A Project Report On

Authenticated Access Control for Vehicle Ignition System by Driver's License and Fingerprint Technology

Submitted in partial fulfillment of the requirement for the 8^{th} semester

Bachelor of Engineering

in

Computer Science and Engineering

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560111

Submitted By

Bindu B S 1DS20CS404

Darshini B S 1DS20CS406

Dhanushree M S 1DS20CS407

Tarun K P 1DS19CS752

Under the guidance of

Prof. Prasad A M

Professor, CSE , DSCE

And

Yash Shah

Co-Guide-Big Data Devops at Informatica

2022 - 2023

Department of Computer Science and Engineering

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Bengaluru - 560111

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Dayananda Sagar College of Engineering

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560111

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that the project entitled **Authenticated Access Control for Vehicle Ignition System by Driver's License and Fingerprint Technology** is a bonafide work carried out by **Bindu B S [1DS20CS404]**, **Darshini B S[1DS20CS406], Dhanushree M S[1DS20CS407]** and **Tarun K P[1DS19CS752]** in partial fulfillment of 8th semester, Bachelor of Engineering in Computer Science and Engineering under Visvesvaraya Technological University, Belagavi during the year 2022-23.

Prof. Prasad A M	**Dr. Ramesh Babu D R**	**Dr. B G Prasad**
Professor	Vice Principal & HOD	Principal
CSE, DSCE	CSE, DSCE	DSCE
Signature:.....	Signature:.....	Signature:.....

Name of the Examiners: Signature with date:

1..... .....

2..... .....

Acknowledgement

We are pleased to have successfully completed the project **Authenticated Access Control for Vehicle Ignition System by Driver's License and Fingerprint Technology**. We thoroughly enjoyed the process of working on this project and gained a lot of knowledge doing so.

We would like to take this opportunity to express our gratitude to **Dr. B G Prasad**, Principal of DSCE, for permitting us to utilize all the necessary facilities of the institution.

We also thank our respected Vice Principal, HOD of Computer Science & Engineering, DSCE, Bangalore, **Dr. Ramesh Babu D R**, for his support and encouragement throughout the process.

We are immensely grateful to our respected and learned guide, **Prof. Prasad A M**,Professor CSE, DSCE and our co-guide **Mr. Yash Shah**, for their valuable help and guidance. We are indebted to them for their invaluable guidance throughout the process and their useful inputs at all stages of the process.

We also thank all the faculty and support staff of Department of Computer Science, DSCE. Without their support over the years, this work would not have been possible.

Lastly, we would like to express our deep appreciation towards our classmates and our family for providing us with constant moral support and encouragement. They have stood by us in the most difficult of times.

Bindu B S 1DS20CS404

Darshini B S 1DS20CS406

Dhanushree M S 1DS20CS407

Tarun K P 1DS19CS752

Abstract

In the modern world, our vehicles are a valuable asset to us, yet we have little control over their security. It has been observed recently in recent years that automobile thefts and the usage of stolen cars in shady activities by thieves have escalated. The criminals steal various autos using cutting-edge, contemporary techniques. To stop the theft of vehicles, substantial measures must be found. The system was created and is installed in the car. The system's command centre is the microcontroller. The ignition and fuel flow into the engine can then be controlled by reading the signals the mobile device receives. Due of the system's ability to track vehicles, transportation and travel businesses find it to be highly helpful. One of the most widely used and trustworthy personal biometric identification techniques is fingerprint identification. We can stop those without valid licences from driving and thereby creating accidents by employing this biometric authentication. The proposed method comprises of a smart card that may store a specific person's fingerprint. The particular person's fingerprint is to be saved in the card while the licence is being issued. Cars and other vehicles should have a card reader that can read the specific licence. The same vehicle should be equipped with a fingerprint reader.Anyone who wants to operate the vehicle must first insert their smartcard inside it before using their finger to operate it. Alcohol detection and seatbelt checks begin if the fingerprint matches the fingerprint on the smart card. The car will be lit once all authentications have been successful. If any of the authentications are unsuccessful, the vehicle won't start and won't move on to the next phase. By avoiding accidents, this improves vehicle security and assures safe driving. The Master controller makes advantage of the ignition system prototype.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Recently, we have focused on fingerprint scanning when talking about biometrics. As a scanner for this, we are using a FIM 3030N high voltage module. EEPROM and RAM are incorporated into this module. We can store as many users' fingerprints as 'n' in this. There are two operating modes for this module: Master mode and User mode. The fingerprints will be registered in Master mode and given a special ID before being saved in the scanner's ROM. We'll be utilising this module in user mode once it's connected to the Arduino. This mode will be used to compare the scanned and saved photos for accuracy. Citizens' photographs will be saved in a module with a special ID when they visit our application. Police must scan citizens' images as necessary, which are compared to the images in the fingerprint module and updated in the citizen's record. Serial communication is enabled to connect this scanner to Arduino. We will be able to control the scanning process by utilising this controller. The outcome of the scanning is saved in the controller after it is finished. The information on the person can be obtained by just pressing a switch. For this project, a controlled 500mA, 5V power source is used. Voltage regulation is accomplished using the 7805 three terminal voltage regulator. The secondary output of the 230/12V step down transformer's ac output is rectified using a bridge type full wave rectifier.Fingerprints are straightforward to use, inexpensive, and best suited for miniaturisation. They also have specific characteristics that don't alter over the course of a lifetime.The crime that is perhaps expanding the quickest in India is vehicle theft. Experts and political commentators agree that there is a growing issue with the lack of parking in residential neighbourhoods. Over 100 vehicles are reported stolen daily in some major areas, and the numbers aren't any better in rural areas.

1.1 The Problem

When traditional physical car keys are replaced by digital ones, wireless key fobs, and mobile applications, auto thieves can enter the vehicle without being seen. If the owner is still close to their vehicle, this can be done by intercepting communication between a smartphone or wireless key fob and the vehicle, utilising gadgets that increase the range of the wireless signal, and simulating the wireless key to access a vehicle using the owner's own wireless key fob. If done incorrectly, managing virtual car keys can be just as challenging as managing physical ones. A key's enrollment, an attempt to "unlock" it, and, most crucially, its revocation must all be handled securely.

1.2 Real World Application

The project was created to address a genuine issue and be used in the actual world. utilising the already-existing Face, Fingerprint, and Password recognition. We decrease our reliance on hardware. The following are a some of the most notable real-world applications:

Applications of Biometric In Automobiles : The use of vehicles is a basic requirement for everyone in the modern world, where technology is developing quickly and scientists are making groundbreaking discoveries on a daily basis. Currently utilised extensively in forensics, including criminal identification and jail security, biometrics is a rapidly developing technology that has the potential to be applied in a wide variety of civilian application areas. The use of biometrics can stop unauthorised access to computer networks, desktop PCs, mobile phones, smart cards, and ATMs. It can be used for telephone and online transactions (including electronic banking and electronic commerce). With key-less entry devices, biometrics can take the role of keys in automobiles. Although there are various technologies that fall under the biometric umbrella, each operates somewhat differently.

Vehicle tracking : The GPS receiver in the vehicle tracking system delivers the car's current location in real time. After a predetermined amount of interval, the MCU (Main Control Unit) deposits this real-time data into the MMC (Main Memory Module). The MCU, which is used to send and receive the SMS, is obviously linked to the GSM module. The GSM module extracts the data from the MMC and transmits it to the registered user's mobile phone. Longitude, latitude, altitude, speed over ground, course over ground, real-time time, and date make up this data. We can then find the exact position of the vehicle by utilising Google Maps.

Finger Print Vehicle Starter and Theft Control : One of the oldest and most modified biometric systems is the fingerprint, which is commonly used in biometric forms of identification. As crime has

become more prevalent, vehicle safety has become a critical issue. These days, automobile keys are a huge worry because they are frequently forgotten or misplaced while carried. a system that starts cars using fingerprint authentication. With this technology, the driver can start the automobile using the fingerprint reader. This technique first enables the user to authenticate by scanning their distinctive fingerprint. They might record many fingerprints to start the car. The device alerts security and turns off the ignition by having turned off the petrol nozzle in the event of a breach using GPS when the IC is located by an unrecognised user when the user scans their fingerprint in monitoring mode, if the framework does not recognise or memorise the fingerprint,or if the unknown person scans.

Real Time Biometrics Based Vehicle Security System : In the modern world, when science and technology are developing at a rapid pace and new discoveries are being made every day, security is becoming more and more important everywhere. Currently, everyone uses cars as a basic requirement. Protecting the vehicle from theft is also crucial at the same time. Traditional vehicle security systems are expensive and rely on numerous sensors. When a car is stolen, there is no longer any recourse or any way to assist the owner in recovering their car. This paper's major objective is to safeguard the car from any unauthorised entry utilising a quick, simple, clear, dependable, and affordable fingerprint identification technology.

1.3 Organization of Project Report

The project report is organized as follows:

In Chapter (2) we discuss the problem statement and the proposed solution. We also take a look at the systems that exist today and the drawbacks they face. Chapter (3) with a survey on existing literature available.Chapter (4) looks at the architecture and sys. em design of the proposed solution with an overview of the system design, utilizing system block diagrams and data flow diagrams.Chapter (5) drives into the Implementation of the solution, by describing the hardware and software requirement along with the implementation details.Chapter (6) Comaprison of different test case takes place. Chapter (7) looks at our experimentation process and the obtained results.Chapter (8) summarizes our findings and concludes the paper.

1.4 Summary

Chapter 1 introduces us to the problem caused by the vehicle theft and what precautions need to be taken to prevent theft of vehicles, and all the methods used to provide the security for vehicles and in this it tells us where and all those systems can be used in a real world application to prevent the tragic events caused by the vehicle theft.

Chapter 2

Problem Statement and Proposed Solution

2.1 Problem Statement

The number of bikers in our nation is growing, which means that there are more road accidents and deaths as a result. The majority of these deaths are brought on by the most common neglect of not wearing a helmet, and many other deaths are brought on by the failure to provide the injured party with the appropriate medical attention they require. The initiative attempts to protect bikers from traffic accidents by securing their vehicles.

2.2 Existing Systems

This invention secures the vehicle by utilising both the use of seat belts and new technologies to unlock the automobile door. Only the GPS and GSM modules of the current system are used to identify and inform the driver of their current location.These modules are installed inside of the vehicles. Therefore, this system will send an alarm message to the car owner's mobile device if the driver steers the vehicle in the wrong direction. The current system only keeps track of the car and then informs the owner of its condition. Even the security of the traveller is important to this system.

Recently, a variety of vehicle anti-theft systems have been created, but the results are still unsatisfactory because every gadget has cons. Three technological groups divide domestic and international car anti-theft products:

Mechanical lock devices: A mechanical lock physically turns a lock mechanism with a key to unlock a door, whereas an electrical lock activates the lock mechanism electrically, frequently with the use of a keycard or code. A mag lock, also known as a magnetic lock, is a form of electrical lock that is held in place by an electromagnet that is activated when power is provided to it.

Vehicle tracking: As previously indicated, a vehicle tracking system uses GPS technology to track

the location of a moving vehicle. It helps with vehicle recovery and offers you access to all kinds of information about your car. You can purchase safety product add-ons from Cartrack in addition to stolen car recovery, including the Cartrack panic button. By pressing this panic button in the event of a hijacking, a discreet alarm will be transmitted to our around-the-clock control centre.

Car Alarm System: A car alarm is a piece of electrical equipment that is installed in a car to deter theft of the automobile, its contents, or both. When the criteria required for activating it are met, car alarms work by releasing loud sound (typically a vehicle-mounted siren, klaxon, pre-recorded vocal warning, the vehicle's own horn, or a combination of these).

2.3 Proposed Solution

The fingerprint-based licence checking system will be implemented using a biometric module, an Arduino UNO, a 16x2LCD, a serial monitor, and a keypad. The block diagram depicts how the system will function overall. A fingerprint scanner and keypad will be connected to an Arduino Uno microcontroller, which will also be connected to a 16x2 LCD display, a serial monitor LED, and a buzzer that responds to Arduino Uno's output.For beginners, the Arduino-based fingerprint-based licence system's operation can be a little challenging. The user must first enrol a finger with the aid of pushbuttons or keyboard keys. In order to do this, the user must press the ENROL key. The LCD will then prompt them to enter the location and ID where the finger will be saved. Thus, using the UP/DOWN keys, the user must now enter the ID (Location). The user must then click the OK key (DEL key) after selecting Location/ID. The LCD will now prompt you to place your finger over the fingerprint reader. The user must now place his finger on the fingerprint reader. The LCD will prompt you to take your finger out of the fingerprint module before asking you to put it back in. The user must now place his finger over the fingerprint reader once more. The fingerprint module now uses an image to create templates, which it then saves in its memory according to a chosen ID. Now that the user has registered, they may access. All users can be added to the system using the same procedure. This fingerprint-based licence system's block diagram is very straightforward; it includes an Arduino for controlling the project's entire workflow, a push button for enrolling, deleting, choosing IDs, and accessing purposes, a buzzer for alert, LEDs for indication, and a 16x2 LCD for instructing users and displaying the results as well. Green LED shows that the system is prepared to accept access or check the validity of a licence, while Yellow LED indicates that the fingerprint module is ready to take a finger image.For integrating the fingerprint module with the Arduino board, we used the Adafruit Fingerprint Sensor Library in a programme. Below is a link to the entire Code. The basic features of the Arduino programme are explained here.And here, we have an RFID reader that we utilised to

confirm the driver's licence. This allowed us to determine if the DL belonged to an authorised person or not. If not, the message is sent to the authorised mobile. message that will be registered here will be transmitted over Telegram.Here, a two-step verification process involving driving licence and fingerprint checks will be carried out in order to properly secure the vehicle.

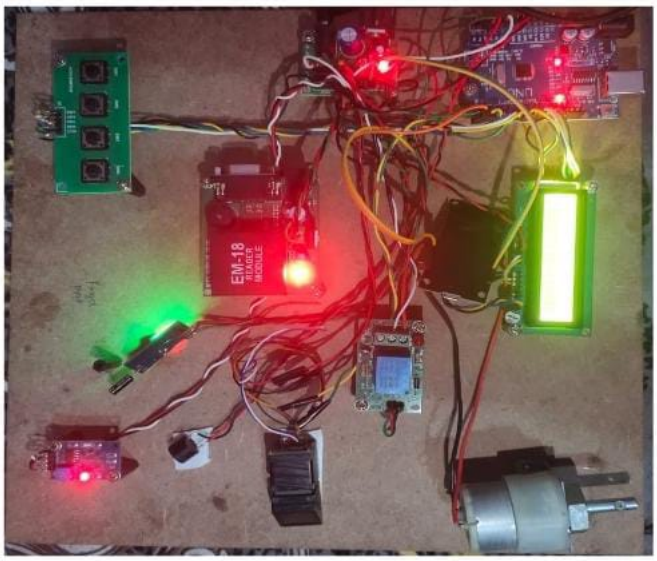

Figure 2.1: All the components are conected

The technology offers a hassle-free, secure way to start (or stop) a vehicle's engine. To start the car, all the user needs to do is scan their finger; there is no need to carry a key. The car can only be started by people who are authorised by the system. By scanning their fingerprints, users can first register on the system. Multiple people can register as authorised users on the system. The system looks for people who want to scan when it is in monitoring mode. When scanning, the system determines whether the user is an authorised user and only allows authorised users to start the vehicle. The owner's fingerprint is required to start the car. Since fingers cannot be copied, using a fingerprint instead of the car's key to start it is more secure. The fingerprint sensors read the user's fingerprint, which then transmits signals to the Arduino. Following that, the Arduino compares the scanned fingerprint to those in its database. The Arduino then transmits the required signal to the vehicle after the fingerprint match, allowing the user to start the vehicle. The users' convenience can be taken into account when adding or removing fingerprints. The fingerprints can be saved in the Arduino because it has some flash memory accessible. A notification is delivered to all registered users if a non-authenticated person tries to scan their fingerprint. Since without the fingerprint, the car will not start. All users who will operate the car must have their fingerprints stored on the vehicle.

