Remote Theft Alert With Car Engine Shutdown

Kuldeep Pande[1*], Ankita Tijare[2], Atish Peshattiwar[3], Swati Nitnaware[4]

[1*]Department of Electronics Engineering Yeshwantrao Chavan College of Engineering Nagpur, India, ycce.kuldeep@gmail.com
[2]Department of Electronics Engineering Yeshwantrao Chavan College of Engineering Nagpur, India, ankita.tijare@gmail.com
[3]Department of Electronics Engineering Yeshwantrao Chavan College of Engineering Nagpur, India, atishp32@gmail.com
[4]Department of Electronics Engineering Yeshwantrao Chavan College of Engineering Nagpur, India, swatitidke02@gmail.com

*Corresponding Author: Kuldeep Pande
*Department of Electronics Engineering Yeshwantrao Chavan College of Engineering Nagpur, India, ycce.kuldeep@gmail.com

ARTICLE INFO	ABSTRACT
	The Global System for Mobile Communication (GSM) and the Global Positioning System (GPS) are two innovative approaches to vehicle intrusion and theft control system design and development that are presented in this article. One of the unique components of the suggested system is its use of GSM technology. The vehicle's position is tracked using a GPS module called the Holux GR89, and analogue data is continually collected using Mercury switches. If there is an incursion, changes in the sensor readings will be noticed. The microcontroller continuously gathers sensor readings, and based on those readings, a decision is made regarding whether or not an intrusion has occurred. If an intrusion occurs, a message from a predefined set of messages is generated to the vehicle's owner, who then has the option to respond via SMS to lock the vehicle's gears or seize the engine from a distance. The vehicle's engine and gearbox are managed by a relay that interfaces with the microprocessor. A system prototype was constructed and evaluated. The outcomes were really promising and favourable.
	Keywords: GSM, Microcontroller, GPS, Car intrusion, Car theft, Sensor

I. INTRODUCTION

The project's goal is to notify the car's owner of any unauthorised entrance using wireless technology. To accomplish this, send the owner an SMS that is automatically generated[11]. One other benefit of this concept is that the owner can disable the vehicle's ignition by sending back the SMS. The need for car security systems is growing due to the rising crime rate. If someone tries to steal the automobile under this suggested system, the GSM modem is instructed to send an SMS via the microcontroller, which receives an interrupt through a switch mechanism attached to the system. The owner gets an SMS saying that someone has stolen his automobile. Then, in order to "stop the engine," he can send another SMS to the GSM modem. After the message is received by the GSM modem interfaced to the microcontroller, a mechanism that disables the vehicle's ignition and stops it is activated [4]. A light is used in the project to show if the engine is running or not [12]. As a result, the owner of the automobile may turn off the ignition from anywhere. The integration of a GPS system, which will provide the vehicle's precise position in terms of latitude and longitude, would improve this idea even more. In addition, this information may be texted to the owner, who can use it to pinpoint the precise location of the car on Google Maps [2], [9]. When utilising a microcontroller in conjunction with a relay [12], the vehicle's engine and gears are controlled. A system prototype was constructed and evaluated. The outcomes were really promising and favourable. Therefore, security and authentication are vital for the present and the future. There has been a lot of advancement in this area, and the majority of it is used in everyday life through things like weather forecasts, firearm detectors, heat detecting devices, and vehicle monitoring and tracking systems. This study describes a sophisticated and efficient GSM-based vehicle tracking and monitoring system.

II. LITERATURE SURVEY

Theft of vehicles is a global issue. Every year, the percentage of cars that are stolen or vandalised rises alarmingly. In Malaysia alone, for instance, statistics from 2004 indicate that 26,566 automobiles were

reported stolen; this is an approximate 33% increase over the same time the previous year. Customers will have to pay a higher premium for auto insurance as a result of this. Consequently, it might be said that the security mechanisms that the car manufacturer placed are insufficiently strong. A wireless car security system that uses mobile communication protocol is suggested as a solution to this issue [1].

The suggested system allows for control and communication between the user and a cellular phone using the short messaging services (SMS) protocol [3], [11]. Both a remote keyless entry system and an immobiliser are interfaced with the proposed system. If an intruder tampers, vandalises, or steals the automobile, the suggested system can notify the user via their mobile device. The alarm will sound simultaneously due to the activation of the immobiliser systems and the remote keyless entry system. The alarm sound will be replaced with a human voice produced by the system.

The user may also operate the car's door remotely with the help of the suggested technology. This system's effective communication coverage is dependent upon the coverage of the user's mobile phone. Both hardware and software components make up the suggested system. A microprocessor, an immobiliser, a GSM modem, a voice-activated alarm module, a cellular phone, a remote keyless entry (RKE) system, and an RKE system remote control are among the hardware components [7],[8],[10].

