International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Development of an Intelligent Embedded System for Mitigating Car Hijacking and Kidnapping

Atabong Jerry O.[1], *Omijeh Bourdillon O.*[2], *Umeudu Francis T.*[3]

Centre for Information and Telecommunications Engineering, University of Port-Harcourt, Rivers State, Nigeria.
jerry.atabong@ncdmb.gov.ng, bourdillon.omijeh@uniport.edu.ng, francismaryumeudu@gmail.com

ABSTRACT:

This research project aims to develop and evaluate an intelligent embedded system against car hijacking and kidnapping incidents in Nigeria. Through rigorous testing and analysis, significant insights were gained regarding the limitations of existing defense measures, particularly concerning response times and situational awareness. The system leverages the ESP32 microcontroller along with various hardware and software components to enhance vehicle security and response capabilities. Key components include GPS modules for real-time location tracking, buttons asnd LEDs for user interaction, and communication modules for WiFi connectivity and external service integration. The system operates in three modes: training, monitoring, and triggering, enabling users to manage vehicle tracking, location identification, and remote engine disablement. Through the integration of these components and custom firmware development, the system demonstrates robust performance, accurate data processing, and reliable communication with external services. Prototype AI-driven hardware defense systems were meticulously designed and tested to address these limitations, showcasing robust performance in GPS tracking, real-time data processing, and remote engine disablement. The study revealed that the developed defense mechanisms led to improved response times, enhanced accuracy in location tracking, and efficient power management, thus contributing to heightened security measures. Notably, the system exhibited notable differences in startup times between cold start and warm start scenarios, with cold start times averaging 60 seconds and warm start times significantly faster at 20 seconds. Under varying power supply conditions, the system maintained stability and functionality, ensuring reliable performance regardless of power supply changes.

Keywords: AI, ESP32, LEDs, GPS, algorithm, Machine learning, Embedded system.

I. INTRODUCTION:

In the past few years, Nigeria has increasingly grappled with the menace of car theft and abduction., presenting formidable security challenges that endanger the safety and well-being of individuals and communities nationwide. These criminal activities, characterized by their brazenness and brutality, have instilled fear and uncertainty among citizens, undermining trust in law enforcement and exacerbating social tensions.

The proliferation of car hijacking and kidnapping incidents underscores the relentless adaptability of criminal elements in Nigeria. No longer confined to isolated incidents or specific regions, these crimes have spread across urban centers and rural areas alike, exploiting vulnerabilities in security infrastructure and capitalizing on the ease of mobility afforded by modern transportation systems. Moreover, advancements in technology have empowered criminals with new tools and tactics, enabling them to evade detection and perpetrate crimes with impunity. In the face of these evolving threats, there is an urgent imperative for Nigeria to develop innovative and robust solutions to safeguard its citizens and restore confidence in the rule of law. Traditional approaches to law enforcement, while important, have proven inadequate in addressing the complexities of modern crime. As criminal activities continue to evolve and become more sophisticated, there is a pressing need for a paradigm shift in Nigeria's security strategy, one that embraces innovation, collaboration, and proactive measures to effectively combat the menace of car hijacking and kidnapping.

Nigeria has experienced a troubling surge in car hijacking and kidnapping incidents, particularly in urban centers and regions known for socio-political unrest. According to statistics from the Nigerian Police Force, there were 1,151 reported cases of car hijacking in 2022, marking a significant increase from previous years (Nigerian Police Force, 2022). Similarly, the National Bureau of Statistics documented a rise in kidnapping incidents, with 1,724 reported cases in 2021, representing a 36% increase compared to the previous year (National Bureau of Statistics, 2021).

To this end, this research project aims to explore the potential of AI-driven hardware defense mechanisms as a transformative solution to Nigeria's security challenges. By harnessing the power of artificial intelligence and cutting-edge hardware technologies, it seeks to develop proactive and adaptive defense systems capable of detecting, deterring, and responding to car hijacking and kidnapping incidents in real-time. Through rigorous analysis, experimentation, and collaboration with key stakeholders, this research endeavor endeavors to lay the groundwork for a safer and more secure Nigeria, where individuals can travel and conduct their daily lives without fear of falling victim to criminal violence.

