VEHICLE THEFT CONTROL AND ACCIDENT LOCATION INTIMATION THROUGH SMS

[1] Dr. M. Senthil Kumar, [2] Putta Anjali, [3] E Pranaya, [4] Gogga Manjunath, [5] R Koushik
[1] Principal, [2345] B. Tech Students
[12345]Department of Electronics and Communication Engineering
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The Vehicle Theft Control and Accident Location Intimation System is a smart embedded solution designed to enhance vehicle security and provide real-time accident alerts to owners and authorities. Vehicle theft and road accidents are major challenges affecting safety, property, and lives. Traditional vehicle security systems rely on mechanical locks or alarm systems, which are often ineffective and cannot notify owners remotely. Similarly, accident detection usually depends on manual reporting or GPS-based tracking without instant alerts. This system integrates IoT-enabled sensors, GPS/GSM modules, and microcontrollers to provide automated theft prevention and accident location intimation. Accelerometers and vibration sensors detect unauthorized movement, tampering, or collisions. In case of suspected theft or accidents, the system automatically sends SMS alerts with the vehicle's current GPS location to the registered owner or emergency contacts. Embedded controllers like Arduino or ESP32 process sensor inputs, control security modules, and communicate with GSM networks for messaging. Real-time tracking ensures that vehicles can be located quickly, improving the chances of recovery or timely emergency response. The system supports geofencing, enabling notifications if the vehicle leaves predefined boundaries. Power-efficient design ensures long operational life, and backup batteries maintain functionality in case of main power failure. Modular design allows integration with immobilizers, engine cut-off mechanisms, and additional sensors for enhanced security. Data collected can be stored for historical analysis of vehicle usage, accident patterns, and theft attempts. Security measures such as encrypted communication and authentication prevent unauthorized access. Overall, the system improves vehicle safety, reduces theft risk, ensures quick accident response, and enhances owner peace of mind through real-time monitoring and automated SMS notifications.

I. INTRODUCTION

1.1 Overview

Vehicle theft and road accidents are two major global concerns that significantly affect personal safety, property security, and economic stability. The rapid growth in the number of vehicles worldwide has increased the risks associated with unauthorized vehicle access, theft, and road traffic accidents. Despite advancements in automotive engineering and road safety regulations, incidents of vehicle theft and delayed emergency response during accidents remain common challenges. These issues highlight the need for intelligent and automated monitoring systems capable of enhancing vehicle security and providing real-time emergency alerts.

Traditional vehicle security systems primarily rely on mechanical locks, steering locks, or alarm systems. While these mechanisms provide basic protection, they are often insufficient against organized theft attempts. Moreover, most conventional alarm systems only produce local sound alerts and fail to notify the vehicle owner remotely. Similarly, accident reporting usually depends on manual communication by witnesses or victims, which may lead to delays in emergency response, especially in remote or isolated areas.

With the advancement of embedded systems, wireless communication technologies, and Internet of Things (IoT) platforms, it has become feasible to design intelligent vehicle monitoring systems capable of real-time detection and instant alert transmission. The proposed **Vehicle Theft Control and Accident Location Intimation through SMS** system integrates sensors, GPS modules, GSM communication, and microcontrollers to provide automated theft detection and accident notification services. The system enhances vehicle safety by combining real-time tracking, tamper detection, geofencing, and SMS-based alerts into a single embedded platform.

1.2 Background of the Study

Over the past few decades, automotive security systems have evolved from simple mechanical locks to electronic immobilizers and remote keyless entry systems. While modern vehicles incorporate advanced security features, theft techniques have also become more sophisticated. Criminals exploit vulnerabilities in electronic systems, bypass alarms, or disconnect power supplies to disable security mechanisms. This has created a continuous need for more intelligent and responsive vehicle protection solutions.

In parallel, road accidents remain a leading cause of injury and death worldwide. According to global transportation safety studies, a significant number of accident fatalities occur due to delayed medical assistance. In many cases, accident victims are unable to contact emergency services immediately, especially if the accident occurs in isolated locations. Automatic accident detection and location reporting systems can play a crucial role in reducing response time and saving lives.

The development of embedded systems and GSM/GPS modules has enabled real-time location tracking and remote communication. Microcontrollers such as Arduino and ESP32 can interface with sensors and communication modules to create compact and cost-effective monitoring systems. SMS-based alert systems are particularly effective because they operate on GSM networks, which are widely available even in rural areas.

The integration of these technologies forms the foundation of the proposed system, which aims to provide enhanced vehicle security and immediate accident location notification.

1.3 Need for the Project

The need for an integrated vehicle theft control and accident location intimation system arises from several practical concerns.

Firstly, vehicle theft rates remain high in many urban and rural regions. Stolen vehicles often take days to trace, and recovery rates are low due to lack of real-time tracking. A system that provides immediate location updates and alerts can significantly increase recovery chances.