Additionally, an LCD display is employed to show the status of fingerprint addition, deletion, or successful authentication.

2.4 System Requirements

2.4.1 Hardware Components

1.Arduino UNO

One type of microcontroller board built on the ATmega328 is called the Arduino Uno, and uno is an Italian word that signifies one. I/O pins, an ICSP header, a power jack, 6 analog I/Ps, a ceramic resonator operating at A16 MHz, a USB port, and 14 digital I/O pins.

2. Power Supply

The most practical and user-friendly breadboard component is the 3.3V/5V output MB102 Breadboard power supply module, which may be added to any applications involving breadboards where 5V, 3.3V, or both power requirements are necessary.

3.LCD(Liquid Crystal Display)

A type of flat panel display known as an LCD (Liquid Crystal Display) operates primarily using liquid crystals.Since they are frequently used in cellphones,televisions, computers, and instrument panels, LEDs offer a wide range of applications for consumers and enterprises.

4.RFID (Radio Frequency Identification) Reader

Tags and readers are the two halves of the wireless system known as Radio Frequency Identification (RFID). The reader is an electronic gadget with one or more antennas that transmit radio waves and take in signals from RFID tags.

5.Relay

Relays have the benefit that only a modest amount of electricity is required to run the relay coil. However, a relay switch circuit can be used to control motors, heaters, lamps, or AC circuits, all of which have the potential to consume a significant amount of additional electrical power.

6.DC motor

Any of a group of rotating electric motors that use direct current (DC) electricity to create mechanical energy is referred to as a DC motor. The most prevalent kinds depend on the forces created by induced magnetic fields brought on by current flowing through the coil.

7.Node mcu

A low-cost System-on-a-Chip (SoC) called the ESP8266 serves as the foundation of the open-source NodeMCU (Node MicroController Unit).

8.Buzzer

A beeper or buzzer, for example, could be electromechanical, piezoelectric, or mechanical in design. The signal is converted from audio to sound as its primary function.

9.Vibration sensor

The quantity and frequency of vibration in a system, machine, or piece of equipment are measured by a vibration sensor. Vibration sensors can be used to provide maintenance teams with information about conditions inside crucial assets that could cause equipment failure.

2.4.2 Software Components

1.Arduino IDE

Sketches are computer programmes created using the Arduino Software (IDE).

2.Embedded C

The C Standards committee created Embedded C as a set of language that is an extension for the C programming language to address concerns that were shared by C extensions for various embedded systems.

2.5 Summary

Here we have defined the problem statement of our proposed system and existing system,and to overcome these drawbacks, we have used different technologies such as a Fingerprint sensor module for fingerprint verification, an RFID reader as the two step authentication for validating the driving licence, and Vibration sensor for unauthorized detection and speed limit.To overcome the drawbacks mentioned in the existing system we used this approach.

Chapter 3

Literature Survey

3.1 Design and Implementation of Bio-metric Based Smart Antitheft Bike Protection System,

This paper proposes a biometric based smart antitheft bike protection system to ensure more security and avoid unauthorized use of motorbikes. The proposed system uses a finger print based simple and efficient electric engine starter, which is designed, implemented and tested with motorbikes. Test results show that the developed system can identify the correct person and allow the right person to start the bike. The cost of existing systems is high, so there is a need to design a low cost security system for the two wheelers. The proposed security system uses an Arduino microcontroller and a fingerprint scanner to increase the security aspect of vehicles.

It is designed to provide proper compatibility between the finger print unit and the microcontroller unit, allowing the starter unit associated with the engine to be anable to provide proper security. The existing system uses a key switch short circuited by pressing the self starter, causing the electro motive force to be induced in the relay, causing the metal rod to contact the terminal and start rotating. The solenoid assembly is used to open the contacts and to stop the motor if necessary. The proposed system consists of an Arduino microcontroller, a fingerprint scanner, an OLED display, a battery, a relay, and a voltage regulator. The battery provides the continuous power supply to the ignition system, while the 7809 voltage regulator regulates the voltage to 9v and the 7805 voltage regulator provides 5v supply to the fingerprint scanner module, OLED display, and relay.

If the fingerprint is matched, the control of Arduino will move to the relay, which ignites the ignition system. If the key is turned on and fingerprint is matched, the ignition system will be turned on and bike gets mobilized. The finger print scanner is a light sensitive micro chip which consists

of either a Charge Coupled Device or a Complementary Metal Oxide Semiconductor image sensor which produces a digital image. The second type of image scanner is made with capacitance principle, which measures the finger electrically. Relay switches are used to open and close the ignition system according to the voltage applied through it.

A voltage regulator is a circuit used to maintain a constant output voltage in a circuit, irrespective of changes in the incoming voltage or load current. Relay module for Arduino is one of the most powerful. Arduino Uno is a microcontroller that can be used to control both A.C and D.C devices by giving 5V to a relay. This relay can be used to control high voltage and low voltage electronic devices. The main hardware unit used is Arduino Uno, which has fourteen digital inputs and outputs and six digital inputs and outputs.

3.2 Improving Driver Identification for the Next-620 Generation of In-Vehicle Software Systems

Using convolutional neural networks and recurrent neural networks, this study offers a new driver identification model that is based on data gathered from smartphone sensors and/or the OBD-II protocol. It is used in Automotive Grade Linux Framework as a real-time anti-theft and driver profiling system after being tested on various datasets. The suggested approach was put into practise in the Automotive Grade Linux Framework as a real-time anti-theft and driver profiling system after being evaluated on various datasets. The automotive sector is transitioning from a product-based to a service-based economy, where all parties (vehicle manufacturers, communication and software businesses) are collaborating to offer improved services for the connected automobile. A modern car may contain numerous built-in and mobile sensors, as well as numerous ways to link to other cars, roadways, and other drivers digitally.

Many standardised methods, like the OBD-II protocol, can be used to obtain this data, which contains details about the car and the driver. In order to improve driver profiling and vehicle security in connected automobiles and other emerging paradigms like shared mobility and car sharing, this article examines driver identification and fingerprinting utilising driver behaviour data. It views driver identification as a multivariate time series classification problem and driver personal data as a time series.

The primary contribution of this study is the treatment of driver personal information as a time series and driver identification as a multivariate time series classification issue. Using a deep learning model, this paper's goal is to pinpoint the driver of certain unknown driving data.

In order to accomplish this, a comprehensive end-to-end framework for driver identification is proposed, consisting of four steps: data collecting, data processing, data classification, sensor data anomaly detection, and technical realisation of the technique within the Auto-Motion Grade Linux Framework. The UAH-Driveset, OSF, OSF + Physio, and HCILAB datasets are used to evaluate the proposed model.

3.3 New and Simple Offline A uthentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles

For car sharing vehicles, this study suggests an offline authentication method based on the TOTP algorithm and an extra security biometric component. This strategy is split into online and offline schemes to offer a secure solution, and the originality is that it can let authorised drivers start and function in a secure manner while offline simply by utilising their mobile devices. It also offers defence against the common replay assault used against keyless start autos. Urban transportation networks use more sophisticated smartphone-based applications to provide access to this infrastructure as the worldwide car-sharing business has risen tremendously over the past ten years. One of the most popular options for individual users and viewed as an alternative to the availability and upkeep of private vehicles is car-sharing services.

It offers a smart automobile rental service where registered users can access and store shared for short- or long-term use, automobiles without any human involvement. A variety of mobile automotive sharing applications have been developed by businesses, along with common cars and automotive sharing systems.like Kwikcar, SOCAR, and GoCar in Malaysia. The Internet of Things (IoT) is a cloud-based network of physical things for data collection, monitoring, and exchange that includes apps, sensors, actuators, network connectivity, and other objects. It allows for remotely handled or sensed devices based on network connectivity. Since external staff members could be present on the assembly line, offline authentication is a crucial problem in the context of vehicles.

The majority of current systems rely on the constant availability of wireless networks, although this isn't always the case. With more attack surfaces because to the Internet of Things, cybercriminals can now thoroughly test their techniques. An alarming example of the dangers of connected cars and the Internet of Things was recently encountered by a technology reporter for The Guardian. Kari Paul had bought a car with GIG Car Share, but the rental Prius refused to go since the telematics system lost its cell signal and it was left unpaved.

3.4 Secure Biometric-Based Authentication Protocol for Vehicular Ad-hoc Network

This study suggests an embedded IoT-based system for vehicle security and driver monitoring that requires biometric verification to enter the car. Open source software, a high-resolution camera, a vibration sensor, and Raspberry Pi were used in the system's design and development. In the event that vehicle entry is denied or an accident occurs, it employs biometric authentication to gain access to the vehicle, takes pictures, and emails them to the owner or authorised person. This makes it possible to watch the driver and the interior of the car, which will aid in catching criminals. New automobiles with cutting-edge technologies have been released as a result of the exponential rise in vehicle production, yet these features are insufficient to stop crimes like vehicle theft and misuse.

A remedy, such as "Biometric Authentication" for vehicle access, is being developed as a response to this. India is one of the nations that uses the most internet data, so it's crucial to make the "Biometric Authentication" system user-friendly by including IP addresses for internet communication and offering driver surveillance. The methods and concepts discussed in this work that are utilised to prevent car theft, such as GPS and biometric verification (finger, eye, and face), are the most crucial information. While GPS provides a vehicle's position in terms of latitude and longitude, biometric authentication makes use of facial recognition, voice recognition, retinal scanning, finger scanners, and voice commands. Additionally, biometric systems give awareness by sounding alarms, stopping the fuel supply, locking doors, and transmitting images to another system.

Most of the time, data is transmitted by SMS or MMS using GSM/GPRS modules. The fact that a vehicle's tracking aids in its recovery and that the actual victim is not named is the text's most crucial nugget. This approach, like SMS and MMS, has drawbacks of its own, such as excessively high costs and battery drain. In the event of a collision, urgent surveillance is required to check on the driver or the interior of the car. Adding a driver surveillance system is the suggested remedy since it can deter crime, aid in victim identification, and offer more features without raising complexity or cost.

For Alay man, a low-cost, less sophisticated, incredibly reliable, and user-friendly embedded technology is the suggested remedy. It is powered by a 5V/ 2A power supply, a voltage regulator IC, a vibration sensor, and a 5MP camera. Voltage regulator ICs are used to down convert the 12V AC to DC SMPS adapter's power supply. In order to capture images, the camera functions as a transducer; the vibration sensor, on the other hand, detects vibrations and lowers the output pin voltage.

3.5 Design and Fabrication of a Password Protected Vehicle Security and Performance Monitoring System

A Password Protected Vehicle Security and Performance Monitoring System's design and construction procedure are described in this article. On a PCB, a relay switch, a 4*4 matrix membrane keypad, and a liquid crystal display (LCD) are all used in the system.

During operation, the engine's fuel injection is managed by the relay installed in the gasoline line next to the fuel pump that only turns on when the owner enters the right password. The proximity switch that serves as a motion sensor and displays the vehicle's speed at any given moment is used to create the performance monitoring system. The vehicle's security and monitoring are greatly enhanced by this technology, which also guards against theft and other security issues.

The most crucial information in this text is the alarming rise in car thefts and the fact that an ignition key is a vehicle's principal security measure. The speedometer is the most crucial part of a vehicle performance monitoring system, and security and performance monitoring systems work hand in hand. Modern automobiles also contain pre-existing systems like sensors and an Engine Control Unit (ECU) coupled to the Info-Security Circuit Board.

The invention of a car theft control strategy employing a password-protected encryption technology is the most crucial information in this work. The Electronic Fuel Injection (EFI) pump is energised when the battery is, and this system uses a password-protected relay switch fitted between them.

The three main goals are to increase security by ensuring that a vehicle's starting system is encrypted, To assure these two goals, security, track the vehicle's performance, and create an attachable module for the vehicle. Using a buzzer, a horn, and a password, the proposed Password Protected Fuel Injection System

When the provided password does not match the set password three times in a row, the engine will start thanks to a potentiometer and LEDs. The system was modelled using a simulation circuit, and Autodesk Circuit was used to run the algorithm. Entering a password, changing the password, and entering a master password in case one forgets the previously established password are the three primary operational steps of the vehicle security system. PROTEUS software was used to create the PCB's schematic design.

3.6 Authenticating Vehicles and Drivers in Motion Based on Computer Vision and RFID Tags

The design and construction process of a password protected vehicle security and performance monitoring system is covered in this article. Relay switch, 4*4 matrix membrane, and PCB

The system uses both a keypad and a liquid crystal display (LCD). The relay located in the fuel line adjacent to the gasoline pump turns on when the owner inputs the correct password, controlling the fuel injection.

inside the motor. The performance monitoring system is made using the proximity switch, which also functions as a motion sensor and shows the current speed of the vehicle. This technology considerably improves the security and monitoring of the car and protects against theft and other security issues.

The most important topic in this essay is the worrisome increase in vehicle thefts and the fact that a car's unique ignition key is its primary security mechanism. The speedometer is the most important component of a vehicle performance monitoring system, and security and performance monitoring systems for automobiles go hand in hand. There are also pre-existing systems in modern cars, such as sensors and an Engine Control Unit (ECU) connected to the Info-Security Circuit Board.

The most important topic in this article is how to create a theft prevention strategy for vehicles that makes use of password-protected encryption technology. A password-protected relay switch is located between the battery and the Electronic Fuel Injection (EFI) pump, which is powered when the system is turned on. The three primary objectives are to produce an attachable module for the automobile, track the performance of the car, and assure an encrypted starting mechanism for a car to boost security.

Assure these two objectives. If the supplied password does not match the predetermined password, the proposed Password Protected Fuel Injection System can start the engine utilising a buzzer, a potentiometer, and LEDs. for three continuous days. A simulation circuit was used to represent the system, and Autodesk Circuit was employed to execute the algorithm. The three main operational processes of the car security system are entering a password, changing the password, and entering a master password in case one forgets the previously created password. The PCB schematic was designed with PROTEUS software.

