Vehicle Theft Authentication System

Mrs. Smitha P [1], Basavaraju Gari Sreedhar [2], Bhuvana N [3], Pavitra L[4], Sahana B S [5]

[1]*Assistant Professor, Dept. of AI&DS, East West Institute Of Technology, Bengaluru*

[2, 3, 4 , 5] *Student, Dept. of AI&DS, East West Institute Of Technology, Bengaluru*

---***---

Abstract - This thesis presents a robust security system designed to tackle the escalating issue of vehicle theft and unlicensed driving. By integrating a suite of cutting-edge technologies including Arduino, driver's permit card (DL),radio-frequency ID scanner (RFID),biometric fingerprint sensor (FP), Face Recognition (FR), and Global System for Mobile Communication modem (GSM), the system aims to fortify vehicles against unauthorized access. At its core, Arduino serves as the central intelligence, capable of storing and processing authorized driver data such as facial recognition and fingerprint records. When a driver inserts their license into the RFID reader, the system cross-references the information with stored data. If the license is validated, the system proceeds to authenticate the driver's identity through facial recognition and fingerprint scanning. Successful verification enables the ignition system, granting access to the vehicle. However, any discrepancy triggers an immediate SMS alert via the GSM modem to the vehicle owner, while simultaneously disabling the ignition to thwart unauthorized use. Additionally, an alcohol detection module further enhances safety by preventing vehicle ignition if alcohol is detected in the driver's system. This comprehensive approach not only safeguards vehicles from theft but also promotes responsible driving practices, exemplified by timely license renewal reminders and the enforcement of alcohol-free driving.

Key Words: Vehicle security system,Arduino integration,Driver's license card (DL), radio-frequency ID scanner (RFID),Fingerprint module (FP) Face Recognition (FR), GSM-enabled mobile communication device, Unauthorized access prevention,Facial recognition,Fingerprint scanning SMS alerts,Alcohol detection module,Responsible driving practices,License renewal reminders,Alcohol-free driving enforcement.

1. INTRODUCTION

Driving without a license poses significant risks, with unlicensed drivers, drunk driving, and seatbelt negligence being key contributors to accidents. These incidents stem from various factors, including inadequate training and a lack of compliance with traffic laws. Unlicensed drivers may disregard legal repercussions and safety incentives, leading to a disregard for road safety. This paper aims to address these issues by proposing solutions to two main problems: the criminal exploitation of motorized road traffic and weaknesses in enforcement and penalties. By tightening regulations, enhancing document verification systems, and expanding the functionality of driver's licenses to include payment features, digital signatures, and penalty point collection, the goal is to enhance road security and curb illegal driving practices.

Existing System

Despite recent advancements in vehicle anti-theft technology, the effectiveness of these devices remains limited due to inherent drawbacks. Both domestic and international markets offer anti-theft products categorized into three main types: mechanical lock devices such as steering wheel locks, hood locks, and tire locks; vehicle alarm systems; and vehicle tracking/recovery systems like the LoJack tracking system, the ProScout GPS Vehicle Tracking System, and the Travel Eyes2 Vehicle Tracking System, among others. Among these, vehicle tracking and recovery systems are commonly utilized, often relying on radio signals for operation. However, while these systems offer the promise of locating stolen vehicles, their effectiveness can be hampered by factors such as signal interference or geographical limitations. As such, the search for an ideal anti-theft solution continues, driven by the persistent challenge of enhancing vehicle security against theft.

Proposed System

A comprehensive anti-theft system leveraging Face and Fingerprint Sensors, Wi-Fi, Mobile Phone, and Android technologies is proposed to overcome existing limitations. Vehicle owners register their fingerprints and faces in a database, enabling ignition only upon matching stored values. Failure to match triggers an OTP authentication request to the owner, who grants permission via mobile phone. Pre-registered drivers gain access, with stolen vehicle alerts sent to owners via Wi-Fi, allowing tracking through an Android app. GPS modules continuously monitor vehicle location, transmitting data to a central server via IoT connectivity. Owners receive alerts and can monitor vehicles through a mobile app. In case of theft, alerts are sent to the nearest crime station, while RFID verification checks driving license validity. Additionally, alcohol and accident monitoring systems notify owners or nearby hospitals, with regular software and hardware updates ensuring system effectiveness.