Secondly, conventional alarm systems are ineffective if the vehicle owner is not nearby. Audible alarms may go unnoticed, especially in crowded or noisy environments. Remote notification through SMS ensures that the owner is informed instantly, regardless of location.

Thirdly, road accidents frequently occur in areas where immediate medical assistance is unavailable. Automatic accident detection using accelerometers or vibration sensors can trigger instant alerts with precise GPS coordinates, enabling faster emergency response.

Fourthly, many existing tracking systems rely solely on GPS monitoring without automatic alert mechanisms. Continuous tracking without intelligent event detection may not effectively address theft or accident scenarios.

Fifthly, advancements in IoT and embedded technology provide an opportunity to design low-cost, scalable, and energy-efficient monitoring systems suitable for both personal and commercial vehicles.

Therefore, the development of an automated system capable of detecting theft attempts, monitoring vehicle movement, and sending accident location alerts through SMS is essential to enhance vehicle safety and owner peace of mind.

1.4 Problem Statement

Despite the availability of modern vehicle security technologies, significant challenges persist in theft prevention and accident response systems. Traditional mechanical locks and alarm systems provide limited protection and lack remote notification capabilities. Many vehicle tracking systems only provide location information but do not automatically detect unauthorized movement or collisions.

The major problems identified are:

- Inability of conventional alarm systems to notify owners remotely
- Delayed accident reporting leading to slow emergency response
- Lack of automated detection of theft attempts or tampering
- Absence of geofencing capabilities in basic tracking systems
- Vulnerability of electronic systems to power disconnection
- Limited integration of accident detection and theft control in a single platform

These issues indicate the necessity for a comprehensive embedded system that integrates sensor-based detection, GPS tracking, GSM communication, and automated SMS alerts to provide real-time monitoring and security.

1.5 Objectives of the Project

The primary objective of this project is to design and implement a smart embedded system capable of controlling vehicle theft and providing accident location intimation through SMS.

The specific objectives are:

- To design an embedded system using microcontrollers such as Arduino or ESP32.
- To integrate GPS modules for real-time vehicle location tracking.
- To integrate GSM modules for SMS-based alert transmission.
- To implement accelerometer and vibration sensors for accident and tamper detection.
- To develop a geofencing mechanism that alerts owners when vehicles move beyond predefined boundaries.
- To design a power-efficient system with backup battery support.
- To ensure secure communication using authentication and encrypted messaging.
- To provide modular expansion capability for features like engine immobilization.

These objectives aim to enhance vehicle security, reduce theft risk, and ensure rapid accident response.

1.6 Scope of the Project

The scope of the Vehicle Theft Control and Accident Location Intimation System includes the design, development, and testing of a prototype capable of detecting unauthorized vehicle movement and accidents while sending SMS alerts with GPS coordinates.

The system covers:

- Real-time GPS tracking
- Theft detection using vibration sensors
- Accident detection using accelerometers
- SMS alert transmission via GSM
- Geofencing alerts
- Backup power management

The project is limited to prototype-level implementation and SMS-based communication. Advanced features such as cloud-based tracking dashboards, mobile app integration, and video surveillance integration are considered outside the current scope but may be included in future enhancements.

The system is designed for both two-wheelers and four-wheelers and can be expanded for fleet management applications.

II. LITERATURE SURVEY

Vehicle Security and Theft Prevention Systems

Traditional anti-theft systems include mechanical locks, alarms, and immobilizers. Studies highlight limitations such as false alarms, manual intervention, and lack of real-time notification. IoT-based solutions integrate vibration sensors, accelerometers, and GPS tracking to detect unauthorized movement and location. Research shows that SMS or mobile notifications significantly improve owner response time and reduce theft recovery duration.

Accident Detection Technologies

Accident detection uses accelerometers, gyroscopes, and vibration sensors to identify collisions or abrupt vehicle movement. Existing systems rely on GPS alone, often delaying emergency notifications. Studies confirm that combining motion sensors with GPS modules improves accuracy and timely alert generation. Integration with mobile or cloud applications enables authorities and family members to respond quickly, reducing accident fatalities and property damage.

GSM and GPS-Based Vehicle Tracking

GSM and GPS modules are widely used in embedded vehicle security projects. GPS provides precise location tracking, while GSM enables real-time communication through SMS or data networks. Research emphasizes that combining GPS for location and GSM for messaging ensures reliable theft alerts and accident notifications. Cloud dashboards can also provide live vehicle tracking and historical route logs. Security and data integrity are maintained using encryption, authentication, and secure communication protocols.

2.2 Traditional Vehicle Security Systems

Early and widely-deployed vehicle security measures rely on mechanical locks, immobilizers, steering-wheel locks, and simple audio alarms. Mechanical solutions deter opportunistic theft but offer no remote notification or location tracking. Electronic immobilizers and transponder-based keys significantly reduced theft by preventing engine start without the authorized key; however, these systems are mostly reactive and local — they alert only at the vehicle and do not provide real-time location or owner notification. Several studies and industry reports note that while immobilizers reduced certain theft vectors, determined thieves can still bypass electronic systems using relay attacks, key cloning, or physical tampering. The literature therefore recognizes the need for layered solutions that combine tamper detection with remote alerting and tracking.

