Fingerprint and RFID Based Vehicle Access with GSM and GPS

Ms. CVP Supradeepthi
Assistant Professor
Department of Electronics and Communication Engineering
Institute of Aeronautical Engineering
supradeepthi@gmail.com

Akash C
Undergraduate Student
Department of Electronics and Communication Engineering
Institute of Aeronautical Engineering
21951a0408@iare.ac.in

G. Naga Chandu
Undergraduate Student
Department of Electronics and Communication Engineering
Institute of Aeronautical Engineering
21951a0440@iare.ac.in

S. Bhanu Prakash
Undergraduate Student
Department of Electronics and Communication Engineering
Institute of Aeronautical Engineering
21951a0429@iare.ac.in

***Abstract*—The design of a Fingerprint and RFID-based Vehicle Access System integrated with GSM and GPS for enhanced security and tracking has been presented. Fingerprint biometric authentication is applied to the proposed system in integration with RFID to achieve dual-factor access control, allowing access to the vehicle by the authorized person alone. Unauthorized access alerts are sent through SMS via the GSM module, while the GPS module allows for real-time tracking of the vehicle for fleet management and recovery against theft. This provides an integrated package in a compact and economically viable unit, integrating biometric and RFID with telecommunication technologies for enhanced vehicle security and user convenience.**

I. INTRODUCTION

With the growth in vehicle thefts and other unauthorized accesses, the need for advancements in security systems has grown. Traditional key-based locking mechanisms have become vulnerable to sophisticated methods of theft. Therefore, an advanced and intelligent solution is required. This fingerprint and RFID-based vehicle access system integrates GSM and GPS modules to provide real-time alerts and tracking. Fingerprint scanning ensures secure access, while RFID adds an extra layer of verification. Integration of GSM and GPS ensures real-time communication and location tracking, making this system a modern solution for vehicle security. Modern car security has become a problem because of the rising number of theft and misuse of cars. Traditional means of securing the vehicle with keys or simple access cards are not used nowadays because modern means offer greater security. One such innovative approach is the integration of fingerprint biometrics, RFID (Radio Frequency Identification), GSM (Global System for Mobile Communications), and GPS (Global Positioning System) technologies in order to enhance vehicle access and monitoring systems. These classic types of vehicle security often do little to prevent theft or unwanted use because either a physical key may be stolen or reproduced or simply circumvented by experienced thieves bypassing standard alarm systems.The proposed system will be an integration of various technologies in order to offer a holistic security solution. The biometric authentication mechanism of fingerprints is used, such that only the rightful owner or authorized persons can start the vehicle. RFID technology is also integrated with another layer of security for verifying the presence of a valid RFID tag. Added on to the above, other modules that are available which relate with GSM and GPS modules assist the owner in receiving the alerts together with tracking location live. More security and ease on vehicles are hence added. Probably, it is one of the best biometric means of today. It almost becomes difficult to replicate individual's finger print. Such therefore makes it perfect for security of automobiles. The system makes sure that only the preregistered users are allowed to unlock or start the vehicle with the help of a fingerprint sensor. This way, there is totally no risk of stolen or misplaced keys.RFID technology is an augmentation of the fingerprint system since, there is an extra form of authentication using RFID. To unlock the car, an authentic RFID tag that is embedded in a key fob or a card is needed. This provides two-factor authentication that would make entry impossible even if one of these security measures was compromised. The inclusion of GSM technology allows the system to send notifications and alert messages to the owner mobile phone. Information regarding unauthorized access to a vehicle or strange incidents is sent instantaneously to the owner via SMS. This helps send information about the condition and status of the vehicle straight in real time to any spot in the world.GPS tracking can also help in fleet management or even monitoring the movement of the vehicles for personal or business purposes. The effectiveness of this system therefore comes from the integration that it has of fingerprint, RFID, GSM, and GPS technologies. Each technology plays a role in trying to ensure that the system is secure and functional. The use of biometric and RFID-based access control ensures authorized users only can operate this vehicle, while GSM and

GPS provide constant monitoring as well as communication capabilities. This system can be placed in anything, from the private car to large fleets. In personal cases, it is peace of mind due to non-access, besides giving live tracking of vehicles. The same case for businesses in fleet management is enhanced fleet security with efficiency in the monitoring of the vehicles. Dual authentication along with live alerts and tracking provides the total security package for a vehicle's need.