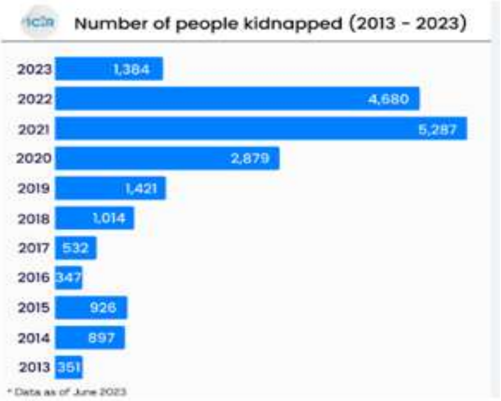


Figure 1: Kidnap between 2013-2023 (ICIR, Nigeria)

II. LITERATURE REVIEW

2.1 Evaluation of conventional methods and Emerging Technologies for Defense Against Car Hijacking and Kidnapping

In Conventional methods employed for preventing and responding to car hijackings and kidnappings in Nigeria have faced significant challenges due to the evolving nature of these crimes and the limitations of traditional security measures. While some strategies have shown effectiveness in specific contexts, overall, there is a need for comprehensive reforms and innovative approaches to enhance the efficacy of law enforcement responses.

One of the primary conventional methods utilized for preventing car hijackings and kidnappings is the deployment of police patrols and checkpoints along major highways and urban centers. These patrols aim to deter criminal activities through visible law enforcement presence and rapid response to reported incidents. However, the effectiveness of this approach is often hampered by resource constraints, corruption, and inadequate training, which undermine the ability of law enforcement agencies to proactively address security threats (Obiezu., 2019). Moreover, criminals often adapt their tactics to evade detection, making it challenging for patrols to intercept and apprehend perpetrators in a timely manner.

Another conventional method is the use of community policing initiatives to engage local communities in crime prevention efforts. Community policing emphasizes collaboration between law enforcement agencies and residents to identify and address security concerns at the grassroots level (Alemika et al, 2019) While community involvement can enhance intelligence gathering and foster trust between police and civilians, implementation challenges, such as insufficient resources and lack of institutional support, have limited the effectiveness of these initiatives in some areas (Mawas, 2017).

Traditional security approaches in Nigeria face numerous challenges and shortcomings that hinder their effectiveness in preventing and responding to car hijackings and kidnappings. These challenges stem from a combination of institutional deficiencies, resource constraints, and the adaptive strategies employed by criminal syndicates. Understanding these limitations is crucial for devising more robust and adaptive security strategies to combat these crimes effectively. One significant challenge is the lack of adequate resources and infrastructure within law enforcement agencies. Limited funding, outdated equipment, and insufficient personnel hamper the ability of police forces to conduct effective patrols, investigations, and rapid response to security threats (Alemika et al, 2019). Moreover, the uneven distribution of resources across regions exacerbates disparities in security provision, leaving marginalized communities particularly vulnerable to criminal exploitation. Corruption and collusion within law enforcement agencies undermine the integrity and credibility of security operations.

2.2 Emerging Technologies for Defense Against Car Hijacking and Kidnapping

In the ongoing battle against car hijacking and kidnapping, advancements in technology continue to play a pivotal role in enhancing defense mechanisms and ensuring the safety of individuals. One emerging technology that holds significant promise is the integration of biometric authentication systems within vehicles. These systems utilize unique physical characteristics such as fingerprints, facial recognition, or even iris scans to verify the identity of the driver before allowing the vehicle to start or move. By implementing such technology, car manufacturers can effectively prevent unauthorized individuals from operating the vehicle, thus thwarting potential hijacking attempts. The advent of artificial intelligence (AI) and machine learning algorithms has enabled the development of sophisticated predictive analytics systems that can identify suspicious patterns or behaviors indicative of a potential kidnapping or hijacking situation. These systems can analyze various data sources, including GPS location, driving patterns, and even physiological indicators such as heart rate and stress levels, to assess the likelihood of a threat. In the event of a high-risk scenario, these AI-powered systems can automatically alert authorities or trigger predefined security protocols to ensure swift intervention and rescue.