3.7 Unified Biometric Privacy Preserving Three-factor Authentication and Key Agreement for Cloud-assisted Autonomous Vehicles

In order to provide safe access to both the cloud and autonomous vehicles, this article suggests a cloud-centric three-factor authentication and key agreement protocol (CTAKA) incorporating passwords, biometrics, and smart cards. Fuzzy vault, Fuzzy commitment, and Fuzzy extractor are three common biometric encryption techniques that are suggested to guarantee secure access to both cloud and AVs. The protocol allows for the remote control capabilities to be abused by bad parties while simultaneously ensuring the safety of pedestrians and passengers. Autonomous vehicles (AVs) have the potential to enhance traffic flow, driving comfort, and safety while also consuming less fuel. The National Natural Science Foundation of China and the China Postdoctoral Science Foundation Funded Project (2018M640962) provided funding for this research.

To provide three-factor authentication without jeopardising biometric privacy, the CT-AKA protocol is unified. In order to allow safe remote control, two session keys are negotiated: one is between the user and the AV, and the other is between the mobile device and the cloud. This creates resilience against the compromising of transient security settings. The results show that the protocol provides strong security at acceptable computation and communication costs. In order to facilitate autonomous driving, cloud-assisted AV (CAV) was developed, enabling the storage and processing of data from the cloud. A remote control capability for AVs is expected to be essential for things like delivering security updates and letting a human driver take charge.

If the vehicles can be operated remotely, driverless testing without a backup driver is permitted in California. A user's mobile device, such as an Android or iOS device, can also be used for remote control. Autonomous vehicle (AV) remote control poses a number of security threats, including the chance for nefarious actors to exploit flaws and seize power. Unauthorized access to an AV and the cloud can also result in the loss of control and the exposure of sensitive data. Terrorist organizations can even remotely command AVs to take part in planned strikes.

It's crucial to make sure that only authorized users are able to access the cloud and their AVs. To do this, secure pathways between the AV, the user, and the cloud should be developed in order to stop unauthorized actions like eavesdropping, interception, tampering, and forgery. However, each authentication method has its own flaws, therefore autonomous vehicle security cannot be sufficiently provided by a single-factor authentication.

3.8 An Attempt to Develop an IOT based Vehicle Security System

In order to ensure secure access to both the cloud and self-driving cars, this study proposes a three-factor authentication and key agreement system (CTAKA) for the cloud that integrates smart cards, biometrics, and passwords. Three popular biometric encryption methods—fuzzy vault, fuzzy commitment, and fuzzy extractor—are given to offer secure access to both the cloud and AVs.

Protocol is intended to protect the safety of passengers and pedestrians, even though it allows for hostile actors to abuse the remote control capability. The China Postdoctoral Science Foundation is able to provide funding for autonomous vehicles (AVs) (2018M640962). Less petroleum may be consumed if traffic flow, driving comfort, and safety are all improved. Chinese organisations the National Natural Science Foundation and the National The CT-AKA protocol has been created in order to perform three-factor authentication without compromising user privacy regarding their biometrics. In order to enhance resistance against the compromise of temporary security parameters, two session keys are negotiated: one between the user and the antivirus programme to enable secure remote control, and the other between a mobile device and the cloud.

The findings demonstrate that the protocol offers superior security at reasonable computational and transmission costs. Data from the cloud may now be stored and processed by autonomous vehicles thanks to the development of cloud-assisted AV (CAV). Remote control is predicted to be a significant part of AVs in order to issue security upgrades and allow a human driver to take command.

Driverless testing without a backup driver is allowed in California if the cars can be controlled remotely. Another option for remote control is to use a user's mobile device, such as an iOS or Android smartphone. There are a variety of security risks associated with remote control for autonomous vehicles (AV), including the potential for malicious actors to take advantage of weaknesses and take over control. Sensitive data may be exposed and control lost as a result of unauthorized access to an AV and the cloud. Even remotely controlled AVs can be used in premeditated attacks by terrorist organizations. It's essential to guarantee that only approved users can access the cloud and their AVs.

In order to prevent unauthorised operations like eavesdropping, interception, tampering, and forging, secure paths between the AV, the user, and the cloud should be created. But because each type of authentication has its own drawbacks, a single factor authentication is insufficient to ensure the security of autonomous driving.

3.9 Authentication Based Systamatic Driving License Issuing System

The Internet of Things (IoT) is a physical network of items or things that are equipped with electronics, software, sensors, and network connectivity to collect and share data. Anything intended to stop or discourage unauthorised usage of a vehicle is considered an anti-theft system. In this research, a novel security system based on wireless communication and a cheap Bluetooth module is proposed. From the user's mobile phone or any other device with a potential Internet connection, the system uses a Bluetooth module and controller to control the security system. The Internet of Things (IOT) is a network of physical things containing electronics, software, sensors, and connectivity that allows them to exchange data with other devices to provide better value and service.

Designing and implementing a security system that provides controllability through via IOT, a hand-held mobile phone. In addition to going beyond M2M and including a wide range of protocols, domains, and applications, IOT is anticipated to provide advanced connectivity of objects, systems, and services. The linking of various embedded devices is anticipated to bring about automation in almost all disciplines are affected, and cutting-edge applications like a smart grid are made possible.

The project focuses on car safety and security to avoid vehicle thefts, and it has features like keyless unlocking of doors, ignition control through both Keypads, and wearing of seat belts. These are the most crucial facts in this text. Intruder issues from the window of the house are also addressed. The car's security should be improved by these improvements. The goal of this project is to create an IOT system for securing vehicles. By using innovative technology to open the automobile door and fasten the seatbelt, the user is then satisfied to turn the key in the ignition. At the 2018 IEEE, the project is presented.

The iSES is an international symposium on smart electronic systems. This survey offers a summary of the numerous studies that have been conducted to complete the project. Vehicle anti-theft tracking systems built on the Internet of Things are intended to give owners all-around active service. Vehicles with sensor networks are used to prevent car theft. Information about latitude and longitude is stored using GSM and GPS devices. There is also a comparison of Android JAVA performance. Although it uses more energy, Sun embedded JVM running on Angstrom Linux offers better VM architecture.

3.10 Smart Vehicle Card Using IoT

The present Smart Card will be expanded to contain data about vehicle registration, vehicle type, owner's licence details, vehicle pollution details, vehicle challan details and vehicle insurance details.

It uses sensor devices to carry device-related information to the Internet. The Smart Card will hold information about car registration, vehicle type, owner's licence details, vehicle pollution details, vehicle challan details and vehicle insurance details. The Internet of Things can connect anything and everyone anywhere in the world. Road traffic paperwork and physical labour are being reduced through the use of web portals, RFID, smart cards, and the Internet of Things. The World Health Organisation estimates that more than 1.25 million individuals lose their lives to traffic-related injuries each year.

The lack of parking spaces and the backed-up traffic caused by toll booths on highways are the two main causes of these road disasters. The World Health Organisation has suggested using the Smart Card, Internet of Things, RFID, and web portals to lessen traffic congestion and manual labour. In order to minimise manual involvement and conserve paper, this study suggests an intelligent automated parking and toll system. The device comes with a smart card that may be used to save data about the vehicle, including its registration, kind, owner's license, pollution level, challan, and insurance information. This data will be kept in a central database or repository from which the front-end application can retrieve the needed information. The Internet of Things (IoT) is the fundamental idea behind the smart card. The incorporation of RFID technology in the prototype reduces the likelihood of automobiles being stolen because the cards created using RFID technology cannot be duplicated. The creation of an automated parking and toll system with a front-end web portal is covered in this paper. In order to update the database at the back end, sensors connect with the website. Recharging RFID cards allows for cashless transactions and cuts down on toll booth wait times.

Additionally, the RFID card can contain details about the vehicle, including its insurance, emissions, and registration. The discussion of the architecture and implementation of the system, the technique used, and the features that could be added to an RFID card in the future round out the paper's conclusion. Real-time parking is one automated method that has been created using smart cards. A mathematical model was created to represent the offline problem, and an algorithm was suggested to schedule the task from online to offline. This research offers a prototype for an automated automobile parking system. Bonde et al. previously described work to automate the entire car and car parking.

Kwan and Mogharverni created a credit system for prepaid metering systems using smart card technology. For students in educational institutions, Omar and Djuhari created a card system that could be used for banking, the educational sector, transit, and retail. The number of vehicles parked during a specific time period and in a specific parking space is managed by this system using an

Android application.

3.11 An Ineligible and Unauthorized Motor Vehicle Driver Access control and Sleep State Alert System: An Offline based Model

In order to prohibit unauthorised and ineligible access to motor vehicles for driving, this article suggests an offline-based method that will block anyone from driving until they have a valid driving licence. To determine a driver's eligibility, a hardware-based implementation is used in conjunction with a mobile application that is based on encrypted communication. To determine whether to start, the motor vehicle will include a hardware component with a memory chip attached to the ignition module. An offline working model for identifying and alerting drivers to sleep activities is presented in this paper. It comes with a motor vehicle and is prepared to manage emergencies and hardware problems.

The system is equipped to manage hardware breakdowns and crises and is capable of detecting and alerting the driver to sleep activities. It is also capable of recognising and alerting the driver's face to verify the driver's eligibility and authenticity. This system is made to be able to deal with emergencies and hardware breakdowns. The way to start a car's engine is suggested in this document, but it can only be used if the driver is qualified to do so and has permission from the car's primary owner. A hardware module based on a Raspberry Pi is used for the implementation, and a mobile application that is directed by the principal owner is used for secure access.

Through a secure communication method known as Kerberos, the data from the Regional Transport Authority (RTA) is fetched in to the local memory of an Android application and saved as a JSON object in the local memory of the Android device. The information is subsequently transmitted over a connected or wireless connection to the Raspberry Pi's MYSQL database, which is housed in a memory chip. Only if the Raspberry Pi sends high signals to it will the Kanpur, India mechanism function. A constant monitoring camera will catch the driver dozing off, and a 10-digit Numeric keyboard will handle crises, hardware malfunctions, and dangerous scenarios. In the parts that follow, the system implementations are explained, beginning with the Secured Kerberos-based Mobile Application that starts the engine.

A hardware module using a Raspberry Pi, camera module, and deep learning techniques was built by the RTA Software development and maintenance team to identify drivers. The battery of the vehicle, which has voltage regulators, will supply power to the hardware. The RTA licence

data includes fields for name, birthdate, licence type, issue date, expiration date, face data, and car manufacturing data.

3.12 Summary

This chapter describes about techniques, methods introduced by different researchers and how they proposed system was accurate than other methods. Some of them were iot components based and some of them were software based. So here different methods were introduced by different resreachers for providing security and safty for vehicles by preventing thefts using different methods.

Chapter 4

Architecture and System Design

4.1 System Block Diagram

1. The ignition line and battery of the engine starting system are attached to this relay, which is coupled to the biometric finger print scanner.

2. The power supply from the microcontroller to the car ignition system is managed by a relay switch.

3. An electrical switch known as a relay serves as a ground or a power source in an electrical circuit. The common terminal and NO terminal are connected when the coil is powered. Anytime a gadget that draws greater current and has a higher voltage can be turned on or off by turning a crank.

4. The starter motor for the electric engine system is linked to the ignition switch, and the electric engine receives power from the battery as well9. When the key is turned in, the circuit closes, supplying power to the starter motor, which then turns the engine over.Here, the engine ignition system is managed by the fingerprint security system.

5. The microprocessor receives power via a controlled power supply board. The vehicle's battery is connected to this system. As a result, the battery provides current to the fingerprint sensor. Rather than using a normal board, a digital switch is employed to manage high voltage and current.

6. Relay switches to enable current to flow or cut it off based on wiring when supplied logic voltage. The engine is started by the starting coil when this relay is activated by providing an authorised person's fingerprint as an input.

7. The self-motor begins to rotate when the ignition is turned on, which also causes the switch coil to rotate. Following this procedure, the Bendix gear catches the switch coil or starting coil, and the car's engine fires. The crank shaft starts to rotate constantly as soon as the engine starts.

8. Write the full program's code in the Arduino Uno IDE software before uploading it to the

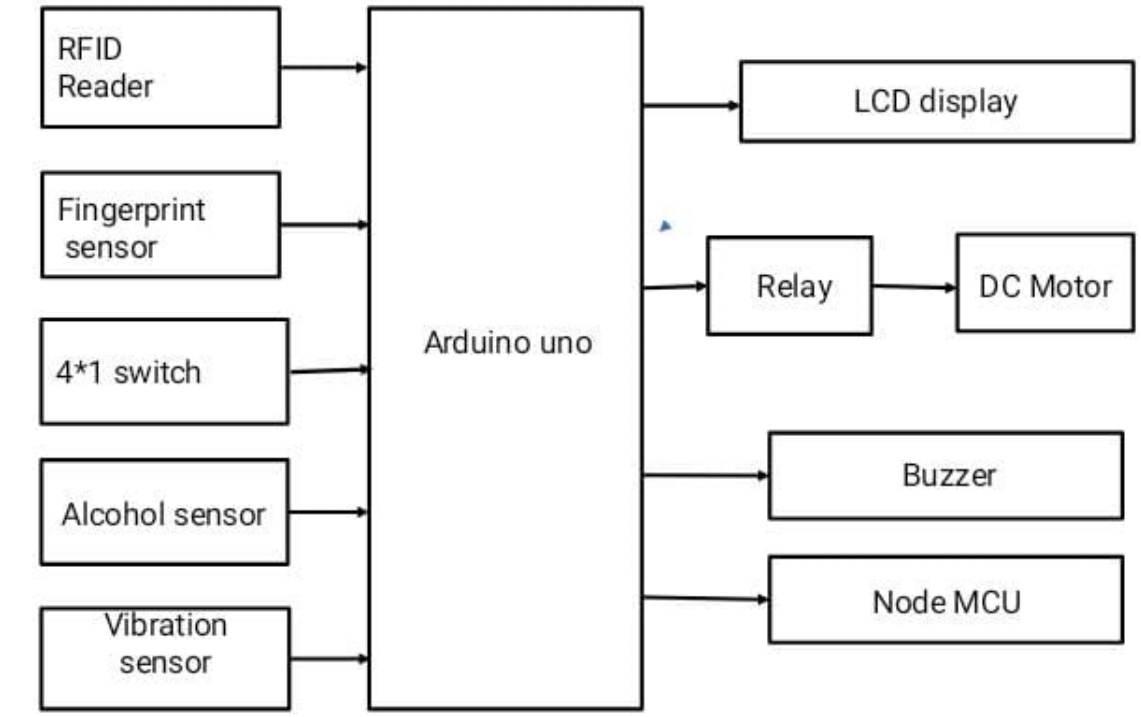

Figure 4.1: System Block Diagram

Arduino board.

