VEHICLE IGNITION AND SECURITY USING BIOMETRICS

S .P. MANIRAJ[1], ASWATHY GOPALAKRISHNAN[2], OVIYA SIVAKUMAR[3], HARIHARA SUDHAN N[4]
[1]ASSISTANT PROFESSOR(Sr. G), [2,3,4] UG SCHOLARS
DEPARTMENT OF COMPUTER SCIENCE
SRM INSITUTE OF SCIENCE AND TECHNOLOGY

Abstract: **Vehicles have been used in one form or other since the invention of wheel. In earlier times crank shaft mechanism were used to ignite the vehicles. Then came keys. This project was started with the sole purpose of eliminating keys as conventional method of starting the vehicle and replacing that with biometrics. The reason for going into biometrics is that its chances of being duplicated are very less. There two main purposes for this project. First, the elimination the use of key completely for igniting the vehicle. The second purpose is to cut the cost for this technology that only the premium car makers are imposing in the market. This project has been simplified to such an extent that it can also be implemented in two wheelers as well. The system only allows authorized users to start the vehicle. For a car, the Facial Recognition/Iris scanner software permits access to the user. Users can first register into the system by scanning fingerprints. The system allows multiple users to register as authorized users. When into monitoring mode, the system checks for users to scan. On scanning, the system checks if user is authorized user and starts vehicle for authorized users only. The fingerprint sensor is connected to the microcontroller and also, we have an LCD display along with push buttons and starter motor. The motor is used to demonstrate as vehicle starter. This system automates vehicle security using a fingerprint-based system.**

Keywords—Vehicle; Security; Biometrics; Authorization; Ignition.

I. INTRODUCTION

Biometrics have been around for as long as humans have been around. Biometrics is the utilization of particular natural and additionally social qualities to distinguish a person. In spite of the fact that the historical backdrop of biometrics goes back a few thousand years B.C. With time, biometric innovation advanced rapidly and the current distinguishing frameworks offer an extensive variety of securing gadgets and robotized usefulness. These frameworks perceive diverse biometric highlights, for example, fingerprints, palm prints, confront, voice, DNA, iris, and retina Correspondent with the accessibility of various biometric frameworks is the known helplessness of these frameworks to misdirection assaults – endeavors to "trap" the framework into perceiving a fake reproduction of the organic quality as the real one. One perspective that encourages framework "satirizing" is the simplicity with which a biometric test can be acquired. By their own particular nature, most biometric frameworks can get and break down data from a separation: face, voice and iris qualifications, for instance, can be gotten without the subject's assent.

In view of expanding number of burglary instances of the Vehicle there is a need to improve the security level of the vehicles. Customary and ordinarily utilized key locks accessible in the vehicles are effortlessly opened by the expert cheats. With the assistance of ace key it turns out to be anything but difficult to open the bolt of the vehicles by the hoodlums. This makes the request of such sort of bolt which is new and gives an extra security level. The new and present day bolt should be novel i.e. it must be opened by extraordinary and particular key. This compose of highlight is accessible in the biometrics locks i.e. the bolt which must be bolted and opened by the human body highlights. Biometrics can include: facial recognition, voice recognition, fingerprint recognition, eye (iris) recognition. The idea of this paper is to remove and replace traditional ways of securing vehicles (using keys) to an advanced method of securing vehicles while eliminating the chances to lose or misplace keys.

Fingerprint of a person is examined by an exceptional sort of sensor. Fingerprint sensors can be interfaced with a microcontroller. Through keypad we can, in like manner recognize the customer by picking relating decision through keypad by the specific password. For this we utilize an ARDUINO microcontroller to activate the ignition function if the checked information and the officially existing information match. Examination is done inside the unique fingerprint module itself and its result is given to microcontroller. Result is shown in a LCD display whether the client is approved or not. An IRIS sensor is utilized along with fingerprint sensor for broadened security purposes.