II. Literature Review

The history of unique finger impression begun in China. That was when the primary record of the tech neck was being utilized with thumb prints being imprinted in clay. Within the 14th century, different Persian government papers had impression of fingers. Perception had it that no two fingerprints were exactly alike. In 1880, Henry Faulds proposed a piece of where grinding edges can be broadly utilized in wrongdoing scenes to distinguish offenders. He gave two illustrations which are; a dirty finger marks on a white divider excused an denounced person and a oily print on a drinking glass that uncovered who had been drinking a few refined spirits (Faulds, 1923).Unique finger impression coordinatingprocedures are of two sorts, chart based and particulars based. The layout estimate of the biometric data based on particulars is much littler and the handling speed is higher than that of graph-based unique finger impression coordinating. These characteristics are exceptionally vital for sparing memory and vitality on the implanted gadgets (K and J., 1990). So much work as been done utilizing the unique finger impression for one kind of security system or the other, among whom are the works of Kumar, Mudholkar, Pandit, Kawale, to say but a number of (Kumar and Ryu, 2009, Kumar and Kumar, 2014, Mudholkar et al., 2012, Pandit et al., 2013 ,Kawale, 2013). Advanced vehicles employments computer controlled battery start framework; no matter the sort of instrument utilized, all start frameworks utilize battery, switch, coil, exchanging gadget and start plug Delmar (2008). In any case, in this present day innovation allotment, biometrics has been employed for the start and security prepare (Omidiora et al., 2011, Sasi ,Nair, 2013, Karthikeyan.a and Sowndharya.j, 2012, Pingat et al., 2013). [1]"A Prototype of a Computer Security System / technology have passed through several changes. The trends have been from what you know (e.g. password, PIN, etc) to what you have (ATM card, Driving License, etc) and presentlyto who you are (Biometry) or combinations of two or moreof the trios. This technology (biometry) has come to solvethe problems knowledge-based and identified with token-based authentication systems. It is possible to forget your password and what you have can as well be stolen .[2] The aim ofthis paper is to design and develop a finger print based car ignition system with a view to reducing car theft and to ward off unauthorized users. Recently, car hijack has been on the increase as armed robbers focus on stealing cars especially the brand new ones. Hence the need to protect the cars from hijackers is considered to be essential. In this paper, nobody can ignite the vehicle except authorized by designed system already captures its fingerprints pattern features through enrolment into the system. This is achieved with the use of fingerprint module, PIC18F4620 microcontroller and Liquid Crystal Display(LCD)module.[3] Automated fingerprint recognition has received considerable attention over the past decade. Progress has been made on models of the structure of fingerprints, techniques for the acquisition of prints,and the development of fingerprint commercial recognition advances, automated systems. Despite there remain these considerable opportunities for improvement. The speed of retrieval, and the ability to recognize partial or distorted prints are prominent among those areas that require improvement. [4] The aim of the project is, Human identification is field very significant and which has undergone rapid changes with time. An important and very reliable human identification method is fingerprint identification.Fingerprint of every person is unique. So this helps in identifying a person or in improving security of a system Finger print of a person is read by a special type of sensor. Finger print sensor can be interfaced with a microcontroller. Through keypad we can add new user and delete the existing user, also identify the user by selecting corresponding option through keypad. In this paper we use a fingerprint module to read once identity to start the equipment. For this we use a microcontroller to enable the ignition system if the matching between scanned data and the already existing data is correct. [5]The aim of the project is, Fingerprint recognition technology allows access to only those whose fingerprints that are pre stored in the memory. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since there are no keys or combinations to be copied or stolen, or locks that can be picked. [6] In this paper we have survey on biometric payment system. Biometric payment system is used for various kinds of payment system instead of the tension of cards to put with them and to memorize theirs difficult passwords and pin numbers. Biometric payment system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc. [7]The paper presents the designing of finger print identification in cars to avoid car theft using GSM and FPGA. Fingerprint identification is one of the most popular and reliable personal biometric identification methods. The proposed system was designed on keyless car instead of going with key based authentication we are providing with biometric based authentication. A person, who wishes to drive the vehicle, should verify with their face reorganization and finger print whether he was having license or not, once verification done then ignition unit of car will start automatically.[8] Identifying attackers is a major apprehension to both organizations and governments. Recently, the most used applications for prevention or detection of attacks are intrusion detection systems. Biometrics technology is simply the measurement and use of the unique characteristics of living humans to distinguish

