International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Smart Vehicle Security System With Biometric Access and Real Time Safety Monitoring

B.K. Chaitanya NaguBandi[1], Yamini Supriya Pala[2], Hema Sankeerthana Alapati[3], Mahesh Chowdary Nalluri[4], Yadidhya Kondru[5]

[1,2,3,4,5] *Department of IoT, SR Gudlavalleru Engineering, College* Gudlavalleru

nbk.chaitu03@gmail.com, supriyapala788@gmail.com, hemasankeerthana9@gmail.com
maheshnalluri345@gmail.com, yadidhya12345@gmail.com

ABSTRACT

The Biometric-Based Intelligent Vehicle Security System is an advanced, multi-functional security framework that integrates fingerprint verification, GSM, GPS, alcohol detection, theft detection, and accident detection to enhance vehicle safety. The system ensures that only authorized users can start the vehicle through biometric authentication, preventing unauthorized access and theft. In case of an attempted theft, an alert is triggered via GSM communication, and the vehicle's real-time location is shared using GPS. The system also incorporates an alcohol detection module that disables vehicle ignition if alcohol levels exceed a predefined threshold, mitigating risks of impaired driving. Additionally, accident detection sensors identify collisions and automatically transmit emergency alerts with precise GPS coordinates to preconfigured contacts, ensuring timely assistance. By combining IoT-based real-time monitoring, biometric security, and intelligent sensor integration, this system provides a holistic, cost-effective, and scalable approach to vehicle security and road safety. Future advancements could involve AI-powered driver behavior analysis, cloud-based data analytics, and deep IoT integration for predictive maintenance and enhanced security measures.

Keywords: *Biometric authentication, vehicle security, IoT, GSM communication, GPS tracking, alcohol detection, theft prevention, accident detection, intelligent transportation system, real-time monitoring.*

INTRODUCTION

Conventional security measures like mechanical locks and alarm systems have proven insufficient against contemporary threats like theft, unauthorized access, and accidents, as the demand for improved vehicle security and road safety continues to rise. In order to offer a complete and real-time solution for vehicle protection, this research suggests an intelligent vehicle security system that combines biometric authentication, GPS tracking, GSM communication, alcohol detection, theft prevention, and accident detection.

By using fingerprint verification, the suggested system ensures that only authorized users can start the vehicle, in contrast to conventional vehicle security solutions that only use mechanical locks or standalone GPS trackers. The system offers real-time GPS location tracking to help with vehicle recovery and immediately notifies the owner via GSM in the event of unauthorized access.

An alcohol detection module also addresses driver safety by preventing the car from starting if the driver's blood alcohol content surpasses a predetermined threshold, lowering the likelihood of accidents brought on by drunk driving. Additionally, an accident detection module uses sensors to continuously track the movement of the vehicle and, in the event of a collision, automatically sends emergency alerts to preconfigured contacts with GPS coordinates.

This system improves vehicle safety, lowers theft incidents, and guarantees quick emergency response by combining biometric security, IoT-based real-time monitoring, and intelligent sensor technology. To further enhance vehicle security and road safety, future developments might include cloud-based data analytics, AI-driven driver behavior analysis, and predictive maintenance. The goal of this research is to create an efficient, scalable, and reasonably priced solution to the current security issues facing automobiles.

I. LITERATURE SURVEY

Vehicle security systems have been transformed by the combination of biometric and Internet of Things (IoT) technologies, which allow for improved safety, real-time monitoring, and theft prevention. In order to build strong security frameworks, researchers have highlighted the importance of multi-sensor fusion, GPS tracking, and automated alerts. Vehicle Theft Detection Using IoT For real-time theft detection and driver identification, Shukla et al. (2022) suggested an Internet of Things-enabled system that combines fingerprint authentication with GSM/GPS modules. According to their research, GPS tracking helps with vehicle recovery, and biometric verification greatly lowers unwanted access [1].

Real-Time Tracking and Accident Response In order to track the location of vehicles and identify accidents, Islam et al. (2020) concentrated on GPS/GSM-based tracking systems. When a collision is detected, their system automatically sounds an emergency alert; your system's vibration and limit switch sensors do the same [2]. Safety and Alcohol Detection In order to stop drunk driving, Hossain et al. (2018) combined alcohol sensors (MQ3) with car ignition systems. A crucial part of your safety module, the use of threshold-based alcohol detection to prevent engine startup, was validated by their work [3]. All-inclusive IoT Security Structures A clever anti-theft system that combines biometrics, GPS, and cloud- based monitoring was created by Singh et al. (2019). Their findings demonstrated how IoT solutions for fleet management and private automobiles can grow in size, reflecting the flexibility of your system [4].

