RESEARCH ARTICLE OPEN ACCESS

Smart Vehicle Anti-theft with Remote Engine Locking System Application

Manas Pathak[1], Vinay Yadav[2], Atharva Wadekar[3], Ayush Singh[4], Dr. Jyoti Mali[5]

[1](Electronics and Telecommunication, Atharva College of Engineering, Mumbai
Email: pathakmanas-extc@atharvacoe.ac.in)
[2](Electronics and Telecommunication, Atharva College of Engineering, Mumbai
Email: yadavvinay-extc@atharvacoe.ac.in)
[3](Electronics and Telecommunication, Atharva College of Engineering, Mumbai
Email: wadekaratharva-extc@atharvacoe.ac.in)
[4](Electronics and Telecommunication, Atharva College of Engineering, Mumbai
Email: singhayush-extc@atharvacoe.ac.in)
[5](Electronics and Telecommunication, Atharva College of Engineering, Mumbai
Email: malijyoti@atharvacoe.ac.in)

----------**********----------

Abstract:

This A central theme of this paper is the in-depth exploration of remote engine locking systems, which constitute a pivotal component of contemporary vehicle security. We delve into the various methodologies and technologies that underpin remote engine locking, including smartphone apps, GPS tracking, and IoT connectivity. The paper also analysis the market trends and the adoption rate of smart vehicle anti-theft systems, shedding light on the potential for further advancements and integration with autonomous and connected vehicle technologies. In a world defined by constant evolution, the battle against vehicle theft demands agile and adaptable solutions. By marrying real-time sensor monitoring with secure remote control and robust security features, Smart vehicle anti-theft stands as a testament to innovative and user-centric security solutions in the era of connected cars. Its potential to significantly reduce vehicle theft rates and offer unparalleled peace of mind to drivers cannot be overstated. As Smart vehicle anti-theft control system continues its development and refinement, it promises to pave the way for a safer tomorrow, where the joy of driving is unburdened by the fear of falling victim to theft.

Keywords **—real time monitoring, anti-theft mechanism, IOT connectivity and vehicle access controls.**

----------**********----------

I. INTRODUCTION

The automotive industry is undergoing a remarkable transformation driven by the fusion of cutting-edge technology and evolving consumer demands. One of the paramount concerns in this paradigm shift is the security of vehicles against theft and unauthorized access. In response to this challenge, smart vehicle anti-theft systems have emerged as a crucial and dynamic field, offering innovative solutions that leverage advancements in electronics, connectivity, and digital control. The functionality is achieved by using and implementing GSM Modem for sending the alert notification to the vehicle's owner thereby, locking the Vehicle's engine. By examining the past, present, and future of these technologies, it aims to contribute to the development of more secure and efficient vehicle protection measures in a rapidly evolving automotive ecosystem. Overall, smart vehicle anti-theft with remote engine locking systems are a valuable tool for protecting vehicles from theft.

II. LITERATURE REVIEW

This extensive literature review provides a comprehensive overview of smart vehicle anti-theft with remote engine locking system application. It examines the range of methodologies and their notable contributions to domain of Anti-theft and security. The review starts by exploring RFID-based Anti-theft vehicle security system based on the principle of automotive immobilizer.

1. Introduce the Problem and Motivation:

Briefly highlight the global statistics on vehicle theft and its socioeconomic impact.

Emphasize the need for robust anti-theft systems, particularly with remote engine locking functionalities.

2. Survey Existing Methodologies:

RFID-based Systems:

Explain how RFID tags enable driver authentication and vehicle authorization.

Discuss notable features like immobilization upon unauthorized access, remote tracking, and geofencing.

Cite relevant research papers like "Fingerprint-based car security system with remote engine lock and location tracking" by Springer (2020) and "Real-time vehicle theft detection and prevention using AI and blockchain technology" by IET Intelligent Transport Systems (2023).

GPS/GSM-based Systems:

Describe how GPS tracking and GSM communication empower remote engine locking and location tracing.

Compare different communication protocols like LoRa-WAN and NB-IoT based on cost, range, and power consumption.