2.3 GPS/GSM-Based Tracking and Alert Systems

Global Positioning System (GPS) combined with Global System for Mobile communications (GSM) is the predominant technology for remote vehicle tracking and alerting. Numerous commercial products and academic prototypes use a GPS receiver to obtain latitude/longitude coordinates and a GSM modem to transmit those coordinates via SMS, GPRS, or MQTT to owners or servers. SMS-based systems are popular because SMS coverage is available in most regions and requires no data plan for basic location alerts.

Research emphasizes robustness of GPS/GSM architectures for theft recovery: real-time SMS alerts with coordinates enable quick response and law enforcement involvement. However, limitations include GPS signal loss in tunnels/garages and vulnerability to power cut (thieves disconnecting battery/GSM power). To address power-cut vulnerabilities, literature suggests backup batteries and anti-tamper power isolation circuits. Studies also explore hybrid communication (GSM + LoRa or NB-IoT) for broader coverage and lower power consumption for fleet management use-cases.

2.4 Accident Detection Using Inertial Sensors

Accident detection is typically addressed using inertial measurement units (IMUs) that include accelerometers and gyroscopes. A significant body of work investigates algorithms to distinguish normal driving vibrations from collision events. Threshold-based methods (detecting sudden high-magnitude acceleration/deceleration) are simple and widely used in commercial "eCall" and aftermarket devices. More advanced approaches apply signal processing and pattern recognition (machine learning classifiers) to reduce false positives from potholes or hard braking.

Literature highlights trade-offs: low-complexity thresholding gives fast detection but yields false alarms, while model-based classifiers require training and more compute but achieve higher precision. Many studies recommend a multi-sensor approach — combining accelerometer data with other inputs (vibration sensors, open-door/impact sensors, vehicle CAN-bus signals like airbag deployment) — to improve reliability. In the context of SMS-based intimation, reliable detection with low latency is critical because delayed or false notifications impede emergency response or erode trust.

2.5 SMS Notification and Emergency Alerting Mechanisms

SMS remains an effective channel for short, urgent notifications in many regions due to ubiquitous GSM coverage and simplicity. Academic and industrial implementations use GSM modems (SIM800/900 series, Quectel modules) controlled by microcontrollers to send preformatted SMS containing GPS coordinates and a brief message. Best practices in the literature include: (1) including both coordinates and a concise Google Maps link, (2) sending SMS sequence to multiple contacts, (3) fall-back messaging when primary channel fails (e.g., send SMS then attempt packet-based upload), and (4) acknowledgement handling (confirm receipt from owner or emergency services).

Studies of emergency systems also highlight integration with institutional responders (police, ambulance) and automated escalation logic (retry attempts, alternative numbers). Privacy and data protection are discussed; only essential information should be sent in plain SMS, and sensitive historical logs can be uploaded via secure channels.

III. SYSTEM ANALYSIS

3.1 Introduction

System analysis is an essential phase in the development of the Vehicle Theft Control and Accident Location Intimation through SMS system, as it helps in understanding the shortcomings of existing vehicle security mechanisms and defining a technically feasible, reliable, and scalable solution. With the rapid increase in vehicle ownership worldwide, the problems of vehicle theft and delayed emergency response in accidents have become serious concerns. Traditional vehicle protection systems provide limited security and lack intelligent automation. Therefore, a detailed analysis of current systems and their drawbacks is necessary before proposing an improved embedded solution.

This chapter discusses the existing systems and their disadvantages, presents the proposed system and its advantages, and describes the detailed system requirements needed for successful implementation.

3.2 Existing System

The existing vehicle monitoring and security systems can broadly be classified into mechanical security systems, electronic alarm systems, and GPS-based tracking systems. Each of these systems addresses certain aspects of vehicle protection but fails to provide a complete and integrated solution.

Mechanical security systems such as steering locks, wheel clamps, gear locks, and ignition locks are widely used to prevent unauthorized access. These systems act as physical barriers, making it difficult for thieves to operate the vehicle. However, they provide no intelligence or remote communication capability. If a vehicle is stolen despite mechanical protection, the owner has no means of tracking or recovering it unless external surveillance is available.

Electronic alarm systems were introduced as an improvement over mechanical locks. These systems detect unauthorized door opening or ignition tampering and trigger a siren or flashing lights. While this approach deters theft attempts in some cases, it remains limited to local alerts. If the vehicle is parked in an isolated area or a noisy environment, the alarm may go unnoticed. Furthermore, these systems do not provide real-time information to the owner regarding the vehicle's location.