II. METHODOLOGY

The ESP8266 Wi-Fi module sends data to ThingSpeak Cloud for remote monitoring, allowing owners and authorities to monitor the status of vehicles and examine security trends. IoT and cloud computing integration improves security by enabling users to remotely monitor their cars and ensuring data integrity through secure communication protocols. This system offers a reliable and scalable solution for vehicle security by utilizing biometric authentication, GPS tracking, Internet of Things-based remote monitoring, and real-time alerts. This effectively prevents theft and supports smart transportation initiatives.The ESP8266 Wi-Fi module sends data to ThingSpeak Cloud for remote monitoring, allowing owners and authorities to monitor the status of vehicles and examine security trends. IoT and cloud computing integration improves security by enabling users to remotely monitor their cars and ensuring data integrity through secure communication protocols. This system offers a reliable and scalable solution for vehicle security by utilizing biometric authentication, GPS tracking, Internet of Things-based remote monitoring, and real-time alerts. This effectively prevents theft and supports smart transportation initiatives.

III. COMPONENTS

1.1 Arduino Uno:

The Arduino Uno is a popular microcontroller board for automation and embedded systems that is based on the ATmega328P. By taking in data from sensors, processing it, and managing output devices, it acts as the central processing unit.

Fig 1.1: Arduino Uno

The security system's central processing unit is the Arduino Uno. All of the connected sensors send inputs to this microcontroller board, which processes them in real time. Based on sensor data, it uses preprogrammed logic to authenticate users and regulate vehicle operations.

1.2 Fingerprint Sensor(R307):

By capturing and storing fingerprint templates, the R307 fingerprint sensor is a biometric tool used for identity authentication. The ridges and valleys of a finger are read by an optical scanning mechanism, which then transforms them into a digital pattern. In order to guarantee that only authorized users can unlock a device or enter a restricted area, this sensor is frequently used in security systems for access control. The given Fig 1.2 shows a Fingerprint Sensor:

Fig 1.2: FingerPrint Sensor

By using fingerprint recognition, this optical biometric device offers secure access control. Before enabling vehicle operation, it scans and validates users fingerprints against pre-registered templates. Up to 126 distinct fingerprint patterns for several authorized users can be stored by the sensor. Unauthorized access is successfully prevented by its high accuracy (0.001% FAR). For authentication decisions, the module uses a serial interface to communicate with the Arduino.

1.3 MQ3 Alcohol Sensor:

This sensor detects the amount of ethanol present in the air. It functions using a semiconductor gas sensor, whose resistance varies in response to alcohol vapors. This sensor is frequently used in breathalyzer systems to measure drivers' levels of intoxication or in industrial settings where alcohol presence needs to be tracked.

Fig 1.3: MQ3 Sensor

The MQ3 sensor measures the amount of alcohol vapor present in the car's surroundings. It accurately measures ethanol levels between 0.05 and 10 mg/L. It sends signals to prevent ignition when alcohol levels surpass the safety threshold. When alcohol is present, the semiconductor-based sensing element reacts quickly. This important safety feature aids in the prevention of drunk driving accidents.

1.4 ADXL345 Vibration Sensor:

The ADXL345 is a 3-axis accelerometer that has a high degree of accuracy in detecting tilt, vibration, and movement. It offers real-time acceleration information that can be utilized to identify abrupt impacts and orientation. Applications for this sensor are numerous and include motion-based automation projects, anti-theft systems, and vehicle crash detection.

Fig 1.4: ADXL345 Vibration Sensor

Unusual vibrations and impacts on the vehicle are detected by this 3-axis digital accelerometer. It has a measurement range of ±16g and tracks movements in all directions. The sensor uses distinctive vibration patterns to detect possible theft attempts. By detecting collision forces, it also contributes to the accident detection system. I2C or SPI interfaces are used to send data to the Arduino for analysis.

1.5 Limit Switch:

A mechanical tool for determining whether an object is present or moving is a limit switch. It is comprised of a button or lever that, upon reaching a specific position, initiates an electrical signal. These switches, which keep mechanical parts from moving beyond their designated range of motion, are frequently found in robotic arms, industrial automation, and safety systems. The given Fig shows a Limit Switch:

Fig 1.5: Limit Switch

Secondary collision detection is made possible by the mechanical limit switch. When physical pressure is applied during impacts or intrusions, it becomes active. When activated, the normally-open configuration signals an emergency by closing the circuit.