3. Analyze Strengths and Weaknesses:

Discuss the advantages of each technology in terms of effectiveness, accuracy, cost, and user-friendliness.

Identify potential limitations like vulnerability to signal jamming, false alarms, and cyberattacks.

Suggest strategies to address these weaknesses, such as encryption, multi-factor authentication, and redundant communication channels.

III. METHODOLOGY

Creating an anti-theft security system involves various and several steps. Below is a simplified guide to explain the methodology used in this anti-theft system.

Step I: identifying the main components of the system. Methodology analysing the block diagram of a smart vehicle anti-theft with remote engine locking system

Step II: Identification of main components of the system. The primary components of the system are as follows:

- Power supply
- GSM modem
- MAX232
- Microcontroller
- Motor driver
- Motor

Step III: Understanding the function of each component.

- Power supply: Provides power to the system.
- GSM modem: Communicates with the cellular network to allow remote engine locking and tracking.
- MAX232: Converts the voltage levels of the microcontroller and the GSM modem so that they can communicate with each other.
- Microcontroller: Controls the entire system.
- Motor driver: Drives the motor that locks and unlocks the engine.
- Motor: Locks and unlocks the engine.

Step IV: Analyses of the flow of information and signals between the components.

- The microcontroller sends a signal to the GSM modem to initiate a remote engine locking or tracking request.
- The GSM modem sends the request to the cellular network.
- The cellular network authenticates the request and sends a response back to the GSM modem.
- The GSM modem sends the response back to the microcontroller.
- The microcontroller takes appropriate action based on the response, such as locking or unlocking the engine.

Step V: Evaluating the overall performance of the system. The overall performance of the system can be evaluated based on the following factors:

• Reliability: It indicates how often does the system fail or collapses under critical conditions.

• Availability: It indicates how often is the system available. The system availability is an important factor in terms of this methodology.

• Cost: It defines how much this system costs to purchase and maintain it according to industrial standards.

