Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 2, Pages 265-267, March 2017

Smart Vehicle Authentication and Due Date Monitoring System using IoT

C.Viji[1], R.Gokul[2], N.Hari Krishnan[3] and BP.Kathiresan[4]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, SVS College of Engineering, Coimbatore, India.*
[2]*UG Scholar, Department of Electronics and Communication Engineering, SVS College of Engineering, Coimbatore, India.*
[3]*UG Scholar, Department of Electronics and Communication Engineering, SVS College of Engineering, Coimbatore, India.*
[4]*UG Scholar, Department of Electronics and Communication Engineering, SVS College of Engineering, Coimbatore, India.*

Article Received: 12 March 2017 *Article Accepted: 22 March 2017* *Article Published: 25 March 2017*

ABSTRACT

Vehicle accidents are one of the most leading causes of fatality. More accidents are because of improper driving of vehicles by non-licensed persons. One approach to eliminate the authentication of vehicles by non-licensed persons is to use a smart vehicle authentication technique for vehicles. This authentication is done by the fingerprint scanner which is the most secure system for vehicle and the smart license card which has the biometric details in it, the vehicle will start if the details in both the license and the fingerprint matches else it won't. This will stop the authentication of vehicles by non-licensed persons. Another problem is that the many person are not aware of their vehicle insurance due dates. The most popular existing system to monitor the due dates is by the GSM technique but it has lots of disadvantages. To eliminate those disadvantages the Wi-Fi system is used to send intimations. So that the person can pay the due on date without any penalty.

Keywords: Fingerprint, License, Fingerprint reader and Wi-Fi module.

1. INTRODUCTION

Unlicensed driving is a matter of concern for several reasons. It is possible that drivers who have not undergone appropriate training and testing may be deficient in some aspect of the knowledge and skills required to drive safely and efficiently. Also, drivers who are unauthorized may have less incentive to comply with road traffic laws in that they would not be influenced by the rewards and penalties set up under the licensing system. On this argument, drivers who do not hold a valid license may disregard the threat of license sanctions or the benefits of reduced insurance premium due to not having made a claim. It is noticeable in the literature [1] that the term "unlicensed" is used interchangeably to mean one of the below subcategories, as follows:

A) Drivers who drive but who have never possessed any form of license.
B) Drivers who have previously held a license but who have been disqualified.
C) Drivers possessing only a provisional license but whom, nevertheless, drive unaccompanied.

For many unlicensed drivers, enforcement and penalties are not strong deterrents and in addition there are also administrative loopholes which some exploit. There appears to be a general laxity in the system of checking the validity of documents and their ownership – for example it is claimed to be straightforward for an unlicensed driver to pass himself off as a friend (with a license) and later present the friend's documents at a police station. According to a survey by the AA Foundation for Road Safety Research it has been estimated that in Sweden approximately half of all drunken driving takes place with drivers who do not have a valid driving license (Goldberg, 1997). Also in Sweden, unlicensed driving has been estimated as the cause of 100 deaths and 2500 injuries per year at a cost of more than one billion US dollars. In the USA, in 1995, more than 10,000 lives were lost in fatal accidents with unlicensed drunk drivers (approximately a quarter of all road deaths in that year). The equivalent figure in Great Britain would therefore be over 900 deaths if this rate prevailed. An in built system [2] in an automobile which prevents such cases has therefore become vital. This paper aims to introduce a hardware architecture which detects the fingerprint as well as the validity of the license of the driver and takes a robust decision to turn on or off the ignition system based on the validity. And another major problem is that in this busy world one cannot remember his vehicle insurance date and due to this many of them got stuck up with the traffic police and paying fine to them and also to the company. This proposed system will eliminate the authentication of vehicle by unlicensed person and also make the due date payments on time.

1.1 Overview

The vehicle will ignite if the fingerprint in the driving license and the fingerprint details scanned during ignition of vehicle. If the detail doesn't match the vehicle won't start and the user cannot access the vehicle which means he is not a registered license holder according to the government data. This system can also be used to safeguard the vehicle from theft. The user needs regular key along with the proper license to access the vehicle. The vehicle need to be insured once in a year most of them won't remember the exact date and paying the fine unnecessarily. To overcome this, Wi-Fi module is used to monitor the vehicle due date and give intimation prior 2 days before the due date. This will make the user to pay the due on date and if again the user didn't pay the due means then the respective company will stop the vehicle. The vehicle will start after the successful payment of the due.

1.2 Existing System

In present days there is no proper intimation about the due dates of insurance because we are using the GSM technology. In the GSM technology there is a chance of missing the message sent by the company due to traffic in the network.

Till now the two wheeler vehicles doesn't have any specific authentication mechanism only the high rated cars have the smart mechanisms to access the vehicle.