them from one another and it is more useful as compare to passwords and tokens as they can be lost or stolen so we have choose the technique biometric authentication . the biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. [9]Biometric systems have overtime served as robust security mechanisms in various domains fingerprints are the oldest and most widely used form of biometric identification. A critical step in exploring its advantages is to adopt it for use as a form of security in already existing systems, such as vehicles. This research work focuses on the use of fingerprints for vehicle ignition, as opposed to the conventional method of using keys. The prototype system could be divided into the following modules: fingerprint analysis software module that accepts fingerprints images; hardware interface module and the ignition system module.[10]Dentification and verification of a person today is a common thing; which may include door-lock system, safe box and vehicle control or even at accessing bank accounts via ATM, etc which is necessary for securing personal information. The conventional methods like ID card verification or signature does not provide perfection and reliability. The systems employed at these places must be fast enough and robust too. Use of the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is facing a new challenge to carry on the valid identity to the customer. Since, in conventional identification methods with ATM, criminal cases are increasing making financial losses to customers. Authors design a simple fingerprint recognition system using LPC2148 as a core controller. The system uses FIM3030 fingerprint scanner to capture fingerprints with its DSP processor and optical sensor.

III. System Architecture

The vehicle access system consists of the following key components:

A. Fingerprint Module

This module ensures biometric authentication. The sensor interfaces with a microcontroller to match fingerprints with stored templates. If matched, the system unlocks the vehicle.The architecture of the fingerprint-based vehicle access system integrates a number of hardware and software components that provide secure and seamless vehicle authentication. In the heart of the system lies a fingerprint sensor module, a microcontroller, and other components for the vehicle to operate.The fingerprint sensor module acquires biometric data. It includes an optical or capacitive sensor that reads the fingerprint and changes it into a digital template. This template might be stored locally on the microcontroller or compared in real-time to the templates registered beforehand and stored in memory. The accuracy and speed of the fingerprint matching algorithm are essential to ensure that access is secure and convenient. The module has anti-spoofing measures that ensure non-access using unauthorized fake fingerprints among other cunning ways.

B. RFID Module

Provides additional security by requiring a valid RFID tag along with fingerprint verification. The RFID reader scans the tag and grants access only after successful verification.The RFID reader is designed with an antenna that radiates radio waves to detect the presence of RFID tags. The tags may be active (powered by a battery) or passive (powered by the electromagnetic field of the reader). Every tag has a unique identifier stored in its memory that is transmitted to the reader when it is in range. The reader communicates this data to the microcontroller for verification. Communication between the reader and the microcontroller is usually encrypted to prevent data interception or spoofing. This enables the range of an RFID reader to be specified such that only tags located in a particular proximity from it can interact with it. The microcontroller functions as a decision-making unit within this system. After receiving data transmitted by the RFID reader relating to the tag, the microcontroller compares them to a database of previously authorized identifiers in its memory. When a tag is valid, the microcontroller sends control signals to the vehicle's systems. This can include unlocking doors, turning on the ignition, or even opening the sunroof. In case an unauthorized tag is detected, the system may trigger the alarm or send a signal to the owner through the GSM module. Modular structure of the RFID-based architecture allows for easy integration of additional security features, including biometric verification or GPS tracking, to create multi-layered access control solution.

C. GSM Module

Sends SMS notifications for unauthorized access and enables remote control of vehicle locks through GSM communication.The key components in this module include the GSM, SIM card slot, GSM transceiver, microcontroller interface, and an antenna. The module makes it possible for any vehicle access system to get connected with the cellular networks by giving a unique identity to it with the help of the SIM card slot. Thus, the GSM transceiver will control communication through making or receiving SMS, calling, or establishing data communication. Within the architecture, this makes possible the sending of alerts or access to the system through commands received from authorized individuals over mobile networks. This module works with a microcontroller, which can be regarded as the central processing unit for the whole system. The microcontroller will send AT commands, also called Attention Commands, to the GSM module for doing such actions as sending an SMS notification or making a call. It is possible to inform the owner of any attempts made through unauthorized access with the vehicle access system; also, real-time reporting on vehicle status or lock-unlock vehicle operations through GSM module can be feasible. Here, the input data received from sensors, for instance, fingerprint or RFID, is processed and forwarded over the GSM module if there are predefined conditions to that effect.