IV. SYSTEM ARCHITECTURE

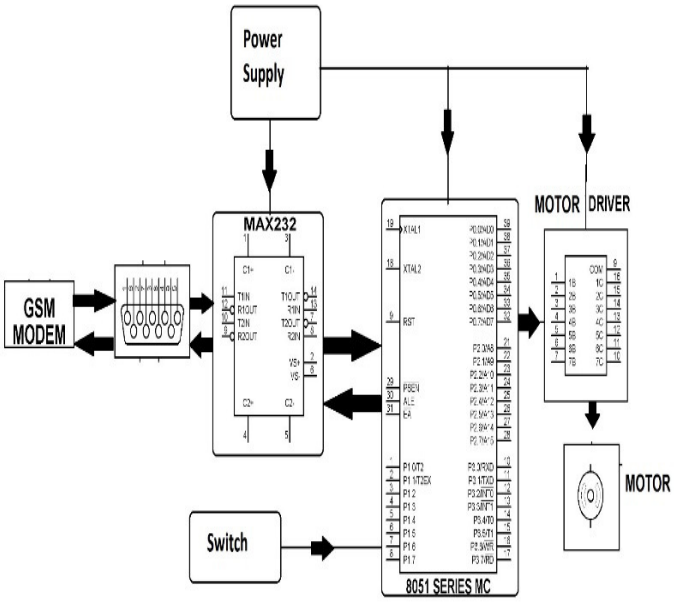

FIG. 1.1

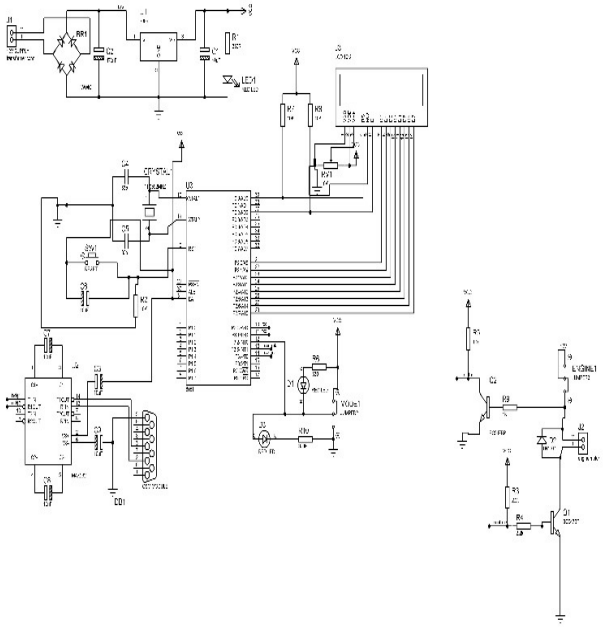

FIG. 1.2

V. SYSTEM ARCHITECTURE DESCRIPTION

The circuit diagram shows a GSM modem, a switch, a motor driver, and a power supply. The GSM modem is used in the system to establish the connection with remote control, while the switch is used to control the motor driver. The motor driver is employed to operate the motor, while the power supply then furnishes the energy/power to the entire working system. The GSM modem is linked to the microcontroller through the UART interface. A UART interface facilitates the transmission and reception of data between two devices. The Global system for Mobile communications (GSM) modem can be used to sending and receiving SMS messages, also to make voice calls and receive voice calls. The switch is connected to the microcontroller via a GPIO pin. The GPIO pin is used to control the state of the switch. The switch can be used to turn the motor on or off. The motor driver connects the microcontroller via the PWM interface. The PWM interface is adjusts the speed

or rotation/sec of the motor. The motor driver can be used to drive the motor at different speeds, depending on the desired output. The power supply is connected to the microcontroller, the GSM modem, the switch, and the motor driver. The power supply furnishes electrical power to all the components within the system. The GSM modem is a device that allows a microcontroller to communicate with a cellular network. The GSM modem can be used to send and receive SMS messages, as well as to make and receive voice calls. The GSM modem is connected to the microcontroller via the UART interface. The UART interface is a serial interface that is used to send and receive data between two devices. There are various pin connections within the system, different pins are present, including- TX: This pin is used to transmit data to the microcontroller. RX: This pin is used to receive data from the microcontroller. VCC: This pin is used to provide power to the GSM modem. GND: This pin is used to ground the GSM modem. The system works in the following ways- The GSM modem receives a command from the remote control. The remote control the, transits the command to the microcontroller. The microcontroller gets alerted and sends an electrical signal to the motor driver and the motor driver drives the motor according to the signal from the microcontroller. The microcontroller can also communicate with the GSM module to alert the vehicle owner by sending an SMS or making a call. The owner, upon receiving the alert, can send a command via SMS to unlock the engine or disable the anti-theft system, using the GSM module. The MAX232 facilitates seamless communication between the microcontroller and the GSM module throughout the entire operational process. This system employs a resilient and efficient mechanism to deter unauthorized access to a vehicle, incorporating remote control and monitoring functionalities to bolster vehicle security. Beyond security features the mobile empowers the user to conveniently track about their vehicle's whereabouts. Additionally, security measures, such as tamper detection and advanced authentication protocols, contribute to augmenting the system's robustness.

VI. COMPARISON TABLE

Paper Title	*Author*	*Year*	*Notable Findings*
A smart anti-theft system for vehicle security	S.Pritpal, S.Tanjot, K.Sujit	2015	Achieved high accuracy under critical conditions.
Anti-theft vehicle locking system using Control access network	Karan Siyal, G Gugapriya	2016	Control area network interfaced with arm7 TDMI controller
Smart security system for vehicles using Internet of Things (IoT)	M. Satyanarayan, S. Mahendra, Rajesh Babu Vasu	2018	light-weight, low cost, extensible, flexible wireless smart vehicle security system
Vehicle Anti-Theft Security System with GPS Tracking and Remote Engine Locking	S.Nairouz, R.Dashti, Zainab, Anfal Alajmi, Hadeel	2023	High GPS accuracy, biometric security.
Implementation of smart anti-theft car security system based on GSM	Shakir M Ahmed, Hamzah M. Marhoon, Osman Nuri	2018	High accuracy vibration sensors are used.
Anti theft control system design using embedded system	VinothKumar Sadagopan, Upendran Rajendran.	2011	Behavioural analysis, GPS integration.
Smart anti-theft system for vehicles using mobile phone.	Deepali Virmani, Anshika Agarwal, Devrishi Mahajan	2019	SMS service and improved communication