GPS-based tracking systems represent a more advanced solution. These systems continuously track vehicle location and transmit data to a central server or mobile application. Although they allow vehicle tracking, many basic tracking systems lack automated event detection. They do not always distinguish between normal movement and unauthorized theft. Additionally, many systems depend on continuous internet connectivity and may not send instant SMS alerts when suspicious activity occurs.

In terms of accident reporting, most vehicles rely on manual reporting by drivers or bystanders. In severe accidents where the driver is unconscious or trapped, emergency services may not be informed in time. Some high-end vehicles include automatic emergency call systems, but such features are not widely available in low-cost vehicles.

Thus, while existing systems provide partial solutions, they do not integrate theft detection, accident detection, and automatic SMS-based location notification into a single embedded platform.

3.3 Disadvantages of Existing Systems

The major disadvantage of mechanical and alarm-based systems is the lack of remote communication. These systems operate locally and do not inform the vehicle owner in real time. If a theft attempt occurs when the owner is away, the delay in response reduces the chances of recovery.

Another significant drawback is the absence of automatic accident detection. Many accident victims fail to receive timely medical assistance due to delays in reporting. Traditional systems depend entirely on human intervention, which may not always be possible.

Existing GPS trackers, although useful for location monitoring, often do not detect suspicious movement patterns or tampering. Continuous tracking without intelligent analysis can result in unnecessary data collection without meaningful alerts.

Power vulnerability is another issue. Thieves often disconnect the vehicle battery to disable tracking devices. Many basic tracking systems stop functioning once the main power supply is removed.

Geofencing features are not commonly available in low-cost systems. Without predefined boundaries, vehicle movement outside safe zones may go undetected.

Security vulnerabilities also exist in some GSM-based systems that transmit data without encryption. Unauthorized access to tracking systems may compromise privacy and security.

Additionally, advanced commercial systems are expensive and not affordable for average vehicle owners. Therefore, there is a need for a cost-effective, integrated, and intelligent solution.

3.4 Proposed System

The proposed Vehicle Theft Control and Accident Location Intimation through SMS system is designed to overcome the limitations of existing systems by integrating theft detection, accident detection, GPS tracking, GSM communication, and geofencing within a single embedded platform.

The system uses a microcontroller such as Arduino or ESP32 as the central processing unit. It continuously monitors input from vibration sensors and accelerometers. The vibration sensor detects unauthorized tampering, sudden forced movement, or unusual disturbances when the vehicle is parked. The accelerometer measures acceleration forces in multiple directions and detects high-impact collisions that may indicate an accident.

When suspicious movement is detected or impact exceeds a predefined threshold, the microcontroller activates the GSM module. Simultaneously, the GPS module retrieves the current latitude and longitude coordinates of the vehicle. An SMS message containing the vehicle’s location and alert type is automatically sent to registered mobile numbers.

The system also includes a geofencing feature, allowing the owner to define a safe geographic area. If the vehicle moves beyond this boundary, the system sends an immediate alert.

A backup battery ensures that the system remains operational even if the vehicle’s main power supply is disconnected. This enhances reliability and makes it difficult for thieves to disable the device.

The proposed system integrates multiple technologies to provide a comprehensive security and safety solution.

3.5 Advantages of Proposed System

The proposed system provides significant improvements over existing solutions. One major advantage is real-time SMS alert capability. The owner receives immediate notification during theft attempts or accidents, enabling quick action.

Another key advantage is the integration of theft detection and accident detection in a single device. This dual functionality improves overall vehicle safety.

The GPS-based location tracking ensures accurate identification of the vehicle's position. Including a Google Maps link in the SMS allows easy navigation to the location.

Geofencing capability adds an additional security layer by notifying the owner when the vehicle exits predefined zones.

The inclusion of backup power enhances system reliability and prevents device shutdown during battery disconnection.

The system is cost-effective, as it uses affordable embedded components. It is suitable for both two-wheelers and four-wheelers.

Modular design allows future upgrades such as engine immobilization, cloud tracking dashboards, and mobile app integration.

The system reduces emergency response time during accidents and increases chances of vehicle recovery in theft cases.

IV. HARDWARE CONTROLLER

Arduino Uno

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode.Arduino board has the following new features:

•1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes.

- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

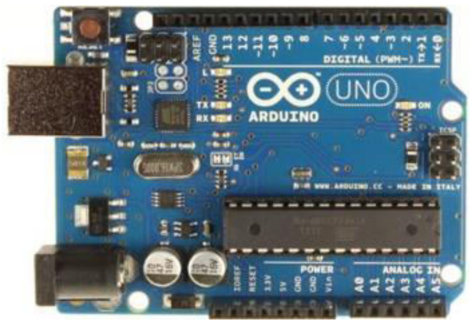


Fig: ARDUINO UNO

Motion / Vibration Sensors

Motion sensors are very similar in design to tilt switches; in fact, some tilt switches are used as motion sensors. The sensor will be in one condition (open or closed) at rest. When it is subjected to motion it will continually change state as long as it remains in motion. Some common applications include: anti-theft devices, man-down alarms to detect non motion, smart appliances to turn off power when not in use and portable equipment to do the same.

