

Research Paper

IoT-Based Anti-theft Protection of Vehicle with SMS Alert

K. Harsha Prateek¹, Nandam Tanusha², K Venkatesh Sharma³

^{1,2} B.Tech Student ,Department of Computer Science & Engineering, CVR College of Engineering, Rangareddy Dist, Telangana, India

³ Professor, Department of Computer Science & Engineering, CVR College of Engineering, Rangareddy Dist, Telangana, India

e-mail: harshaprateek777@gmail.com , tanu.nandam@gmail.com , venkateshsharma.cse@gmail.com

*Corresponding Author: venkateshsharma.cse@gmail.com

Received: 18/05/2023,

Revised: 23 /06/2023,

Accepted: 09/07/2023

Published: 28/07/2023

Abstract: - Nowadays, automobile thefts and the production of vehicle are increasing in yearly world. So, vehicle theft is a universal problem. To solve this problem, most of the vehicle owners have started using the theft protection systems. The main purpose of this paper is to prevent the vehicle theft and the functionality is achieved by detecting vehicle status in theft mode and by sending an SMS is generated automatically. This SMS is then sent to the owner of the vehicle. The owner can then send back the SMS to disable the ignition of the vehicle. Thus, in this way crimes can be reduced to a great extent as vehicles today are being stolen in large number. Hence, the vehicles today require high security which can be achieved with the help of this application that how the system works is when a person tries to steal the vehicle, the microcontroller in it is interrupted and the command is sent to the GSM modem to send SMS. On the receipt of the message, the owner sends back the SMS to the GSM modem. This is done to stop the engine. This GSM modem is interfaced to the micro controller. This microcontroller on the receipt of the message uses a mechanism that helps to stop engine. Motor is being used to indicate vehicle ON/OFF state.

Keywords- Automobile Theft Prevention, Theft Protection Systems, Vehicle Status Detection, SMS Alert System, Microcontroller Interfacing, Engine Disabling Mechanism

1. Introduction

Vehicle theft is a major problem worldwide, with millions of vehicles stolen each year. In order to address this problem, we propose a new IoT-based anti-theft protection system for vehicles. The proposed system uses a GSM modem and a GPS module to track the vehicle's location and send an alert to the owner if the vehicle is stolen. The system also provides real-time information about the vehicle's speed, location, and fuel level.

The proposed system has several advantages over existing vehicle theft prevention systems. First, it is more secure because it uses a GSM modem and a GPS module[1]. Second, it is more versatile because it can provide real-time information about the vehicle's location. Third, it is more affordable than some existing vehicle theft prevention systems.

The proposed system does have some limitations. First, it requires a GSM modem and a GPS module. Second, it may not be effective against professional thieves. However, we believe that the advantages of the proposed system outweigh the limitations.

The existing security alarm systems have become susceptible to theft due to the familiarity thieves possess about their workings. These systems can be circumvented with ease, undermining their purpose [2]. Additionally, some security systems rely on external servers to analyze data, causing privacy concerns and introducing delays due to network latency. To address these issues and improve security, the research endeavors to develop a Chrome browser plugin that performs classification locally without relying on external servers.



The proposed anti-theft security system employs an embedded system design featuring Dual Tone Multi-Frequency (DTMF) and a Global System for Mobile Communications (GSM) module to safeguard vehicles. This system automatically immobilizes the vehicle upon activation by disconnecting the ignition key supply from the battery, rendering the vehicle inoperable. In case of unauthorized access, such as attempts to open doors or the trunk, the system triggers an alarm and sends a text message to the vehicle owner. This design intends to counteract the escalating rate of vehicle thefts and provides real-time monitoring through GSM network coverage.

The research primarily aims to design, develop, and implement a GPS-based vehicle theft prevention system using GSM technology. This system will be integrated into vehicles to send alarms to owners during unauthorized access. Data will be collected from likely vehicle owners to inform system development.

