Vehicle Security System

Arvind Kumar Pandey, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

ABSTRACT: ***Driving without a valid driver's license is a leading cause of traffic accidents. This proposal is based on a smart driver's license card that would improve vehicle security and road safety. The card assists in limiting vehicle operation based on three parameters: the expiration date of the driver's license, vehicle ownership, and the type of the vehicle for which the driver's license is granted. It is being created the hardware and software technologies necessary to increase safety and security. A secret code and the data of the vehicle with which it is related are encoded on a one-of-a-kind identification card. The authentication card will enable anybody other than the vehicle owner to operate the vehicle. When a person tries to start the car without being permitted, the short message service [SMS] system transmits the driver's license data to a pre-registered mobile number and disables the vehicle's ignition system. The simulation work of the system is described in this publication. One of the most common and reliable personal biometric identification technologies is fingerprint identification. We can prevent non-licensed drivers from driving and causing accidents by employing biometric authentication. The suggested method comprises of a smart card that can store a specific person's fingerprint. The individual person's fingerprint is to be saved in the card when issuing the license. Cars, for example, should have a card reader that can read the specific license. A fingerprint reader device should be available in the same vehicle. A person who intends to operate the vehicle must first insert the smartcard and then swipe his or her finger. If the fingerprint matches the one saved on the smart card, the system will proceed to the alcohol detection and seatbelt check. The car will be started when all authentications have been completed. If any of the authentications fail, the car will not be started and will not progress to the next phase. This improves vehicle security while simultaneously ensuring safe driving by averting collisions. The Master controller uses a prototype of the ignition system.***

KEYWORDS: ***Automotive Electronics, Automotive Theft, Fingerprint module, Road safety, Smart card reader.***

1. INTRODUCTION

In many nations, driving without such a valid driver's license is a serious problem. According to the survey, unlicensed drivers, intoxicated drivers, and drivers who do not wear seatbelts are the main causes of accidents[1]. In India, the number of accidents has been high due to dangerous road conditions. According to WHO figures from 2002 [2], [3], India was responsible for 84,674 fatalities out of a total of 11.8 million road accident deaths worldwide. The number of fatalities has risen to 92,618 in 2004. In India, the death rate is 8.7 per 100,000 people, compared to 5.6 in the United Kingdom, 5.4 in Sweden, 5.0 in the Netherlands, and 6.7 in Japan. In India, the rate of death per 10,000 automobiles is as high as 14, compared to fewer than two in affluent nations. For the years 2005, 2006, and 2014, the expected number of fatalities in India was 1, 10,300, 1, 05,725, and 1, 54,600, respectively.

Keys were utilized to start the car in the previous technique. Vehicles may be readily taken with this strategy, and accidents can be avoided. The suggested system comprises of a smart card (driver's license) capable of storing a person's fingerprint[4]. The individual person's fingerprint is to be saved in the card when issuing the license. The individual must first insert the smart card (driver's license) and produce a fingerprint. If the fingerprint matches the one saved on the smart card, the system will proceed to the alcohol detection[5] and seatbelt check. An alcohol detector is used to determine whether or not a person is inebriated. The seat belt detector confirms that the individual is wearing their seatbelt and advises them to do so.

The car will be started when all authentications have been completed. If any of the authentications fail, the car will not be started and will not progress to the next phase. If your driver's license has any of the problems listed below, the smart card reader will not accept it.

- If the validity of the driver's license has expired.
- If the driver's license[6] is a learner's permit.
- If the driver's license card has been suspended.

If the driver is inebriated or does not wear a seat belt, the ignition will cut off and a buzzer will sound. If the gasoline level sensor is low or the vehicle's speed is too high, a buzzer will sound and the fuel level and speed will be shown on the LCD display.

Modern autos are equipped with a variety of pricey security measures. The project's goal is to create a low-cost, reliable security system for autos. The "Licentronic System" is a user-friendly device that uses a microcontroller and other peripherals such as a GSM (Global System for Mobile)[7] and RFID (Radio Frequency Identification) [8] reader. If a person has a driver's license for a specific vehicle category, the system will allow the vehicle to be used once both the authentication and the driver's license cards have been validated. The vehicle-specific authentication card holds the vehicle's ownership information. The authentication card must be authenticated before anybody other than the registered owner may use the vehicle. Before the vehicle starts, the RFID reader reads three parameters from the smart driving license [expiry date, vehicle ownership, and vehicle category for which the driving license is issued].