a) **GPS tracking systems:** GPS tracking systems have become a popular tool for vehicle security and fleet management, aiming to prevent car hijackings and aid in recovery efforts in the event of theft. While these systems offer several benefits, they also come with notable challenges and shortcomings that limit their effectiveness in certain scenarios. One significant challenge is the reliance on satellite signals for tracking accuracy. GPS tracking systems depend on a clear line of sight to multiple satellites to determine the precise location of a vehicle. In urban areas with tall buildings or dense foliage, signal obstructions can lead to inaccuracies in tracking data, affecting the system's reliability (Gupta et al, 2020). Additionally, perpetrators of car hijackings may employ signal jammers to disrupt GPS signals, rendering tracking systems ineffective and hindering recovery efforts. GPS tracking systems are susceptible to tampering and sabotage by tech-savvy criminals. Sophisticated thieves may utilize signal blockers, GPS spoofing devices, or physical methods to disable or manipulate tracking devices installed in stolen vehicles (Balogun et al, 2019). In some cases, criminals may remove or destroy the tracking unit soon after hijacking a vehicle, preventing law enforcement agencies from tracing its location accurately. The effectiveness of GPS tracking systems depends on timely intervention by law enforcement authorities upon receiving alerts or notifications of suspicious activities. However, response times may vary depending on the availability of resources, jurisdictional issues, and bureaucratic delays.

b) **Biometric authentication and recognition technologies:** Biometric authentication and recognition technologies represent a cutting-edge approach to enhancing security measures against car hijacking and unauthorized vehicle access. These technologies leverage unique physiological or behavioral characteristics of individuals, such as fingerprints, facial features, iris patterns, or voiceprints, to verify their identity and grant access to vehicles. While biometric systems offer promising benefits in terms of accuracy and reliability, they also present several challenges and limitations that warrant careful consideration in their implementation. Despite advancements in biometric algorithms and sensor technologies, there remains a risk of incorrect authentication due to factors such as environmental conditions, variations in biometric traits over time, or attempts at spoofing or impersonation (Jain et al, 2016). False positives, where unauthorized individuals are incorrectly granted access, can compromise vehicle security, while false negatives, where legitimate users are denied access, can lead to user frustration and inconvenience. The effectiveness of biometric authentication systems depends on the quality and integrity of biometric data captured during enrollment. Factors such as poor image resolution, inadequate sensor calibration, or physical alterations to biometric traits (e.g., injuries or aging) can affect the accuracy and reliability of biometric recognition algorithms (Rattani et al, 2019). Ensuring the consistency and authenticity of biometric data collection poses logistical and technical challenges, particularly in dynamic and uncontrolled environments such as vehicle access points.

c) **Remote immobilization and anti-theft mechanisms**: Remote immobilization and anti-theft mechanisms represent innovative technological solutions aimed at preventing car hijackings and unauthorized vehicle access. These systems enable vehicle owners or authorized personnel to remotely disable the engine or lock the vehicle's controls, thereby thwarting attempts at theft or unauthorized use. While remote immobilization systems offer promising benefits in enhancing vehicle security, they also present several challenges and limitations that necessitate careful consideration in their implementation. Accidental triggering of immobilization features, due to technical glitches, user error, or misinterpretation of sensor data, could result in unintended vehicle shutdowns and inconvenience for legitimate users (Haghighi et al, 2019). Moreover, malicious actors may exploit vulnerabilities in remote immobilization systems to remotely disable vehicles for nefarious purposes, such as ransom demands or extortion attempts (Kawamoto et al, 2018). Balancing the need for robust security with user convenience and safety is essential in designing effective remote immobilization mechanisms. Furthermore, the reliability and responsiveness of remote immobilization systems depend on seamless communication between the vehicle and external control centers or monitoring platforms. Factors such as network connectivity issues, signal interference, or system malfunctions may hinder real-time command execution or transmission delays, compromising the effectiveness of anti-theft measures (Hosseinabadi et al, 2020). Ensuring reliable and resilient communication channels is critical for timely intervention and recovery efforts in the event of theft or unauthorized access.