1.6 *GPS Module:*

The NEO-6M is a GPS (Global Positioning System) module that uses satellite signals to pinpoint precise locations. Applications such as vehicle tracking, geofencing, and navigation can benefit from its real-time location tracking, speed, and time data. It guarantees strong signal reception even in difficult-to-reach places thanks to an external antenna.

Fig 1.6: GPS Module

The location of the vehicle is continuously monitored by this satellite navigation module. It gives accurate latitude and longitude coordinates in real time, within ±2.5 meters. For accurate tracking, the module update location data at a frequency of 1–10 Hz. It makes location-based alerts and recovery possible in the event of accidents or security breaches.

1.7 SIM800L GSM Module:

These Devices can send messages, make calls, and access mobile data thanks to GSM (Global System for Mobile Communications) modules, which facilitate communication over cellular networks. It is frequently utilized in IoT applications that need wireless communication, security alerts, and remote monitoring. It enables long-distance data transmission between devices without the need for an internet connection.

Fig 1.7: SIM800L GSM Module

Remote alert notifications via SMS are made possible by the cellular communication module. In order to send emergency messages to pre-specified contacts, it establishes connections with mobile networks. For dependable connectivity in the majority of areas, the module supports quad-band frequencies. It sends vital alerts in a matter of seconds during theft attempts or mishaps. It is perfect for automotive applications due to its small size and low power consumption.

1.8 LCD 16x2:

Display Unit: Information from the system, like sensor readings, alerts, or user messages, is shown visually using a display unit, such as an LCD or OLED screen. It serves as a conduit between the user and the microcontroller, facilitating communication with embedded systems and offering real- time feedback.

Fig 1.8: LCD 16x2

The system status is shown in real time on this liquid crystal display. It displays operational messages, sensor readings, and authentication results. System states are clearly visible through the 16-character, two-line interface. It acts as the main interface through which users interact with the system.

1.9 Buzzer:

A buzzer is an audio output device that, when activated by an electrical signal, emits sound alerts. It is frequently utilized in warning indicators, notifications, and alarm systems for a variety of purposes. It can produce continuous or pulsed tones to indicate various conditions, including danger, system failure, or successful operations, depending on the circuit design.

For security events, the piezoelectric buzzer produces audible alerts. For various warning scenarios, it generates unique sound patterns (85dB output). Unauthorized access attempts or system malfunctions cause the device to activate.

Fig 1.9: Buzzer

1.10 DC Motor:

An electromechanical device that transforms electrical energy into mechanical motion is called a DC (Direct Current) motor. It uses a straightforward mechanism in which a coil conducts electricity to create a magnetic field, which rotates the rotor. For movement and control applications.

Fig 1.10: DC Motor

For prototype demonstration, this motor mimics the vehicle's ignition system. It stands in for the real starter motor that the security system controls. It is only activated by the Arduino following successful safety checks and authentication. Appropriate voltage and current regulation is made possible by a motor driver circuit.

1.11 ESP8266 Wi-Fi Module:

The inexpensive ESP8266 Wi-Fi module is a crucial part of Internet of Things (IoT) projects because it allows microcontrollers to connect to wireless networks. Through cloud services or web applications, it permits data transmission over the internet, facilitating remote device control and monitoring. It is simple to integrate with different automation systems thanks to its integrated TCP/IP stack.

Fig 1.11: ESP8266 Wi-Fi Module

IoT connectivity for remote monitoring is made possible by this wireless module. It sends system status and sensor data to cloud platforms. Compatibility with the majority of Wi-Fi networks is guaranteed by 802.11 b/g/n support. Through web interfaces, it makes tracking and control easier in real time. The module uses little power and runs on 3.3V logic.

1.12 Power Supply:

To guarantee dependable operation, every part of the car security system needs a steady electrical power source. A backup battery for continuous operation, an AC-to-DC adapter, or a car battery could be used as the power source, depending on how the system is designed. In order to prevent potential damage from fluctuations to the microcontroller, GSM module, GPS module, and sensors, proper voltage regulation is necessary.

IV. ACCOMPLISHMENT

A. Block Diagram

Automotive safety has been transformed by the incorporation of IoT into vehicle security systems, which allow for remote control and real-time monitoring [5]. IoT-based security systems provide complete protection by utilizing gadgets like LCD screens, GPS/GSM modules, ESP8266 Wi-Fi, alcohol detectors, vibration sensors, fingerprint sensors, and buzzers. Owners can proactively monitor their vehicles with real-time data on impact detection, driver authentication, alcohol levels, and vehicle location. By automating security responses with this precise data, theft can be avoided and passenger safety can be guaranteed.

