IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134158

IMPLEMENTATION OF LONG RANGE SHARED VEHICLE COMMUNICATION SYSTEM BY USING LoRaWAN PROTOCOL

Prof. Savitri G P [1], Achyuth D[2], Ashitosh G Mane [3], Shakeenabhanu [4]

Assistant Professor, Electronics and Communication, East West Institute of Technology, Bengaluru, India [1]

Student, Electronics and Communication, East West Institute of Technology, India [2-5]

Abstract: The development of LPWAN (low power wide area network) technology is gradually becoming an evolution of IoT (Internet of Things) applications, for its significant improvements of signal sensitivity and noise tolerance. In this a long-range vehicle monitoring system, based on the LoRaWAN protocol. We clarify the system parameters and determine its communication range. Finally, the communication range is concluded and a solution is proposed for setting up a Authenticated Access Control for Vehicle Ignition System and Long range Vehicle monitoring system based LoRaWAN.

Keywords: LPWAN, LoRa WAN, IOT.

I. INTRODUCTION

The prevalence of unlicensed driving poses a significant challenge in many countries, with surveys indicating a high correlation between accidents and factors such as drunken driving, seatbelt negligence, and unlicensed operation of vehicles. This issue is multifaceted, as unlicensed drivers may lack essential training and skills required for safe driving, and they may disregard traffic laws without the fear of license-related sanctions. The term "unlicensed" encompasses various categories, including individuals who have never possessed a license, those previously disqualified, and even those driving with provisional licenses but unaccompanied.

Addressing this problem requires tackling key concerns, such as criminal activities exploiting motorized road traffic for fraudulent purposes, and the weak enforcement and penalties associated with unlicensed driving, exacerbated by administrative loopholes. Therefore, the main objective of this paper is to mitigate road insecurity caused by illegal drivers, with additional goals focusing on reducing unlicensed driving instances, combating fraud within licensing systems, and enhancing driver's license functionality through features like payment integration, digital signatures, and penalty point collection.

Through these efforts, the paper aims to contribute to safer roads and a more robust licensing system.

II. OBJECTIVES

The objectives of this work are described below

- To explore the feasibility of LoRaWAN to improve the shared-vehicle communication system.
- Aim to develop the communication range of LoRaWAN to satisfy the vehicle monitoring and authentication system in real.
- Deploying LoRaWAN protocol to monitor and access the vehicle

DOI: 10.17148/IJARCCE.2024.134158

III. METHODOLOGY

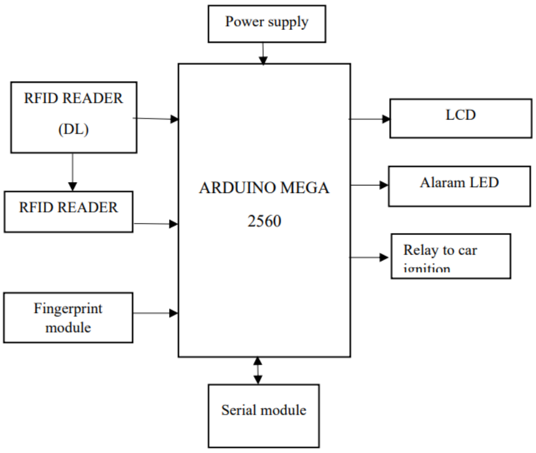

Fig 1**:** Block Diagram of Implementation of Long Range Shared Vehicle Communication System By Using LoraWan Protocol

The LoRa SX1276 is a wireless communication module that utilizes Long Range (LoRa) technology. It's designed for long-distance, low-power data transmission in various applications, especially in the Internet of Things (IoT). Key features include long-range communication, low power consumption, operation in different frequency bands, high sensitivity, support for various data rates, and versatile applications. It communicates with microcontrollers via SPI and is based on Semtech's LoRa technology. The module can be customized for specific requirements, making it suitable for applications like smart agriculture, asset tracking, and environmental monitoring. ARM MCUs come with integrated peripherals and have a robust development ecosystem. They are scalable, offering different configurations to suit specific needs, and can run various operating systems.

IV. IMPLEMENTATION

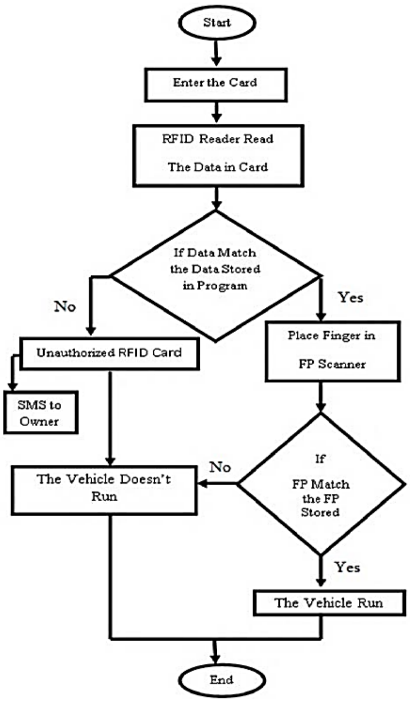
Start
Enter the Card
RFID Reader Read The Data in Card
If Data Match the Data Stored in Program
No
Yes
Unauthorized RFID Card
SMS to Owner
Place Finger in FP Scanner
If FP Match the FP Stored
No
The Vehicle Doesn't Run
Yes
The Vehicle Run
End

Fig 2 : Flow Chart of Implementation of Long Range Shared Vehicle Communication System By Using LoraWan Protocol

When the system is running, this message appears “enter the card” . The user enters the driver’s license card in the RFID reader.