II. SYSTEM DESCRIPTION

A. EXISTING SYSTEM

The traditional method for unlocking any door was a lock and key mechanism. It’s pretty simple in terms of working. Most mechanical locks are fitted to things like entryways and organizers and have two physically isolate parts. One section is fitted to the casing (the static piece of the entryway) and is basically a durable, metal fortification for a gap cut into the entryway itself (to keep the bolted entryway from being opened with savage power). The other piece of the bolt fits into a rectangular gap in the entryway (known as a mortise) and comprises of a metal instrument that moves an overwhelming jolt into or out from the strengthened gap. The jolt (now and again called a deadbolt) slides from side to side when you turn a key clockwise or anticlockwise, so it must be worked by a component that can change over revolving movement (the turning key) into responding movement (the sliding jolt)— something like a cam or wrench. On the off chance that that were everything that a bolt comprised of, each key would have the capacity to open each bolt. So the other basic piece of a bolt's instrument is an arrangement of settled or moving metal pieces (wards or tumblers) that connect with spaces cut into the key, guaranteeing just a single key can pivot, turn the cam, slide the jolt, and open the entryway. The system isn’t false proof and can be duped. Moreover, it’s easy to misplace keys and if the keys are lost, the user won’t be able to open the door.

B. PROPOSED SYSTEM

This system completely discards the use of keys by replacing it with biometric systems. In this task the equipment and the product both play an equivalent and a vital part. As opposed to utilizing the regular techniques to begin the vehicle, another strategy is utilized to begin the vehicle. Fingerprint, facial recognition of the proprietor of the vehicle can begin the vehicle. As opposed to utilising the key of the auto to begin the vehicle fingerprint is utilized to touch off, since fingers can't be copied. The 16 bit AVR microcontroller is utilized which is the focal point of the user authentication and the vehicle ignition. The fingerprint sensors take in the fingerprint of the client which in turns sends the signs to the microcontroller. The microcontroller at that point matches the examined fingerprint with the ones that are put away in its database. Once the fingerprint is coordinated, the microcontroller at that point sends the coveted flag to the vehicle after which the client can begin the vehicle. Fingerprints can be included or erased according to the clients' comfort. Since the microcontroller has a smidgen of streak memory accessible, the fingerprints can be put away in it. Three catches are present which A GSM module is likewise utilized which additionally assumes an essential part. At whatever point a non-validated individual endeavours to examine his fingerprint, a message is sent to all the enlisted clients. Since the vehicle won't begin without the fingerprint, the vehicle needs Fingerprints spared off every one of the clients who are going to drive the vehicle. A LCD show is additionally utilized which would show the status whether the fingerprints are being included, erased or effectively confirmed. The framework involves the availability with the sensors, LCD and control supply, Ignition framework, GSM Module. Giving Power Supply is additionally one of the main considerations. Since, All the equipment utilized work on +5V supply and the supply that we get in the auto is a +12V DC. Henceforth, an extra IC has been utilized to control the stream of intensity supply, with the goal that the equipment doesn't consume. GPS is additionally coordinated into it, which can pinpoint the correct area of the vehicle. This can prove to be useful if the vehicle is stolen.

III. HARDWARE USED

The main hardware used in this project are the Arduino Module, the fingerprint sensor, the GSM component and the iris recognition component. The Arduino used is Arduino UNO and the fingerprint sensor is R307. The GSM Module used in this project is SIM900A. For iris recognition, Gemini Module Camera is used, and Gemini-core 1711LQ55 is used under that.

A. R307 FINGERPRINT MODULE

This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port.

B. GEMINI MODULE CAMERA

Gemini module camera is a dual iris scanning OEM module at extended capture range of 55 cm. Gemini-core 1711LQ55 is a small form-factor module storing up to 10,000 templates (expandable up to 200,000 IDs) and versatile to various application sectors, which leverages the use of Gemini in local recognition or in heterogeneous system.

C. GSM MODULE - SIM900A

SIM900 delivers GSM/GPRS 850/900/1800/1900MHz performance for voice, SMS, Data, and Fax in a small form factor and with low power consumption. With a tiny configuration of 24mm x 24mm x 3 mm, SIM900 can fit almost all the space requirements in M2M applications, especially for slim and compact demands of design. Features include Quad-Band 850/900/1800/1900 MHz, GPRS multi-slot class 10/8, GPRS mobile station class B, Compliant to GSM phase 2/2+, Class 4 (2 W @850/ 900 MHz), Class 1 (1 W @ 1800/1900MHz), SAIC (Single Antenna Interference Cancellation) support, Control via AT commands (GSM 07.07 ,07.05 and SIMCOM enhanced AT Commands).

D. ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328. Arduino is an open-source, prototyping platform and its simplicity makes it ideal for hobbyists to use as well as professionals. The Arduino Uno has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. The Arduino Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 microcontroller chip programmed as a USB-to-serial converter. Features include ATmega328 Microcontroller, 5V Operating Voltage, 7-12V Input Voltage (recommended), 6-20V Input Voltage (limits), 14 (of which 6 provide PWM output) Digital I/O Pins, 6 Analog Input Pins, 40 mA DC Current per I/O Pin, 50 mA DC

Current for 3.3V Pin, 32 KB of Flash Memory of which 0.5 KB used by bootloader, 2 KB (ATmega328) SRAM, 1 KB (ATmega328) EEPROM, 16 MHz Clock Speed.

IV. *ARCHITECTURE*

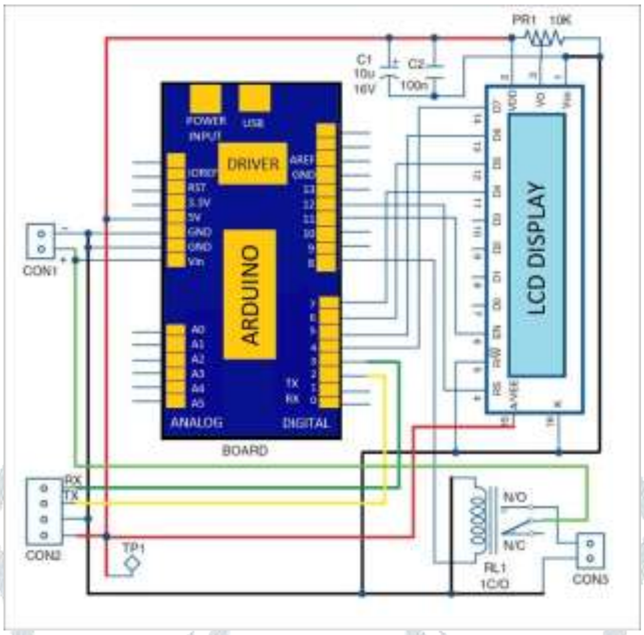

Fig.1: System Architecture of Fingerprint Module

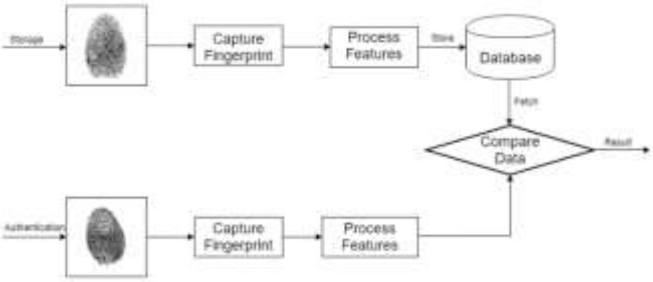

Fig.2: Fingerprint Module Working Principle

V. LITERATURE SURVEY

Our base paper is titled Vehicle Ignition Using Biometric Data by Mani Susarla, Chiranjeevi Akhil, Aravind Reddy and Shamela Rizwana [1]. The main objective of this paper is to study the biometric vehicle ignition. Keys need to be carried and misplacing keys or losing them will cause a serious issue. This can be solved by incorporating a fingerprint scanner. User just needs to scan finger to start the car, no need to carry any key. The system only allows authorized users to start the vehicle. Users can first register into the system by scanning fingerprints. The system allows multiple users to register as authorized users. The next paper is titled Changeable Biometrics for Appearance Based Face Recognition written and published by MinYi Jeong, Chulhan Lee, Jongsun Kim, Jeung-Yoon Choi, Kar-Ann Toh and Jaihie Kim [2]. This paper emphasizes on enhancing security and privacy in biometrics. This concept transforms a biometric signal or feature into a new one for enrolment and matching. The system proposes changeable biometrics for face recognition using an appearance-based approach. The paper Biometric Identification via Retina Scanning with Liveness Detection Using Speckle Contrast Imaging by Nazariy K. Shaydyuk and Timothy Cleland [3] tells us about current biometric modalities that include fingerprint, palm, voice, face, gate, iris and even DNA recognition. Also, another known biometric technique involves subject identification using retinal blood vasculature pattern matching. The paper says that there is an inherent requirement for liveness detection so as to make the acquisition system less susceptible to deception. So the authors have elaborated on the Laser Speckle contrast imaging concept. Laser speckle contrast imaging is a common method of blood flow detection and could be used to explicitly confirm liveness. The dynamics of the speckle pattern can be statistically quantified and interpreted as the regions with and without flow. To support the incorporation of an iris scanner in our project, the paper The Human Iris Structure and Its Application in Security System of Car published by Sreekala.P, Victor Jose, James Joseph and Shibin Joseph [4] deals with the security features of a car incorporated with an iris recognition. Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eyes. Iris technology has the smallest outlier group of all biometric technologies. The only biometric authentication technology designed for use in a one-to many search environments, a key advantage of iris recognition is its stability. Iris recognition method performs better than all other image processing systems. The next paper is titled Intelligent Safety and Security Systems in Automobiles written by Raja Raghavan.M and Dr.N.S.Bhuvaneswari [5]. This paper aims at giving an overview of implementing safety and security systems in automobiles for today and future development. The objective to minimize the road accidents using Arduino platform. In this paper, few concepts are proposed related to implementing security systems in automobiles. Other proposed concepts to be implemented are regarding safety systems to reduce or avoid road accidents due to disobeying of traffic rules.