The proposed vehicle theft detection system offers a pivotal solution to enhance vehicle security. Cost-effective and reliable, it introduces a switch for toggling between user and theft modes. The system proves advantageous for various areas, especially large parking lots, offering real-time data such as vehicle speed, rash driving instances, and start-stop times via SMS. Notably, the system ensures reliability and security, promptly alerting owners to unauthorized access and facilitating a proactive response.

Strengths include applicability to various transportation settings, such as companies, schools, and industries. Weaknesses involve sensor limitations and restricted vehicle use during emergencies. Opportunities lie in heightened security awareness, while threats encompass device discovery, management, and potential breaches.

In the political context, the government's involvement in implementing this system could prevent car theft. Economically, the impact of IoT technology on vehicle security is anticipated to grow. Socially, user awareness is crucial. Technological advancements pose a challenge, and legal considerations involve intellectual property and innovation protection.

The paper is organized as follows: section 2 presents Literature Survey

2. Literature Survey

2.1 GSM Technology

GSM (Global System for Mobile Communications)[3] is a cellular network technology that is used by mobile phones and other wireless devices. GSM technology is used in the proposed system to track vehicles because it is a reliable and widely available technology. GSM networks have a wide coverage area, which means that the vehicle can be tracked even if it is taken to a remote location. Additionally, GSM networks are relatively secure, which means that the data transmitted between the vehicle and the tracking system is protected from unauthorized access.

2.2 Face Recognition

Face recognition is a biometric technology that can be used to identify people based on their facial features. Face recognition is used in the proposed system to verify the identity of the user before the vehicle can be started. This helps to prevent unauthorized access to the vehicle. Face recognition is a reliable and accurate technology, and it can be used even in low-light conditions.

2.3 Microcontroller

A microcontroller is a small computer that is used to control electronic devices. The microcontroller[4] in the proposed system is responsible for processing the data from the sensors and activating the alarm system if an intruder is detected. The microcontroller is a powerful and versatile device that can be used to control a wide variety of electronic systems.

A survey was conducted to gather data on the awareness of vehicle theft detection tools among vehicle owners. The survey results showed that a majority of vehicle owners are aware of the existence of vehicle theft detection tools, but only a small percentage of vehicle owners actually use these tools. The survey also showed that vehicle owners are most concerned about theft of their car stereos and other valuables.

The survey data suggests that there is a need for more education and awareness about vehicle theft detection tools. Vehicle owners should be aware of the different types of vehicle theft detection tools that are available and the benefits of using these tools. Vehicle owners should also take steps to secure their vehicles, such as installing a security system and locking the doors and windows when the vehicle is unattended.

The benefits of using a layered approach to theft-proofing your vehicle

A layered approach to theft-proofing your vehicle involves using a combination of different security measures. This can help to deter thieves and make it more difficult for them to steal your vehicle. Some of the different security measures that you can use include:

- * A security system
- * A steering wheel lock
- * A car alarm
- * A GPS tracker
- * A kill switch

The different techniques that can be used to detect vehicle theft

In addition to the audible alarm system that is used in the proposed system, there are a number of other techniques that can be used to detect vehicle theft. These techniques include:

- * GPS tracking
- * Engine immobilizers
- * Tilt sensors
- * Break-in sensors

- * Door and window sensors

The importance of taking steps to secure your vehicle

Even if you have installed a security system in your vehicle, it is important to take steps to secure your vehicle when it is unattended. This includes:

- * Parking in a well-lit area
- * Locking the doors and windows
- * Hiding your valuables
- * Not leaving your keys in the ignition

3. Proposed System Design

The proposed system aims to enhance vehicle theft detection and prevention using IoT and GSM technology. The system utilizes the following methods for effective operation:

The proposed system flow model is as follows:

1. The user turns on the vehicle.
2. The microcontroller checks if the ignition switch is on and the enable switch is also on.
3. If both switches are on, the microcontroller activates the GSM modem and sends an SMS to the user's phone.
4. The user receives the SMS and can then remotely disable the vehicle.
5. If the ignition switch is turned off or the enable switch is turned off, the microcontroller deactivates the GSM modem and stops sending SMS messages.

