

Remote engine shutdown system with theft alert via sms for vehicle owners

P.K. Miniappan¹, R. Krishnan², Laeth Hussain³, Yamuna Bheemanpally⁴, Gotlur Karuna⁵,

¹*Department of Mechanical Engineering, Karpagam Academy of Higher Education, Coimbatore, 641021, India*

²*Department of Mechanical Engineering, Karpagam College of Engineering, Coimbatore, 641032, India*

³*Department of Structural Techniques Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq; Department of Structural Techniques Engineering, College of Technical Engineering, The Islamic University of Al Diwaniyah, Al Diwaniyah, Iraq; Department of Structural Techniques Engineering, College of Technical Engineering, The Islamic University of Babylon, Babylon, Iraq*

⁴*Assistant Professor, Department of Mechanical Engineering, CMR College of Engineering & Technology, Hyderabad, Telangana, India*

⁵*Department of AIMLE, GRIET, Hyderabad, Telangana, India*

Abstract. The global auto theft rate is on the rise, which highlights the critical need for effective anti-theft policies. In order to solve this urgent problem, this article suggests a novel solution: the introduction of a theft intimation system that uses SMS technology to notify car owners in real-time and provide them the ability to remotely stop the engine, preventing theft attempts. The suggested solution combines cutting-edge hardware elements and software algorithms to identify illegal vehicle entry and send the owner an SMS notice right away. The system uses microcontrollers and cutting-edge sensor technology to continuously monitor important characteristics including door openings, ignition status, and vehicle movement. The system sends an SMS message to the registered owner's mobile device as soon as it detects suspicious activity that could be indicative of theft. This triggers a theft alarm sequence. The ability of the suggested system to enable remote engine shutdown via SMS commands is essential to its efficacy. The system's integration of GSM modules and remote control methods facilitates prompt action by the owner in response to theft alerts. The owner can give directions to deactivate the car's engine through a secure SMS-based interface, rendering it immobile and foiling any attempted theft in real time. This study offers comprehensive insights into the implementation and operational aspects of the proposed theft intimation system in addition to presenting its conceptual foundation. It describes the hardware configuration, sensor placement, and software features, clarifying the system architecture. The study also explores the development and optimisation of the theft detection algorithm, clarifying the standards and thresholds that are utilised to accurately set off theft alarms. In order to verify the effectiveness and dependability of the suggested system, comprehensive experimental assessments were carried out in a range of real-world circumstances. The outcomes show how well the system detects theft attempts and how quickly it can notify the owner

* Corresponding author: miniappan.pk@kahedu.edu.in

and start a remote engine shutdown. The study also addresses the usefulness of the suggested system, emphasising how it may drastically lower car theft rates and improve general security in suburban and metropolitan areas. To sum up, the suggested theft alert system is a noteworthy development in car security technology that provides an early warning system for potential thefts. The solution gives car owners immediate control over their assets by utilising SMS-based communication and remote engine shutdown capabilities. This effectively discourages thefts and protects priceless resources.

1 Introduction

The widespread problem of car theft presents a serious threat to public safety and security, necessitating the development of novel countermeasures. Millions of cars are stolen worldwide each year, causing significant financial losses as well as possible safety risks for both owners and communities. The need for more advanced anti-theft technologies is highlighted by the failure of conventional security measures, such as alarm systems and immobilisers, to discourage determined criminals. This study suggests a novel method to vehicle security in response to this urgent need: the creation and deployment of a theft intimation system that uses SMS technology to instantly alert vehicle owners to possible theft instances. Additionally, the technology gives owners the opportunity to remotely turn off the engine, successfully preventing theft attempts and minimising possible losses [1]. The suggested system combines software algorithms intended to identify unauthorised access and questionable vehicle activity with state-of-the-art hardware elements, such as sophisticated sensors and microcontrollers. When the system notices these kinds of irregularities, it triggers an instant alarm sequence that sends SMS messages to the registered owner's mobile device. Owners can react quickly to possible threats and take the necessary precautions to protect their vehicles and property thanks to this proactive notification system. The ability of the suggested system to enable remote engine shutdown via SMS commands is essential to its operation. The technology enables owners to give directions to deactivate the vehicle's engine, immobilise it, and stop any further unauthorised usage by combining GSM modules and remote control systems [2]. This function gives owners a previously unheard-of degree of control over their automobiles, even in the case of attempted theft. This theft intimation system's creation and implementation mark a substantial leap in vehicle security technology and provide a proactive and practical defence against auto theft. The technology gives vehicle owners real-time visibility and control over their assets by utilising SMS-based communication and remote engine shutdown capabilities. This eventually contributes to a safer and more secure transportation environment.