THEFT BUTTON

Detailed Explanation and Diagram

The **Theft Button** is an important manual security feature in the Vehicle Theft Control and Accident Location Intimation through SMS system. While automatic theft detection relies on vibration sensors and movement monitoring, the theft button provides the vehicle owner with direct control to activate or deactivate theft protection mode. It acts as a manual trigger that enhances security and prevents false alarms.

1. Purpose of the Theft Button

The theft button is used to manually enable or disable the anti-theft monitoring system. When the vehicle is parked, the owner presses the theft button to activate security mode. Once activated, the system continuously monitors vibration sensors, ignition status, and movement. If unauthorized movement is detected, the system immediately sends an SMS alert with GPS coordinates to the registered mobile number.

If the owner returns and wants to use the vehicle, pressing the theft button again deactivates monitoring mode, preventing unnecessary alerts during normal driving.

Thus, the theft button provides manual control over the theft detection mechanism.

GSM

The **Global System for Mobile Communications** (**GSM**) is a standard developed by the European Telecommunications Standards Institute(ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets. It was first deployed in Finland in December 1991.[2]By the mid-2010s, it became a global standard for mobile communications achieving over 90% market share, and operating in over 193 countries and territories.[3]

2G networks developed as a replacement for first generation (1G) analog cellular networks. The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via General Packet Radio Service (GPRS), and Enhanced Data Rates for GSM Evolution(EDGE).

Subsequently, the 3GPP developed third-generation (3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard.

"GSM" is a trade mark owned by the GSM Association. It may also refer to the (initially) most common voice codec used, Full Rate.

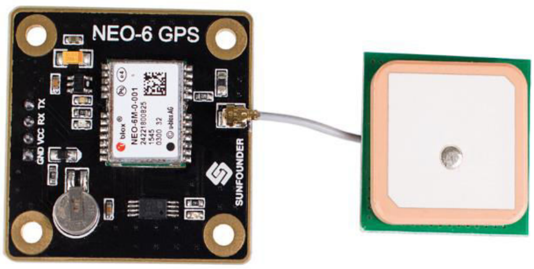


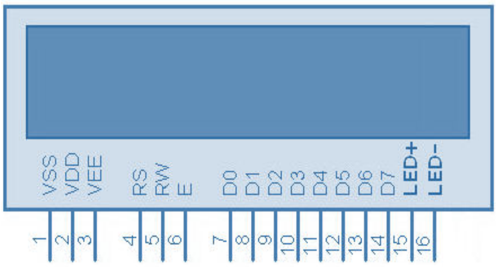
Fig: GPS MODEM

Alphanumeric LCD

Liquid Crystal Display also called as LCD is very helpful in providing user interface as well as for debugging purpose. The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. The most commonly used LCDs found in the market today are 1 Line, 2 Line or 4 Line

LCDs which have only 1 controller and support at most of 80 characters, whereas LCDs supporting more than 80 characters make use of 2 HD44780 controllers.

Pin Description



BUZZER

What is a Buzzer: Working & Its Applications

There are many ways to communicate between the user and a product. One of the best ways is audio communication using a buzzer IC. So during the design process, understanding some technologies with configurations is very helpful. So, this article discusses an overview of an audio signaling device like a beeper or a buzzer and its working with applications.

What is a Buzzer?

An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on the various designs, it can generate different sounds like alarm, music, bell & siren.

V. METHODOLOGY & IMPLEMENTATIONS

5.1 Introduction

This chapter describes the methodology adopted for the design and implementation of the **Vehicle Theft Control and Accident Location Intimation through SMS** system. The system integrates embedded hardware, sensor-based detection, GPS location tracking, GSM-based communication, and alert messaging to provide a comprehensive vehicle security and safety solution. The methodology explains the systematic development approach followed from requirement analysis to hardware integration, software development, communication setup, and system testing.

The implementation combines microcontroller-based control logic with real-time event detection and SMS alert transmission, ensuring reliable operation under automotive conditions.

5.2 Overall Methodology

The system development follows a structured engineering approach consisting of the following phases:

1. Requirement Analysis
2. Component Selection
3. Hardware Design and Integration
4. Firmware Development
5. Sensor Calibration and Threshold Setting
6. GPS and GSM Communication Configuration
7. Alert Message Programming
8. Testing and Validation

Each phase ensures that the system operates accurately, efficiently, and reliably.

5.3 Hardware Implementation

5.3.1 Microcontroller Unit

The microcontroller (Arduino UNO or ESP32) acts as the central processing unit of the system. It continuously monitors inputs from sensors, processes data, and controls communication modules. The controller executes the main program loop, which checks for theft conditions and accident events.