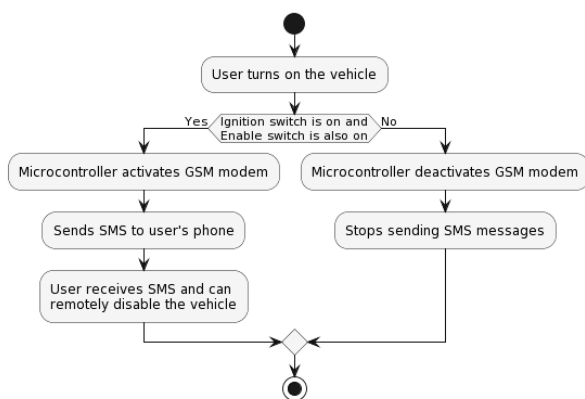


Figure:1 Proposed system flow model

1. Main Setup:

- **gsm.available():** Checks for incoming SMS.
- **check_sms():** Processes received SMS.
- **Read_sms():** Reads SMS content.
- **Del_sms():** Clears SMS storage for the next message.

2. Loop:

- **search_modem():** Continuously searches for the GSM modem.
- **configured_modem():** Initializes modem configuration.

3. Indicate Function:

- Triggers LEDs and a buzzer for indicating system status.

4. Register User:

- Allows the registration of users by saving their numbers in EEPROM.

3.1. System Architecture

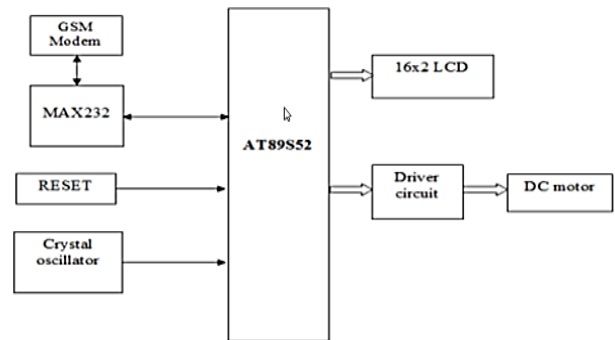


Figure2. Proposed System Architecture[5]

The system consists of the following components:

- **GSM Modem:** This is the component that allows the system to communicate with the cellular network. It is used to send and receive SMS messages.
- **Microcontroller:** This is the brain of the system. It controls all of the other components and processes the data from the sensors.
- **Sensors:** These sensors are used to detect unauthorized access to the vehicle. They can include door sensors, window sensors, and motion sensors.
- **Alarm System:** This system is activated when the sensors detect unauthorized access to the vehicle. It can include a siren, lights, and a buzzer.
- **LCD Display:** This display is used to show the status of the system and the messages that are sent and received.

The operational model of the system is as follows:

1. The GSM modem is turned on and connected to the cellular network.
2. The sensors are turned on and begin monitoring the vehicle for unauthorized access.
3. The microcontroller is turned on and begins processing the data from the sensors.
4. If the sensors detect unauthorized access to the vehicle, the alarm system is activated.

5. The microcontroller sends an SMS message to the owner of the vehicle.
6. The LCD display shows the status of the system and the messages that are sent and received.

The system can be configured to send SMS messages to multiple recipients, such as the owner of the vehicle, the police, and a security company. The system can also be configured to send different types of messages, such as a warning message or an emergency message.

The system is a valuable tool for preventing vehicle theft and protecting property. It is also a valuable tool for law enforcement, as it can be used to track down stolen vehicles.

3.2 Technology Description:

The system leverages IoT and GSM technology to prevent vehicle theft. An enable switch is used to activate the protection unit. If unauthorized ignition attempts occur, a message is sent to the vehicle owner, and an alarm is triggered. Users can also send SMS commands to stop the vehicle at any time. The system's architecture comprises microcontroller-based operation, GSM communication, and user interaction through SMS commands.