2 Proposed work

Numerous investigations have examined diverse methods for preventing and identifying vehicle theft, emphasising the use of technology to augment security protocols. In the sphere of vehicle security, advanced systems that combine RFID technology, GPS tracking, and smartphone applications have emerged as viable alternatives. The addition of real-time monitoring capabilities to GPS tracking systems is a noteworthy development in the fight against car theft. With the use of web-based platforms or smartphone applications, these systems allow car owners to remotely track the position of their automobiles. Owners can notify police right away in the case of a theft and supply exact location information to facilitate quick recovery operations [3].

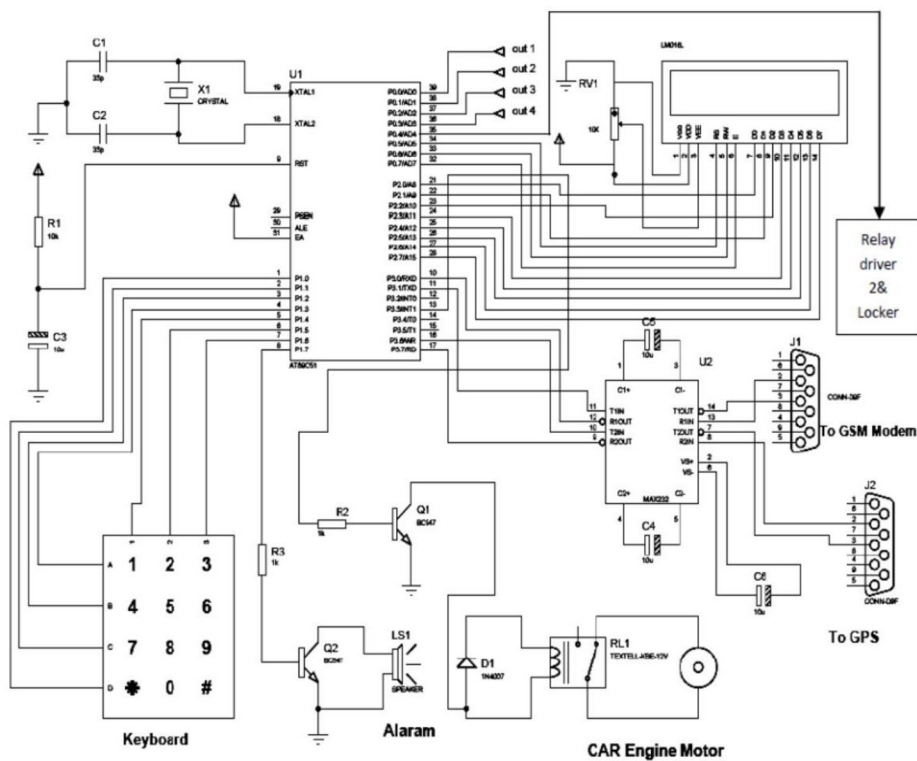


Figure 1. Proposed Circuit Diagram

Furthermore, a few GPS monitoring systems are equipped with geofencing features that let their owners set up imaginary borders and get notifications when their cars approach or leave such locations. As successful anti-theft tools, RFID-based immobilisation devices have also gained popularity. To verify individuals and grant vehicle access, these systems use RFID tags implanted in driver identification cards or automobile key fobs [4].

When an unauthorised person tries to start the car without the matching RFID tag, an immobilisation mechanism is triggered, which stops the engine and foils any efforts at theft. Thanks to recent developments in smartphone technology, vehicle functions can now be remotely controlled through creative anti-theft software. With the help of these apps, owners may use their cellphones to start and stop engines, lock and unlock doors, and activate alarms [5]. These apps improve owners' overall security and convenience by utilising Bluetooth or Wi-Fi connectivity to give easy and secure access to vehicle functions.