9. The fingerprint sensor is then attached and prepared for enrollment, which is utilised for authentication. Every person's fingerprint is saved in a separate location on the fingerprint sensor.

10. This whole model is installed in the car, and the engine starts when an authorised individual scans their finger.

4.2 Data Flow Diagram of System Design

The creation of a vehicle theft-protecting anti-theft security system is the aim of this project. In order to detect any vehicle tilt, a tilt sensor has been included in this protection. A microprocessor is PIC16F876A. Three switches are used as input in this case.

The functional block diagram for the vehicle protection anti theft security system is shown in Figure 4.1 . The vehicle will start to run when the proper RFID, password, or fingerprint is entered.

The security system will thereafter be turned off. The security will activate when someone enters the incorrect RFID, password, or fingerprint, at which point the engine switch will be turned off. With the aid of the WiFi module, the owner will automatically get a message via Telegram even while the vehicle is not moving.

The tilt sensor detects movement of the vehicle when someone tries to pick it up. There will be an alarm activation. Through GPS, the owner is informed of the vehicle's whereabouts.

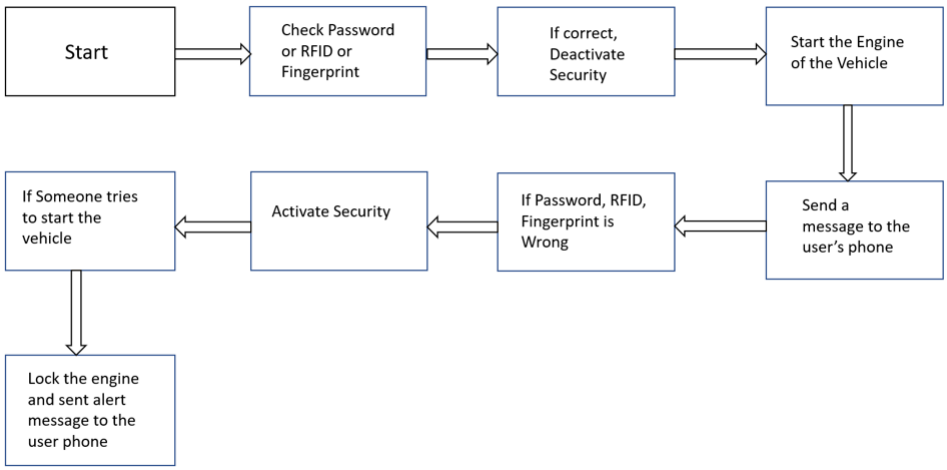

Figure 4.2: Data Flow Diagram

4.3 System Operation Flow Chart

STEP 1 : The first step is for someone who wants to drive a car to place their finger on the fingerprint sensor. The process advances to step 2 if the put finger matches the fingerprint enrollment. If not, it will display an error notice that reads, "Please place a valid fingerprint," followed by the same message again. If the fingerprint accessing procedure fails more than three times, the fingerprint process will resume with the starting condition, which is to place a valid fingerprint

STEP 2: In this step, the user must present a valid RFID tag (licence) for that specific vehicle. If the identification is not valid, an error message stating that the RFID tag is invalid will be displayed. If no valid RFID is presented, the message will be repeated. If the RFID tag presented in this process fails more than three times, then, similar to step 1, following the fingerprint process, the RFID tag process will go to the original condition, which is the fingerprint placement step. A valid RFID tag will advance to the following phase if it is presented

STEP 3: A person who wants to operate a vehicle goes through step 1 in this step, which is then validated before moving on to step 2. The kit is moving forward with system ignition after step 2 confirmation, which comes after fingerprint scanning and RFID tag (licence) verification. The ignition system won't function if any of the processes involved in it fail to complete.

STEP 4: The ignition system will start, the user can operate the vehicle, and the procedure continues if the fingerprint matches and the RFID (licence) of the vehicle is verified. If the fingerprint does not match the original fingerprint collected, the controller issues an error message, cancels the verification, and returns to step 1 of the verification procedure

The whole system operation flow is depicted in Figure 4.4

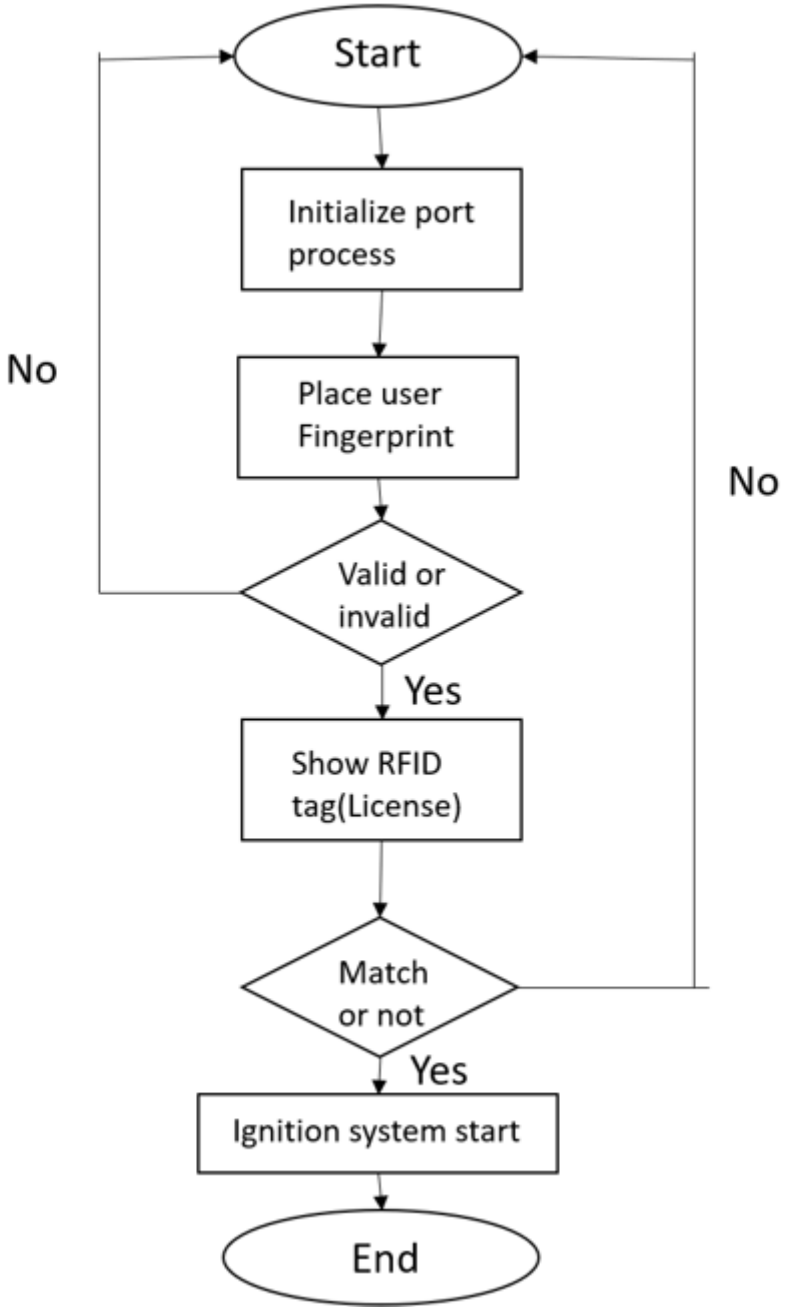

Figure 4.3: System Operation Flow

In order to read the data from the card and scan the fingerprint, we are using simple hardware as an interface. The card reader's job is to read a unique 12-digit RFID tag, which is displayed on the screen, while the fingerprint scanner's mission is to read the finger that is placed on it. A RFID tag card has a film with a 12 digit unique RFID and the number is printed on the card itself for recognition purposes. This means that each fingerprint scanned has a unique template identifier for a specific person.When the power supply is turned on, the LCD screen shows "MOTOR CONTROL" at the top.When the power supply is turned on, the LCD screen shows "MOTOR CONTROL" at the top. then use the fingerprint module with their fingerprint. The LCD display will read "PLACE A VALID FINGER" if the placed finger is invalid. The LCD display will read "FINGERPRINT VERIFIED" if the placed finger is legitimate. When the user presents the RFID tag to the RFID tag reader module for driver authentication, it displays "WAITING FOR LICENCE" in LCD display after a brief delay. If the user displays the incorrect RFID tag, the LCD display reads "INVALID LICENCE PLEASE SHOW VALID LICENCE," however if the RFID tag is correct, the DC motor will eventually start.

4.4 Use Case Diagram of System Design

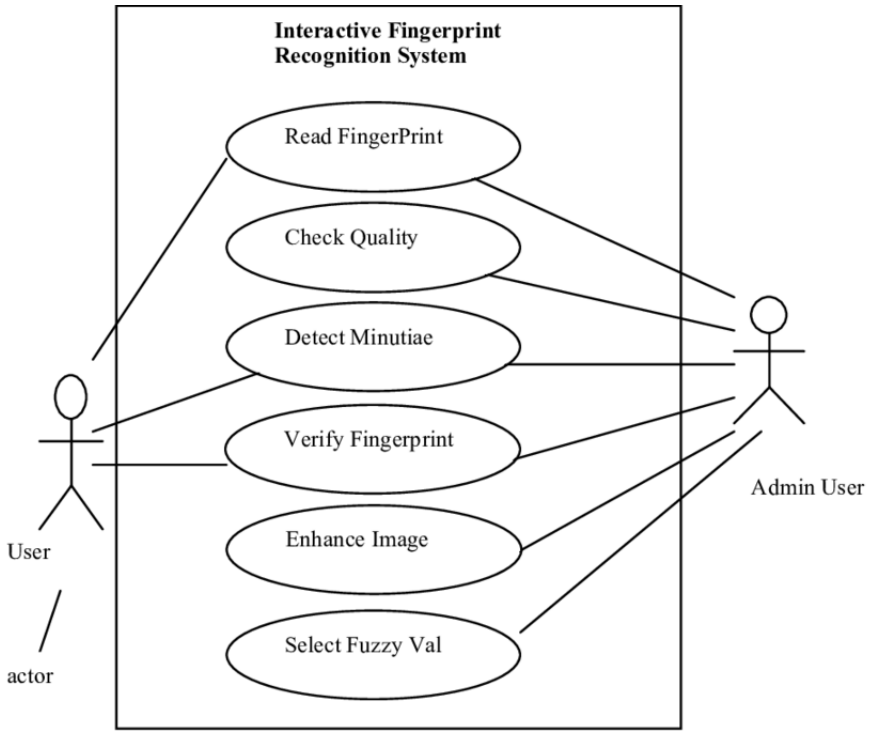

Figure 4.4: Use Cse Diagram

At its most basic level, a use case diagram is a depiction of a user's interaction with the system and shows the requirements of a use case. A use case diagram can illustrate the various system user types and their varied modes of interaction.

A potential replacement for password-based authentication is biometrics-based authentication. One of the most developed and tested biometric identifying methods is fingerprint-based identification. A high resolution fingerprint scanner is used at the ATM terminal to capture a fingerprint image at the time of the transaction. Bank security measures can be a vital, contributing factor in averting client attacks.When determining vulnerabilities and causation in civil suit, these precautions are of the utmost importance. In order to provide their consumers with a safe and secure banking environment, banks must adhere to specific requirements.Using a biometric measure can help the banking system be more secure for both customers and bankers. While the real cardholder is unable to complete the transactions, we also suggested using nominees' fingerprints for identification.

4.5 Summary

By employing diagrams like block diagrams, data flow diagrams, use-case diagrams, and system operation flow chart, we are finishing this chapter by discussing several models used to depict the proposed system design. The system flow and the connections between the various components were represented by all four models. Devices/sensors,and an alert system are all displayed together with user involvement. Finally, it displays a representation of each actor together with their actions and the whole workflow of the suggested system.

Chapter 5

Implementation

5.1 Hardware Implementation

5.1.1 Arduino UNO

One type of microcontroller board built on the ATmega328 is called the Arduino Uno, and uno is an Italian word that signifies one. The Arduino Uno Board 1.0 microcontroller board will soon be released, hence the name Arduino Uno. This board has 14 digital I/O pins, an ICSP header, a power jack, 6 analog I/Ps, a ceramic resonator operating at A16 MHz, a USB port, and 14 digital I/O pins. Connecting this board to the computer, all of these can help the microcontroller's future operations. This board's power source can be accomplished via a battery, a USB cable, or an AC-to-DC adaptor. Power Sources, a USB port.The voltage range for the USB bus specification is 4.75 to 5.25 volts. While third-party boards may include a miniUSB, microUSB, or USB-C connector, the official Uno boards have a USB-B connector.barrel jack connector, 5.5mm/2.1mm. Although 6 to 20 volts are supported, it is advised to use 7 to 12 volts for official Uno boards.

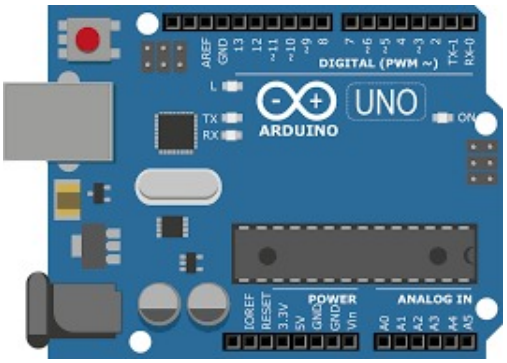

Figure 5.1: Arduino UNO

5.1.2 Power Supply

The most practical and user-friendly breadboard component is the 3.3V/5V output MB102 Breadboard power supply module, which may be added to any applications involving breadboards where 5V, 3.3V, or both power requirements are necessary. Due to its simplicity of use, customers can connect any DC power supply unit with a barrel jack and a power output range of 6.5 to 12 VDC. Two separate channels of power output for breadboards are available on the board. These power channels can be independently set up to operate at 3.3V, 0V, and 5V. A push switch is also provided by the module to turn the complete power supply module ON and OFF.A USB input with two 5V, two 3.3V, and four GND pinouts is an added feature for devices that need more power pins.The user will be informed of the status of input power availability by the power LED.

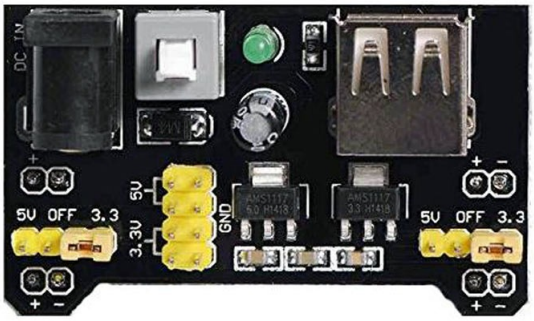

Figure 5.2: Power Supply

5.1.3 LCD(Liquid Crystal Display)

A type of flat panel display known as an LCD (Liquid Crystal Display) operates primarily using liquid crystals. Since they are frequently used in cellphones, televisions, computers, and instrument panels, LEDs offer a wide range of applications for consumers and enterprises. When compared to the technologies they replaced, such as light-emitting diode (LED) and gas-plasma displays, LCDs represented a significant advancement. Compared to cathode ray tube (CRT) technology, LCDs permitted screens to be far thinner. As opposed to LED and gas-display displays, LCDs operate on the idea of blocking light rather than emitting it, which results in a significant reduction in power consumption. The liquid crystals in an LCD use a backlight to form an image where an LED emits light. LCDs started to be superseded by new display technologies like OLEDs as they took the place of earlier display technologies.