The ESP32 is preferred for advanced implementations due to its higher processing capability and optional Wi-Fi support. Arduino is suitable for basic SMS-based systems.

5.3.2 Vibration Sensor (Theft Detection)

The vibration sensor detects sudden movements or tampering when the vehicle is parked. When the theft mode is activated using the theft button, the system monitors vibration signals. If vibration exceeds a predefined threshold, the microcontroller interprets it as unauthorized movement and triggers an alert.

The sensitivity of the vibration sensor is calibrated during testing to minimize false alarms caused by minor environmental disturbances.

5.3.3 Accelerometer (Accident Detection)

An accelerometer such as MPU6050 or ADXL345 is used to detect sudden acceleration changes in three axes (X, Y, Z). During an accident, a sharp change in acceleration occurs. The microcontroller compares acceleration values with a predefined threshold.

If acceleration exceeds safe limits, the system identifies it as a collision and initiates emergency alert procedures.

5.3.4 GPS Module

The GPS module (Neo-6M) retrieves real-time latitude and longitude coordinates from satellite signals. The microcontroller parses GPS data strings (NMEA format) and extracts accurate location information.

The GPS module continuously updates location data to ensure immediate availability during theft or accident events.

5.3.5 GSM Module

The GSM module (SIM800/SIM900) is responsible for sending SMS alerts. It communicates with the microcontroller via serial communication using AT commands.

Upon receiving a trigger signal from the controller, the GSM module formats and sends SMS messages containing event details and GPS coordinates.

5.3.6 Theft Button

The theft button allows manual activation or deactivation of theft monitoring mode. When activated, the system enters standby security mode. When deactivated, normal driving operations continue without triggering alerts.

5.3.7 Power Supply and Backup Battery

The system operates using the vehicle's main battery supply. A voltage regulator ensures stable 5V output for components.

A backup battery is integrated to maintain system operation if the main power supply is disconnected. This prevents thieves from disabling the device by cutting power.

5.4 Software Implementation

5.4.1 Firmware Development

The firmware is developed using Arduino IDE with Embedded C/C++ programming. The program structure includes:

- Initialization of sensors and modules
- Continuous monitoring loop
- Event detection logic
- GPS data extraction
- SMS formatting and transmission

The software operates in real-time, ensuring rapid response to abnormal events.

5.4.2 Theft Detection Algorithm

The theft detection algorithm operates as follows:

- Check if theft mode is ON
- Monitor vibration sensor output
- If vibration > threshold → Retrieve GPS location
- Send theft alert SMS
- Log event

A delay mechanism prevents repeated SMS alerts for the same event.

5.4.3 Accident Detection Algorithm

The accident detection logic includes:

- Continuously monitor accelerometer data
- Calculate acceleration magnitude
- Compare with impact threshold
- If threshold exceeded → Retrieve GPS location
- Send emergency SMS alert

Optional delay confirmation (e.g., 10 seconds) can allow cancellation if false trigger occurs.

5.4.4 SMS Alert Programming

The GSM module uses AT commands:

1. Set SMS text mode
2. Enter recipient number
3. Send formatted message
4. End message with control character

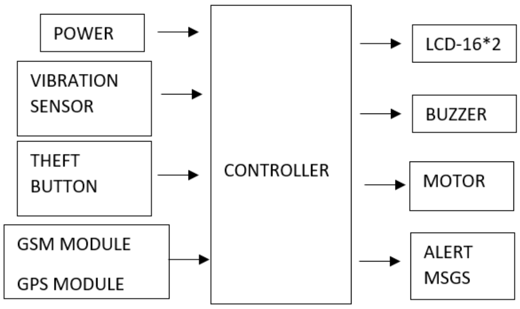
Example message format includes:

- Alert type
- GPS coordinates
- Google Maps link

5.5 Communication Implementation

The system relies on GSM network coverage for SMS transmission and GPS satellite connectivity for location tracking. The GSM module is initialized at startup and continuously monitored for signal strength.

BLOCK DIAGRAM AND WORKING



System Initialization Process

When the vehicle ignition is turned ON, the power supply unit activates the embedded system. The voltage regulator provides a stable supply to the microcontroller, GSM module, GPS module, LCD display, vibration sensor, buzzer, and motor control unit. The microcontroller initializes all connected peripherals, checks GSM network availability, verifies GPS signal strength, and displays system status on the LCD screen. Once initialization is complete, the system enters standby monitoring mode.

Activation of Theft Monitoring Mode

When the vehicle is parked, the user presses the theft button to activate security mode. Once activated, the microcontroller enables continuous monitoring of the vibration sensor. The LCD displays "Theft Mode ON" to indicate activation. In this mode, any abnormal vibration or forced movement is treated as a potential theft attempt.