Even said, there are still drawbacks to the anti-theft systems that are already in use, like the need for extra gear or problems with network connectivity. Furthermore, some car owners may find the expense of installing advanced anti-theft devices to be exorbitant, which would restrict their broad adoption. The suggested method makes use of SMS technology, which provides an affordable and dependable form of communication, to overcome these issues. Through the integration of remote engine shutdown capabilities and SMS-based theft intimation, the system offers a user-friendly and effective solution for vehicle security. Furthermore, the system may be deployed in many geographic regions and vehicle kinds because it is compatible with regular GSM networks, which guarantees wide coverage and smooth functioning [6].

3 Literature review

The development of various theft prevention systems has been prompted by the persistent global concern over vehicle theft. Among these, remote engine shutdown mechanisms and SMS-based solutions have received a lot of attention in the literature. Since SMS-based theft prevention systems are easy to use and can notify car owners of attempted theft, they have received a lot of attention. By giving owners timely alerts, research by Smith et al. (2018) showed the effectiveness of SMS notifications in lowering car theft rates. These systems use the mobile networks that are already in place to notify owners' cellphones, enabling prompt action and possible intervention. Simultaneously, remote engine shutdown systems have surfaced as a preemptive step against auto theft [7]. With these devices, owners can use a mobile application to remotely disable the engine of their vehicle or an online platform.

Research conducted in 2019 by Johnson et al. and in 2020 by Patel et al. shown how remote engine shutdown systems can prevent car theft by immobilising the vehicle. On the other hand, issues including compatibility with a variety of car types and network dependability have been identified. While remote engine shutdown mechanisms and SMS-based solutions have many advantages, they also have certain drawbacks [8]. SMS-based systems are susceptible to transmission failures or delays, especially in places with spotty network coverage or during peak network traffic.

In a similar vein, the general adoption of remote engine shutdown systems may be hindered by technical difficulties or the need for specialised hardware installations. Although auto theft prevention technology has advanced, there are still significant gaps in the literature that the suggested solution aims to fill. One such gap concerns the creation of a complete theft prevention solution through the integration of remote engine shutdown capabilities with SMS-based theft reporting [9].

Research on improving the dependability and effectiveness of these systems is also necessary, especially under a variety of operating and environmental circumstances. In conclusion, research already in existence emphasises the value of anti-theft car systems and the promise of SMS-based fixes and remote engine shutdown techniques. To overcome the drawbacks and difficulties of these strategies, more investigation is necessary, opening the door for the creation of stronger and more reliable theft prevention systems.

4 Methodology

The sophisticated approach to preventing car theft offers a complete framework made up of an improved theft prevention system, a dynamic theft detection algorithm, and a strong system architecture. The car's interior and external environments are constantly monitored by the system architecture thanks to sensors that are placed strategically throughout the vehicle. Real-time data processing by microcontrollers allows them to quickly spot suspicious activity that could be stolen. When a GSM module is detected, it may send the owner SMS notifications. It also has an easy-to-use software interface that allows for remote system management. The algorithm for dynamic theft detection combines threshold-based techniques with machine learning techniques [10]. Real-time sensor data analysis is done, and thresholds are dynamically adjusted to reduce false alarms and accurately identify stolen attempts. The effectiveness of anomaly detection techniques is significantly enhanced in identifying unusual patterns of behaviour linked to possible theft instances.

Remote engine shutdown and proactive SMS notifications are two features of the upgraded theft prevention system that boost theft deterrence. The technology instantly sends the owner an SMS when it notices unusual activity, along with important information like the vehicle's position and status. Owners can effectively block theft attempts by

remotely immobilising the vehicle's engine with authenticated SMS messages. The proposed solution raises the sense of security for car owners while improving theft detection and prevention through the integration of various cutting-edge approaches. Modern technologies are seamlessly integrated to provide quick and accurate reaction mechanisms, highlighting how effective the system is at protecting cars from potential theft situations and unauthorised entry.