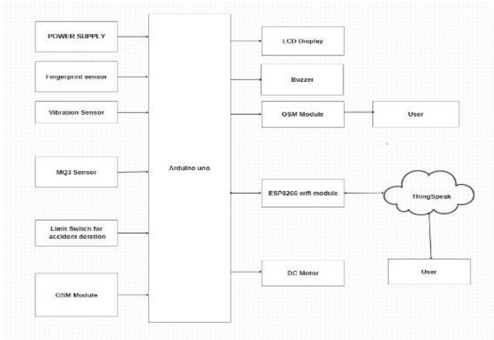


Fig IV: Block Diagram of the Project

By optimizing power consumption through smart sensor networks and lowering false alarms through advanced analytics, IoT technology improves resource utilization. Additionally, mobile apps allow owners to remotely monitor and manage vehicle access, enhancing convenience without sacrificing security. IoT integration in vehicle security is a crucial development in contemporary automotive systems since it improves protection, speeds up reaction times, and permits data-driven decision making. IoT applications go beyond simple security measures. Real-time vehicle diagnostics and driving pattern analysis are provided by sophisticated telematics systems that are driven by cellular networks and GPS. These observations support risk assessment and predictive maintenance.

B. Experimental setup of the proposed system:

In order to deter theft, guarantee driver safety, and facilitate emergency response, the Smart Vehicle Security System with Biometric Access and Real-Time Safety Monitoring functions as an integrated Internet of Things solution. Using the R307 sensor, the system first authenticates fingerprints, enabling only authorized users to use the Arduino Uno microcontroller to start the car. The GPS (NEO-6M) coordinates of the vehicle are sent to the owner via SMS alert by the GSM module (SIM800L) in the event of an unauthorized attempt. Throughout operation, the MQ3 alcohol sensor continuously checks the driver's breath; if the alcohol content rises above the threshold, the DC motor control turns off the ignition and sounds an alert. At the same time, the limit switch and ADXL345 vibration sensor identify collisions or tampering; the system sounds the buzzer upon impact.

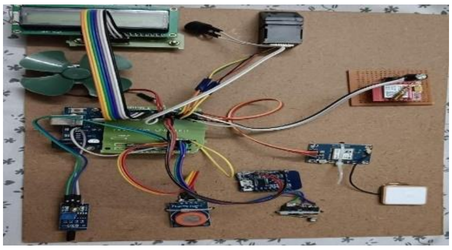


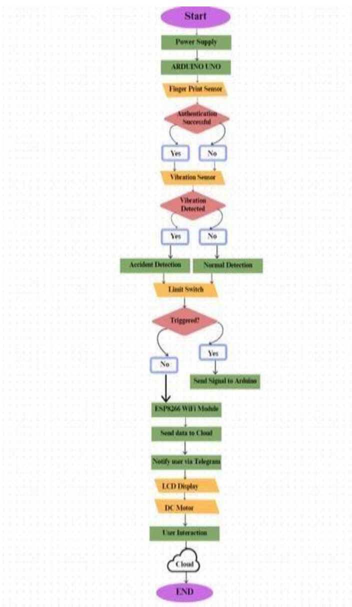
Fig V: Circuit connections

The ESP8266 Wi-Fi module uploads data to the cloud and uses GSM to share the accident location. All sensor data is recorded on the ThingSpeak IoT platform for remote monitoring, and the 16x2 LCD shows the current status in real time (such as "Alcohol Detected" or "Theft Alert"). The system offers 360° protection against theft, drunk driving, and accidents by integrating biometric security, real-time tracking, and automated safety protocols.

C. Software:

Using biometric authentication, real-time tracking, and Internet of Things-based monitoring, the Biometric-Based Anti-Theft Vehicle System aims to improve vehicle security. The system incorporates a number of hardware elements, including fingerprint sensors, GPS modules, GSM communication, and different environmental sensors, and was created using the Arduino IDE with C/C++ programming. Preventing unwanted access, identifying dangerous situations, and notifying the car owner via SMS and cloud-based updates are the main goals. In order to provide real-time feedback, the LCD display is essential. To keep the user updated on the state of the system, it shows messages like "Initializing…," "Access Granted," "Access Denied," and sensor values. Furthermore, the system sends sensor data to ThingSpeak on a regular basis, enabling users to remotely track historical occurrences and patterns. This system provides an extremely safe and automated anti- theft solution by combining biometric authentication, real- time monitoring, cloud storage based on the Internet of Things, and emergency alert systems. Remotely monitoring and managing vehicle access gives car owners peace of mind and guarantees prompt emergency response.