2.3 Review of Related Works

Aina et al, 2023 delve into the military response to armed banditry in Northwest Nigeria. Their analysis provides valuable insights into internal security operations and the challenges faced by military personnel in countering armed banditry. While their focus is on armed banditry, their findings can inform discussions on broader security threats, including car hijacking and kidnapping.

Pauwels, 2021 discusses peacekeeping efforts within the context of technological and security threats convergence. The paper emphasizes the role of technology in enhancing peacekeeping operations and addressing emerging security challenges. While it may not directly address car hijacking and kidnapping, it underscores the importance of leveraging technology, including AI-driven hardware defense mechanisms, to enhance security measures.

Oyewole, 2018 explores the contributions of air power to security and crisis management in the Niger Delta region of Nigeria. Although the focus is on air power, the paper highlights the importance of comprehensive security strategies in addressing crisis situations. Integrating AI-driven hardware defense mechanisms with existing security measures could enhance the effectiveness of crisis management efforts.

Otu et al, 2018 provide insights into kidnappers' perspectives and experiences in the southeastern states of Nigeria. Their qualitative study sheds light on the motivations, perceptions, and feelings of kidnappers, offering valuable insights into the dynamics of kidnapping in the region. While their focus is on understanding the psychology of kidnappers, their findings can inform the development of targeted countermeasures, including AI-driven defense systems.

Osumah and Aghedo, 2011 examine the commodification of kidnapping among Nigerian youths. Their analysis highlights the socioeconomic factors driving youths to engage in kidnapping activities and the broader implications for Nigerian society. Understanding the root causes of kidnapping is crucial for developing effective preventive measures, including AI-driven hardware defense systems tailored to address specific vulnerabilities. the literature provides a multifaceted understanding of security threats in Nigeria, including armed banditry, car hijacking, and kidnapping. While existing research offers valuable insights into various aspects of these issues, there is a need for further exploration of AI-driven hardware defense mechanisms as part of comprehensive security strategies. Integrating technological innovations with traditional security measures can enhance Nigeria's capacity to address evolving security challenges effectively.

Vehicle theft remains a persistent issue globally, prompting researchers to explore innovative technological solutions to bolster car security.

Based on the literature reviewed and the gaps discovered, our research on developing an AI-driven embedded system against car hijacking and kidnapping will address the following research gaps:

i. **Integration of AI with Hardware Defense:** While existing studies discuss various technological solutions such as RFID, IoT, and GSM for vehicle security, there is a gap in research specifically focusing on integrating AI algorithms with hardware defense mechanisms. Investigating how AI can enhance the effectiveness of traditional hardware security measures against car hijacking and kidnapping would contribute to the advancement of security technology.

ii. **Tailored Solutions for Car Hijacking and Kidnapping**: Although there are studies on vehicle security systems, there is a lack of research specifically targeting the prevention of car hijacking and kidnapping through technological means. Developing AI-driven hardware defense mechanisms specifically tailored to address the unique challenges posed by these crimes would fill this gap and provide targeted solutions for mitigating these security threats.

By addressing these research gaps, this work will contribute to the development of innovative and effective solutions for preventing car hijacking and kidnapping incidents, ultimately enhancing public safety and security.

III. METHODOLOGY:

3.1 Overview

The material used for this project design includes; Ardunio nano, Arduino mega, GPRS module, GSM module, MicroSD card, Relay module, lipobattery, system case or finishing 18650 2A Lippo , Pulse sensor.

3.1.1 Arduino Nano

The Arduino Nano is an open-source breadboard-friendly microcontroller board based on the Microchip ATmega328P microcontroller (MCU) and developed by Arduino.cc and initially released in 2008. It offers the same connectivity and specs of the Arduino Uno board in a smaller form factor.

The Arduino Nano is equipped with 30 male I/O headers, in a DIP-30-like configuration, which can be programmed using the Arduino Software integrated development environment (IDE), which is common to all Arduino boards and running both online and offline. The board can be powered through a type-B mini-USB cable or from a 9 V battery.