An interface for a programme controller is part of the software. The suggested system has been effectively conceived and constructed, as shown by the outcomes of simulations and real-world testing.

Fig. 1: Trying to steal the car

III. METHODOLOGY

The approach used in the suggested model is that a microcontroller is being used to establish an interface between Mercury switches, a GPS module, and a GSM module. Serial communication is used to exchange data between the microcontroller and other system components. The microprocessor continually receives data from the GPS module and mercury switches, and it makes decisions based on the information gathered [10], [14]. When an intrusion occurs, the microcontroller will send out a message to the car's owner or to a predetermined phone number, indicating the vehicle's present position and the type of entry—whether it was through the trunk, doors, or bonnet. Upon receiving the message, the user will be able to initiate an action from a distance, such as locking the doors, taking control of the engine, or cutting the supply line. By using a GSM module, the owner's message will be transmitted to the microcontroller. The microcontroller will then use the received message to switch a relay, which will perform an action such as locking the doors, stopping the engine, or cutting the supply line.

Features of Proposed Modal:
1. Each time the messaged would be send to the owner.
2. The system is dynamic and automatic, reduces involvement of human resource in the process; thus reducing cost and probability of human consequently increasing efficiency in overall process.
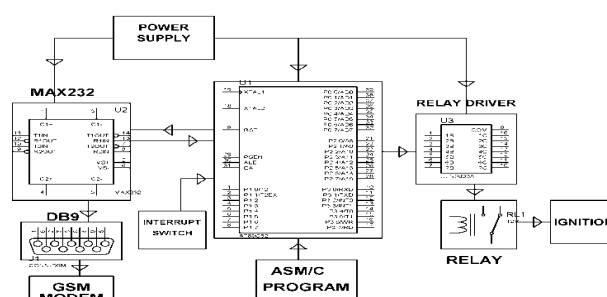
IV. PROPOSED BLOCK DIAGRAM

Fig. 2: Block Diagram

A GSM is a component of the system that acts as a bridge between the system as a whole and the outside world (vehicle owners) [4], [5]. It is in charge of texting the owner of the vehicle and taking calls for system activation and deactivation. Dual Tone Multi-Frequency (DTMF) decoder IC receives its frequency output and transforms it into digital voltage levels of ones and zeros. DTMF decoder digital voltage values are now sent into the integrated circuit of the microcontroller. A programmed programme that is kept in its Read Only Memory (ROM) controls the micro controller, which serves as the design's brains and control circuit. The controller coordinates the system's functioning in the following ways, following the guidelines in the written programme:

I.   When the system is in operation, it keeps an eye on the trunk and the car doors to see whether someone is opening them.
II.   Uses the actuator to cut the ignition line from the battery supply, demobilising the vehicle.
III.   Texts the owner of the vehicle to let them know where the attempt is coming from, and then sounds the alarm to serve as a warning. But,
IV.   The microcontroller turns off all outputs and sensor inputs while the system is not in use.

Working:

1. Firstly, we have to check the availability of network in the GSM and if the modem is in range, when a call is send the buzzer present in the circuit will ring.
2. The circuit would be fitted inside the vehicle near the dash board and one connection would be at the relay where the ignition of engine gets on and off.
3. As soon as any person enters into that vehicle the system is on and a predefined message "WELCOME" and "ENTER THE PASSWORD" would be displayed.
4. The person who wants to drive that vehicle has to enter the correct password.
5. If the password is correct then the vehicle will get ignition and will be in driving condition.
6. But if the entered password is wrong, message would be "WRONG PASSWORD ".
7. The relay of the engine would not start, the vehicle would not get ignition and it would be in off condition.
8. The message that is stored in the microcontroller would be send to the owner whose mobile number is stored in microcontroller via GSM modem that "YOUR VEHICLE IS ACTIVE".
9. Thus the owner would know the vehicle is stolen and it would help to save his vehicle.
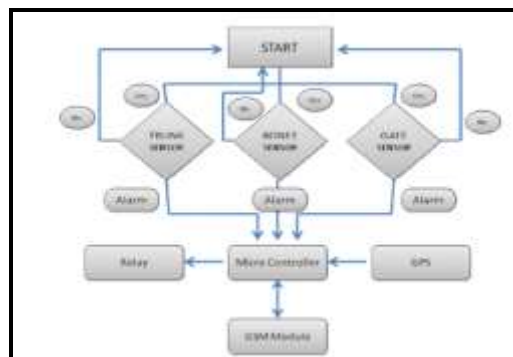
V. IMPLEMENTATION