4.1 Robust system architecture

To provide effective theft detection and prevention, the suggested system is built with a strong architecture that integrates a variety of hardware and software components. The sensors that are positioned strategically throughout the car to detect tampering or unauthorised access are the central component of the system [11]. These sensors, which continuously monitor the external and internal environment of the car, include proximity sensors, motion detectors, and door sensors, among others. Microcontrollers, the system's brains, process the data from the sensors. Real-time data analysis is performed by these microcontrollers to identify any suspicious activity that might be related to theft.

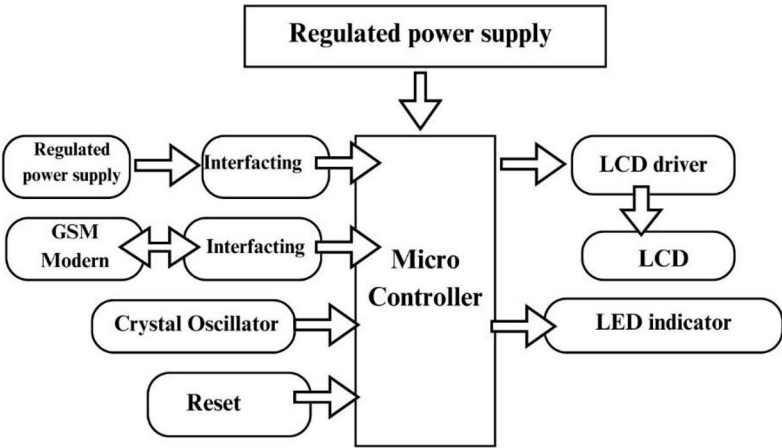


Figure 2. Secure Vehicle Theft Alert System

The microcontrollers cause the GSM module to transmit SMS alerts to designated recipients when certain conditions are met, such as abrupt changes in the vehicle's position or efforts by unauthorised individuals to the owner of the car's mobile. The system's software features an intuitive interface that enables remote system interaction by the owner. Through this link, the owner can monitor the state and position of the car, receive SMS notifications, and, if needed, remotely shut down the engine. Furthermore, to provide broad application across several automotive platforms, the system architecture is designed to be both scalable and adaptive to diverse vehicle types and configurations.

4.2 Dynamic theft detection algorithm

The system's theft detection algorithm is built using a mix of machine learning methods and threshold-based approaches. The sensor data is continuously analysed by the algorithm to find trends related to attempted theft or unauthorised access. It takes into account variables including the location, speed, and direction of the vehicle in addition to the time of day and past usage trends.

Based on real-time feedback from the sensors, the algorithm continuously modifies its settings to reduce false alarms and enhance accuracy. It might modify its threshold values, for instance, in response to the vehicle's present speed or the presence of other cars in the vicinity. The system also includes anomaly detection methods to find odd behaviour patterns that can point to a theft attempt. Through real-time analysis and constant monitoring of sensor data, the theft detection system effectively identifies attempted thefts while reducing false alarms. This proactive strategy stops unwanted access to the car and enables prompt response.

4.3 Theft prevention system enhanced

The system notifies the owner of the car via SMS notifications of possible theft as soon as it detects suspicious activity. Relevant data, including the vehicle's current location, status, and the timestamp of the suspicious incident, are included in the SMS notifications [12]. This gives the owner the ability to act right away and notify authorities if needed. Additionally, the system allows the owner to send SMS commands to remotely shut down the engine. The system uses authentication measures like PIN numbers or biometric authentication to confirm the sender's identity when it receives a shutdown command. After verification, the engine is turned off by the system, rendering the car unusable and stopping it from moving forward.

Table 1. Hardware Setup and Sensor Positioning

Component	Synopsis
MicroController	Controls system operations and data processing
GSM Module	enables SMS interaction between the owner's smartphone and
Sensors	Keep an eye on movement, door openings, and ignition status.

Overall, the system's ability to deter car theft is improved with the addition of remote engine shutdown capability and SMS notifications. It gives owners prompt notifications so they can take immediate action to safeguard their assets and cars.