The RFID reader read the data stored in the tag (DL), this data is (ID, car number). In this proposed design, it was consider that the data the data stored for only one driver’s license in order to achieve the project goals. After reading the driver’s license card contents and matching them with the data stored in the program if this happens, this means that the driver license is reliable and the owner can use the vehicle; but before the vehicle can work, it must also be verified that the person who holds the DL card is its owner and not another person.

This is done by placing the DL holder of his finger on the fingerprint scanner module. In advance, the fingerprints of trusted or authorizer persons to drive a vehicle are stored in the memory of fingerprint module. If a fingerprint match occurs, this will start the car and can be driven by this person, this message appears “system ignition” and green LED shines else cases the red LED always shines.

If an unreliable driver’s license is used, the data doesn’t match the data stored in the program. The system doesn’t respond, so the vehicle doesn’t work. This message will appear “UNAUTHORIZE _RFID” . These two steps must be taken in succession to ensure that the car works and the opposite is incorrect.

If an unreliable driver’s license is entered twice in a row, a SMS message will be sent via GSM module to the vehicle owner telling him that there is an attempted theft of his vehicle.

The driver’s license card has validity period and therefore must be renewed before the expiry of the validity period. Therefore, it is possible through the GSM module to send an SMS to notify the driver’s license holder of the remaining time to renew before expiration and to be able to drive a vehicle.

V. RESULT

The prototype model was made according to the circuit diagram and the results were as expected.

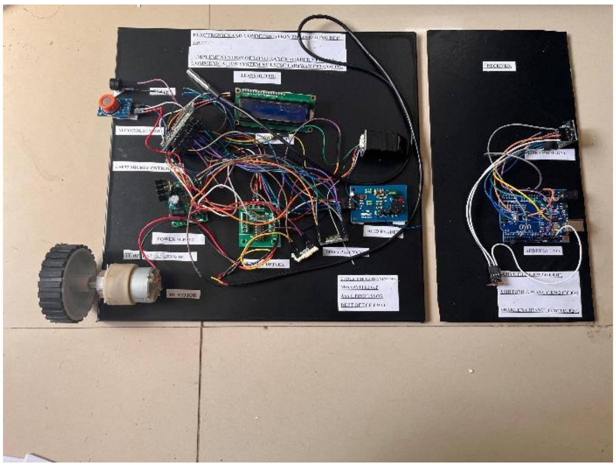

Fig 3 : Prototype of the model.

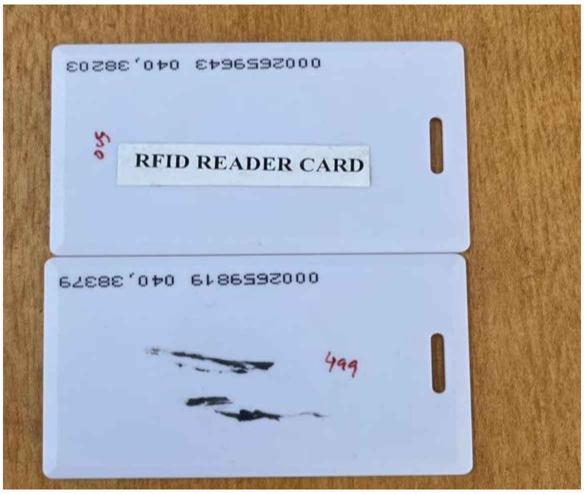

Fig 4: RFID Card

VI. CONCLUSION

In this thesis it designed security system for vehicle based on driver's license and fingerprint technology. This system prevents vehicle theft and driving without proper driving license. It achieved through select authorized driver's license his/her holder allows running the car, also to provide extra security the system contains biometrics in form of fingerprint recognition to grant access to vehicle. To prevent all possible ways to vehicle theft, GSM module is used to send SMS alter to the owner of car tell him unauthorized driver's license entered. Also used GSM module to send SMS to holder of driver's license for remember him to renewal his license before expiry. As a result the vehicle doesn't start only when the authorized driver's license entered after that verify the authorized fingerprint if these two conditions are achieved the car will be running else, the system block the vehicle ignition.

REFERENCES

[1]. Rajatabh Agarwal, Boominathan P," Vehicle Security System Using IoT Application", IRJET, Volume 05, Issue 04, Apr-2018.

[2]. A. Z. Loko, A. I. Bugaje, Usman Abdullahi," Microcontroller Based Smart Card Car Security System", International Journal of Engineering Trends and Technology, Volume 29, NO 3 November 2015.

[3]. Priti K Powale, G. N, Zade," Real time car antitheft system with accident detection using AVR microcontroller", international journal of advance research in computer science and management studies, Volume 2, Issue 1, January 2014.

[4]. Mr. Raj Rai, Prof. Dinesh Katole, Miss. Nayan Rai," Survey paper on vehicle theft detection through face recognition system", international journal of emerging trends & technology in computer science (IJETICS), Volume 3, Issue 1, January - February 2014.

[5]. C Saikrishna Prasad*, U. Sravan Kumar M.Tech, Dr.M.Narsing Yad av M.S., PhD (U.S.A), " Advanced Authentication and Security system In Vehicles", IJESMR,January 2016.