Implementation & Testing:

- The system is powered by a regulated +5V supply.
- The microcontroller (ATMEGA328)[6] controls input monitoring and generates outputs.
- GSM modem configuration and communication are managed using AT commands.
- The microcontroller interfaces with GSM through UART communication.
- Proper LCD display and alert SMS sending are ensured via programming.
- Testing involves continuity checks, voltage verifications, and connection tests.
- The system operates in two modes: alert mode and regular mode.
- Communication between microcontroller and GSM modem is established through serial communication.

3.3 System Implementation

The implementation model description involves several key components and steps to achieve the desired vehicle theft detection and prevention system. Let's break down the process step by step:



Figure 3. System Setup

1. Power Supply Regulation:

- A 12V DC power source is used to power the system.
- The power is regulated using a 7805 voltage regulator to obtain a stable +5V output.
- This regulated +5V supply is distributed to all the components of the system to ensure proper functionality.

2. GSM Modem Integration:

- The project heavily relies on a GSM Modem infrastructure for communication.
- The GSM modem operates at +5V power supply, consistent with the regulated output.
- The system interacts with the GSM modem using AT commands, a standardized command set used to control and communicate with GSM modems.

3. Sending and Receiving SMS:

- The project leverages the GSM system for sending and receiving SMS messages.
- When an SMS is sent, it goes through the GSM system, just like with a regular mobile phone.
- The GSM modem communicates with the microcontroller using serial data in ASCII format[7].
- The microcontroller uses AT commands to interact with the GSM modem and read incoming SMS messages.

4. SMS Processing and Validation:

- The microcontroller decodes the incoming SMS message to extract useful information.
- The system validates the SMS by checking its content against a predefined password or identifier.
- If the password matches, the system considers the SMS arrival valid; otherwise, it ignores the SMS.

5. Modes of Operation:

- The project operates in two modes: active mode and normal mode.
 - In active mode, if someone attempts to start the vehicle, the system sends an alert SMS to the registered user's phone.
 - In normal mode, the user can turn on the vehicle without triggering an alert.
6. **Microcontroller Control:**
- The microcontroller (ATMEGA 328) is the brain of the project, responsible for input monitoring and generating outputs.
 - The microcontroller programming is done using the Arduino compiler, utilizing C programming logic.
7. **LCD Display and User Interface:**
- The microcontroller interfaces with a 16x2 LCD display to provide visual information to the user.
 - The programming ensures proper display of SMS arrival status and other relevant information.
8. **Intruder Detection and SMS Alert:**
- If an intruder is detected, a predefined SMS is sent to the authorized mobile number using the GSM communication.
 - The GSM modem has been configured to handle SMS sending, and the microcontroller controls this process based on the program.
9. **UART Communication:**
- The interface between the microcontroller and the GSM modem uses UART communication.
 - UART (Universal Asynchronous Receiver-Transmitter) is a serial communication protocol that allows reliable data exchange between the microcontroller and the GSM modem.

4. Result and Analysis

4.1 System Specifications

The software requirements for the IoT system are as follows:

- **Sensors:** The sensors used in the system are a vibration sensor and a microcontroller. The vibration sensor is used to detect unauthorized access to the vehicle. The microcontroller is used to process the data from the vibration sensor and send an SMS message to the owner of the vehicle if unauthorized access is detected.
- **Microcontroller:** The microcontroller is the brain of the system. It is responsible for processing the data from the sensors, sending SMS messages, and displaying information on the LCD screen. The microcontroller is programmed in C language.
- **LCD Display:** The LCD display is used to show the status of the system and the messages that are sent and received. The LCD display can show up to 16 characters per line.