1.3 Proposed System

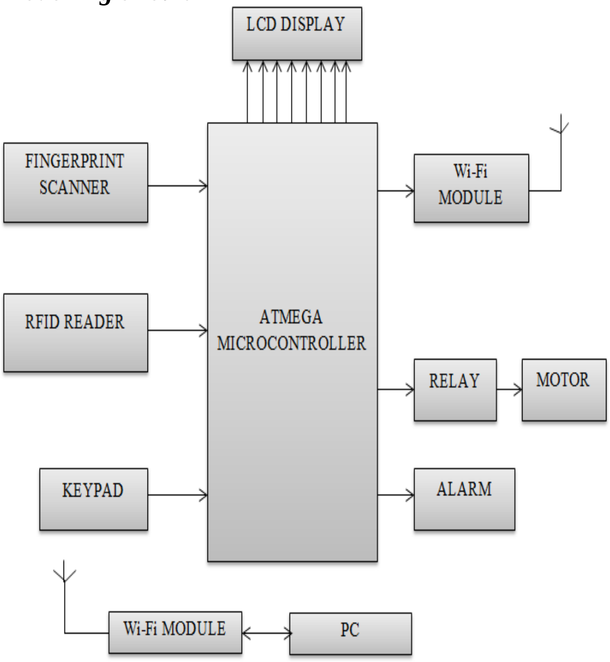
In this system we have implemented the embedded technology to authenticate [3] the vehicle and we have used the Wi-Fi module to communicate with the vehicle. This communication will help the user to get remind of the due date of the vehicle so that he will pay the due on time. On the payment date the user will be intimated about the due by the alarm so that he will pay it. In-case he fails to pay the due buzzer will be activated and stop the flow of oil to the engine by blocking the engine control unit.

For safety purpose an additional key is connected with the circuit in-case if the user is in any busy streets there is a chance of traffic congestion problems. At that time he may press that button, the vehicle will run for some time even-though the user paid the due. This is done for the safety purpose for the user and all for others.

1.4 Literature Survey

S. No.	Project Title	Author Name	Year of Publication	Approach and Concept About Work
1.	Simulation of Smart Card Interface with PIC for Vehicle Security System	Ayob Johari, Mohd. Amin bin Mohd. Zin, Mohd. Helmy Abd Wahab and Siti Zarina Mohd. Muji	2008	This system works on same machine ID for different users and smart cards of different ID, the EEPROM chip is used as the smart card for recognition. This system uses the 16F877A microcontroller chip.
2.	Smart Vehicle Security System for Defending Against Collaborative Attacks by Malware	S.Asif Hussain, Chandra Shekar Ramaiah, Yahya Al Balushi and S.Zahid Hussain.	2016	This system will ensure that only the authorized person will be able to activate and use the vehicle and thus ensuring that unauthorized access is prevented. The Person Authentication System (PAS) will prevent the person to operate the car and it will send the alert information image to the system controller.
3.	Advanced Vehicle Security System	Bibhuti Bhushan Biswal, Bunil Kumar Balabantaray, Pritpal Singh and Tanjot Sethi.	2015	This system uses the GPS and GSM techniques to prevent theft and to determine the exact location of the vehicle in case of accidents.
4.	Fingerprint Verification System on Smart Card	Masahiro Mimura, Shuichi Ishida and Yoichi Seto	2002	This system is based on fingerprint verification system operating on smart card. The card matches the cardholder‘s fingerprint and the template in it, then executes the electronic authentication process based on the PKI if they are identified. The authentication is done over the internet.
5.	A Novel IoT Access Architecture for Vehicle Monitoring System	Fang Gao, Shulong Wang, Xinrong Ji and Yibin Hou.	2016	In this system, a novel IoT access architecture is used based on field programmable gate array and system on chip (SoC), which can provide a unified access to the IoT for a wide variety of devices with associated extendibility and configurability. It uses the IEEE1451.2 standard for this design and applied the proposed design to monitor the vehicle.

1.5 Modelling circuit



Fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template which is stored and used for matching. Many technologies have been used including optical. Capacitive, RF, thermal, piezo-resistive, ultrasonic, piezoelectric, MEMS.

RFID Reader Module, are also called as interrogators. They convert radio waves returned from the RFID tag into a form that can be passed on to Controllers, which can make use of it. RFID tags and readers have to be tuned to the same frequency in order to communicate.

RFID systems use many different frequencies, but the most common and widely used & supported by our Reader is 125 KHz. An RFID system consists of two separate components: a tag and a reader. Tags are analogous to barcode labels, and come in different shapes and sizes.

The tag contains an antenna [4] connected to a small microchip containing up to two kilobytes of data. The reader, or scanner, functions similarly to a barcode scanner; however, while a barcode scanner uses a laser beam to scan the barcode, an RFID scanner uses electromagnetic waves. To transmit these waves, the scanner uses an antenna that transmits a signal [5], communicating with the tags antenna. The tags antenna receives data from the scanner and transmits its particular chip information to the scanner.

2. CONCLUSION

Thus the non-licensed persons cannot access the vehicle providing safety to oneself and to the society. And the due date payments can be done on time reducing the risk of penalty.

ACKNOWLEDGEMENT

We would like to acknowledge the Faculties of Electronics and Communication Engineering at SVS College of Engineering for their timely support.

REFERENCES

[1] Ayob Johari, Mohd. Amin bin Mohd. Zin, Mohd. Helmy Abd Wahab, Siti Zarina Mohd. Muji, "Simulation of Smart Card Interface with PIC for Vehicle Security System", *2008.*

[2] S.Asif Hussain, Chandra Shekar Ramaiah, Yahya Al Balushi, S.Zahid Hussain, "Smart Vehicle Security System for Defending Against Collaborative Attacks by Malware", *2016.*

[3] Bibhuti Bhushan Biswal, Bunil Kumar Balabantaray, Pritpal Singh, Tanjot Sethi, "Advanced Vehicle Security System", *2015.*

[4] Masahiro Mimura, Shuichi Ishida, Yoichi Seto," Fingerprint Verification System on Smart Card", *2002.*

[5] Fang Gao, Shulong Wang, Xinrong Ji, Yibin Hou, "A Novel IoT Access Architecture for Vehicle Monitoring System", *2016.*