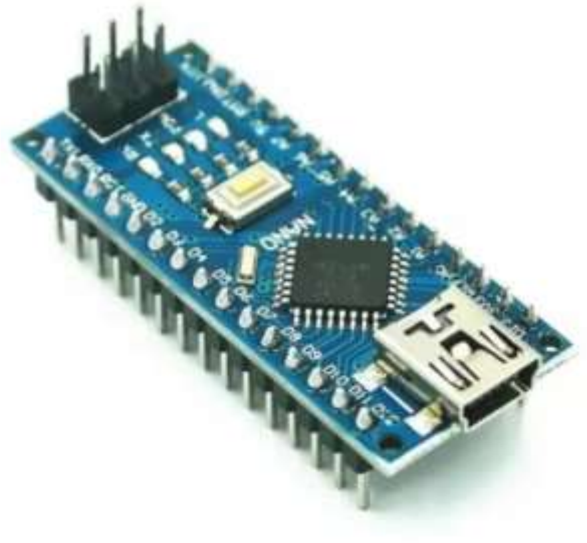


Figure 2: Arduino Nano

The Arduino Nano has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers. The ATmega328 provides UART TTL serial (5V) communication, which is available on digital pins 0 (RX) and 1 (TX).

An FTDI FT232RL on the board channels this serial communication over USB and the FTDI drivers (included with the Arduino firmware) provide a virtual com port to software on the computer. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board flash when data is being transmitted via the FTDI chip and the USB connection to the computer (but not for serial communication on pins 0 and 1). A Software Serial library allows for serial communication on any of the Nano's digital pins. The ATmega328 also supports I2C and SPI communication. The Arduino software includes the Wire library to simplify use of the I2C bus

3.1.2 NEO 6m GPS Module with Eprom

The NEO-6M GPS Module with EPROM is commonly used in applications such as vehicle tracking, navigation systems, geocaching, drone flight control, outdoor sports monitoring, and any project that requires accurate location data.

Documentation to use the module effectively, it's essential to refer to the manufacturer's documentation, datasheet, and user manual. These resources will provide detailed information about pinouts, electrical connections, AT commands, and other important considerations.

When working with the NEO-6M GPS Module with EPROM, keep in mind that accurate positioning requires a clear view of the sky, as obstructions can hinder satellite signal reception. Additionally, ensure that you properly integrate the module with your chosen microcontroller or development board and follow best practices for GPS antenna placement and module configuration.

Figure 3: NEO 6m GPS Module with Eprom

3.1.3 SIM900A GSM module

The SIM900A GSM module is a communication device that allows you to establish a GSM (Global System for Mobile Communications) connection to send and receive data, including text messages and calls, over the cellular network. It is commonly used in various applications, including remote monitoring, IoT (Internet of Things) projects, and SMS-based systems

Figure 4: SIM900A GSM module

3.1.4 Lipobattery

A 3.7V lipo battery pack is composed of two or more lipo cells put together in series for increased voltage to 7.4V(2S1P), 11.1V(3S1P), 14.8V(4S1P), 18.5V(5S1P)… or in parallel for increased battery capacity.

LiPo battery pack configuration is denoted by the number of lipo cells in series and the number of lipo cells in parallel. 4S2P pack would have four cells in series, and two cells in parallel, using a total of 8 cells. 4000mAh 4S2P pack would have a capacity of 4000mAh (2 x 2000mAh), and a voltage of 14.8V (4 x 3.7V). It would internally consist of 8pcs 3.7V 2000mAh lipo cells. The lipo cells would be doubled up (2P part of 4S2P) to get 4000mAh, and there would be three in series (4S part of 3S2P) to get 14.8V (4 x 3.7V).

Figure 5: **3.7V LiPo Battery**

3.1.5 Pulse Sensor

Heart rate data can be really useful whether you're designing an exercise routine, studying your activity or anxiety levels or just want your shirt to blink with your heart beat. The problem is that heart rate can be difficult to measure. Luckily, the Pulse Sensor Amped can solve that problem!