The ignition system will be turned on after the microcontroller has confirmed these specifications. The microcontroller will not enable the vehicle to be driven if the driver's license card has expired or if the individual is not licensed to drive the vehicle type. If vehicle operation is not permitted in any situation, the system sends an alarm to a pre-registered cell phone number. The information of the driving license that is being used to drive the car is sent to the cell phone number. The major goal of this project is to determine whether or not a person is permitted to operate a car based on their driver's license and vehicle ownership. To operate a car, a driver must have a valid driver's license. This stops unlicensed drivers from operating a car and helps to reduce road accidents.

2. DISCUSSION

2.1. Cortex-M3 Lpc1768

The Cortex-M3 LPC1768 microcontroller[9] is used in this project to collect different vehicles variables. The core of the device, the Cortex-M3 LPC1768 microcontroller, is the fundamental block of authorized access control for vehicle ignition. The needed input signals from different parameters are sent into the micro controller. The different settings transmit signals to the microcontroller's separate pins. The microcontroller then branches off to any of the logical routes and provides the output to one of the ignition system unit's pins. The authentication procedure is checked using the controller. To control the device operations, all of the devices are linked to the controllers. The fingerprint of the smart card and the individual are shown on the LCD block.

The submitted finger print of the user will be compared to the finger print saved on the smart card by the microcontroller. If the driver's license card's validity has expired, the controller will not accept it. It also won't let you use your driver's license card if your driver's license is suspended for any reason. If the driving license date is close to expire, it will send an alert to the user about the driving license card's expired condition. When a legitimate driver's license is inserted but the finger print is inaccurate, the driver's license is rejected.

2.2. Smart Card Reader

In order to send and receive signals to and from the microcontroller, a smart card reader is connected to it. The smart card reader[10] can read the picture of a finger print stored on the smart card. The person's finger print image is kept on the smart card. The fingerprint reader reads the person's finger print that is saved on the smart card. The microcontroller will check for a match between the person's finger print and the finger print recorded on the smart card when the person's finger print is received.

2.3 Fingerprint Module

The fingerprint module[11] was utilized to read the pictures of the finger prints. We're utilizing the KY-M6 fingerprint module in this example. It has a capacity of 160 pictures. When someone places their finger on the reader, the LED emits infrared rays. The photons are absorbed by hemoglobin in our blood. The area where the IR rays are absorbed will seem black, while the rest will appear bright. The picture will now be captured by the CCD camera underneath the fingerprint reader. The signals will be sent to the microcontroller.

2.4. Alcohol Detector

MQ3 is the alcohol sensor in use here. The sensitivity of this sensor is great, yet the detection range is short. This sensor is designed to detect the presence of alcoholic gases. If alcohol is found, a signal is sent to the microcontroller, a buzzer is emitted, and the car is instantly halted.

2.5 Seatbelt Detector

As a seatbelt detector, we are employing infrared emitters and detectors in our project. A series resistance IR led is used to create an IR transmitter. The IR receiver component has a photodiode that collects IR photons and produces voltage variation based on IR intensity. The resulting analog voltage falls between the maximum and lowest operational ranges. The microcontroller receives this analog voltage fluctuation. When the emitter is in one knob and the detector is in another, the car will only start if these two knobs are correctly linked (i.e., the detector detects the IR light).

2.6 The Cortex-M3 LPC1768

The "LICENTRONIC" system is shown in the block diagram below. The card reader prepares to scan the authentication card and smart driving license card when the ignition key is turned "ON." The microprocessor turns on the ignition system once both cards have been validated. If the authenticity of one or both cards cannot be determined, the microprocessor transmits the invalid card's data to a pre-registered mobile number, and the vehicle does not start.