Figure 5.3: Liquid Crystal Display

5.1.4 RFID

Tags and readers are the two halves of the wireless system known as Radio Frequency Identification (RFID). The reader is an electronic gadget with one or more antennas that transmit radio waves and take in signals from RFID tags. Tags can be passive or active, using radio waves to transmit their identity and other information to adjacent readers. Without a battery, passive RFID tags are powered by the reader. Batteries are used to power active RFID tags. RFID tags can contain a variety of data, ranging from a single serial number to many pages of information. Readers can be fixed on a post or suspended from the ceiling, or they can be portable so they can be carried by hand. Reader systems may also be included into the design of a cabinet, room, or structure.

Figure 5.4: RFID

5.1.5 Relay

Relays have the benefit that only a modest amount of electricity is required to run the relay coil. However, a relay switch circuit can be used to control motors, heaters, lamps, or AC circuits, all

of which have the potential to consume a significant amount of additional electrical power. The electro-mechanical relay is a type of output device (actuator) that can be used in a wide variety of electrical circuits. It is available in a wide variety of shapes, sizes, and designs. But even if electrical relays can be used to turn relatively high currents or voltages "ON" or "OFF" in low power electronic or computer type circuits, a relay switch circuit must be employed to do so.

Figure 5.5: Relay

5.1.6 DC Motor

Any of a group of rotating electric motors that use direct current (DC) electricity to create mechanical energy is referred to as a DC motor. The most prevalent kinds depend on the forces created by induced magnetic fields brought on by current flowing through the coil. For a portion of the motor's current to occasionally shift direction, almost all types of DC motors contain an internal mechanism that is either electromechanical or electronic.Due to their ability to be supplied by existing direct-current lighting power distribution networks, DC motors were the first type of motors that were widely employed.

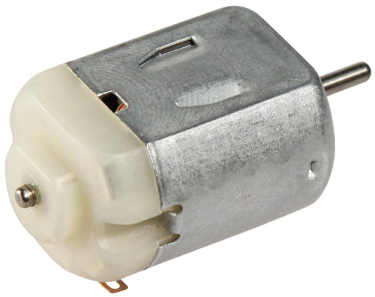

Figure 5.6: DC Motor

A DC motor's speed can be varied across a large range by varying the supply voltage or the amount of current flowing through its field windings. Appliances, toys, and tools all employ small DC motors. Both direct current and alternating current can be used to power the universal motor, a small, light brush motor used in portable power equipment and appliances. Larger DC motors are

being employed for steel rolling mill drives, lift and hoist propulsion and electric vehicle propulsion. AC motors can now be used in many applications in place of DC motors thanks to the development of power electronics.

5.1.7 Node MCU

low-cost System-on-a-Chip (SoC) called the ESP8266 serves as the foundation of the open-source NodeMCU (Node MicroController Unit). The Espressif Systems-designed and -produced ESP8266 has all of the essential components of a computer, including CPU, RAM, networking (WiFi), and even a contemporary operating system and SDK. This makes it a fantastic option for all types of Internet of Things (IoT) projects.The ESP8266 is difficult to access and use as a chip, though. For the simplest operations, like turning it on or sending a keystroke to the "computer" on the chip, you must solder wires with the necessary analogue voltage to its pins. Additionally, you need to programme it in low-level machine instructions that the chip hardware can understand. Using the ESP8266 as an embedded controller chip in mass-produced devices is not problematic at this degree of integration. For amateurs, hackers, or students who want to test it out in their own IoT projects, it is a significant burden.

Figure 5.7: Node MCU

5.1.8 Buzzer

A beeper or buzzer, for example, could be electromechanical, piezoelectric, or mechanical in design. The signal is converted from audio to sound as its primary function. It is often powered by DC voltage and used in timers, alarm clocks, printers, computers, and other electronic devices. It can produce a variety of sounds, including alarm, music, bell, and siren, according on the varied designs. The buzzer's pin configuration is displayed below. It has two pins: a positive pin and a negative pin. The '+' symbol or a longer terminal is used to indicate this's positive terminal. While the positive

terminal is shown by the '+'symbol or long terminal and is connected to the GND terminal, the negative terminal is represented by the '-'symbol or short terminal.

Figure 5.8: Buzzer

5.1.9 Vibration Sensor

The quantity and frequency of vibration in a system, machine, or piece of equipment are measured by a vibration sensor. Vibration sensors can be used to provide maintenance teams with information about conditions inside crucial assets that could cause equipment failure. This information enables them to anticipate the maintenance of the machinery, which lowers total costs and improves the performance of the machinery. A seismic mass is linked to a piezoelectric crystal, which is the basis of their manufacture. When a crystal is under tension or compression stress, it produces an electrical charge that is inversely proportional to the amount of acceleration it is going through. This signal is transformed internally into an output voltage or current (4-20mA) for data loggers or process control loops.

Figure 5.9: Vibration Sensor

5.1.10 Fingerprint Sensor

Processing is the main factor in fingerprint sensors. Enrollment and matching are the two key components of the fingerprint processing. Every user must place their finger twice during the enrollment process for fingerprints.In order for the system to process, create, and store the finger's pattern, it must first verify the photographs of the finger. When a user places their finger on an optical sensor, the system creates a pattern of the finger and compares it to template fingers in the finger library. The system will analyse the exiting finger with a specific pattern that is chosen within the module in order to perform 1:1 fingerprint matching. The scanning system will similarly search for the whole finger records for the finger matching for 1: N matching. The scanning system will return to the appropriate result in either case of success or crash.

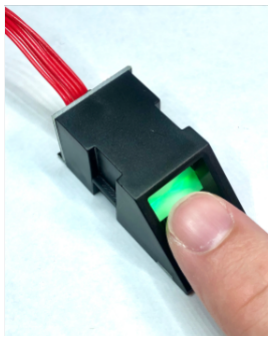

Figure 5.10: Fingerprint Sensor

5.1.11 Alcohol Sensor

Alcohol, CH4, benzene, petrol, hexane, CO, and LPG may all be detected with the alcohol gas sensor module. In order to detect alcohol gas, it has a sensitive substance called SnO2, which has a decreased electrical conductivity in fresh air. It is a semiconductor alcohol gas sensor that keeps track of whether alcohol is present or not. As a result of the resistance shift that occurs when the sensor is exposed to alcohol gas, it is also known as chemiresistors.

MQ3 Alcohol Sensor The SnO2 conductivity rises as the sensor gets nearer to the alcohol gas. The content of alcohol directly relates to the increase in sensor conductivity. As a result, any microcontroller can readily measure the alcohol concentration. Fast and highly sensitive to alcohol, smoke and petrol is the MQ3 alcohol gas sensor. This alcohol sensor can be used to create an alcohol detector. The MQ3 sensor can detect alcohol gas concentrations between 0.04 mg/L and 4 mg/L in ambient air or environment, which is appropriate for breathalysers. It operates between -10°C and 50°C with a 5V power supply and consumes 150 mA.

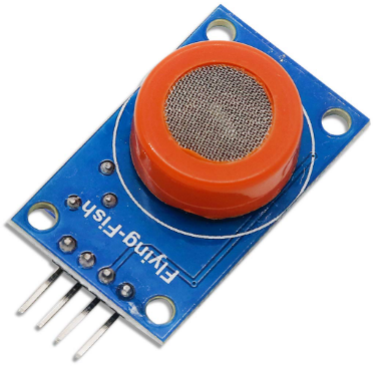

Figure 5.11: Alcohol Sensor

5.2 Software Implementation

5.2.1 Arduino IDE

Sketches are computer programmes created using the Arduino Software (IDE). These drawings are created in a text editor and saved as files with the.ino extension. The editor offers functions for text replacement and text searching. When saving and exporting, the message section provides feedback and shows errors. The console shows text generated by the Arduino Software (IDE), including error messages in their entirety and other data. The configured board and serial port are visible in the window's bottom right corner. You may create, open, and save sketches, validate and submit programmes, view the serial monitor, and more using the toolbar buttons.

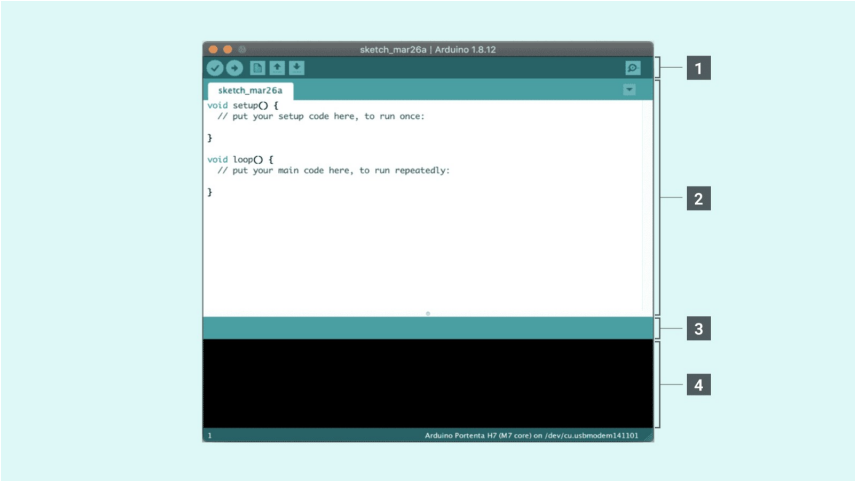

Figure 5.12: Aurduino IDE

5.2.2 Embedded C

The C Standards committee created Embedded C as a set of language that is an extension for the C programming language to address concerns that were shared by C extensions for various embedded

systems. The C Standards Committee initially expanded the C programming language to address these problems by establishing uniform standards that would allow all implementations to adhere to its commonality. Fixed-point arithmetic, named address spaces, and fundamental I/O hardware addressing are just a few of the characteristics that are available in embedded C language that are not present in regular C language.In the early years of microprocessor-based systems, programmes were developed in assemblers and assembled into EPROMs. Embedded C adheres to the most fundamental syntax and semantics of normal C language. Because there are no displays to read, there are no procedures for determining what the programme was doing precisely. Instead, they employ LEDs, switches, and other similar devices to verify if a programme is being executed correctly inside a device. Some'very fortunate' developers had simulators like In-circuit Simulators (ICEs), but these are prohibitively expensive to buy and their results aren't particularly dependable.The next most popular programming language for embedded processors and controllers is C. Assembly is also used, but it is only used when the part of the code needs to be particularly accurate in terms of timing, efficient in terms of code size, etc. for the overall requirements. Assembly language didn't provide any system portability since programmes written in assembly language are exclusive to a processor. Several high level languages, notably C, were created to address this issue. Other languages like PLM, Modula-2, Pascal, etc. also emerged but failed to gain widespread recognition. Among these, the C programming language gained complete adoption for desktop programmes as well as embedded systems. Although the C programming language may not be as popular as it once was for general-purpose applications, it nevertheless holds a strong position in embedded programming. Because C language is so widely used in embedded systems, supporting tools such compilers and cross-compilers, ICE, etc. are highlighted, which makes it easier to design embedded systems using C language. Later looks to be a natural substitute for assembly language when programming embedded devices. However, assembly language is only used for creating code that is small, quick, and accurate. Additionally, the cost of buying assembly codes as a software development tool has increased, and code portability is not available. The major issue isn't so much with writing little codes as it is with how difficult it is to maintain massive projects and programmes in assembly language. Finding competent assembly programmers is a problem that is getting worse today. As a result, high level device languages are chosen for programming embedded devices.

5.3 Implementation Details

5.3.1 EM18 RFID Reader Module

RFID, often known as radio frequency identification, is a technology. In this technology, digital data is encoded in RFID tags and deciphered by an RFID reader utilising radio waves. In that it uses a device to decode data from a tag, RFID is comparable to barcoding. Security, staff attendance, RFID door locks, RFID-based voting machines, toll collecting systems, etc. are just a few of the uses for RFID technology.It runs at a 125 kHz frequency.It has an 8–12 cm range and outputs data serially. The serial communication specifications are 9600 baud rate, 8 data bits, and 1 stop bit.

Figure 5.13: RFID cards

EM18 Features:

Operating voltage: DC between +4.5 and +5.5 Operating frequency: 125KHZ; operating temperature: 0 to 80 degrees Celsius; communication baud rate: 9600; current consumption: 50mA; 8 to 12 cm for reading distance; built-in antenna;

A module that can read the ID data from RFID tags is called the EM18 Reader. An EM18 reader module can decode the 12-digit unique number that the RFID tag contains when it is within range of the reader. This module runs on a 5 volt DC power supply and includes an internal antenna.

using an RFID reader to decode. The reader outputs the unique codes via the serial port output when we swipe the RFID tag close to it. Upload the following code to the Arduino after connecting it to the RFID reader as indicated in the circuit diagram. Open the serial monitor when the code has been successfully uploaded, and set the baud rate to 9600. Swipe the card next as closely to the Reader as you can. The 12-digit code will then start to appear on the serial monitor. All RFID tags in use should go through this process, and a record of it should be kept for future use.

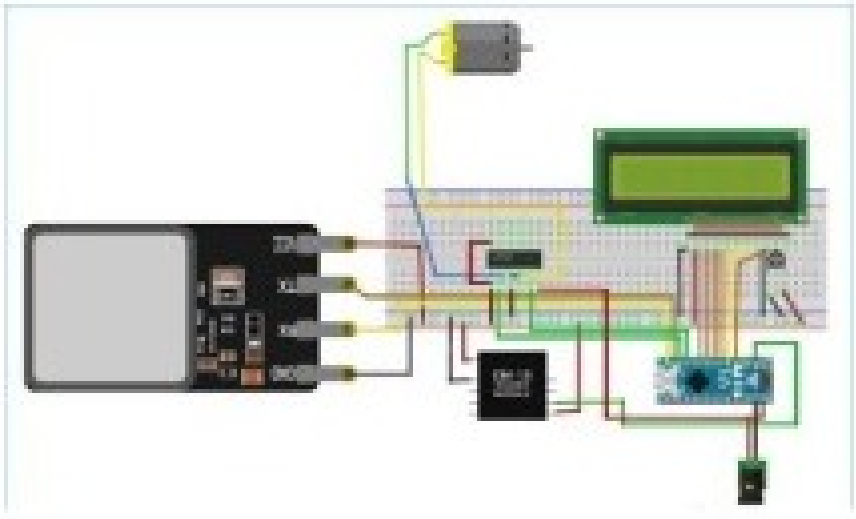

Figure 5.14: Circuit diagram for this Fingerprint based Ignition System

5.3.2 Programming For RFID Keyless Ignition

1. Include all necessary libraries as the initial step. For using the R305 fingerprint sensor, "Adafruit Fingerprint.h" is utilised here. The serial port where the fingerprint sensor will be connected can then be configured. We have designated pins 12 and 11 as RX and TX, respectively.