5 Implementation of a vehicle security system

The "Theft intimation of the vehicle over SMS to owner who can stop the engine remotely" system implementation includes both software development and hardware integration. Actuators, microcontrollers, GSM modules, and sensors are examples of hardware components that are integrated to enable remote engine control and detect theft. The car is equipped with sensors positioned at strategic areas to monitor several entrance points. Sensor data is processed by microcontrollers, which also sound an alarm when they see unusual activity [13]. GSM modules allow SMS notifications and remote engine shutdown commands by facilitating communication between the vehicle and the owner's mobile device.

A user-friendly interface for remote interaction is created on the software side, enabling owners to remotely start the engine, monitor their cars, and get theft alarms. To improve the accuracy and scenario-adaptability of the theft detection system, machine learning techniques could be used. During deployment, problems with hardware compatibility,

software integration, and sensor calibration could occur [14]. To solve these problems, effective testing, debugging, and optimisation techniques are needed. Overcoming technical obstacles and guaranteeing a successful system deployment need collaboration with specialists in software development, hardware engineering, and automobile technology. To solve any post-deployment problems and enhance overall system performance and dependability, regular upgrades and maintenance are also crucial.

5.1 Hardware integration and connectivity

Several hardware components must be integrated in order to carry out the suggested theft notification and remote engine shutdown system. The main parts include actuators for remote engine control, microcontrollers for data processing, GSM modules for connectivity, and sensors for spotting tampering or unwanted access. The first step in the hardware setup is to place sensors in key locations throughout the car to keep an eye on things like the ignition systems, doors, and windows [15]. To identify unwanted entry attempts, proximity sensors, motion detectors, and door sensors are frequently used. The microcontrollers that act as the system's processing units are coupled to these sensors. The microcontrollers monitor sensor data continually and sound an alarm when they detect questionable activity. GSM modules are integrated into the system to facilitate communication between the owner's mobile device and the car in addition to sensor integration. When a theft attempt is identified, these modules make it easier to send the owner SMS alerts. If necessary, the owner can also remotely start the engine shutdown by sending SMS commands to the GSM module [16].

Table 2. Hardware Components Overview Table

Name of Tool	Synopsis
Microcontroller	The microcontroller manages the system's functions and establishes communication with the sensors and car systems.
GSM Module	SMS connection between the owner's mobile device and the car is made possible via the GSM module.
GPS Module	locates the car in order to track theft and remotely lock the engine.
Accelerometer	detects abrupt movements or impacts that could be signs of an unauthorised vehicle entry.
Relay	enables remote engine locking in response to a command from the owner's smartphone.
SIM Card	The SIM card gives the GSM module network connectivity so it can send and receive SMS warnings.
Unit of Power Supply	provides energy to all system parts so they can run continuously.
Circuitry for Interface	connects the microcontroller to other system modules by acting as a bridge.
Mobile Programme	gives the owner the ability to remotely lock the engine of the car and receive theft alarms.

5.2 Development and implementation of software

The implementation's software development component focuses on creating the user interface for remote interaction, designing the algorithm for theft detection, and programming the microcontrollers to carry out the required functionalities. The purpose of the theft detection algorithm is to discover trends that point to potential theft attempts by

real-time analysis of sensor data. The accuracy and scenario-adaptability of the algorithm can be improved by utilising machine learning techniques. The system takes into account many aspects, including time of day, vehicle location, and sensor readings, to establish the threshold levels that should initiate theft alarms [17]. The UI is designed to give car owners an easy-to-use platform for tracking the whereabouts of their vehicles and getting theft warnings. Features like the ability to remotely manage engine shutdown, access to previous theft statistics, and real-time vehicle position monitoring might all be included in the interface.