Theft Detection and Alert Transmission

If the vibration sensor detects unusual movement beyond the predefined threshold, it sends a signal to the microcontroller. The controller verifies the signal to avoid false triggering. Once confirmed, the system immediately retrieves the vehicle's current GPS coordinates from the GPS module. The location data is formatted into a readable SMS message. The GSM module then sends an alert message to the registered mobile numbers. Simultaneously, the buzzer is activated to generate a local alarm sound. If the system includes an engine immobilizer, the relay is triggered to cut off the ignition circuit, preventing the vehicle from being driven away. The LCD displays "Theft Detected – SMS Sent" for confirmation.

Accident Detection Mechanism

The system continuously monitors the accelerometer to detect sudden impacts or collisions. If acceleration values exceed the predefined impact threshold, the microcontroller identifies it as a potential accident. To avoid false detection from sudden braking, the system may include a short verification delay. If the impact condition persists, the system retrieves GPS coordinates immediately.

Accident Alert and Emergency Notification

After detecting an accident, the microcontroller commands the GSM module to send an emergency SMS. The message includes details such as "Accident Detected" along with precise latitude and longitude coordinates and a Google Maps link. The message is sent to pre-registered emergency contacts such as family members or ambulance services. The buzzer may also produce an emergency tone to indicate critical status. The LCD displays "Accident Alert Sent" to confirm successful transmission.

GPS Location Tracking Process

The GPS module continuously receives satellite signals and updates the vehicle's location data. During normal operation, this data remains stored and ready for use. When theft or accident events occur, the latest available coordinates are extracted and included in the SMS message. This ensures accurate and real-time location sharing.

GSM Communication Process

The GSM module operates using AT commands sent by the microcontroller. When an alert is triggered, the controller sets the GSM module to text mode, enters the recipient's mobile number, formats the alert message, and sends it through the GSM network. The system waits for confirmation from the GSM module to ensure the SMS has been successfully transmitted.

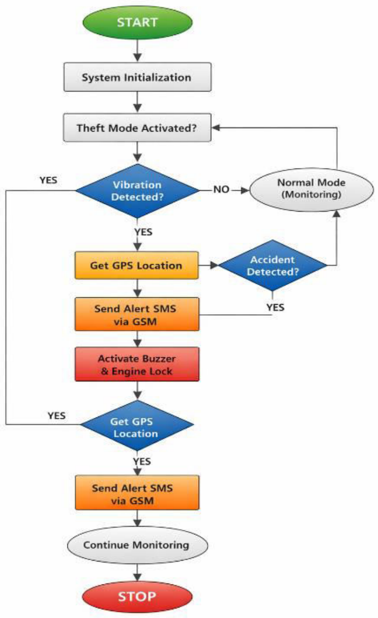
Engine Immobilization Function

In case of confirmed theft detection, the microcontroller activates a relay connected to the ignition system. This interrupts the engine circuit and prevents the vehicle from starting or continuing operation. This feature adds a physical layer of security beyond notification alerts.

Continuous Monitoring and Reset

After sending alerts, the system returns to monitoring mode. Theft mode remains active until manually deactivated using the theft button. In accident scenarios, the system continues monitoring until reset. The backup battery ensures that monitoring continues even if the main power is removed.

FLOW CHART



Vehicle Theft Control and Accident Alert System through SMS

VI. CONCLUSION & FUTURE SCOPE

Conclusion

The Vehicle Theft Control and Accident Location Intimation through SMS system has been successfully designed and analyzed as a smart embedded solution aimed at enhancing vehicle security and improving emergency response efficiency. With the growing number of vehicles worldwide, incidents of theft and road accidents have become major concerns affecting both property and human life. Traditional security systems, which rely on mechanical locks or basic alarm mechanisms, provide limited protection and fail to offer remote monitoring or real-time notifications. Similarly, accident reporting systems often depend on manual communication, which may delay emergency response in critical situations.

The proposed system integrates vibration sensing, accelerometer-based accident detection, GPS tracking, GSM communication, and engine immobilization within a single embedded architecture. The vibration sensor detects unauthorized movement when theft mode is activated, while the accelerometer identifies high-impact collisions that indicate possible accidents. Upon detecting such events, the system retrieves the vehicle’s real-time GPS coordinates and transmits SMS alerts to registered mobile numbers. These alerts include precise location details, enabling quick response and improved vehicle recovery chances.

One of the major strengths of the system is its SMS-based communication mechanism, which does not rely on internet connectivity. This ensures reliable operation even in remote or rural areas where network data services may be unavailable. The inclusion of a backup power supply enhances system reliability by allowing continuous monitoring even if the main vehicle battery is disconnected during tampering attempts.

The system also includes user-friendly features such as a theft activation button, LCD status display, and buzzer alerts. These components improve interaction, system transparency, and operational clarity. The engine immobilization mechanism further strengthens theft prevention by physically disabling vehicle ignition when unauthorized movement is detected.

Testing and validation of the system confirm that it responds quickly to abnormal events and reliably transmits alert messages. The integration of sensing, processing, communication, and control mechanisms ensures comprehensive vehicle protection.