2. Declare every variable that will be utilised in the code in the following step. Then, declare an object of the LiquidCrystal class after defining the LCD connection pins with Arduino.

3. The unique 12-digit RFID tag numbers are then obtained and stored in an array using code that is written inside the loop() function. To obtain the details of the authenticated person, the array's elements will here be compared to the unique codes that have been recorded in the memory.

4. After that, the received array and the tag codes kept in storage are compared. If the code matches, the licence is regarded as legitimate and the user may enter a legitimate fingerprint. It will display an invalid licence if not.

5.The next step is to write a method called getFingerprintID that will return a legitimate fingerprint ID for a fingerprint that has already been registered.

6. To obtain a valid fingerprint ID, the getFingerprintID method is used inside of the fingerprint() function, which is called following a successful RFID match. The information about verified person data is then compared using an if-else loop, and if the data match, the vehicle is lit; otherwise, it will ask for the wrong fingerprint.

7. So that's how the two-layer security that the RFID car ignition system adds to your vehicle works.

5.3.3 RFID Rader Analysis

Three parts make up every RFID system: a scanning antenna, a transceiver, and a transponder. An RFID reader or interrogator is the term used when the scanning antenna and transceiver are integrated. Fixed readers and mobile readers are the two different categories of RFID readers. The RFID reader is a network-connected gadget that can be carried about or fixed to a surface. It sends signals that turn on the tag using radio waves. After being turned on, the tag returns a wave to the antenna, where it is converted into information.

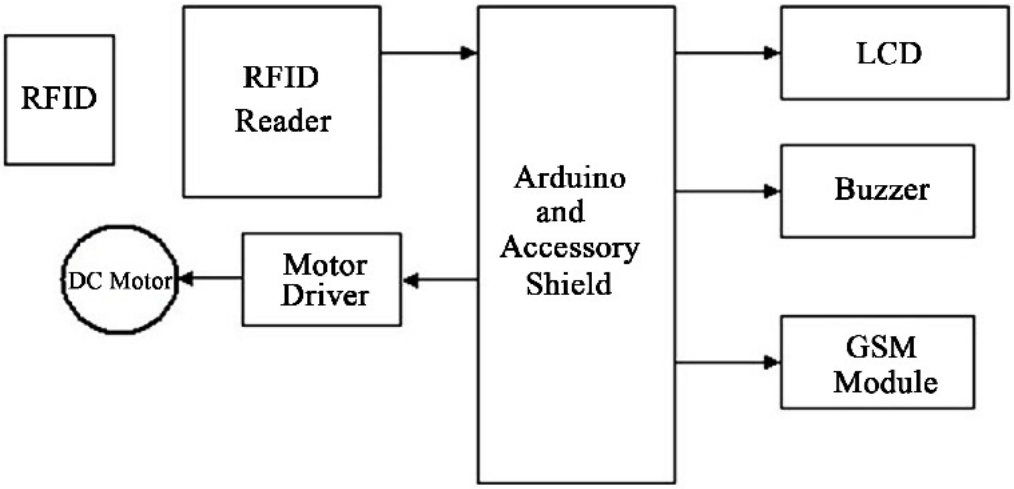

Figure 5.15: Simple block diagram of RFID based security system

The RFID tag's built-in transponder. The type of tag, reader, RFID frequency, and interference from other RFID tags and readers are some of the variables that affect the read range of RFID tags. The read range of stronger power source tags is also longer.

5.3.4 Fingerprint Sensor Module

The Finger Print Sensor Module, also referred to as the Finger Print Scanner, is a module that records the image of a finger's print, transforms it into an equivalent template, and keeps it in its memory on an ID (place) that has been defined by Arduino. Arduino is in charge of all the operations, including taking a fingerprint image, translating it into templates, and saving the position.

Steps for Fingerprint Enrolment

1. Select File > Examples > Adafruit Fingerprint Sensor Library > Enrol in the Arduino IDE.
2. Open the Serial monitor with a baud rate of 9600 and upload the code to the Arduino.
3. If you want to store your fingerprint, you need enter an ID for that fingerprint. I entered 1 in the top-left field because this is my first fingerprint, and then I clicked the Send button.
4. At that point, the fingerprint sensor's light will begin to flicker, signalling that you should place

your finger on it and then proceed as instructed on the serial monitor until your successful enrollment is confirmed.

5.3.5 The Fingerprint Analysis Process

Analysing a print is evaluating it to see if it may be used as a comparison. The inspection comes to an end and the print is labelled as unsuitable if the print is not appropriate for comparison due to the quality or amount of features. The analysis specifies the features to be utilised in the comparison and their tolerances (the amount of variation that will be permitted) if the print is suitable. Physical characteristics including recurves, deltas, wrinkles, and scars that serve as starting points for comparisons may also be discovered through analysis.

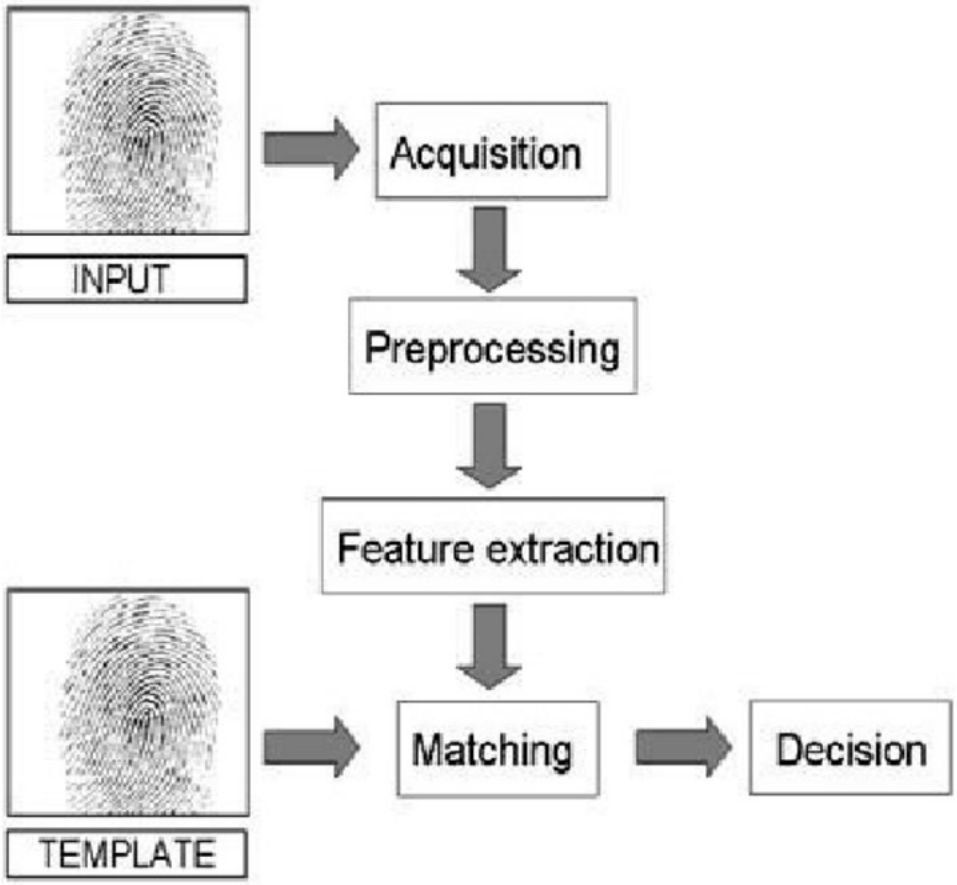

Figure 5.16: Block diagram of a typical Automation Fingerprint Verification System

An analyst makes comparisons by comparing known and questionable prints side by side. To see if they match, the analyst compares minute details like locations. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is one fingerprint database that can be searched to find known prints. Other sources of known prints include victims, persons of interest, witnesses, and

other people who were present at the scene. IAFIS is the world's largest fingerprint database, and as of June 2012, it contained more than 72 million prints from criminals, soldiers, government workers, and other civilian employees.

In the evaluation phase, the examiner determines whether the prints are from the same source (identification or individualization), come from distinct sources (exclusion), or are inconclusive. Poor sample quality, a lack of comparable areas, or an inadequate number of related or contrasting traits may all contribute to inconclusive results.

Verification is the process by which a second examiner independently examines, compares, and evaluates the prints in order to confirm or deny the findings of the first examination. The examiner may additionally check if the conclusions drawn during the analytical step are appropriate.

5.3.6 Examination of Vibration Sensors

Monitoring vibration levels and looking into the patterns in vibration signals are both done through the technique of vibration analysis. It is frequently conducted on both the frequency spectrum, which is derived by applying Fourier Transform to the time waveform, as well as the time waveforms of the vibration signal directly.

The root-mean-square (RMS), standard deviation, peak amplitude, kurtosis, crest factor, skewness, and other parameters are extracted from chronologically recorded vibration waveforms and studied to determine when and how severe the abnormal vibration events are. The general state of the targets being observed can be assessed using time domain analysis.

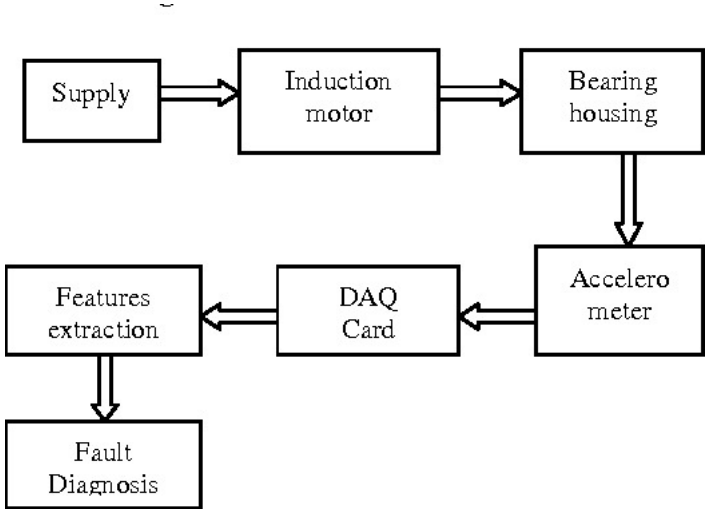

Figure 5.17: Block diagram of Fingerprint based Ignition System

It is highly desirable to combine the frequency spectrum analysis in addition to the time domain analysis in real-world applications, particularly in rotating machinery. A complicated machine with

numerous moving parts will produce a mixture of vibrations that are the result of the vibrations produced by all the moving parts. As a result, it is challenging to assess the state of a big rotating equipment's key components, such as gears, bearings, and shafts, using simply time waveforms. Frequency analysis breaks down time waveforms and reveals how repeating vibration patterns are so that each component's associated frequency can be explored.

5.4 Summary

This Chapter describes about the software requirements like different components, sensors, methods used for execution of the system and also defines about the integrity of requirements,design process of system. Such as components used for implementation,Arduino UNO operating system supported for execution and fingerprint sensor for verification of authorized persons, RFID reader for driving license verification and vibration sensor for limiting speed and alcohol sensor for detecting alcohol.

Chapter 6

Testing

Test Case No.	TestCase	Objective	Steps	Expected Outcome	Actual Outcome
1	Sensor Integration	Verify the arduino UNO,alcohol sensor,vibration sensor,fingerprint sensor,RFID reader and other components	Connect the arduino UNO, by power supply, relay, LCD display, Fingerprint sensor, Vibration sensor RFID reader, DC motor, Node MCU.Ensure that the arduino UNO can successfully communicate with all the sensors connected.Verify that the sensor data being received and processed by the arduino uno	All device and sensor data is recieved and processed by the arduino UNO	All device and sensor data is recieved and processed by the arduino UNO
2	Fingerprint Analysis	Validate the accuracy of fingerprint for security purpose	Store the images and assign the numbers to each Fingerprint. Stored images should be able to connected to the arduino UNO. Store the library of Fingerprint and then verify it is accurately detects the Fingerprint	The Fingerprint analysis is accurated and security is been provided to the vehicle correctly and effeciently	The Fingerprint analysis is accurated and security is been provided to the vehicle correctly and effeciently

Table 6.1: Test Case Accuracy Comparison Table

3	Driving license analysis	Ensure the license is analysed accurately to provide security and Driving license ID number should be stored in the code and then dumped into the arduino UND. Check whether it is validating the both stored and unstored driving license Id number.	The driving license analysis is an efficiently and security is provided to the vehicle correctly	The driving license analysis is an efficiently	security is provided to the vehicle correctly.
4	Speed analyser	This is mainly used to analysis the speed and then give the beep sound if it cross the limit	While writing the code we need to set the speed limit and write the rule that if it crosses the limit it should give the beep sound	The speed analysis is done efficiently and speed is been detected properly	The speed analysis is done efficiently and speed is been detected properly
5	Message analysis	Unauthorized person tries to ride the vehicle message need to be sent to the registered mobile number	The app which we use should be decided here we are using telegram to that bot will be created to the registered number.As soon as vehicle started message need to be sent to the mobile number.Access need to be sent by the owner if unauthorized person tries to access	Message analysis is been done properly and working accurately and efficiently	Message analysis is been done properly and working accurately and efficiently

Table 6.2: Test Case Accuracy Comparison Table

Chapter 7

Experimentation and Results

7.1 Experimentation

Step 1 , Initially the owner will get the message sush as Vehicle authentication using fingerprint sensor via Telegram and display shows the same

Figure 7.1: Vehicle authentication using fingerprint sensor

Step 2 , To begin the process user has to press the switch button

Figure 7.2: To start the system

Step 3 , Display shows place the finger for verification

Step 4 , If the fingerprint matches with the stored fingerprint in the database

Step 5 , Then user goes for next step authentication that is Driving License

Step 6 , ID stored in the database is displayed

Figure 7.3: Place finger for verification

Figure 7.4: When finger is matched

Figure 7.5: Show your license ID

Figure 7.6: Show your ID of license

Figure 7.7: Whether it is invalid license

Step 7 , If the license is not matched , then this message is displayed

Step 8 , Show valid License for accessing the vehicle , otherwise the owner will get notified about unauthorized access via message

Figure 7.8: Again showing ID

Step 9 , allows for starting vehicle if it is valid license

Figure 7.9: When it is valid license ID

Step 10 , The ignition will turn on

Figure 7.10: The ignition will turn on

Step 11 , If the alcohol sensor detects alcohol , the buzzer produces beep sound

Step 12 , If the speed limit is greater than actual speed then vibration sensor produces sound

Step 13 , If the finger not stored in the database tries to access the vehicle , owner will get message

Step 14 , wait untill owner gives permission

Step 15 , then access is granted

Figure 7.11: When alcohol is detected

Figure 7.12: If speed limit is exceed

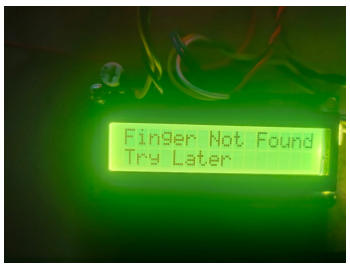

Figure 7.13: unauthorized access

Figure 7.14: waits for owners permission

Figure 7.15: When owner gives permission

7.2 Results

This module was created with the intention of focusing on the machine's state utilising fingerprints. This technology's goal is to make cars more resistant to typical threats while also enhancing their security. If they are accepted, the engine starts right away when the user authenticates by placing his finger on the scanner. The engine is immediately wired to the sensor, and the cables are connected so that the machine can start up. The primary reasons are that it is reasonably priced and the biometric authentication method utilised cannot be duplicated by two people. As a result, even when the user only has access to their own car, it gives precise data for certifying the car.