- **Connectivity:** The system is connected to the cellular network using a GSM modem. The GSM modem has a SIM card slot that allows it to connect to the cellular network.
- **Data Processing:** The system processes the data from the sensors and sends SMS messages to the owner of the vehicle if unauthorized access is detected. The system also stores data about the vehicle's location and the time and date of any unauthorized access.
- **User Interface:** The user interface is used to configure the system and view the data that is stored by the system. The user interface is a web-based interface that can be accessed from any computer or mobile device.

The software requirements for the IoT system are specific to the hardware that is used in the system. For example, if the system uses a different type of vibration sensor or microcontroller, the software requirements will need to be updated.

The software requirements for the IoT system are also specific to the features that are implemented in the system. For example, if the system is able to track the location of the vehicle, the software requirements will need to include the code for the tracking functionality.

The software requirements for the IoT system are an important part of the system design process. The software requirements must be carefully specified so that the system can be implemented correctly.

The hardware requirements for the IoT system are as follows:

- **LCD:** The LCD is used to display information about the system, such as the status of the sensors, the messages that are sent and received, and the location of the vehicle. The LCD is a 16 character, 2-line alphanumeric LCD display.
- **PIC Microcontroller:** The PIC microcontroller is the brain of the system. It is responsible for processing the data from the sensors, sending SMS messages, and displaying information on the LCD screen. The PIC microcontroller used in this system is the ATMEGA328P.
- **Relay Board:** The relay board is used to control the DC motor. The relay board consists of a number of relays that can be used to switch on and off electrical devices.
- **DC Motor:** The DC motor[8] is used to activate the alarm system. The DC motor is powered by the battery and can be turned on and off using the relay board.
- **GSM Modem:** The GSM modem is used to connect the system to the cellular network. The GSM modem has a SIM card slot that allows it to connect to the cellular network.

The hardware requirements for the IoT system are specific to the features that are implemented in the system. For example, if the system is able to track the location of

the vehicle, the hardware requirements will need to include a GPS module.

The hardware requirements for the IoT system are an important part of the system design process. The hardware requirements must be carefully specified so that the system can be implemented correctly.

4.2 Result and Analysis:

The described GSM-based vehicle theft control system aims to provide vehicle owners with the ability to monitor the status of their vehicles and take appropriate actions in case of theft. The system involves several components working together to achieve this goal.

1. **Retrieving Vehicle Status:** The system retrieves the vehicle's status to determine whether it is in theft mode or not. This information is crucial to identify unauthorized access attempts.
2. **GSM Modem and Microcontroller Interface:** The microcontroller is interfaced with a GSM modem. The microcontroller is the central processing unit that controls the system's actions based on the retrieved vehicle status.
3. **Generating Vibrations and Sending SMS:** The microcontroller generates vibrations as a response to the retrieved vehicle status. This action triggers the microcontroller to send an SMS to a predefined authority, such as the vehicle owner or security personnel. The SMS is sent over the GSM network using the GSM modem[9].
4. **Periodical SMS Intervals:** The SMS notifications are sent at regular intervals, as set by the user. This feature allows continuous monitoring of the vehicle's status and helps ensure timely notifications in case of unauthorized access or theft.
5. **LCD Display Interface:** An LCD display[10] is connected to the microcontroller. The purpose of the display is to show the data received from the system before it is sent over the GSM network. This provides a visual confirmation of the information being transmitted.
6. **Enhancements and Future Development:** The project has potential for further enhancements. For instance, the system could be expanded to include the ability for the vehicle owner to remotely stop the ignition of the vehicle by sending an SMS, thus immobilizing the vehicle in theft situations. This additional layer of control could help prevent theft more effectively.
7. **System Activation and Alert Display:** When the user activates the theft mode, the LCD display shows a message indicating "System Active." On the other hand, if the theft mode is not activated, the display shows "System Disabled." In the event of an unauthorized ignition attempt, the system displays an "ALERT" message, showing the registered user's number, and initiates a siren sound through a buzzer to alert nearby individuals.