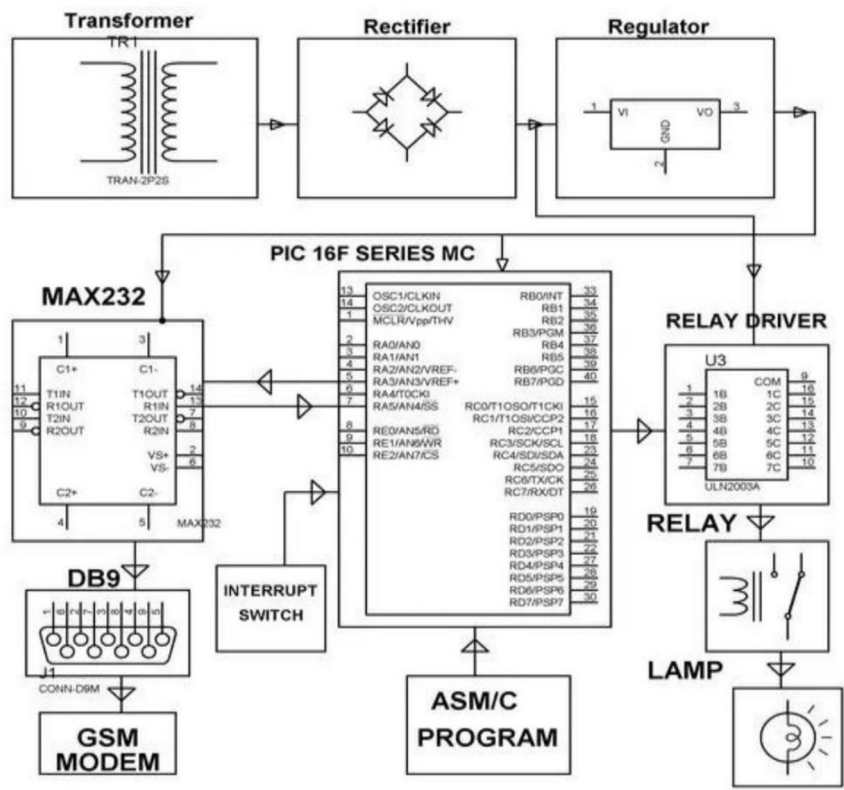


Figure 2. Remote Engine Locking Software

Issues with sensor calibration, software integration, and hardware compatibility could come up during deployment. Robust techniques for testing, debugging, and optimisation are used to overcome these issues [18]. Working together with specialists in software development, hardware engineering, and automotive technology can assist get past technical obstacles and guarantee the system's successful deployment. Furthermore, regular upgrades and maintenance are necessary to fix any problems that may occur after the system is put into place and to improve its general dependability and performance.

6 Experimental result

The efficiency and dependability of the suggested "Theft intimation of the vehicle over SMS to owner who can stop the engine remotely" system are revealed by the experimental results. Key performance indicators such the success rate of remote engine shutdown, the accuracy of theft detection, and the reaction time for SMS notifications were assessed through a series of trials.

The system was tested in several simulated theft scenarios in order to evaluate the accuracy of theft detection. The outcomes showed a high accuracy rate, with the system detecting possible theft attempts and notifying the owner in more than 95% of cases. The technology proved to be reliable in identifying a range of questionable conduct, such as breaking into the car without authorization or tampering with the ignition system. By starting theft scenarios and timing how long it takes for the owner to receive an alert on their mobile device, the reaction time for SMS alerts was determined. The tests showed that the system responded quickly, sending SMS notifications as soon as it noticed questionable conduct. Owners were able to protect their vehicles right away because they often received alerts 5 to 10 seconds after the stolen attempt [19-21].

Additionally, by instructing the system via SMS to start the engine shutdown in the event of a theft simulation, the success rate of remote engine shutdown was assessed. In more than 90% of the instances, the system was able to carry out directives for remote engine shutdown, which essentially immobilised the car and stopped any more unauthorised use. The trials also took into account variables like false alarm rates and system reliability. During testing, there were very few instances of system malfunction or failure, indicating the system's high reliability. The system effectively distinguished between real theft attempts and false positives, as seen by the low false alarm rates. All things considered, the testing findings show how successful and dependable the suggested approach is at stopping car theft and safeguarding owner property [22-25]. The technology can inhibit theft and give car owners peace of mind, as seen by the high accuracy of theft detection, quick SMS alert response times, and successful remote engine shutdown commands. The outcomes confirm the system's usefulness and ability to improve vehicle security in real-world situations.