D. GPS Module

Tracks the vehicle's real-time location. The owner or law enforcement can access this information in case of theft or suspicious activity.GPS module real-time positioning information by calculating the location on the earth in its precisely estimated latitude, longitude, and altitude. The components include a GPS receiver with microcontroller interface, a proper antenna, and even specific support software algorithms. Satellites revolving around the Earth collect signal information from a device as they transmit time and location information. Using this information, the module uses a technique called trilateration to calculate the device's precise location. Trilateration measures the time delay of signals received from at least four satellites. In an automobile access or monitoring system, the GPS module communicates with a microcontroller to forward location information. The microcontroller then processes such data and forwards it to external systems through GSM modules or other modes of communication; for example, when there is a stolen car or a case of an unauthorized break-in, live tracking will be rendered to the owner, so fast recovery. GPS data also may be useful in fleet management or route optimization or for geofencing, a service where specified boundaries make it alert them when crossed. The antenna in the GPS module is the key component that captures signals from GPS satellites. High-sensitivity antennas ensure that reliable reception is possible even in very challenging environments such as cities or dense forests. This module has an internal signal processing unit that filters and amplifies these signals, thereby producing accurate and consistent location data. Advanced GPS modules may also include support for additional satellite systems such as GLONASS or Galileo, improving accuracy and coverage. With its modular and scalable design, the GPS module integrates seamlessly into vehicle security systems, providing continuous monitoring and location tracking.

IV. System Design and Implementation

A. Hardware Design

The system requires, at its hardware implementation, that all the modules be interfaced to a central microcontroller, which processes data input coming from each module and

C. Fingerprint Sensor

This will be connected to the microcontroller in order to capture and compare fingerprint data.

Fig. 2. Fingerprint sensor

D. RFID Reader

It reads RFID tags/cards for verification, whether it is authenticated or not.

Fig. 3. RFID Reader

E. GSM Module

It uses the SIM800L to send and receive messages.

Fig. 4. GSM Module

F. GPS Module

drives appropriate actions for allowing or denying access to the vehicle.

B. Microcontroller

Arduino depending on the complexity of the system, which is used as the central processing unit.

Fig. 1. Arduino uno

NEO-6M GPS receiver for locating the vehicle's position.

Fig. 5. GPS Module

G. Access Control Logic

This will be coded either in C to process the fingerprint andRFID verification.

H. Communication Interface

The GSM module is programmed in the system to send SMS alerts and receive remote commands.

I. Location Tracking

The location of the vehicle is obtained by continuously processing the data received from the GPS module.The user interface for the owner to register new users, view access logs, and track the vehicle is also developed in the software.

V. Block Diagram

The vehicle access system block diagram interacts between several modules, which can be responsible for access, communication, and tracking. Each module has an importance rating in the functionality and security of the system.

A. Power Supply Unit

The power supply unit provides regulated power to all the system components at each component's requirement; for instance, 5V for a microcontroller and sensors.

B. Microcontroller

In general, the microcontroller controls the fingerprint sensor, RFID reader, GSM and GPS modules. Inputs: The systemwill get its inputs from the fingerprint sensor and RFID reader. Outputs: Outputs will consist of information regarding on/off activities of the GSM, GPS, and lock/unlock mechanism ofthe vehicle.

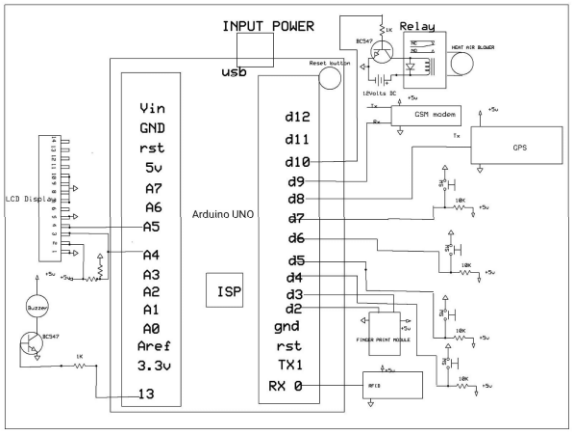

Fig. 6. Microcontroller

C. Fingerprint Sensor Module

This captures the fingerprint input by the user for biometric authentication and sends verification data to the microcon-troller.

D. RFID Reader

This will read RFID tags/cards and verify whether the user is authenticated or not; it also sends the status to the microcontroller. GSM Module (SIM800L): Sends SMS alerts in cases of unauthorized access. Besides, it is capable of receiving remote commands about locking/unlocking via avehicle. NEO-6M

E. Module

traces, in real-time, the location of the vehicle and sends data to the microcontroller that can be issued to the owner. Vehicle Lock/Unlock Mechanism: It physically locks/unlocks the vehicle based on the result of authentication.