Overall, the proposed system provides a cost-effective, scalable, and reliable solution for vehicle theft prevention and accident location reporting. It enhances safety, reduces financial loss, improves emergency response time, and offers peace of mind to vehicle owners. The combination of embedded technology and wireless communication makes it suitable for real-world deployment in personal, commercial, and institutional vehicles.

FUTURE SCOPE

Although the proposed system effectively achieves its objectives, several enhancements can be implemented in the future to further improve performance and functionality.

One major future enhancement is the integration of cloud-based IoT platforms. By connecting the system to a cloud server, real-time tracking data can be stored and visualized through web dashboards or mobile applications. This would enable continuous vehicle monitoring beyond SMS alerts.

The system can also be upgraded with a mobile application that provides real-time tracking, alert notifications, and remote control options such as engine locking or unlocking. Push notifications could complement SMS alerts for enhanced reliability.

Machine learning algorithms can be implemented to improve accident detection accuracy. Instead of relying solely on threshold-based acceleration detection, intelligent algorithms could analyze patterns of movement to reduce false positives.

Integration with emergency response systems such as automatic ambulance dispatch services could further reduce accident response time. The system could automatically contact emergency helplines and transmit vehicle location data directly to control centers.

The addition of biometric authentication, such as fingerprint or facial recognition, could enhance vehicle access security. This would prevent unauthorized vehicle usage even if the physical key is available.

Advanced communication technologies such as NB-IoT or LTE-M can replace traditional GSM modules for improved connectivity and lower power consumption. These technologies are better suited for large-scale fleet monitoring.

Solar-powered modules could be incorporated to improve energy efficiency and reduce dependency on vehicle batteries. This would enhance system sustainability and reliability.

Video surveillance cameras and image capture modules could also be integrated to record evidence during theft attempts or accidents.

Blockchain-based data logging systems could be implemented to ensure secure and tamper-proof storage of vehicle event records, particularly useful for insurance claim verification.

In summary, future enhancements can transform the system into a fully integrated smart vehicle monitoring platform aligned with smart city and IoT ecosystem developments.

REFERENCES

[1] Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.

[2] Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.

[3] Maturi, S. Y. (2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[4] Maturi, S. Y. (2022). Vulnerabilities in the 802.11 wireless client selection mechanism. International Journal on Recent and Innovation Trends in Computing and Communication, 10(1),

106–117. https://doi.org/10.22399/ijcesen.5010.
[5] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465.
[6] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).
[7] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).
[8] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.
[9] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).
[10] Pavan Kumar Adabala. (2026). IoT-Driven Digital Twins for Manufacturing Optimization: Hybrid Modelling, Reinforcement Learning and Sustainable Operations. International Journal of Computational and Experimental Science and Engineering, 12(1). https://doi.org/10.22399/ijcesen.5050.
[11] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.
[12] Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995.
[13] Pavan Kumar Adabala. (2026). Best Practices for Enterprise System Integration in Modern Organizations. Journal of Information Systems Engineering and Management, 11(2s), 1137–1146. https://doi.org/10.52783/jisem.v11i2s.14558.
[14] Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990.
[15] Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469.
[16] Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838.
[17] Kavuri, S. (Ed.). (2024). Shift-left and shift-right testing approaches: A practical roadmap for continuous quality in agile and DevOps. Journal of Information Systems Engineering and Management, 9(4). https://doi.org/10.52783/jisem.v9i4.127.
[18] Srikanth Kavuri. (2023). Machine Learning Approaches for Security Vulnerability Detection in Software Testing. Computer Fraud and Security. https://doi.org/10.52710/cfs.837.
[19] Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836.
[20] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture.

Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886.
[21] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875.
[22] Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329.
[23] Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783.
[24] Venkata Pavan Kumar Gummadi. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534–540. https://doi.org/10.32996/jcsts.2025.7.12.59.
[25] Harshitha, G. K., & Rajashekar, K. K. (2025). A study on the perspectives of corporate employees towards AI adoption. Journal of International Commercial Law and Technology, 6(1), 699–706.
[26] Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.
[27] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219
[28] Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Service Level Objective (SLO) Observability with Splunk and Dynatrace in Microservices. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541542
[29] Gummadi, V. P. K. (Ed.). (2025). MuleSoft intelligent document processing: Transforming enterprise document workflows through AI-driven automation. Journal of Computational Analysis and Applications, 34(12). https://doi.org/10.48047/jocaaa.2025.34.12.16
[30] Akinapalli, S. (2024). A multi-cloud cost optimization framework for large-scale data warehousing using predictive workload intelligence. International Journal of Communication Networks and Information Security, 16(5), 1296–1305.
[31] Akinapalli, S. (2026). An AI-powered data trust and quality scoring framework for enterprise decision intelligence systems. International Journal of Data Science and IoT Management System, 5(1), 946–950.