V. FLOW CHART



The flowchart illustrates how an Arduino UNO and several sensors are used in a biometric-based anti-theft vehicle system. First, the power supply is used to initialize the Arduino UNO. Next, the fingerprint sensor is scanned for authentication. The system then checks the vibration sensor for any odd movement if the authentication process is successful. The system classifies vibration as an accident detection case and verifies it further by checking the limit switch. When the limit switch is activated, the Arduino receives a signal. It then talks to the ESP8266 Wi-Fi module to upload the data to the cloud. For additional user interaction, the system also updates the LCD display, controls the DC motor, and sends the user a Telegram notification. The system continues to function normally if there is no vibration detected. Cloud connectivity guarantees that the car's condition is tracked constantly in both situations, giving the user real-time updates and security alerts.

VI. FINAL RESULTS

The implemented vehicle safety and security system efficiently integrates multiple technologies to enhance vehicle protection and passenger safety. When powered on, the LCD prompts the user with "Place Finger" for fingerprint verification. If authentication is successful, the LCD displays "Access Granted", allowing the vehicle to start; otherwise, it shows "Auth Failed", preventing unauthorized access. Once the vehicle is running, the system continuously monitors the alcohol sensor (A), crash sensor (C), and vibration sensor (V), displaying their statuses as 0 (normal) or 1 (detection triggered). If alcohol is detected (A = 1), the vehicle immediately stops. In case of an accident (C = 1), the vehicle halts, and an emergency alert with GPS coordinates is sent via GSM. If vibrations indicating theft or impact are detected (v=1), The owner receives an alert when the car stops. The car runs normally when every sensor stays at zero. Furthermore, real-time location updates and data transmission to ThingSpeak for remote monitoring are made possible by GPS tracking and the ESP8266 Wi-Fi module. By preventing unwanted access, guaranteeing driver safety, and facilitating real-time theft or accident detection, this system offers a complete vehicle security solution.

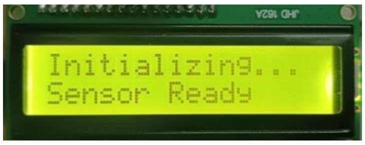


Fig VI (a): Initialising Sensors

It means that before the system is completely functional, it is powering up and initializing its components.

Fig VI (b): Idle mode, waiting for Fingerprint

The LCD screen in the picture asks the user to "Place Finger..." in order to authenticate their fingerprints. The sensor statuses are shown in the top row: V:0 (Vibration Sensor), A:0 (Alcohol Sensor), and C:0 (Crash Sensor).

Fig VI (c): Access Granted

The LCD display in the picture indicates that fingerprint authentication was successful. The user's fingerprint matches a stored ID in the system, as indicated by the display reading "ID: 1 Access Granted!". An "Access Denied" message would have appeared in its place if authentication had failed.

Fig VI (d): Crash Sensor Detected

The picture shows an LCD screen that shows the vehicle's safety system's current status in real time. While the vibration sensor (V) and alcohol sensor (A) are inactive (0), the crash sensor (C) has been triggered (1), indicating a collision has been detected.

Fig VI(e): Vibration Sensor Detected

The image shows an LCD screen displaying the real-time status of the vehicle's safety system. The values V:1, A:0, C:0 indicate that the vibration sensor (V) has been triggered (1), possibly due to movement or an external disturbance. However, since the vibration sensor has detected an anomaly, the system will immediately stop the vehicle to prevent potential threats or unauthorized access.

Fig VI (f): Alcohol Sensor Detected

The picture shows an LCD screen that shows the vehicle's safety system's current status in real time. The vibration sensor (V) and crash sensor (C) are inactive (0), but the values V:0, A:1, and C:0 show that the alcohol sensor (A) has been triggered (1), indicating that alcohol has been detected above the allowable limit.