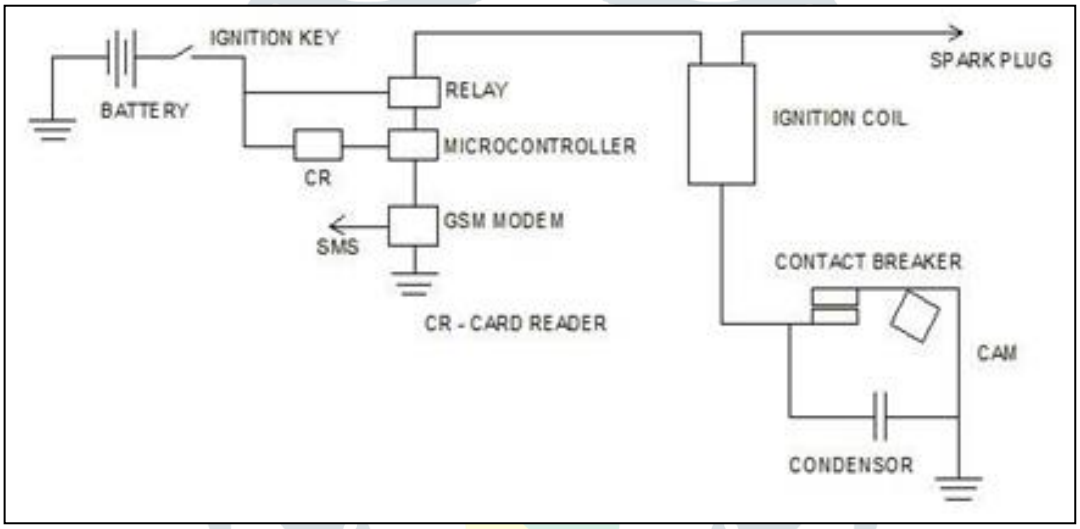

Figure: 1 Licentronic system

2.7 System Implementation

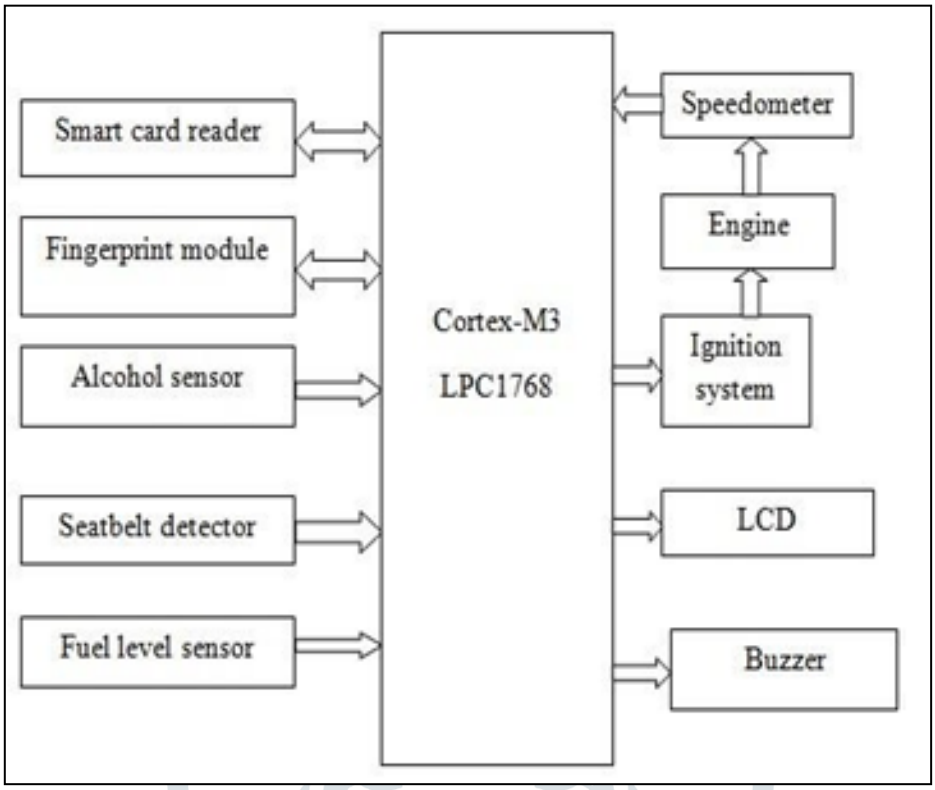

Figure 2: Block Diagram of System Implementation

In this design, the microcontroller is crucial. It accepts signals in the form of bits from different parameters and outputs them. The smart card is first put into the card reader, and then a fingerprint is taken. The given fingerprints will then be compared to the fingerprint recorded on the smart card by the microcontroller. If both match, the next step is to check for alcohol and seatbelts. The car will be lit if all authentications are successful. With these applications, the fuel level sensor will display the level of gasoline on the LCD, and the speedometer will display the vehicle's speed on the LCD.If alcohol is detected or a seatbelt is not worn, the car will be switched off and a buzzer will sound, with a notice shown on the LCD.

3. CONCLUSION

This study is about the design and development of a vehicle security system based on a driver's license. This method guards against car theft and driving without a valid driver's license. The PROTEUS 7.7 program is used to simulate the system. A physical system is being developed and will be put to the test. The technology will improve traffic safety while also reducing car theft. It would be beneficial to society as well as law enforcement if it is put in all cars. This technique might be made more easy and effective by using satellite modems as tracking devices instead of mobile phones, since the current system may fail if there is no cellular network coverage.

A pinhole camera and a GPS tracking device may be added to this setup to make it more powerful. The picture obtained by the camera, as well as GPS data, may be sent to the owner's phone, where the data may be used to identify the thief and retry the car. Based on the findings of this study, I believe that fingerprint authentication is a safe biometric authentication method that will be employed for security reasons. No one can drive without a driver's license under this system, and no one can use