This technique was created to concentrate on identifying the engine using a fingerprint. The purpose of building this system is to boost the cars' level of security and resistance to common threats. When the user touches the fingerprint sensor, it authenticates them, and if they are authorised, it starts the engine for them. The wires are hooked so that the sensor can start the engine when it is directly connected to it. The main benefits of using it are that it is inexpensive and that no two people's fingerprints can be matched.As a result, it produces a correct result for confirming the ownership of the car, as the owner can only access their own car.

7.3 Summary

Finally in this chapter we have shown the execution results of our system or our working model and how it is feasible for all environmental conditions.

Chapter 8

Conclusion

For the purposes of this thesis, a vehicle security system was constructed using fingerprint and driver's licence technologies. This technology helps to prevent unauthorised driving as well as auto theft. It was done utilising a certain form of driver's licence that allows its holder to operate a car as well as an additional layer of security. The technology recognises fingerprints to grant access to the vehicle via biometrics. In order to stop any potential vehicle theft, a GSM module is utilised to send an SMS to the car's owner alerting him that an unauthorised driver's licence has been used. The GSM module was also used to notify licence holders through SMS to renew their licences before they expired.

8.1 Future Enhancement

Integration of many biometric modalities : At the moment, the majority of biometric identification systems for car ignition rely on just one modality, like fingerprint or facial recognition. However, the accuracy and security of the system can be increased by including various modalities, such as fingerprint and iris recognition.

Resistance to environmental changes: Various environmental factors, such as variations in temperature or illumination, might have an impact on biometric authentication systems. Future research could concentrate on creating systems that are resilient to these situations, guaranteeing that they function dependably in any situation. Biometric data is extremely sensitive, hence it is essential to protect its privacy and security. Future work could concentrate on building mechanisms for guaranteeing that the data is only used for the intended purpose and secure techniques for storing and transmitting biometric data.

User experience and acceptance : Users of biometric authentication systems may find them annoying or uncomfortable, which may cause them to avoid using them or not adopting them at all. Future work can concentrate on enhancing the user experience and enhancing the accessibility and

usability of the systems.

Interoperability: Access control or payment systems interoperability with biometric authentication systems for car ignition could be advantageous. Future research might concentrate on creating standards and protocols that allow communication between various biometric authentication system.

Chapter 9

References

[1] K. S. Tamilselvan, G. Murugesan, and S. Sasikumar, "Design and Implementation of Biometric Based Smart Antitheft Bike Protection System," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), 2018, pp. 136-138

[2] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. -K. R. Choo, "Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9390-9401, Sept.2020,doi: 10.1109/TVT.2020.2971254.

[3] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile Driver Fingerprinting: A New Machine Learning Based Authentication Scheme," in IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1417-1426, Feb. 2020,doi: 10.1109/TII.2019.2946626.

[4] A. E. Mekki, A. Bouhoute and I. Berrada, "Improving Driver Identification for the Next-Generation of In-Vehicle Software Systems," in IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7406-7415, Aug. 2019,doi: 10.1109/TVT.2019.2924906.

[5] S. Sharma, K. K. Ghanshala and S. Mohan, "A Security System Using Deep Learning Approach for Internet of Vehicles (IoV)" 2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2018, pp. 1-5, doi: 10.1109/UEMCON.2018.8796664.

[6] R. A. Rashid, N. H. Mahalin, M. A. Sarijari, and A. A. Abdul Aziz, "Security system using biometric technology: Design and implementation of Voice Recognition System (VRS)," 2008 International Conference on Computer and Communication Engineering, 2008, pp. 898-902,DOI: 10.1109/ICCCE.2008.4580735.

[7] M. Ramesh, S. Akruthi, K. Nandhini, S. Meena, S. Joseph Gladwin, and R. Rajavel, "Implementation of Vehicle Security System using GPS, GSM, and Biometric," 2019 Women Institute of

Technology Conference on Electrical and Computer Engineering (WITTON ECE), 2019, pp. 71-75, doi:10.1109/WITCONECE48374.2019.90 92918.

[8] H. Khalid, S. J. Hashim, S. M. S. Ahmad,F. Hashim, and M. A. Chaudary, "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, pp. 1-7, DOI: 10.1109/CSDE50874.2020.9411569.

[9] M. R. Pawar and I. Rizvi, "IoT Based Embedded System for Vehicle Security and Driver Surveillance," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 466-470, doi: 10.1109/ICICCT.2018.8472984.

[10] P. Muddapu, "Camera and Biometric based Vehicle Monitoring System for Public Safety," 2020 IEEE-HYDCON, 2020, pp. 1-6,doi: 10.1109/HYDCON48903.2020.9242840.

[11] M. Ismail, S. Chatterjee and J. K. Sing, "Secure Biometric-Based Authentication Protocol for Vehicular Ad-Hoc Network," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2018, pp. 229-234, doi: 10.1109/iSES.2018.00057.

[12] A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. M. Chowdhury, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM, and RFID," 2018 4th International Conference on Electrical Engineering and Information and Communication Technology (IEEE ICT), 2018, pp. 97-101, DOI:10.1109/CEEICT.2018.8628051.

[13] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan and V. Patel, "An Attempt to Develop an IOT Based Vehicle Security System," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2018, pp. 195-198, doi: 10.1109/iSES.2018.00050.

[14] J. Patel, M. L. Das, and S. Nandi, "On the Security of Remote Key Less Entry for Vehicles," 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2018, pp.1-6,DOI: 10.1109/ANTS.2018.8710105.

[15] B. Siregar, S. Efendi, C. Setiawan, and F. Fahmi, "RFID Wristband for Motorbikes Real-Time Security System," 2019 3rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), 2019, pp. 116- 119,doi: 10.1109/ELTICOM47379.2019.8943903.

[16] S. Khan, O. Rahman and M. Ehsan, "Design and fabrication of a password protected vehicle security and performance monitoring system," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 560-563,DOI: 10.1109/R10-HTC.2017.8289022.

[17] N. Ramakumar, P. S. N. Reddy, R. N. Naik and S. A. K. Jilani, "Authentication based systamatic driving license issuing system," 2017 International Conference on Intelligent Computing

and Control Systems (ICICCS), 2017, pp. 1327-1331, doi: 10.1109/ICCONS.2017.8250685.

[18] Pradesh, R. B S, N. Nagabhushan and T. Madhavi, "Fingerprint-based Licensing for Driving," 2021 6th International Conference for Convergence in Technology (I2CT), 2021, pp.DOI6, DOI: 10.1109/I2CT51068.2021.9418134.

[19] K. Chopra and K. Gupta, "Smart Vehicle Card Using IoT," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 20-24, DOI: 10.1109/COMITCon.2019.8862210.

[20] J. B. K. Gangone, "An Ineligible and Unauthorized Motor Vehicle Driver Access control and Sleep State Alert System: An Offline based Model," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6,DOI: 10.1109/ICCCNT45670.2019.8944492.

[21] T. Banerjee, A. Chowdhury, T. C, Chakravarthy, and A. Ghose, "Driver authentication by quantifying driving style using GPS only," 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2020, pp. 1-6,DOI:10.1109/PerComWorkshops48775.2 156080.

[22] https://ijarcce.com/wp- content/uploads/2021/08/IJARCCE.2021. 10770.pdf

[23] A. Makarov, M. Španović and V. Lukić, "Authenticating vehicles and drivers in motion based on computer vision and RFID tags," 2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics, 2012, pp. 419-424, doi: 10.1109/SISY.2012.6339556.

[24] K M Farhat Snigdah. Md Gulzar Hussain,"Smart Traffic Vehicle Monitoring and Authenticating System using GPS" 2019 Conference: International Conference on Sustainable Technologies for industry 4.0 (STI) doi:10.13140/RG.2.2.10237.92642

[25] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan and V. Patel, "An attempt to develop an iot based vehicle security system", 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (FormerlyiNiS), pp. 195-198, Dec 2018

[26] Ganesh Sharma, et.al., E-Driving License and RC Book Verification System Using QR Code, International Journal of Advances in Electronics and Computer Science, Volume-4, Issue-1, pp. 1-2, Jan- 2017

[27] Kaveri Ningappa Gunjiganvi, et.al., Vehicle Document Verification using Vehicle Number (VCOP-App), International Journal of Engineering Research and Technology (IJERT), ICRTT 2018 Conference Proceedings, Volume 6,Issue 15, pp. 1-5, 2018

[28] Prof. C. S. Pagar, et.al., Electronic Secure Vehicle Verification System using Advanced RTO

System, International Research Journal of Engineering and Technology (IRJET), Volume 7, Issue 4, pp. 5330-5336, Apr 2020

[29] Dr.A.Srinivasarao, S.Gopiraju, M.Raghavendra, E- Driving License Authentication System, International Journal for Research in Engineering Application and Management (IJREAM), pp. 176-178, 2018

[30] Abraham Ziegen, Joel Manova M and Dr. A Akilandeswari, License Verification System with Face Recognition Using IOT, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 656-670, April 2021

[31] Sandeep Gupta, Attaullah Buriro, Bruno Crispo, DriverAuth: Behavioral biometric- based driver authentication mechanism for the on-demand ride and ridesharing infrastructure, The Korean Institute of Communications and Information Sciences (KICS) published by Elsevier, Science Direct, ICT Express, Volume 5, pp. 16-20, 2019

[32] Dr.A.Srinivasarao,S.Gopiraju, M.Raghavendra,E-Driving License Authentication System, International Journal for Research in Engineering Application and Management (IJREAM), pp. 176-178,2018