2. RELATED WORK

Several studies have concentrated on developing cost-effective systems for protecting vehicles from theft. One method involves using microcontrollers to send alerts to the car owner if theft is attempted. Vibration sensors gauge motor velocity and send this data to the microcontroller, which then alerts the owner. Additionally, GPS modules aid in tracking the vehicle's location over time [1].

Another study employed a PIC16F877A microcontroller to store valid RFID numbers from smart cards. When a valid card is scanned, the microcontroller triggers an electromagnetic relay, allowing the user to start the vehicle. In case of an invalid card, the system permits three attempts before notifying the owner via a GSM module [2].

A separate research project implemented a security system using an AVR microcontroller. It stored images in a database for face recognition, granting access if a match was found. In case of an unrecognized face, a password was required. The system also included strain gauge sensors for accident detection [3].

Another system based on face recognition stored images of authorized individuals in a database. When someone attempted to enter the car, the system compared the captured image with stored images and enabled ignition upon a match. If not, it sent an MMS/SMS with the unauthorized person's image and location via GPS/GSM [4].

A proposed system utilized an ARM 7 processor-based LPC2148 controller. It featured a smart card storing fingerprints for authentication, a card reader, and a fingerprint module. If the scanned fingerprint matched, the ignition was enabled; otherwise, it remained off. The system also included IR sensors for seatbelt detection and an alcohol sensor to prevent driving under the influence [5].

3. METHODOLOGY

The proposed system's overall structure is illustrated in Figure 1.

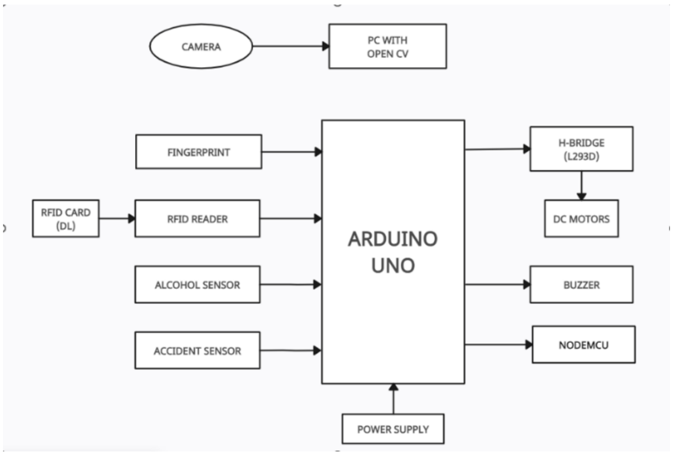


Fig.1.Illustrates the Block Diagram of the Proposed System.

The project utilized the following hardware components:

RFID RC522 Module

RFID, or Radio Frequency Identification, is a technology that uses radio waves to communicate between integrated circuits, tags, readers, and software to identify various items automatically. It relies on unique numbers stored on microchips, enabling seamless and efficient reading. The RFID-RC522 reader module, illustrated in Figure 2, embodies this technology, facilitating the reading and communication process between RFID tags and the associated system.

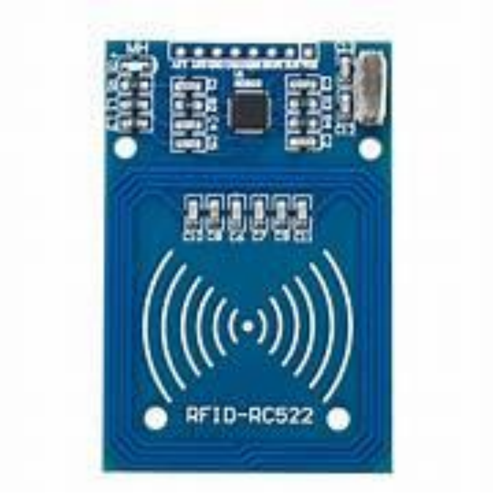


Fig. 2 illustrates the RFID-RC522 reader module.

Tags

For this project, a smart driver's license functions as the tag for object identification. This smart card includes crucial details such as ID, name, age, fingerprint, and image, all stored within the tag and transmitted to the reader. As the reader communicates with tags through radio frequency (RF), it requires one or more antennas. Moreover, the reader needs a network interface for communicating with other devices or servers, which may include serial (UART) for RS232 or RS485, RJ45 jack for Ethernet cables (10BaseT or 100BaseT), or Bluetooth and wireless Ethernet capabilities. Additionally, each reader must have either a microcontroller or microcomputer to implement communication protocols and manage the transmitter.