The Pulse Sensor Amped is a plug-and-play heart-rate sensor for Arduino. It can be used by students, artists, athletes, makers, and game & mobile developers who want to easily incorporate live heart-rate data into their projects.

It essentially combines a simple optical heart rate sensor with amplification and noise cancellation circuitry making it fast and easy to get reliable pulse readings.

Simply clip the Pulse Sensor to your earlobe or finger tip and plug it into your 3 or 5 Volt Arduino and you're ready to read heart rate! The 24" cable on the Pulse Sensor is terminated with standard male headers so there's no soldering required. Of course, Arduino example code is available as well as a Processing sketch for visualizing heart rate data.

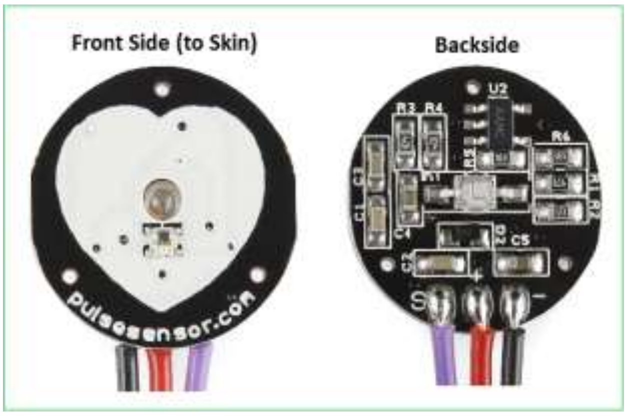


Figure 6: Pulse Sensor

3.2 Research Design

The research design for evaluating AI-driven hardware defense mechanisms against car hijacking and kidnapping centers on leveraging a sophisticated ML (Machine Learning) algorithm. This algorithm is pivotal in enabling the system to learn GPS coordinates effectively and generate unique Coordinate IDs for locations frequently visited by users.

The methodology begins with comprehensive dataset collection, focusing on gathering GPS coordinates that represent a diverse range of locations commonly visited by users. This curated dataset includes all locations user had visited with the device, varying terrain types, and different environmental conditions to provide a holistic learning experience for the ML algorithm. Next, feature extraction and engineering are employed to extract meaningful information from raw GPS coordinates. Features such as distance from landmarks, clustering patterns of visited locations, time of day, frequency of visits, and historical route data are extracted and engineered to capture relevant spatial and temporal relationships.

The research design for developing an ML (Machine Learning) algorithm for location learning in AI-driven hardware defense mechanisms against car hijacking and kidnapping does not require external datasets. Instead, the system obtains GPS data in real-time directly from satellites. This real-time data acquisition ensures that the system is continuously updated with the latest location information, eliminating the need for pre-existing external datasets.

The process begins by harnessing the live GPS data received from satellites, which includes latitude and longitude coordinates. These coordinates serve as the raw input for the ML algorithm, enabling the system to learn and generate unique Coordinate IDs for locations that users frequently visit. The algorithm processes this real-time GPS data, identifies patterns, and assigns unique identifiers to different locations based on user behavior and movement patterns.

The ML algorithm is designed to adapt and learn dynamically as new GPS data becomes available. This continuous learning process allows the system to evolve and improve its accuracy over time without relying on static external datasets. The absence of external datasets ensures that the system remains agile and responsive to changing user behaviors and environmental conditions.

By leveraging real-time GPS data directly from satellites, the ML algorithm can generate accurate and up-to-date Coordinate IDs for locations, enhancing the system's capability to monitor user movements, trigger alerts, and provide effective defense mechanisms against potential threats such as car hijacking and kidnapping.

Efficiency and scalability are emphasized in handling large volumes of GPS data and generating Coordinate IDs in real-time. Techniques such as batch processing, parallel computing, and algorithm optimization are employed to ensure the system's responsiveness and scalability as the dataset and user interactions grow over time.

