



ANTI- THEFT LOCKING SYSTEM

¹Dr. B. Tharani, ²R. Bhumisvara, ³M. Deepika, ⁴T. V. Dhinesh, ⁵R. Karthikeyan,

¹Associate Professor, ^{2, 3, 4, 5}Student,

¹Electrical and Electronics Engineering,

¹Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

Abstract: An IoT-based vehicle theft detection and remote engine locking system using GSM (Global System for Mobile Communication) technology that enables you to use the controlling mechanism technique and assists users in identifying the vehicle in theft mode. These days, there are a ton of cars being stolen. It's a big problem because it's harder to keep cars safe and crime rates are rising. Criminals are becoming smarter and have reached the stage of applications present against the vehicles safety system. Vehicle theft has become a considerable issue which should be traced and prevented. The new system solves many problems and is affordable. Also, the proposed system reducing complications by making use of some high-priced products like ignition key, microcontroller. We add a feature that allows controlling mechanisms to remotely lock the engine of the vehicle and prevent theft to the proposed method. In proposed technique, user can start/stop the vehicle either by using the bylnk application, which tracks exact location of the vehicle using the application. A fantastic automobile anti-theft system is the subject of this project. To locate the vehicle and verify the owner's identity, it makes use of the Global Positioning System (GPS), the Global System for Mobile Communication (GSM), and Android technologies (such as fingerprints).