Fig 3: Vehicle Module

The microcontroller is being programmed using assembly language. The microcontroller receives information about intrusion, including the numbers to whom messages should be sent, the content of the messages, and what should happen in response when the car's owner sends an SMS. The signals from the mercury switches and the message from the car's owner are what the microcontroller uses to make its choice.
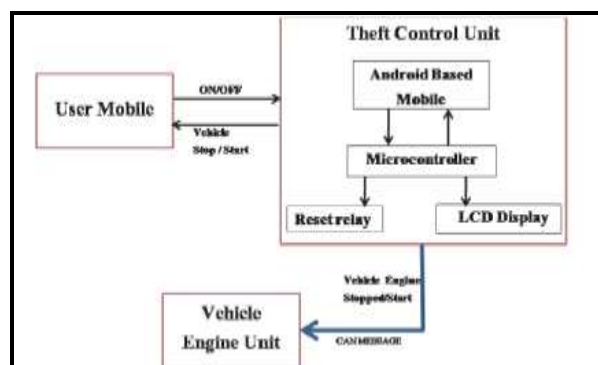

Fig 4: Flow chart for vehicle control

Driver security identification is achieved by the use of a password protection module. Password protection is linked to the PIC so that it may track user information by comparing the password with the information already recorded in the microcontroller's built-in memory. When the user enters the password in the password protection, the engine will start. The processor is connected to the ignition unit, the GSM, the password protection, and the end user, who will be the owner and whose cell number is stored in the data, based on the most recent technological advancements. Once the password has been entered into the password security system, the engine will start. If the password is entered incorrectly, the GPS position is sent to the owner's mobile device. We can halt the automobile and lock all of the doors if someone not authorised is attempting to drive it.

VI.   RESULTS

An innovative and economical method of vehicle security has been suggested in this research. To prevent criminals from reaching it, it might be hiddenly concealed within the car. Technology such as GPS and GSM has been used. It sends an SMS alert signal to the car's owner, and the SMS might jam the vehicle. The system then continues to deliver location updates via SMS every 30 seconds until it is turned off. The suggested method differs greatly from the current car entry and theft control systems, which are either exceedingly costly or ineffectual when viewed from a distance. It has a suitable design, is affordable, and is dependable. In the future, all automobiles might have this technology installed, and police numbers could be added for notice of intrusions. In order to improve even further, sensors with higher performance levels can be used to raise the system's efficiency and performance level.
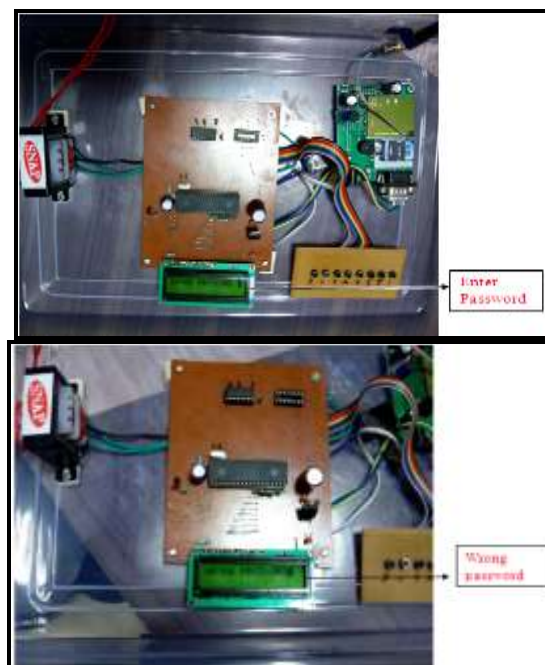

Fig 5: Circuit Module

VII. ADVANTAGE

It should go without saying that using a GSM-based car security system promotes the use of cutting-edge wireless technology, which is why it is less well-known in India. In addition, they provide the following further advantages:
• Enhanced Security: Using this method, we may attempt to rescue our vehicle from any location in the world. This system provides us with information on who is sitting in our car, whether the front doors are open or closed, whether the car is vibrating, who is attempting to start the automobile, and who is pushing or rotating the car. We may obtain information on all parameters, including detected parameters, if anything unusual occurs. Therefore, compared to the basic auto security systems that are now on the Indian market, this system is more sophisticated and practical.
• Improved Customer Service: Because this is far less expensive than a car, it not only offers better customer service but also benefits financially.

VIII. CONCLUSIONS / FUTURE SCOPE

Modern technologies like GPS and GSM are employed in this project's GPS car theft tracking and identification control system to pinpoint the precise location of the stolen vehicle and notify the user,

enabling them to stop the vehicle by sending an SMS. Users may quickly determine the whereabouts of the stolen car, saving both time and money. Furthermore, the user may simply regulate the vehicle's direction, steering moment, fuel injection, acceleration, and motor starting by giving the correct control signals, allowing for an effective implementation of this procedure.