Digital driver's license

The digital driver's license (eDL) marks a significant advancement in preventing fraud and enhancing document security due to its sophisticated design incorporating a microprocessor. This advanced eDL integrates various visual, physical, and electronic security features, making it highly resistant to counterfeiting while also being user-friendly. With the inclusion of a microprocessor, the eDL allows law enforcement personnel to electronically access and verify card data using smartphones, even in motion. This technological advancement promotes better connectivity and communication between police and other government agencies in the field, thereby improving the efficiency and effectiveness of law enforcement operations. Figure 3 depicts the eDL.

.

Fig. 3 displays the Electronic Driver's License (eDL).

Optical Fingerprint Sensor

Improve the security of your project by incorporating an all-in-one optical fingerprint sensor designed for seamless fingerprint detection and verification. These modules, commonly used in safes, feature a powerful DSP chip responsible for image rendering, calculation, feature-finding, and searching, ensuring efficient performance. With TTL serial communication, connecting this sensor to any microcontroller or system is straightforward, enabling functions like capturing photos, detecting prints, hashing, and searching. One notable feature of this sensor is its ability to enroll new fingerprints directly, with the onboard FLASH memory capable of storing up to 162 fingerprints. Additionally, it includes user-friendly Windows software for easy testing and operation, simplifying fingerprint enrollment and allowing users to view fingerprint images on their computer screen. Figure 4 depicts the fingerprint module.

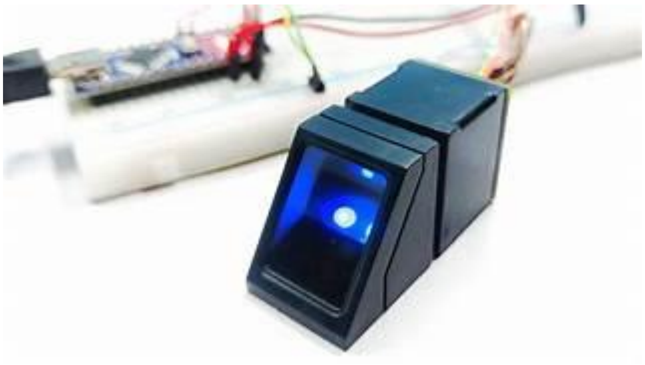


Fig. 4 showcases the Fingerprint Module.

GSM Module

GSM, which stands for Global System for Mobile Communication, is a mobile communication modem that operates as an wireless cellular technology, whether open or digital, continues to evolve rapidly.. It is primarily used for transmitting mobile voice and data services across different frequency bands, including 850MHz, 900MHz, 1800MHz, and 1900MHz.

Within the GSM system, there are several cell sizes designed to optimize coverage and capacity. These cell sizes include macro cells, micro cells, Pico cells, and umbrella cells, each serving specific purposes in providing reliable mobile communication services..

Electromechanical Relay

An Electromechanical relay functions as a switching device that opens and closes in response to an electric current passing through it. When the coil of the relay is energized, it causes the switch based on mechanical operation to close, and when the coil is de-energized, the switch opens.

In this project, the relay is utilized to activate the car's ignition system upon scanning an authorized card and confirming a fingerprint match.

Simulation Scenario

The system instructs the user to insert their driver’s license card into the RFID reader. Subsequently, the reader retrieves data stored in the tag (DL), which includes ID and car number, for verification purposes. The system considers only one driver’s license data to meet project objectives. After comparing the card data with stored program data, if a match is found, it validates the driver's license, permitting vehicle usage. However, prior to operation, ownership verification is mandatory.

The DL holder places their finger on the fingerprint scanner module, and if there's a match with stored fingerprints of authorized individuals, the system initiates car ignition. This is indicated by the display showing "system ignition" and the green LED lighting up. In case of no match, indicating an unauthorized attempt, the red LED stays illuminated, and the system displays "UNAUTHORIZED_RFID."

If an invalid driver’s license is detected, meaning the data doesn’t match stored records, the system remains inactive, displaying "UNAUTHORIZED_RFID." Both verification steps are crucial for the system's proper functioning; otherwise, it remains inactive. Multiple attempts with an invalid driver’s license trigger the GSM module to send an SMS alert to the vehicle owner, alerting them of attempted theft.