Keywords--- BYLNK Application; IOT; GSM; GPS; Controller

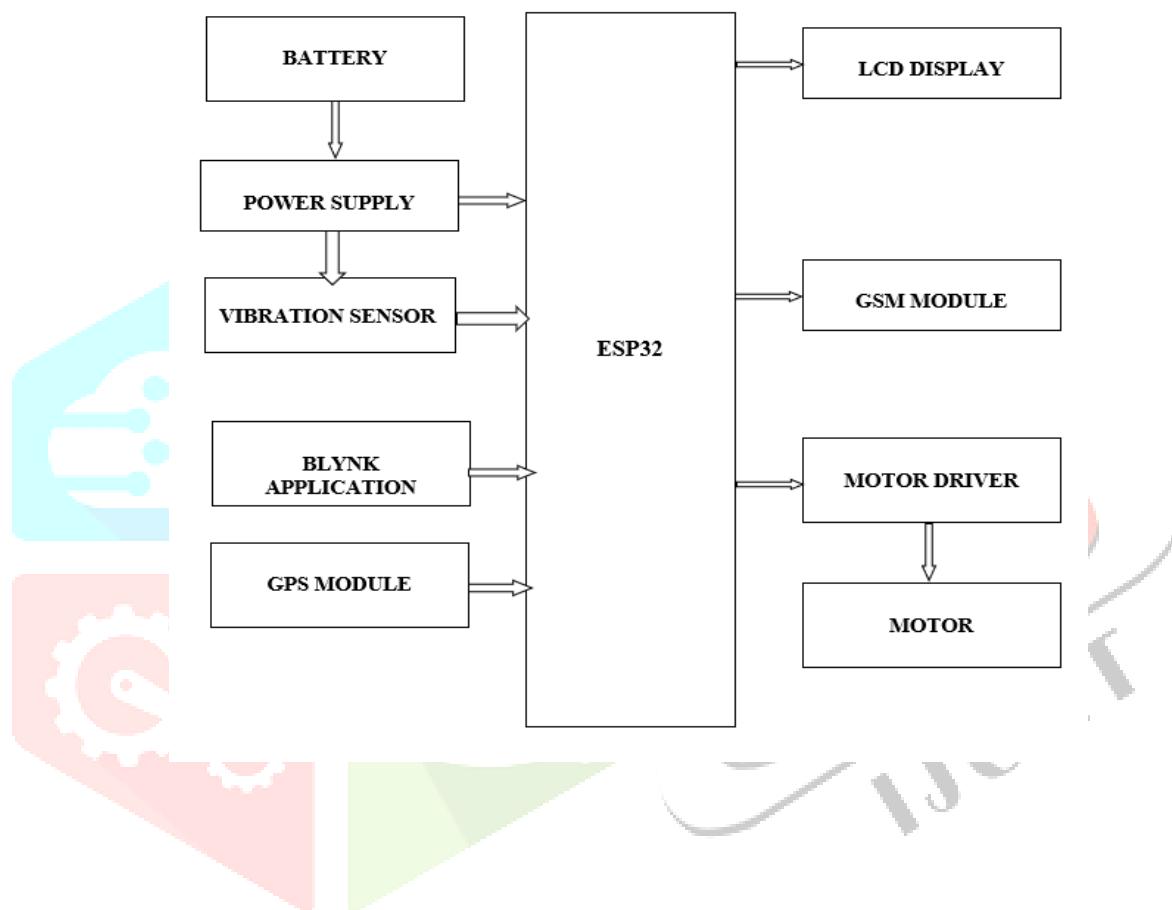
I. INTRODUCTION

Theft of automobiles has developed into a significant issue that is currently affecting people all over the world. The issue of vehicle theft has increased rapidly, mostly at parks. We need a theft alert system that helps vehicle owners stay on top of security to prevent theft and quickly catch anyone attempting to steal or damage our vehicles. GPS (Global Positioning System) and GSM (Global System for Mobile), which are in the vehicle to communicate with the owner's mobile phone, were used in the theft alert system. In GSM technology, SMS or phone calls can be used to communicate, but we prefer SMS (between the owner's mobile phone and GSM). It's like when your car sends you a text message to let you know everything that's going on with it. As a result, you'll be aware of any unusual activity with your vehicle right away. The GPS technology is used here to provide the exact location of vehicle to the vehicle's owner. It means that if someone tries to steal our vehicles without permission, we can use GPS technology to quickly find out where the theft is happening and catch the thief easily. In this system we are going to use two keys to open the vehicle lock, one is the owner's key and other is direct key. The owner uses the owner key, while an unauthorized person uses the direct key. If someone tries to use the key without permission, an alarm goes off and makes a beeping sound to let you know a thief is detected. A warning SMS is sent simultaneously to the registered mobile number of the vehicle's owner by GSM. The owner of the vehicle then sent a message to remotely lock the engine; after that, the engine shuts off and the motor cannot start without the password's permission. An IOT-based vehicle theft detection and remote engine locking system aids in deterring thieves from stealing automobiles in this way.

II. PROPOSED METHOD

We are introducing an advanced technology to tackle vehicle theft. In this system we are going to use a BLYNK app to control the ignition of the vehicle and also to track the location the vehicle. We also implemented a 4-pin keypad unlock system to start the ignition. When the pin entered is wrong a notification through BLYNK app.

III. BLOCK DIAGRAM



The block diagram represents an anti-theft locking system for vehicles using the ESP32 microcontroller. A 12V rechargeable battery provides power to the system, regulated through a power supply circuit. At the core of the system is the ESP32, which manages all components and controls system operations. The GPS module continuously tracks the vehicle's location and sends the data to the ESP32. This location data can be accessed through the Blynk application, a mobile-based platform that allows the vehicle owner to monitor and control the system remotely via Wi-Fi.

To enhance local feedback, an LCD display is included to show system status or alerts. A GSM module is used to send SMS notifications or make calls to the owner in case of suspicious activity. The motor driver, controlled by the ESP32, operates a motor that simulates the vehicle's locking mechanism—enabling or disabling access as needed.

An important security enhancement is the inclusion of a vibration sensor connected to the ESP32. This sensor detects any unusual movement or force applied to the vehicle, such as an attempted break-in or tampering. When vibration is detected, the ESP32 processes this signal and takes immediate action. It can lock the vehicle using the motor driver, trigger alerts through the GSM module, and send a real-time notification to the owner's smartphone via the Blynk app.