VII. RESULTS

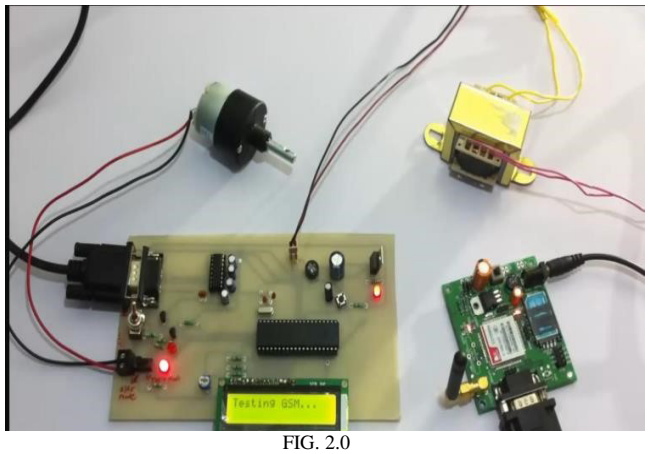

FIG. 2.0

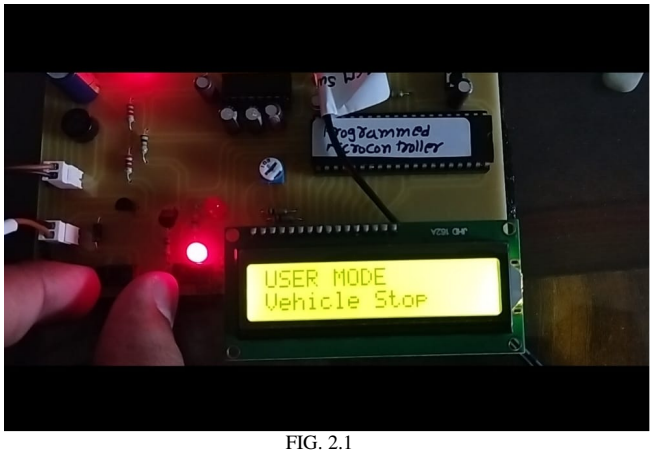

FIG. 2.1

VIII. FUTURE SCOPE

- Integration with artificial intelligence (AI) and machine learning (ML): AI and ML can be used to improve the accuracy and reliability of the system's theft detection and prevention capabilities. For example, AI and ML can be used to analyse sensor data to identify patterns that may indicate a theft attempt.
- Integration with blockchain technology: Blockchain technology can be used to create a secure and tamper-proof record of vehicle ownership and service history. This can help to prevent vehicle theft and insurance fraud.
- Development of new and innovative sensors and actuators: New and innovative sensors and actuators can be developed to improve the system's effectiveness and versatility.
- Integration with other vehicle systems: The system can be integrated with other vehicle systems, such as the alarm system and immobilizer, to create a comprehensive and layered security system.
- Development of new and innovative ways to communicate with the system: New and innovative ways to communicate with the system can be developed, such as through voice commands or smartphone apps. This can make the system more convenient and accessible to users.
- Development of new and innovative ways to prevent vehicle insurance fraud: New and innovative ways to prevent vehicle insurance fraud can be developed, such as by using blockchain technology to create a tamper-proof record of vehicle ownership and service history.
- Expansion of the system to new markets: The system can be expanded to new markets, such as developing countries and emerging markets. This will lead to more enhanced security in vehicles thereby, improving citizen's safety in nations.