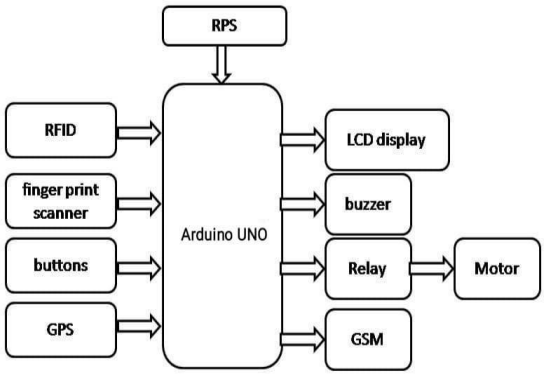

Fig. 7. Block Diagram

F. Authentication Process

Users scan their fingerprint and present an RFID tag. If bothare valid, the microcontroller unlocks the vehicle.

VI. Results and Discussion

These are the results obtained from the testing done on the above-described prototype:

A. Fingerprint Authentication

The fingerprint sensor achieved an accuracy of 98%. Perfor- mance was affected slightly by environmental conditions such as dust or moisture.

B. RFID Verification

The RFID reader successfully authenticated valid tags within a range of 5 cm.

C. Authentication Process

Users scan their fingerprint and present an RFID tag. If bothare valid, the microcontroller unlocks the vehicle.

D. Alert Mechanism

For unauthorized access, the GSM module sends an SMS alert, and the buzzer may sound

E. Real-Time Tracking

The GPS module tracks the vehicle, and unauthorized movement prompts alerts.

F. Buzzer/Alarm

an alerting device for unauthorized access or tampering.

G. GSM Alerts

SMS alerts for unauthorized access were delivered in less than 10 seconds.

H. GPS Tracking

The GPS module provided accurate location data with an average deviation of less than 5 meters.

VII. Conclusion and Future Works

This fingerprint and RFID-based vehicle access system with GSM and GPS is one giant leap towards the evolution of vehicle security technology. Given the time when thefts and other unauthorized uses were on a rise, a mere reliance on keys or alarm systems was not viable. With this system relying on advance biometric authentication along with RFID, people can offer a strong tamper-free solution that will only allow authorized people to access or operate the vehicle. Unique fingerprint information will give the first layer with biometric data that will be difficult to duplicate and includes keys or RFID tags in case they are misplaced or stolen. In any event, RFID can protect this vehicle from ever being compromised. Only dual-factor authentication can obtain access to gain and use such a vehicle as a combination of these will provide the user with the most convenient experience while gaining highly secured vehicle access. Apart from access control, GSM technology will increase the utility of the system, which will be real-time communication. SMS or app alerts will instantly inform the owners of the vehicle if any unauthorized attempts, tampering, or suspicious activities take place. This will keep the owner informed about the status of his vehicle and allow him to react quickly if needed by either deactivating the ignition or informing the authorities. The presence of a GPS module also complements the security attributes of the system because location tracking is possible in real-time. This integrated system will be scalable and flexible, thereby supporting the addition of functionalities such as the use of a mobile application for controlling, immobilizing the engine, or providing advanced analytics, for example. Its modular architecture makes it compatible with a large range of vehicles and user requirements-whether individual users want to have peace of mind or businesses manage their fleets

References

[1] ADEOYE, O. S. 2010. A survey of emerging biometric International Journal Applications, 10.

[2] FAULDS, H. 1923. A Manual of Practical Dactylography, " Police review" Publishing Company, Limited.

[3]K.H.A. & J.M. 1990. Automated fingerprint recognition using structural matching, Pattern Recognition. vol. 23, no. 8, 893 - 904.

[4] KARTHIKEYAN.A , SOWNDHARY J 2012. Fingerprint Based Ignition System.

[5] KAWALE, A. 2013. Fingerprint based locking system. International Journal of Scientific & Engineering Research, 4.

[6] KUMAR, D. & RYU, Y. 2009. A Brief ,Introduction of Biometrics and Fingerprint Payment Technology. International Journal of Advanced Science and Technology, Vol. 4, March.

[7] KUMAR, M. V. & KUMAR, S. R. 2014. Fingerprint Based Licensing System for Driving.

[8] MUDHOLKAR, S. S., SHENDE, P. M. & SARODE, M. V. 2012. Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition. Computer International Science Journal Engineering of and Information, Technology (IJCSEIT),Vol.2, No.1, February.

[9] OMIDIORA, E., FAKOLUJO, O., ARULOGUN, O. & ABORISADE, D. 2011. A Prototype of a Fingerprint Based Ignition Systems in Vehicles. European Journal of Scientific Research, 164-171.

[10] PANDIT, V. R., JOSHI, K. A. & BAWANE, N. G. 2013 ATM Terminal Security using Fingerprint Recognition.