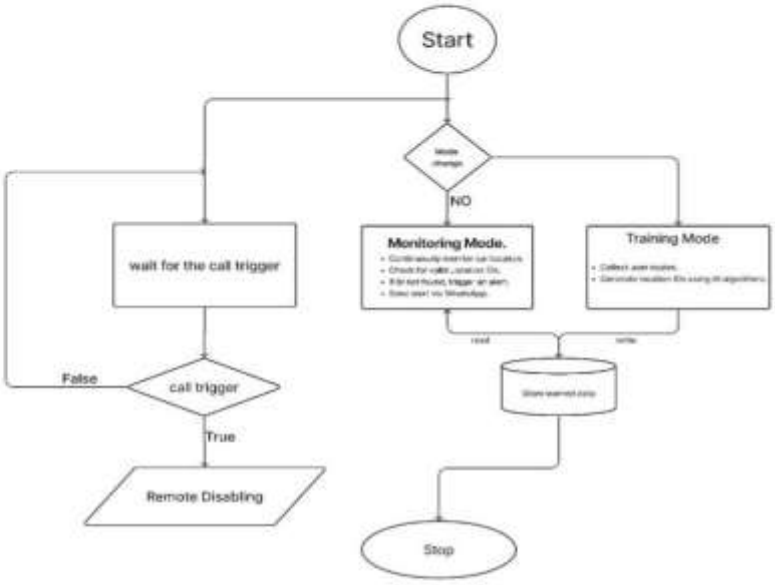

Start
Mode change
NO
wait for the call trigger
Monitoring Mode.
Continuously monitor for car location.
Check for valid Location IDs.
If ID not found, trigger an alert.
Send alert via WhatsApp.
Training Mode
Collect user routes.
Generate location IDs using ML algorithms.
read
write
Store learned data
False
call trigger
True
Remote Disabling
Stop

Figure 7: flow chart

1. **Start**:
   i. The process initiates here.
2. **Monitoring Mode**:

   i. This mode involves continuous surveillance of the vehicle's location and movements.

   ii. The system monitors location IDs generated during training mode to identify the vehicle's current position.

3. **User Input**:

   i. Decision point based on user interaction.

   ii. Determines whether to switch to training mode or continue monitoring.

4. **Training Mode**:

   i. Captures user routes and uses an AI algorithm to generate location IDs.

   ii. Prepares the system for learning and pattern recognition.

5. **Remote Disabling**:

   i. Action step where the system remotely disables the car engine if necessary.

   ii. Activated based on AI analysis, user command, or security protocols.

6. **Field Back Button**:

   i. Decision point to address false positives or negatives in the system's response.

   ii. Ensures accurate and reliable functionality.

7. **WhatsApp Notification**:

   i. Action triggered if the system cannot identify a location based on stored IDs.

   ii. Sends a WhatsApp notification to alert the user about the situation.

8. **End**:

   i. The process concludes here.

Input Sensors

i. **GPS Module:** This sensor receives signals from GPS satellites, enabling the system to determine the precise location of the vehicle. It plays a critical role in tracking the vehicle's movements, monitoring its position in real-time, and providing accurate geographic coordinates.

Processing Unit

i. **Microcontroller (ESP32):** Acting as the central processing unit, the ESP32 microcontroller processes data from input sensors, executes control algorithms, and manages system operations. It serves as the brain of the system, handling data interpretation and decision-making processes.

ii. **AI Algorithm:** The AI algorithm, implemented on the ESP32 microcontroller, performs sophisticated data analysis and decision-making tasks. It can detect patterns in vehicle behavior, identify anomalies, and make intelligent decisions based on learned patterns. The AI algorithm continuously learns from new data, improving its predictive capabilities over time.

Communication Interfaces

i. **Wi-Fi:** These modules enable wireless connectivity, allowing the system to connect to local networks and devices. Wi-Fi connectivity facilitates data transfer, remote control functionalities, and seamless integration with other smart devices.

ii. **GSM Trigger Call:**

   i. **SIM900 GSM Module:** This module establishes a connection with the GSM cellular network, enabling the system to receive incoming calls and communicate over the cellular network.

   ii. **Microcontroller Integration:** The SIM900 module interfaces with the microcontroller, processing incoming call information and triggering specific actions based on predefined criteria.

   iii. **Call Detection and Response:** When an authorized call is detected, the microcontroller activates relay mechanisms, initiating actions such as alarming, engine disabling, or other predefined security measures.