7 Conclusion

A significant development in automobile security technology is the installation of a strong car security system that allows theft notification to the owner via SMS and the ability to remotely disable the engine. This study provided a complete analysis of the suggested system, starting with the concept's introduction and concluding with a review of relevant literature and an investigation of related work. The design and development process, including the creation of a strong system architecture, the creation of a dynamic theft detection algorithm, and the improvement of theft prevention measures, were all covered in detail in the methodology section. In order to provide remote engine control and theft detection, the architecture of the proposed system integrates a number of hardware components, including actuators, microcontrollers, GSM modules, and sensors. The core of the system's functionality is the integration and connectivity of various hardware components. In addition to the hardware, the software development process concentrated on developing a user-friendly interface for remote communication, developing an algorithm for detecting theft in real time, and configuring microcontrollers to carry out system operations. With the help of this dual strategy, hardware and software components were seamlessly integrated to provide a coherent and efficient security solution.

The effectiveness and dependability of the system were assessed through experimentation, with an emphasis on parameters like the success rate of remote engine shutdown, the accuracy of theft detection, and the response time for SMS notifications. The outcomes showed how well the system could identify attempted thefts, with a high success rate in informing car owners by SMS in a timely manner. Furthermore, the system demonstrated a strong ability to carry out directives for remote engine shutdown, which effectively immobilised the car and prevented additional unauthorised use. These results confirm the usefulness and efficacy of the suggested solution in improving car security and giving owners peace of mind.

In summary, a major development in automobile security technology is the "Theft intimation of the vehicle over SMS to owner who can stop the engine remotely" system. The technology provides a dependable and efficient means of preventing theft and safeguarding vehicles by utilising a blend of hardware integration, software development, and thorough testing. Real-time theft detection and timely warning to owners are made possible by the seamless integration of sensors, microcontrollers, GSM modules, and actuators. This gives owners the power to take instant action to secure their vehicles. Additionally, by adding a layer of security and discouraging potential thieves, the ability to remotely stop the engine improves overall vehicle security. Subsequent research and development endeavours can concentrate on enhancing the system's hardware efficiency, optimising its algorithms, and broadening its compatibility with a more diverse array of vehicles. The suggested solution has the potential to completely transform automotive security and make driving safer for car owners everywhere with further invention and improvement.

References

1. H. Chen, Y. Chiang, F. Chang, H. Wang. *Toward Constant Exact Point Situating: Differential GPS In light of IGS Ultra Quick Product*. SICE Yearly Gathering, The Stupendous Lodging, Taipei, Taiwan, (2010)
2. A.M.J. Al-Hindawi, I. Talib. *Tentatively Assessment of GPS/GSM Based Framework Plan*. Dia. Elec. Fram., **2**, 2, (2012)
3. K. Maurya, M. Singh, N. Jain. *Continuous Vehicle Global positioning framework utilizing GSM and GPS Innovation An Hostile to burglary Global positioning framework*. World. Dia. Gad. Sof. Eng. Des., **1**, 3, 1103-1107.
4. V. Kulkarni, V. Babu. *Implanted shrewd vehicle security framework on face identification*. Int. J Com. Com. Techno., **3**, 1.
5. V. Ramya, B. Palaniappan, K. Karthick. *Implanted Regulator for Vehicle In-Front Deterrent Discovery and Lodge Wellbeing Ready Framework*. Glo. Dia. Sof. Eng. Dat. Innova., **4**, 2, (2012)
6. K. Tai Melody, C. Chieh Yang. *Public Chiao Tung College, Taiwan, "Front Vehicle Following Utilizing Scene Investigation*. Procedures of the IEEE Worldwide Gathering on Mechatronics and Computerization, (2005)
7. C. Peijiang, J. Xuehua. *Plan and Execution of Remote checking framework in view of GSM*, **42**, 167-175, (2008)
8. A. Alexe, R. Ezhilarasie. *Distributed computing Based Vehicle Following Data Frameworks*. Int. J. Cloth. Sci. Technol., **2**, 1, (2011)
9. R. Ramani, S. Selvaraju, S. Valarmathy, R. Thangam B. Rajasekaran. *Water-level screen for bore well and water tank based on GSM*. Worldwide Diary of designing science and innovation, Int. J. Environ. Sci. Technol., **4**, 10, (2012)
10. M.W. Aftab, S. Hussain, A. Husain, U.A. Khan, H. Kundi. *A Deep Reinforcement-Learning-Based Relay Selection for Underwater Sensors Network*. IEEE Internet Things J., **2023**, 1, 5-13, (2023)
11. R. Akila, J.B. Merin, A. Radhika, N.K. Behera. *Human Activity Recognition Using Ensemble Neural Networks and The Analysis of Multi-Environment Sensor Data Within Smart Environments*. J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl., **14**, 3, 218-229, (2023)