Driver’s licenses have expiration dates and require renewal before expiry. Therefore, the system sends SMS reminders to the holder, ensuring timely renewal and uninterrupted vehicle usage.

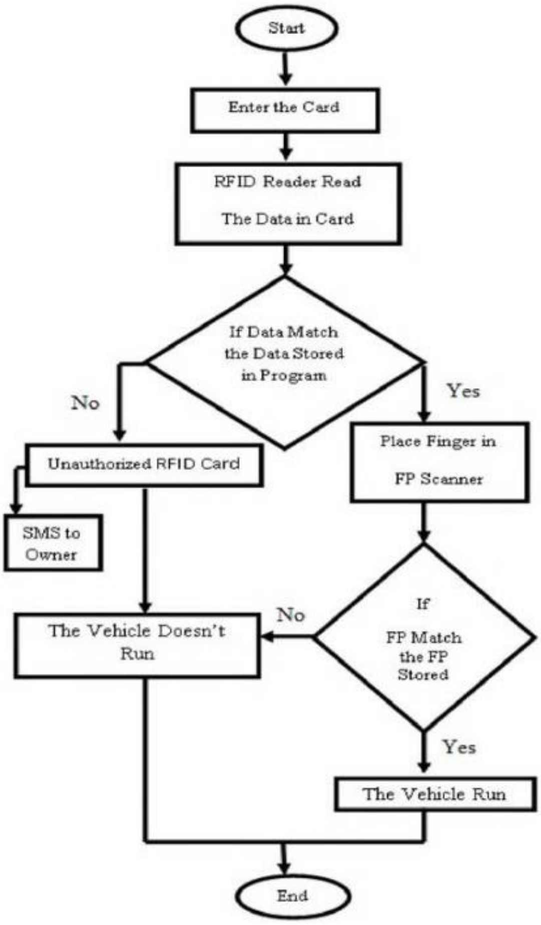


Fig.5. The Proposed System Flowchart is depicted in the following diagram

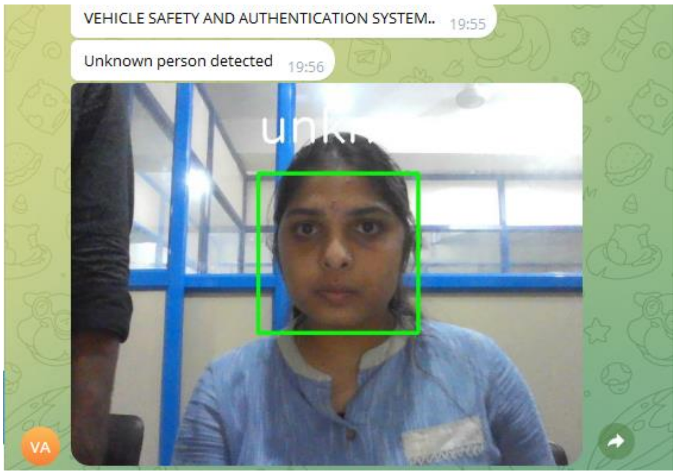
4. IMPLEMENTATION

Creating an a verified access control system for starting vehicles involves setting up a database to store authorized driver information, allowing owners to register fingerprints and facial features. Upon ignition, a robust authentication process verifies the driver's license and fingerprint. Owners receive authentication prompts on their mobile phones and can grant access via OTP or a dedicated mobile app. Real-time tracking is enabled by GPS modules, with a specialized app enabling owners to monitor their vehicles. Collaboration with law enforcement and document validation enhances security measures. Regular updates ensure the system remains effective over time.

5. Results and Discussions

Case 1:

Fig.1. Illustrate when unauthorized person trying to start the ignition system then it detects as a unknown person detected and asking the secret code.