VI. METHODOLOGY

According to this method, vehicle ignition using biometrics instead of keys is implemented. For this, a fingerprint scanner, an iris scanner is required along with a microprocessor and database that stores the registered user's details. The fingerprint scanner and the iris scanner are used to register users' data in the system. The first user authorization is done by the owner when this system is first installed in the vehicle. Then, to add more authorized users, authorization by an already existing user has to be done. Once the authorization is complete, the new user scans their fingerprint and iris and requests to store the information in the database and becomes an authorized user. After this, the recognition devices are activated and put to use. To start the vehicle, the user has to be an authorised user in order to get access to the vehicle. During authentication, first the user requests to be authenticated. The fingerprint scanner and the iris scanner are activated in succession and get the requesting user's details one by one. Then, these are compared with the already existing information stored, and if they match with the stored information access is granted and the user can start and use the vehicle. Else, an error message is displayed that the user's details did not match and authentication failed. The message is displayed on any display device incorporated into the vehicle. Along with an error message, in case of multiple failed attempts, an SMS is sent to all the authorized users, which is done using the GSM module incorporated into the system. This is done in order to notify the user in case any undesired user tries to access the vehicle, or in case of theft.

VII.FUTURE WORK

The first area of improvement would be the accuracy and reliability on the authentication process. The room for error should be brought down to nearly null and that will enhance the dependability of the system. The components can be upgraded too, with enhancement in technology and quality and capability of parts, the accuracy and speed will also increase. The range of compatible vehicles can be increased; instead of just a car being enabled with this system, any vehicle ranging from bikes to Lorries, regardless of the size, which helps reduce thievery on an extremely significantly large scale.

VIII.CONCLUSION

The ignition of vehicles without the use of any key and with the use of biometric authentication instead is definitely a more secure way of using a vehicle which is becoming more and more expensive with more and more technological advancement. The use of fingerprint scanner and iris recognition helps to boost security significantly, owing to the uniqueness of people's fingerprints and irises. The authentication process is well-planned and works in succession and coordination. This concept definitely helps to reduce theft and can become very reliable and extremely widely used in the future.

IX.REFERENCES

[1] Mani Susarla, Chiranjeevi Akhil, Aravind Reddy, Shamela Rizwana, "Vehicle Ignition Using Biometric Data", Journal of Network Communications and Emerging Technologies (JNCET), Volume 8, Issue 5, May (2018).

[2] MinYi Jeong, Chulhan Lee, Jongsun Kim, Jeung-Yoon Choi, Kar-Ann Toh, Jaihie Kim, "Changeable Biometrics for Appearance Based Face Recognition", 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, IEEE.

[3] Nazariy K. Shaydyuk, Timothy Cleland, "Biometric Identification via Retina Scanning with Liveness Detection Using Speckle Contrast Imaging", IEEE, 2016.

[4] Sreekala.P, Victor Jose, James Joseph, Shibin Joseph, "The Human Iris Structure and Its Application in Security System of Car", IEEE, 2012.

[5] Raja Raghavan.M, Dr.N.S.Bhuvaneswari, "Intelligent Safety and Security Systems in Automobiles", 2015 IEEE International Conference on Technological Innovations in ICT for Agriculture and Rural Development (TIAR 2015).

[6] www.circuitstoday.com/arduino-nano-tutorial-pinout-schematics

[7] https://learn.adafruit.com/lesson-0-getting-started/overview

[8] https://www.electroschematics.com/.../how-to-use-fingerprint-identification-modules/

[9] https://forum.arduino.cc/index.php?topic=259190.0

[10] www.academia.edu/6994348/Fingerprint_and_GSM_based_Security_System