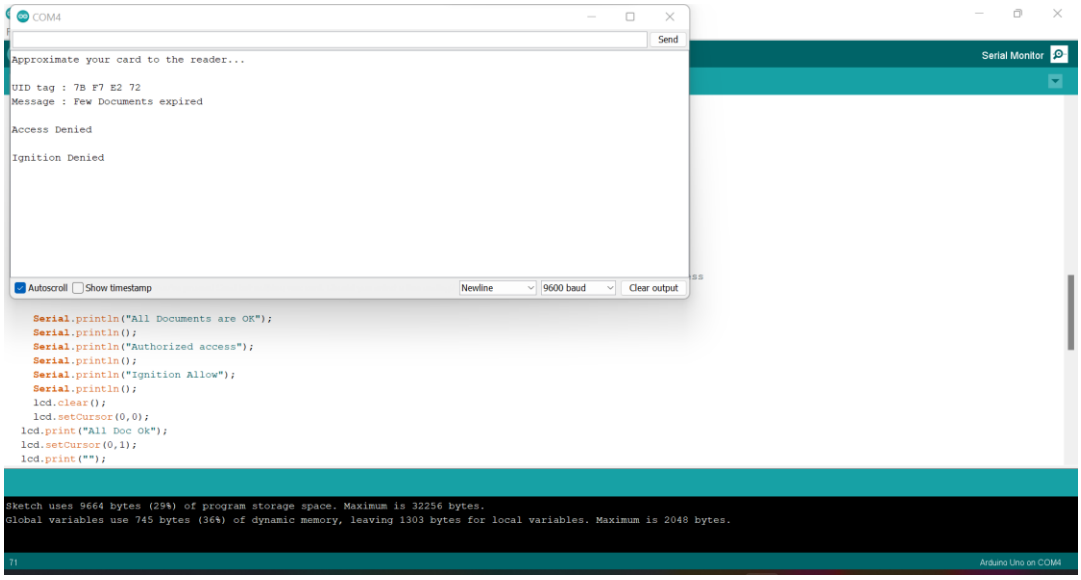


Figure 2: Software demo of denial of vehicle ignition.

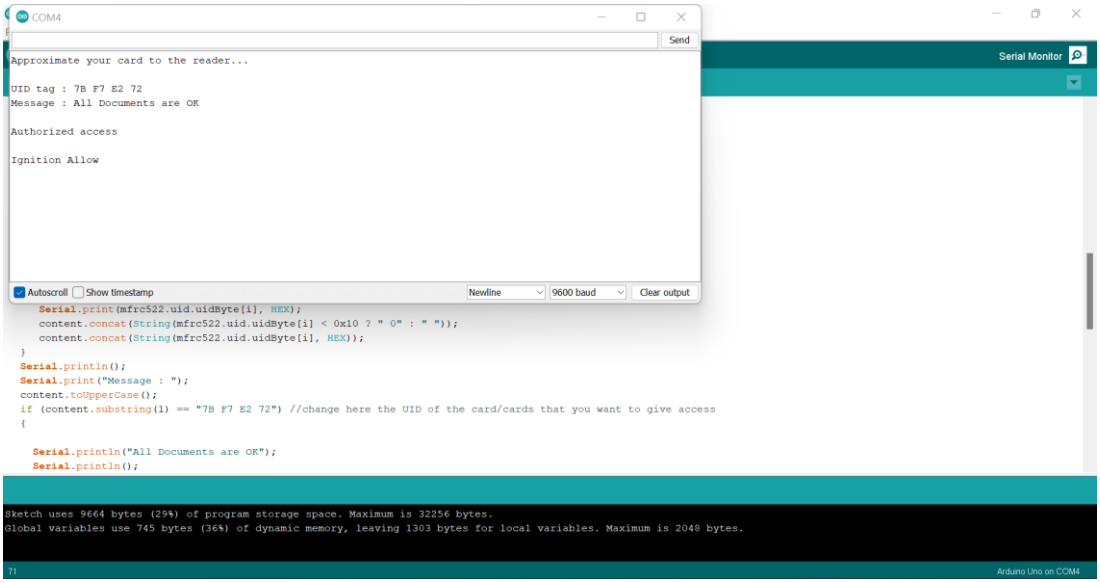
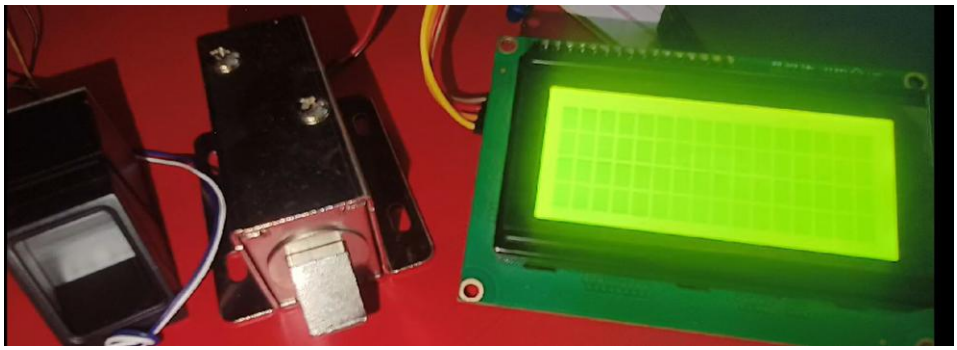