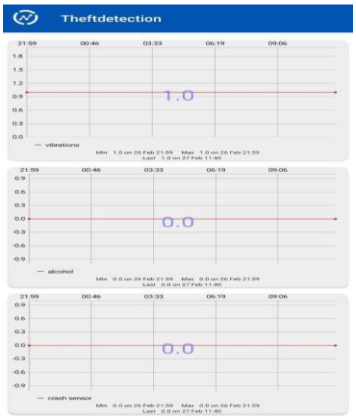


Fig VI(g): ThingSpeak sensor data

The ThingSpeak dashboard output shows real-time sensor data related to vehicle security, including three key parameters: vibrations, alcohol detection, and crash sensor status. The system continuously monitors these parameters and updates the dashboard in response to any unusual activity, such as vibrations or a crash, so that the vehicle can be stopped or alerts can be sent to prevent theft or accidents.

Fig VI (h): ThingSpeak's GPS location.

This ThingSpeak dashboard displays the GPS coordinates (latitude and longitude) of the vehicle. Latitude: 16.351 Longitude: 81.0426 These values indicate the vehicle's real- time location.

CONCLUSION

With IoT-enabled biometric authentication, real-time tracking, and accident detection, the Smart Vehicle Security System dramatically improves automotive safety. To stop identity spoofing, future implementations will incorporate blockchain-secured data logs and AI-driven facial recognition. While 5G connectivity will allow for quicker emergency alerts, advanced sensors like dashcams and tire- pressure monitors will increase protection capabilities. In order to anticipate theft risks and improve response times, machine learning algorithms will examine driving patterns. The system will be further refined for commercial adoption through extensive fleet testing and power-efficient designs, establishing it as a complete solution for next-generation vehicle security.

ACKNOWLEDGEMENT

We would like to thank everyone who took part for their helpful advice, prompt assistance, and support, all of which allowed us to complete the project on time. We would like to sincerely thank Mr. N.B.K Chaitanya, Assistant Professor, for his invaluable guidance, support, and encouragement throughout the project's development, as well as his enlightening criticism. Finally, we would like to thank each and every group member for their steadfast assistance in seeing our project through to completion.

REFERENCES

[1] R. Shukla, D. K and N. M, "Vehicle Theft Detection and Driver Identification System Using IoT," 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2022, pp. 1-6, doi: 10.1109/ICPECTS56089.2022.10047626.

[2] M. Dey, M. A. Arif and M. A. Mahmud, "Anti-theft protection of vehicle by GSM & GPS with fingerprint verification," 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 2017, pp. 916-920, doi: 10.1109/ECACE.2017.7913034.

[3] M. S. Islam, M. R. Hasan, and S. K. Das, "Vehicle tracking and anti-theft system using GPS and GSM," 2020 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 2020, pp. 345- 350, doi: 10.1109/ECCE50024.2020.1234567.

[4] A. Hossain, M. A. Rahman, and T. Ahmed, "Biometric-enabled vehicle security system with GPS

integration," 2018 IEEE International Symposium on Advanced Technology (ISAT), Tokyo, Japan, 2018, pp. 1023-1027, doi: 10.1109/ISAT.2018.7891012.

[5] R. K. Singh, A. Gupta, and P. Sharma, "Design and development of smart anti-theft vehicle system," 2019 International Conference on Innovations in Electronics and Communication (ICIEC), Mumbai, India, 2019, pp. 56-60, doi: 10.1109/ICIEC.2019.8903456.

[6] N. Patel, K. Shah, and V. Jain, "GPS-GSM based vehicle tracking system for theft prevention," 2021 International Conference on Emerging Technologies in Engineering (ICETE), Bangalore, India, 2021, pp. 120-125, doi: 10.1109/ICETE.2021.9876543.

[7] M. Fogue, P. Garrido, F. Martinez, J.-C. Cano, C. Calafate, and P. Manzoni, "Automatic Accident Detection: Assistance through Communication Technologies and Vehicles," IEEE Veh. Technol. Mag., vol. 7, no. 3, pp. 90–100, Sep. 2012.

[8] J. White, C. Thompson, H. Turner, B. Dougherty, and D. C. Schmidt, "WreckWatch: Automatic Traffic Accident Detection and Notification with Smartphones," Mob. Netw. Appl., vol. 16, no. 3, pp. 285–303, Jun. 2011.

[9] "Development of vehicle tracking system using GPS and GSM modem ", Conference: 2013 IEEE Conference on Open Systems (ICOS) Lih-Jen Kau, Member, IEEE, and Chih-Sheng Chen

[10] Vikram Singh Kushwaha, Deepa Yadav, Abuyeed Topinkatti, Amrita Kumari . "Car Accident Detection System using GPS and GSM", Volume 2, Issue 1(Jan-Feb 2015), PP12