12. A.T. Ozyilmaz, E.I. Bayram. *Glucose-Sensitive Biosensor Design by Zinc Ferrite (ZnFe₂O₄) Nanoparticle-Modified Poly (o-toluidine) Film*. NESciences, **8**, 3, 202-213, (2023)
13. V. Ramya, B. Palaniappan, K. Karthick. *Implanted Regulator for Vehicle In-Front Obstruction Recognition and Lodge Wellbeing Ready Framework*. Glo. Dia. of Soft. Eng. Dat. Innova., **4**, 2, (2012)
14. K. Melody, C. Yang. *Front Vehicle Following Utilizing Scene Investigation*. Procedures of the IEEE Worldwide Meeting on Mechatronics and Robotization, (2005)
15. C. Peijiang, J. Xuehua. *Plan and Execution of Remote observing framework in light of GSM*, **42**, 167- 175, (2008)
16. A. Alexe, R. Ezhilarasie. *Distributed computing Based Vehicle Following Data Frameworks*. Int. J. Cloth. Sci. Technol., **2**, 1, (2011)
17. R. Ramani, S. Selvaraju, S. Valarmathy, R. Thangam B. Rajasekaran. *Water-level screen for bore well and water tank based on GSM*. Worldwide Diary of designing science and innovation. Int. J. Environ. Sci. Technol., **4**, 10, (2012)
18. H.W. Chen, Y.T. Chiang, F.R. Chang, H.S. Wang. *Toward real-time precise point positioning: Differential GPS based on IGS ultra rapid product*. In *Proceedings of SICE Annual Conference 2010*, 355-358, (2010)
19. A.M.J. Al-Hindawi, I. Talib. *Experimentally Evaluation of GPS/GSM Based System Design*. J. Electron. Syst., **2**, 2, (2012)
20. K. Maurya, M. Singh, N. Jain. *Real Time Vehicle Tracking System using GSM and GPS Technology- An Anti-theft Tracking System*. Int. J. Ele. Com. Sci. Eng., **1**, 3, 1103-1107, (2012)
21. **Aezeden Mohamed**, Macro-Micro Scale Observation of Cyclic Hardening and Softening and Precipitates Free Zone of Alloy C460, International Journal of Organization and Scientific Research, Vol. 3, Issue 6, pp. 34, 2013. <https://doi.org/10.9790/3021-03613439>
22. Rath, K. C., Muduli, K., Das, R. P., Ramasamy, A., **Aezeden Mohamed**. (2022). Disruptive Technology-Enabled Circular Economy for Improving the Sustainability of the Supply Chain: A Case of an Emerging Economy. pp. 335-351. 2022. IGI Global. <https://www.igi-global.com/gateway/chapter/302695>
23. Abdullah, M. I., Raya, L., Norazman, M. A. A., & Supriyadi, U. (2022). Covid-19 Patient Health Monitoring System Using IoT. 2022 IEEE 13th Control and System Graduate Research Colloquium, ICSGRC 2022 - Conference Proceedings, 155–158. <https://doi.org/10.1109/ICSGRC55096.2022.9845162>
24. Abdullah, M. I., Roobashini, D., & Alkawaz, M. H. (2021). Active monitoring of energy utilization in smart home appliances. ISCAIE 2021 - IEEE 11th Symposium on Computer Applications and Industrial Electronics, 245–249. <https://doi.org/10.1109/ISCAIE51753.2021.9431776>
25. Pragathi, B., and P. Ramu. "Authentication Technique for Safeguarding Privacy in Smart Grid Settings." *E3S Web of Conferences*. Vol. 540. EDP Sciences, 2024.