Figure 3: Software demo of acceptance of vehicle ignition.

Video 1 shows us the working of vehicle when all the documents are valid.



Video 1. Working of Vehicle ignition

6. Conclusions

The suggested system is an effective and consistent way to make sure the vehicles in the road are being used with proper and up-to-date documentation. With the integration of microcontroller, and a Raspberry Pi as the main processor, the system can be used to automatically check the required documents of a vehicle, including the Registration Certificate (RC), Pollution Under Control (PUC) certificate, and insurance. The prototype RTO database has been integrated to make sure that the date of documents being expiry is properly checked and the vehicle will not be allowed to start.

The essence of the system is that it is capable of intertwining hard hardware with the real-time authentication of documentary systems of vehicles. When the ignition is not provided, the ignition would also shut down in case any of the documents is invalid or expired, virtually immobilizing non-compliant vehicles. This does not only enhance road safety by making sure that the cars that have expired or invalid documents will not be on the road but also the adherence to traffic laws will be increased.

To recap it all, this system will be an important move towards the modernization of the vehicle verification system, increased safety and simplified administrative operations among both the vehicle operators and the authorities.

Reference

Nadaf, J. U., Patil, A. V., Mundkar, D. P., & Patil, A. (2019). QR code system for vehicle document verification and stolen vehicle detection. International Journal of Advance Research in Engineering, Science & Technology, 6(12), 45–48. Retrieved from https://ijarest.org/index.php/ijarest/article/view/1971

Sebastian, S. (2019). An algorithm for IoT based vehicle verification system using RFID. International Journal of Electrical and Computer Engineering (IJECE). Retrieved from https://www.academia.edu/91167337/An_algorithm_for_IoT_based_vehicle_verification_system_using_RFID

Reddy, A. V., Yashwanth, L., Nithin, L., & Ramya, K. (2024). Fingerprint and RFID based bike and car ignition system. International Journal for Research in Applied Science and Engineering Technology (IJRASET). Retrieved from https://www.ijraset.com/research-paper/fingerprint-and-rfid-based-bike-and-car-ignition-system

Murdan, A. P., & Kissoon, N. (2024). Implementation and evaluation of a secure keyless ignition and integrated control system for an Arduino-based instrumented car. In R. N. Shaw, P. Siano, S. Makhilef, A. Ghosh, & S. L. Shimi (Eds.), Innovations in Electrical and Electronic Engineering (pp. 343–355). Springer. https://doi.org/10.1007/978-981-99-8289-9_26

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Want, R. (2006). An introduction to RFID technology. IEEE Pervasive Computing, 5(1), 25–33. https://doi.org/10.1109/MPRV.2006.2

Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. IEEE Internet of Things Journal, 1(4), 289–299. https://doi.org/10.1109/JIOT.2014.2327587

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Borgia, E. (2014). The Internet of Things vision: Key features, applications, and open issues. Computer Communications, 54, 1–31. https://doi.org/10.1016/j.comcom.2014.09.008

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

These additional references are from well-known IEEE, Elsevier, Springer, and Computer Networks publications and provide a strong theoretical foundation for IoT-enabled vehicle authentication, RFID technology, intelligent transportation systems, and automated compliance verification.