another person's driver's license. The system will also notify the user of the driving license's validity time using this technique. In automobiles, it also guarantees that the driver is wearing a seat belt, and it can check whether somebody is inebriated using an alcohol detector. This improves vehicle security while simultaneously ensuring safe driving by averting collisions. The current module may be used in conjunction with a GPS and GSM module to determine the position of a vehicle through mobile phone.

REFERENCES

[1] D. MOHAN, "ROAD ACCIDENTS IN INDIA," *IATSS Res.*, 2009, doi: 10.1016/s0386-1112(14)60239-9.

[2] L. O. Idris, O. O. Olaofe, O. M. Adejumobi, A. O. Kolawole, and A. K. Jimoh, "Giant mucocele of the appendix in pregnancy: A case report and review of literature," *Int. J. Surg. Case Rep.*, 2015, doi: 10.1016/j.ijscr.2015.02.042.

[3] Y. Yamamoto *et al.*, "A case of mucocele of the appendix; diffusion weighted MRI appearance," *Japanese J. Clin. Radiol.*, 2007.

[4] N. Kiruthiga, L. Latha, and S. Thangasamy, "Real time biometrics based vehicle security system with GPS and GSM technology," 2015. doi: 10.1016/j.procs.2015.03.231.

[5] P. Shrivastava, V. Lodhi, and S. V. Vargiya, "Vehicle to vehicle safety device - An ease for safe driving," 2015.

[6] M. A. Morrisey, D. C. Grabowski, T. S. Dee, and C. Campbell, "The strength of graduated drivers license programs and fatalities among teen drivers and passengers," *Accid. Anal. Prev.*, 2006, doi: 10.1016/j.aap.2005.08.003.

[7] J. Besson, "Global system for mobile communication (GSM)," *Tech. Sci. Methodes*, 1997, doi: 10.4249/scholarpedia.4115.

[8] C. M. Roberts, "Radio frequency identification (RFID)," *Comput. Secur.*, 2006, doi: 10.1016/j.cose.2005.12.003.

[9] NXP, "Mbed LPC1768," *product data sheet. developer.mbed.org.*, 2016.

[10] C. H. Lim, Y. H. Dan, K. T. Lau, and K. Y. Choo, "Smart Card Reader," *IEEE Trans. Consum. Electron.*, 1993, doi: 10.1109/30.199588.

[11] E. O. Omidiora, O. A. Fakolujo, O. T. Arulogun, and D. O. Aborisade, "A prototype of a fingerprint based ignition systems in vehicles," *Eur. J. Sci. Res.*, 2011.