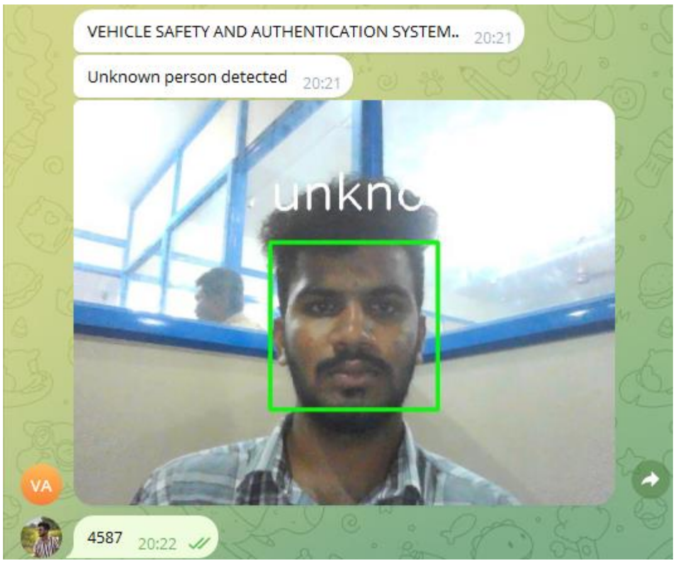
VEHICLE SAFETY AND AUTHENTICATION SYSTEM.. 19:55

Unknown person detected 19:56

Fig.1.Face Authentication System

Case 2:

Fig.2. Illustrate the when owner enters the secret code and ignition system will be send a message to owner giving the permission and and starts asking to fingerprint id .



VEHICLE SAFETY AND AUTHENTICATION SYSTEM.. 20:21

Unknown person detected 20:21

4587 20:22

Fig.2.Owner giving the permission

Case3:

Figure 3 depicts the scenario where the key used to start the vehicle's engine is turned "ON," signaling the device used for reading cards prepare for scanning the authentication card, after which the automobile is switched off.

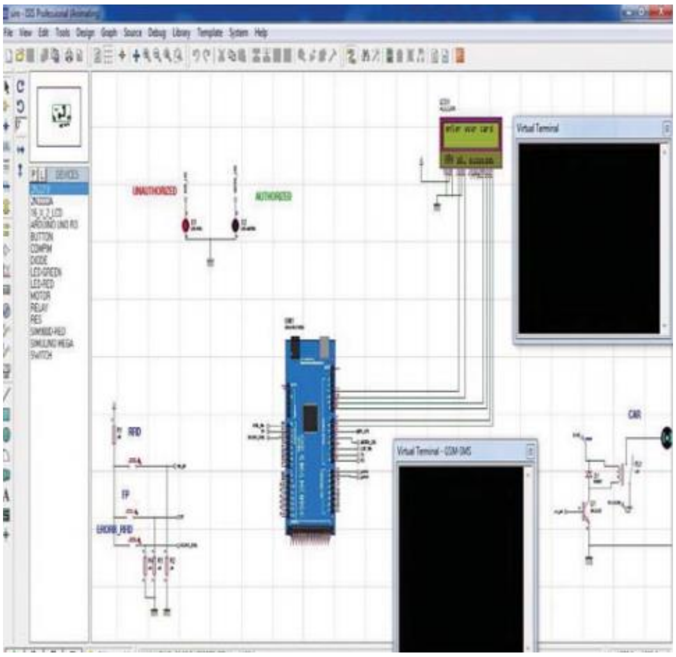


Fig.3.The circuit while in the starting mode

Case 4:

In Figure 4, we observe the process where a user inserts a card, and the RFID scanner scan this data, sending it to an Arduino for detecting a match. If a match is found, indicating a trusted driver's license, the car remains idle. Additionally,the red LED is lit up to signify indicating that the vehicle is stationary.

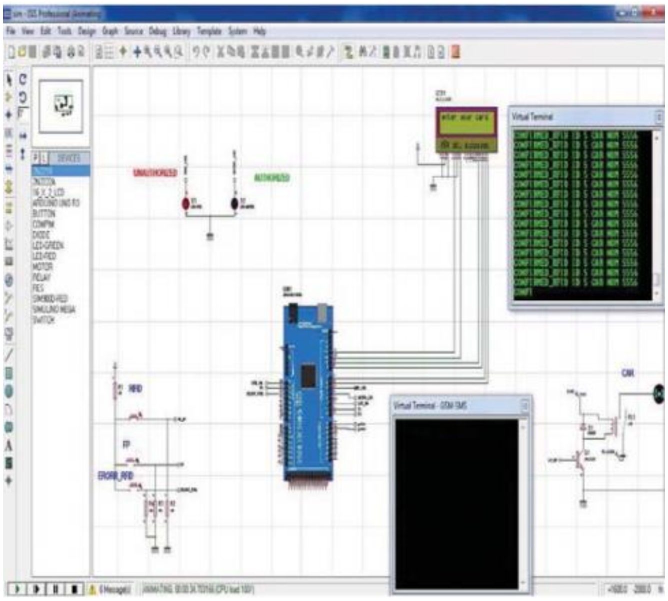


Fig.4. Simulating the insertion of an authorized RFID card (driver's license card).