Any car can use the proposed system theft control unit as one of its electronic control units, and it will add another node to the CAN Bus network. Since the system was created utilising mobile and GSM technology, which is run by sending and receiving messages, it is a less expensive vehicle tracking control system that can be installed in any kind of vehicle. By interpreting the received message, the ignition system of the car may be controlled.

IX. REFERENCES

1. Z. M. Subekti, S. Suhadi, R. Ramdani, A. Suroso, R. B. Agung and M. Surur, "Internet of Things-based Early Warning Car Theft Security System Using Smartphones," 2021 Sixth International Conference on Informatics and Computing (ICIC), Jakarta, Indonesia, 2021, pp. 1-5, doi: 10.1109/ICIC54025.2021.9632901.
2. S. Nairouz, R. Dashti, Z. B. Abbas, A. Alajmi, H. Almutairi and M. Rashdan, "Vehicle Anti-Theft Security System with GPS Tracking and Remote Engine Locking," *2023 5th International Conference on Bio-engineering for Smart Technologies (BioSMART)*, Paris, France, 2023, pp. 1-5, doi: 10.1109/BioSMART58455.2023.10162051.
3. K. Lappanitchayakul, "Anti-theft device for car: Alert system using radio wave," *2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, Shanghai, China, 2019, pp. 351-355, doi: 10.1109/ICIIBMS46890.2019.8991531.
4. M. Saini and S. Khan, "GSM Based Fuel Theft Detection," *2021 1st International Conference on Power Electronics and Energy (ICPEE)*, Bhubaneswar, India, 2021, pp. 1-6, doi: 10.1109/ICPEE50452.2021.9358644.
5. S. Ruengittinun, J. Paisalwongcharoen and C. Watcharajindasakul, "IoT solution for bad habit of car security," *2017 10th International Conference on Ubi-media Computing and Workshops (Ubi-Media)*, Pattaya, Thailand, 2017, pp. 1-4, doi: 10.1109/UMEDIA.2017.8074145.
6. Zhixiong Liu, "A new embedded car theft detection system," *Second International Conference on Embedded Software and Systems (ICESS'05)*, Xi'an, China, 2005, pp. 6 pp.-, doi: 10.1109/ICESS.2005.6.
7. R. Shukla, D. K and N. M, "Vehicle Theft Detection and Driver Identification System Using IoT," *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, Chennai, India, 2022, pp. 1-6, doi: 10.1109/ICPECTS56089.2022.10047626.
8. S. LV, L. Wu, Z. Li, Q. Xu and X. Zhou, "Intelligent Car Security System Based on Fingerprint Identification and Internet of Things," *2021 13th International Conference on Computational Intelligence and Communication Networks (CICN)*, Lima, Peru, 2021, pp. 183-187, doi: 10.1109/CICN51697.2021.9574696.
9. M. O. Hasanuddin, R. Augeetiansyah, G. A. Prakoso and B. R. Hermanto, "Design and Implementation of IMU, BLE Proximity and GPS-Based Theft Detection System," *2022 12th International Conference on System Engineering and Technology (ICSET)*, Bandung, Indonesia, 2022, pp. 1-5, doi: 10.1109/ICSET57543.2022.10010979.
10. P. Bagavathy, R. Dhaya and T. Devakumar, "Real time car theft decline system using ARM processor," *3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011)*, Bangalore, 2011, pp. 101-105, doi: 10.1049/ic.2011.0059.
11. K. J. Prakash, K. P. K. Reddy, K. S. K. Goud and S. T. Reddy, "Vehicle Theft Intimation over SMS and Remote Control of its Engine," *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India, 2021, pp. 1496-1501, doi: 10.1109/ICCES51350.2021.9489106.
a. Krasovsky, S. Vasyukov and I. Murzin, "The Use of Power Line Communication Technology for Electronic Relays of Car Alarms," *2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, Sochi, Russia, 2019, pp. 1-5, doi: 10.1109/ICIEAM.2019.8743066.
12. S. Malathi and J. Preethi, "A Review on RFID based Image recognition for Driver Eligibility and Car Security," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2019, pp. 112-117, doi: 10.1109/I-SMAC47947.2019.9032476.
13. H. Guo *et al.*, "An Automotive Security System for Anti-theft," *2009 Eighth International Conference on Networks*, Gosier, France, 2009, pp. 421-426, doi: 10.1109/ICN.2009.28.
14. L. Lin, W. Xinghao, Z. Yongxin and Q. Jifan, "A Car Security System Based on Internet +GPS," *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, Chengdu, China, 2019, pp. 291-294, doi: 10.1109/ICAIBD.2019.8836969.