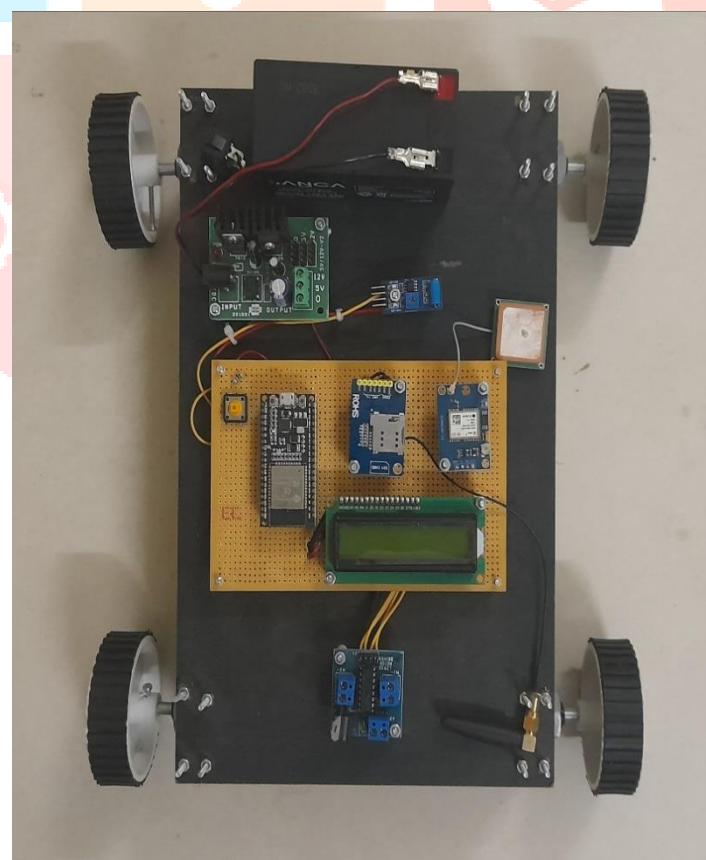
IV. WORKING

The anti-theft locking system operates through the coordination of several hardware modules controlled by the ESP32 microcontroller. When the system is powered on using a 12V battery, the ESP32 becomes the central unit managing inputs and outputs. Under normal conditions, the vehicle remains in an unlocked state. However, when unauthorized activity is detected, the system triggers security measures. A key role is played by the vibration sensor, which constantly monitors for physical disturbances or shocks to the vehicle. If any vibration beyond the normal threshold is sensed—indicating possible tampering—the sensor sends a signal to the ESP32.

Upon receiving this input, the ESP32 immediately activates the motor driver, which controls the motor responsible for locking the vehicle's engine or doors. At the same time, a GSM module connected to the controller sends an alert message or call to the owner's phone, informing them about the unusual activity. The GPS module continuously tracks the vehicle's location, and this information is sent in real time to the owner via the Blynk mobile app, which interfaces with the ESP32 over a Wi-Fi connection. The app also allows the user to monitor status and issue manual control commands, such as locking or unlocking the system.

Additionally, an LCD display provides on-vehicle feedback by displaying relevant alerts or operational data. Together, these modules work in synchronization to detect threats, notify the owner, and respond with immediate locking mechanisms—ensuring that any unauthorized access is quickly identified and neutralized.

V. HARDWARE IMPLEMENTATION



VI. RESULT

The anti-theft locking system using the Blynk application enhances vehicle security through IoT-based remote control. It allows users to lock or unlock the vehicle via a smartphone in real time. The system integrates sensors to detect unauthorized access and triggers alerts on the Blynk app. It provides user-friendly control, improves safety, and ensures rapid response. This project demonstrates the effective use of IoT for modern security solutions.

REFERENCES

- [1] Saad and U. Weinmann, —Automotive software engineering and concepts, || GI. Jahrestagung. vol. 34, pp. 318 – 319, 2003.
- [2] E. Nickel, —IBM automotive software foundry, || in Proc. Conf. Comput. Sci. Autom. Ind., Frankfurt, Germany, 2003.
- [3] M.Wolf, A.Weimerskirch, and T. Wollinger, —State of theart: Embedding security in vehicles, || EURASIP J. Embedded Syst., vol. 2007, no. 5, p. 1, 2007.
- [4] R. Charette, This Car Runs on Code. [Online]. Available: <http://www.spectrum.ieee.org/feb09/7649>.
- [5] T. Nolte, H. Hansson, and L.L. Bello, —Automotive communications past, current and future, || in Proc. IEEE Int. Conf. Emerging Technol. Factory Autom., 2005, vol. 1, pp. 992 – 999.
- [6] The EVITA project, 2008, Webpage. [Online]. Available: <http://evita-project.org>