Case 5:

Figure 5 illustrates the situation in which, following the input of the authenticated driver’s license, the user then places their finger on the fingerprint scanner, leading to a successful match. This sequence allows the driver to initiate the vehicle, with the LCD display indicating the message "System ignition." Moreover, the activation of the green LED indicates the system's authentication of the driver and authorization of the vehicle's operation.

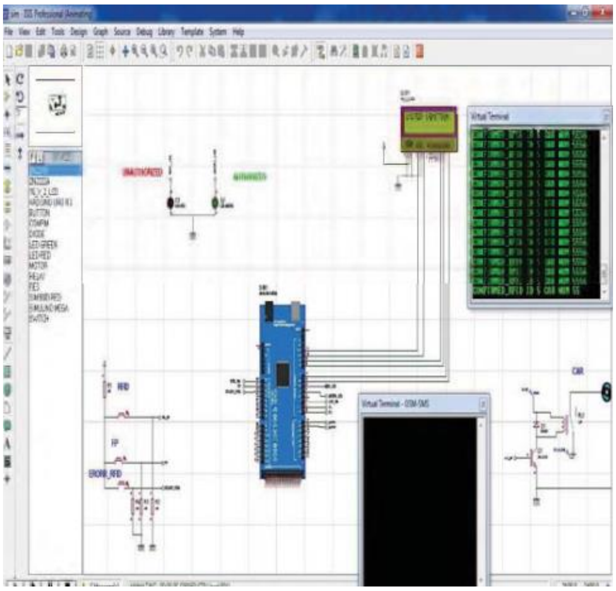


Fig.5. Driver authentication via fingerprint scanner enables vehicle ignition, displayed on LCD as "System ignition" with green LED indicating authorization.

Case 6:

Figure 6 portrays an unauthorized attempt to access the vehicle by an individual who is not the registered owner. Upon the unauthorized person's attempt to use the vehicle with an unauthorized driver’s license card, the security system promptly notifies the owner. It sends an SMS to the pre-registered mobile number and deactivates the ignition system. The SMS includes the alert message "Unauthorized card entered: attempted theft," and concurrently, the red LED is activated to signify the breach in security.

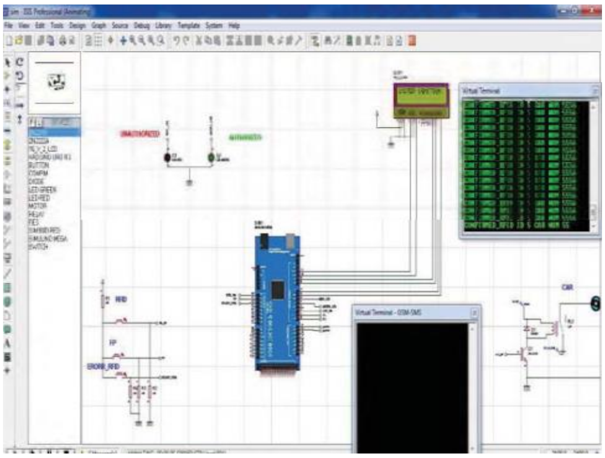


Fig.6.Shows security system response to unauthorized vehicle access: owner SMS alert, ignition disablement, and red LED activation.

Case 7:

In Figure 7, the final image depicts the notification sent to the driver's license holder as a reminder prior to renewal expiration. The text message includes the statement "Your DL validity period expires in 10 days." If the driver's license indeed expires, the vehicle's ignition system is automatically disabled as a security measure.