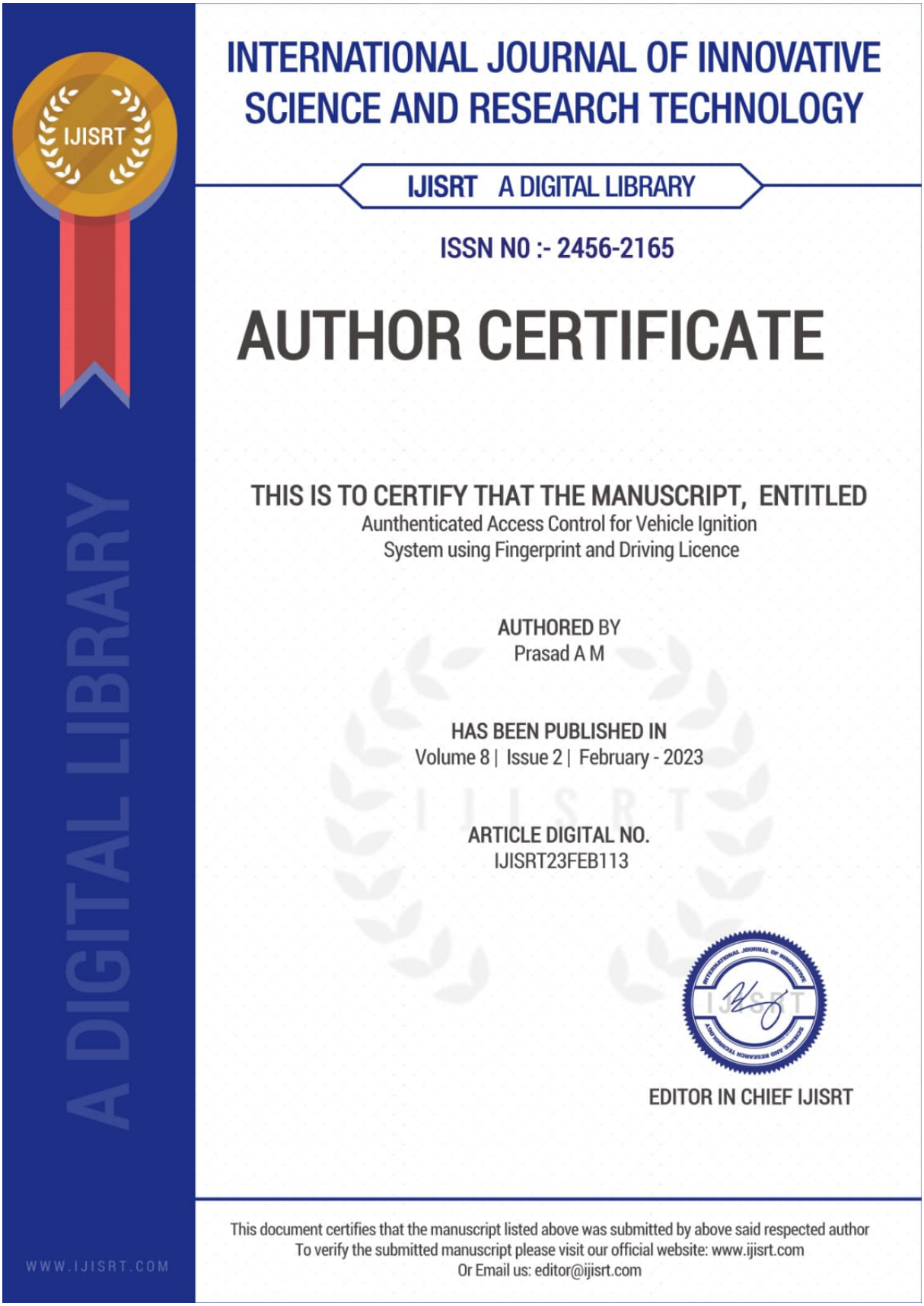

Figure 9.1: Certificate1

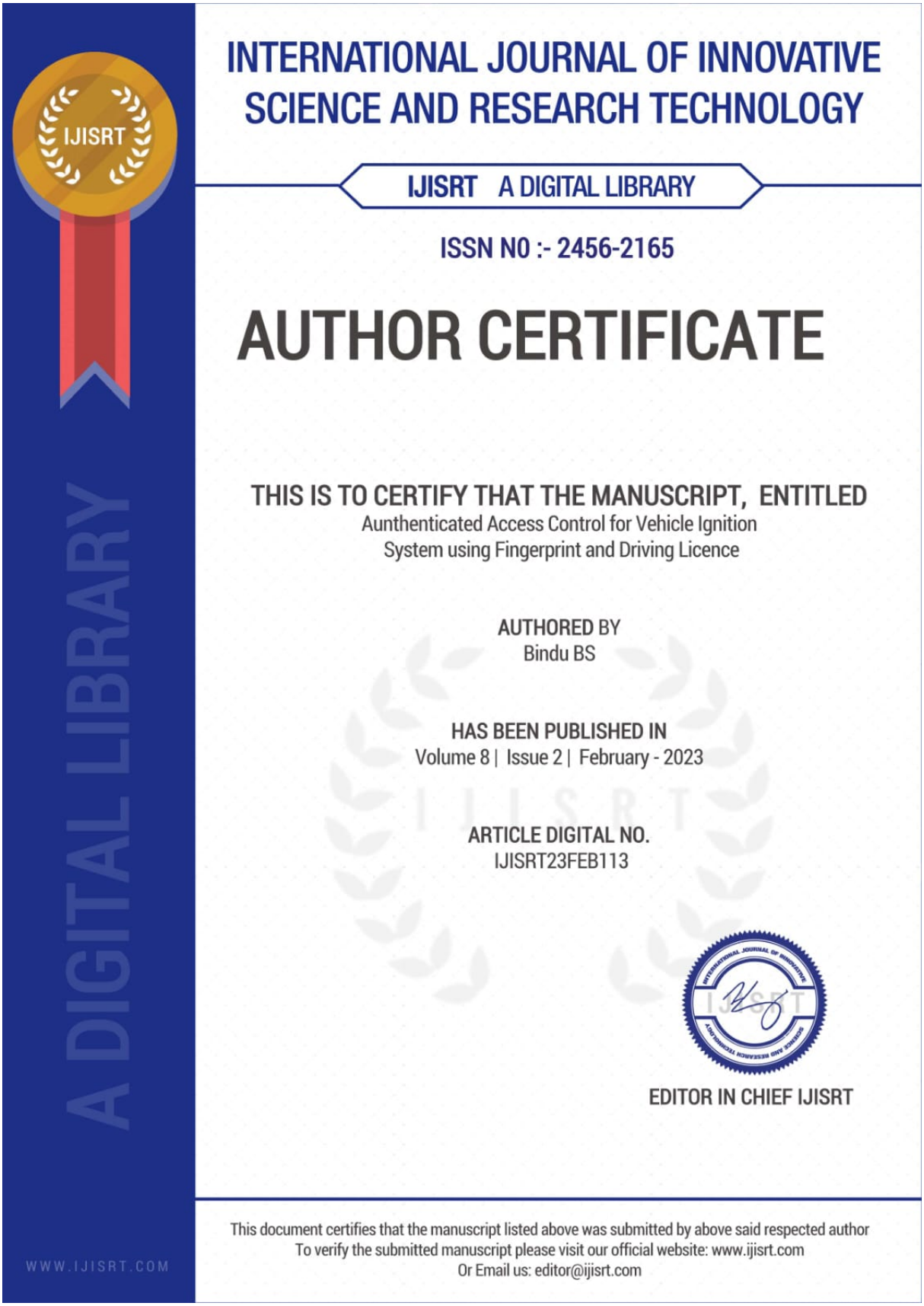

Figure 9.2: Certificate2

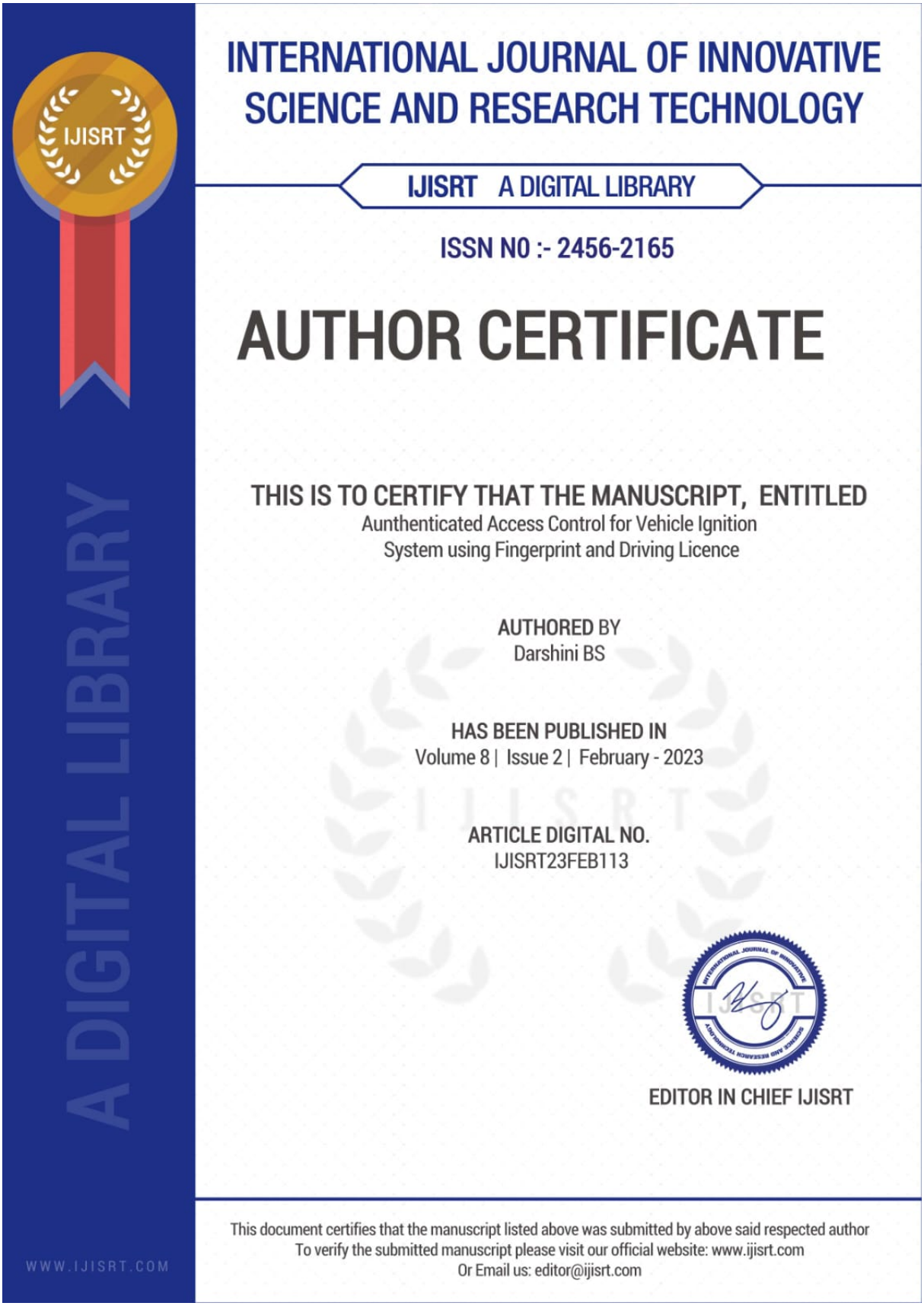

Figure 9.3: Certificate3

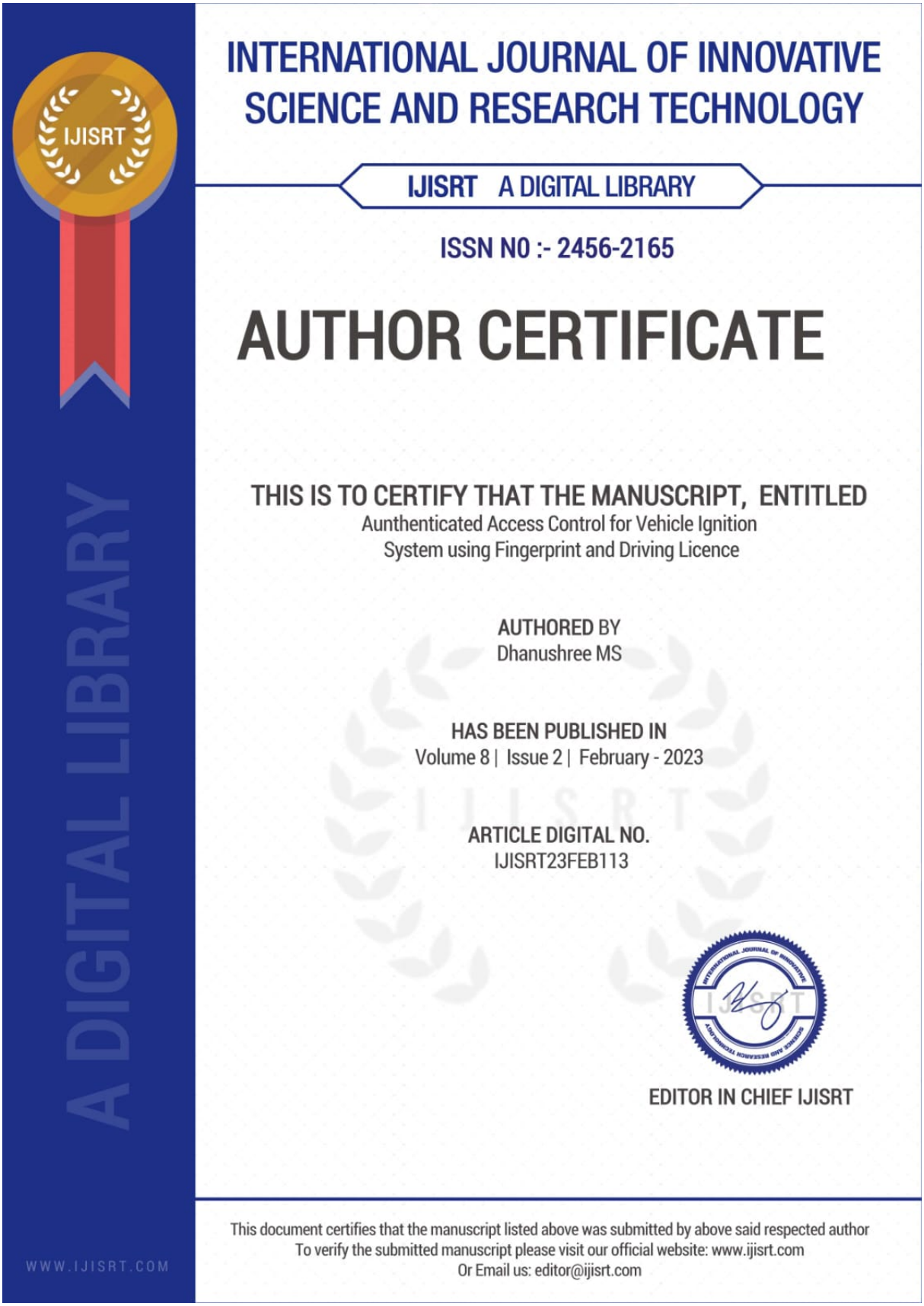

Figure 9.4: Certificate4

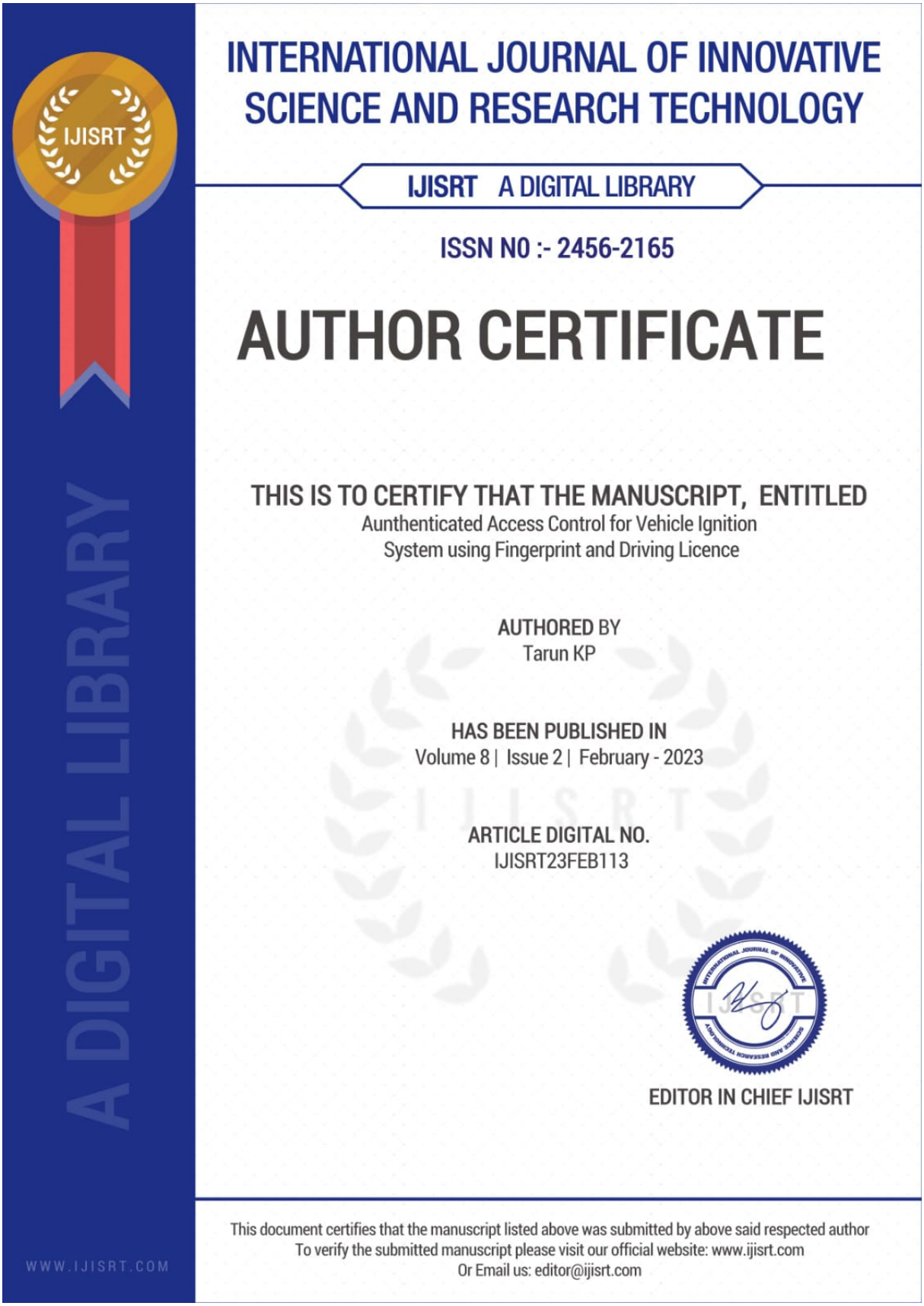

Figure 9.5: Certificate5