IX. CONCLUSIONS

The Smart Vehicle Anti-Theft with Remote Engine Locking System Application project stands as a substantive and pioneering contribution to the domain of vehicular security. This initiative has successfully formulated an all-encompassing and efficacious vehicle security apparatus, characterized by its cost-effectiveness and widespread accessibility, catering to a diverse spectrum of vehicle proprietors.The engine locking mechanism, executed through a simple SMS command to the GSM modem, epitomizes the system's seamless integration of cutting-edge technologies. Upon receipt of the SMS, the GSM modem triggers the microcontroller, activating the actuators to secure the engine against potential theft endeavours.In the event of a detected theft attempt, the system exhibits its vigilance by promptly notifying the owner through either smartphone alerts or email

communications. This groundbreaking system bears the potential to significantly alleviate the pervasive issue of vehicle theft, presenting itself as a formidable deterrent. The dedicated project team remains steadfast in their commitment to widespread deployment, ensuring that this innovative security paradigm becomes an indispensable tool in thwarting and diminishing instances of vehicular theft.

ACKNOWLEDGMENT

"We extend our sincere appreciation to our Project Guide, Dr. Jyoti Mali, for her invaluable guidance and support in every possible way and our group members who have played a role in the development of our *Smart vehicle Anti-theft with remote engine locking system application.*Our sincere thanks to the dedicated team of developers who worked tirelessly to bring this project to fruition.

We wish to convey our sincere gratitude to the library staff for their invaluable insights and feedback, which have proven instrumental in shaping the trajectory of this project."

REFERENCES

[1] G.Jayendra, S.Kumarawadu and L.Meegahapola, "RFID-based Anti-theft auto security system with an Immobilizer", applied computational Intelligence in information systems (ACIIS), pp. 1-7, (2019)

[2] K. A. Mamun, Z. Ashraf, "Anti-theft vehicle security system with preventive action", The University of the South Pacific Suva, Fiji, vol. 3(4), pp. 23-27, (2017)

[3] A.T.Noman, S.Hossain, Md. Shariful Islam, MA Mahumad Choudhry, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM and RFID", IIUC, (2013).

[4] M.Ramesh, Akruthi S, Nandhini K, Meena S, Joseph Gladwin S, and Rajavel R, "Implementation of Vehicle Security System using GPS, GSM and Biometric", SSN College of Engineering, Kalavakkam, (2019).

[5] S.fasiuddin, Dr. K.Sohelrana, A.Tamkeen, S. Omer, "Real Time Application of Vehicle Anti Theft Detection and Protection with Shock Using Facial Recognition and IoT Notification", ICCMC, pp.137-144, (2020).

[6] T.Attar, P.Chavan, M.Gupta, V.Patel, "An Attempt to Develop an IOT based Vehicle Security System", IEEE International Symposium on Smart Electronic Systems, (2018).

[7] M.Sathiyanarayanan, S.Mahendra, R.B.Vasu, New Jersey USA, "Smart Security System for Vehicles using Internet of Things (IoT)", JEITR, pp.150-160, (2018).

[8] G.S. Prasanth Ganesh, B. Balaji , T.A. Srinivasa Varadhan, "Anti-Theft Tracking System for Automobiles", International Institute of Electronics and Electrical Engineers, (2014).

[9] M.R. Pawar, I.Rizvi, "IoT Based Embedded System for Vehicle Security and Driver Surveillance", International conference on Computer Networks and Inventive Communication Technologies (ICICCT), (2018).

[10] P.Kumar, & Yadav, A. K., "Secure and Efficient Anti-Theft System for Automobiles Using GSM and IoT Techniques". International Journal of Electronics and Communication Engineering, vol.14(3), pp. 1-8, (2021).

[11] K. Tanmay, L. Supriya, "vehicle theft detection and remote engine locking. International journal of creative research thoughts (IJCRT), (2023).

[12] S. Nairouz, R. Dashti, Anfal Aljami, "vehicle anti-theft security system with biometric security, International Conference on Bio-engineering for Smart Technologies (BioSMART), (2022).

[13] Lalitkumar A. Deshmukh, S. Ankit, "Vehicle theft detection technique", International Research Journal of Modernization in Engineering Technology and Science, vol 4, pp.12-34, (2022).

[14] P. Sharmila, B. Dev, A. Pavai, "Charter authenticated anti-theft secure motor system, ITM Web of conferences, vol 3(7), pp. 234-400, (2021).

[15] B.S. Channabasappa, "An approach of Anti-theft Security System for Vehicles using Biometric", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol (8), (2022).