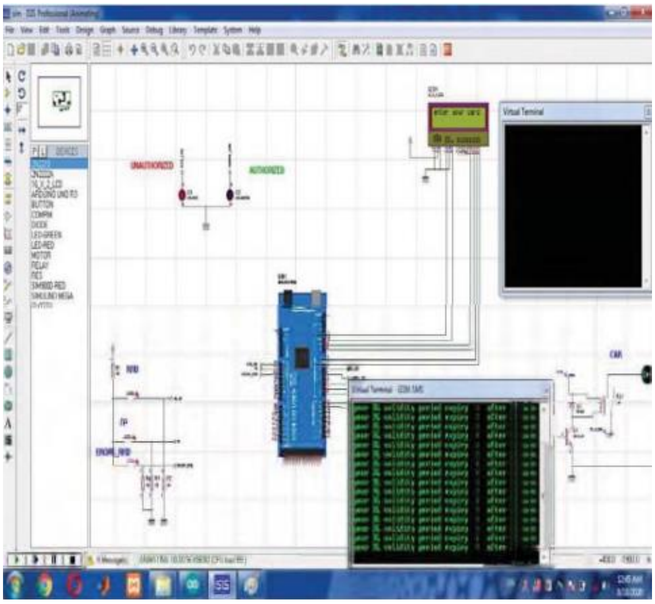
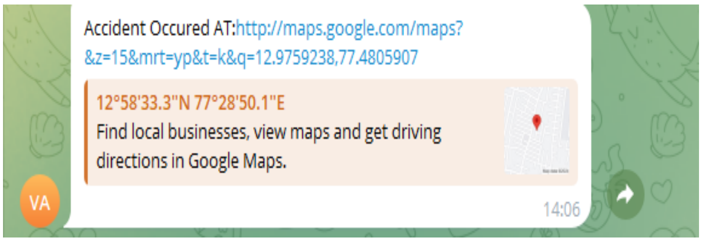


Fig.7.Simulating the sending of an SMS message to remind the holder to renew their driver's license.

Case 8:

Fig.8. Shows when accident occurs then it will sent a live location to the vehicle owner,near hospitals and police station.



Accident Occured AT:http://maps.google.com/maps?&z=15&mrt=yp&t=k&q=12.9759238,77.4805907

12°58'33.3"N 77°28'50.1"E
Find local businesses, view maps and get driving directions in Google Maps.

14:06

Fig.8.Live location

6. CONCLUSIONS

Developing an authenticated access control system for vehicle ignition involves establishing a database to store authorized driver details and enabling owners to register fingerprints and facial features. During ignition, a rigorous authentication process verifies the driver's license and fingerprint, with owners receiving authentication prompts on their mobile phones and granting access via OTP or a dedicated mobile app. Real-time tracking is facilitated by GPS modules, and owners can monitor their vehicles using a specialized app. Collaboration with law enforcement and document validation enhance security measures, with continuous updates ensuring the system's efficacy over time.

REFERENCES

1. Rajatabh Agarwal, Boominathan P," Vehicle Security System Using IoT Application", IRJET, Volume 05, Issue 04, Apr-2018.
2. A. Z. Loko, A. I. Bugaje, Usman Abdullahi," Microcontroller Based Smart Card Car Security System", International Journal of Engineering Trends and Technology, Volume 29, NO 3 November 2015.
3. Priti K Powale, G. N, Zade," Real time car antitheft system with accident detection using AVR microcontroller", international journal of advance research in computer science and management studies, Volume 2, Issue 1, January 2014.
4. Rai, Raj, Dinesh Katole, and Nayan Rai. "Survey Paper on Vehicle Theft Detection Through Face Recognition System." International Journal of Emerging Trends & Technology in Computer Science (IJETICS), vol. 3, no. 1, January - February 2014.
5. Prasad, C. Saikrishna, Sravan Kumar U., and Dr.M.Narsing Yadav M.Tech, PhD (U.S.A). "Advanced Authentication and Security System in Vehicles." IJESMR, January 2016.
6. Upendran Rajendran and Albert Joe Francis,"Anti Theft Control System Design Using Embedded System", Proc. IEEE, Vol. 85, Page no. 239- 242, 2011.
7. Vikram Kulkarni and G. Narsimhulu, "A Low-cost Extended Embedded Smart Car Security System on Face Detection and Continuous Video Monitoring System", Int. Journal of Engineering Science and Advanced Technology (IJESAT), 2012.
8. M.Sunitha, V.Vinay Kumar, and G. Raghu, "Embedded Car Security System", Int. Journal of Engineering Development and Research (IJEDR), 2012.
9. Mohammad A. Al-Khedher and Sharaf A. Al-Kheder, "Intelligent Anti-Theft and Tracking System for Automobiles", Int. Journal of Machine Learning and Computing, 2012.
10. Sukeerti Singh and Ayushi Mhalan, "Vehicle Theft Alert System using GSM", Int. Journal of Engineering Science and Technology (IJEST), 2013.