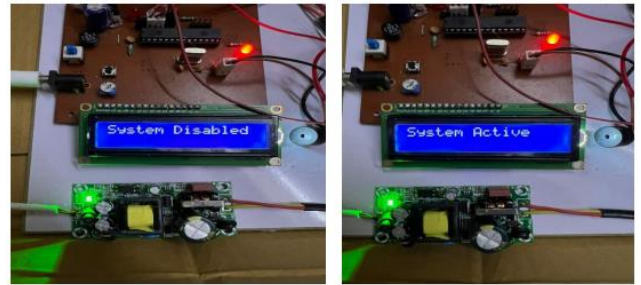


Figure 4. GSM-based vehicle theft control system

Overall, the system's results and analysis indicate that the proposed GSM-based vehicle theft control system effectively addresses the need for vehicle security. It combines microcontroller control, GSM communication, and user interface elements to provide real-time status updates and alerts to vehicle owners. The ability to remotely monitor and respond to theft attempts enhances the security of the vehicle and contributes to its overall protection. The future potential for further development and enhancements adds to the system's versatility and utility.

5. Conclusion and Future scope

The security of vehicles is of utmost importance in today's world, regardless of the presence of existing security systems in modern automobiles. With the rapid advancement of technology, the integration of Internet of Things (IoT) devices can offer an additional layer of security that can be applied to any vehicle. The implementation of such devices has the potential to significantly reduce vehicle-related crimes, which are on the rise due to the increasing number of stolen vehicles. The project "IoT-Based Anti-theft Protection of Vehicle with SMS Alert System" demonstrates the feasibility of this concept. The project's innovative aspect lies in its portability and ease of integration. The device can be conveniently installed in a vehicle and accessed remotely through SMS communication. This approach brings convenience to vehicle owners and enhances their ability to monitor and protect their vehicles from potential theft.

The future holds several exciting possibilities for further improving and expanding the capabilities of the system:

Market Introduction: The project can be taken to the next level by enhancing the capabilities of its components and introducing it to the market. This could be marketed as an aftermarket vehicle security solution that offers a user-friendly and cost-effective way to secure vehicles.

Component Enhancement: Continuous improvement in the quality and features of the components can enhance the effectiveness of the system. Upgrading the microcontroller, GSM module, and other hardware components can lead to better performance and reliability.

Integration with GPS: The system's capabilities could be extended by integrating GPS technology. This would allow the system to provide real-time location tracking of the vehicle, enabling the owner to retrieve the exact location of the vehicle in case of theft. Latitude and longitude information could be sent to the owner via SMS.

References

- [1] Nagaraja, B. G., Rayappa, R., Mahesh, M., Patil, C. M., & Manjunath, T. C. (2008). Design & Development of a GSM Based Vehicle Theft Control System. IEEE. DOI: 10.1109/ICACC.2009.154, pp. 148-152.
- [2] Mazidi, M. A. (2008). The 8051 Microcontroller & Embedded Systems (2nd ed.). Pearson Education Asia.
- [3] Ayala, K. J. (1996). The 8051 Microcontroller Architecture, Programming & Applications. Penram International.
- [4] Kamal, R. (2008). Embedded System Architecture, Programming and Design (2nd ed.). Tata McGraw Hill.
- [5] PREDCO, M. (n.d.). Programming and Customizing 8051 Microcontrollers. Tata McGraw Hill.
- [6] Toshiba. (1993). NAND Flash Applications Design Guide.
- [7] Millman, J., & Grabel, A. (n.d.). Microelectronics (2nd ed.). Combinatorial Digital Circuits & Sequential Digital Circuits.
- [8] National Motor Vehicle Theft Reduction Conference. (2000). Conference Papers (Australia).
- [9] Stolen and Wrecked Vehicles Monitoring Program. (1994). CCMTA June (Canada).
- [10] CCMTA Best Practice Models for Combating Auto Theft. (2006). Version 6.1, Oct. Anti Auto Theft Project Group.