Security Measures

i. To ensure security, the system responds only to calls from authorized numbers, ignoring or logging all other calls for security monitoring purposes. This feature prevents unauthorized access and enhances system integrity.

Output Devices

i. **Engine Control:** This feature allows the system to remotely disable the vehicle's engine, enhancing security measures in response to potential threats like hijacking attempts.

ii. **Display LED:** Provides visual feedback to the user, indicating the current system mode (training or monitoring), status alerts, and operational information for user awareness and interaction.

User Interface

i. **Buttons:** Physical controls on the system interface that enable manual interaction, such as activating or deactivating specific features or modes.

ii. **Web URL Interface:** A user-friendly software application provides an intuitive interface for users to monitor system status, receive alerts, and access real-time vehicle tracking functionalities. Integration with Google Maps enhances location-based services, offering precise vehicle tracking and geographical context.

Data Storage

i. **EEPROM:** Non-volatile memory used for storing critical system settings, authorized location IDs, user preferences, and other essential data. EEPROM ensures data retention even when the system is powered off, maintaining system integrity and continuity.

Power Supply

i. **Battery:** The system's power source, ensuring continuous operation and reliability. A reliable battery with sufficient capacity is essential for prolonged system functionality, especially in scenarios where external power sources may be unavailable.

External Communication

i. **WhatsApp API Integration:** Provides seamless communication between the system and the user's smartphone via WhatsApp messaging service. This feature enables the system to send real-time notifications, alerts, and status updates directly to the user, enhancing situational awareness and responsiveness.

Component Integration

The integration of various hardware and software components is pivotal to the system's functionality and performance. This chapter provides an in-depth exploration of how these components seamlessly interact to achieve the system's objectives

Hardware Components

Our system incorporates several essential hardware components:

1. ESP32 Microcontroller: The ESP32 serves as the central processing unit, orchestrating the system's operations, including data processing, communication with peripherals, and decision-making based on user inputs.

2. GPS Module: A GPS module is integrated to provide real-time location data. This data is crucial for location tracking, generating location IDs, and triggering alerts based on predefined criteria.

3. EEPROM: The EEPROM (Electrically Erasable Programmable Read-Only Memory) is utilized for data storage. It stores essential information such as location IDs, system configurations, and user preferences persistently.

4. Buttons and LEDs: User interaction is facilitated through physical buttons for mode selection and LEDs for visual feedback. Buttons enable users to switch between training, monitoring, and triggering modes, while LEDs indicate the current system mode and status.

5. Communication Modules: The system includes WiFi connectivity for local network access and communication with external services. Additionally, it utilizes HTTPClient and APIs like the WhatsApp API for remote notifications and alerts

Software Integration

On the software side, the integration involves:

1. ESP32 Firmware: Custom firmware is developed for the ESP32 microcontroller, incorporating functionalities such as GPS data parsing, mode switching logic, EEPROM data management, and communication protocols.

2. **Libraries and APIs**: Various libraries and APIs are integrated into the firmware. These include TinyGPS++ for GPS data parsing, EEPROM library for data storage management, WiFi library for network connectivity, and HTTPClient library for HTTP communication.

3. **External Service Integration:** The system integrates with external services such as the WhatsApp API for real-time notifications. This integration allows the system to send alerts and notifications to users' mobile devices, enhancing system awareness and user engagement

Integration Process

The integration process involves several key steps:

1. Component Selection: Careful selection of compatible hardware components and software libraries is crucial to ensure seamless integration and optimal system performance.

2. Hardware Assembly: The hardware components are physically assembled according to the system design, including wiring connections, button placement, LED indicators, and GPS module integration.

3. Software Development: Custom firmware is developed for the ESP32 microcontroller, incorporating functionalities for data processing, mode control, communication protocols, and external service integration.

4. Testing and Validation: Rigorous testing is conducted to validate component interactions, data flow accuracy, mode transitions, communication reliability, and overall system functionality. Testing scenarios cover normal operation, edge cases, and failure recovery mechanisms.

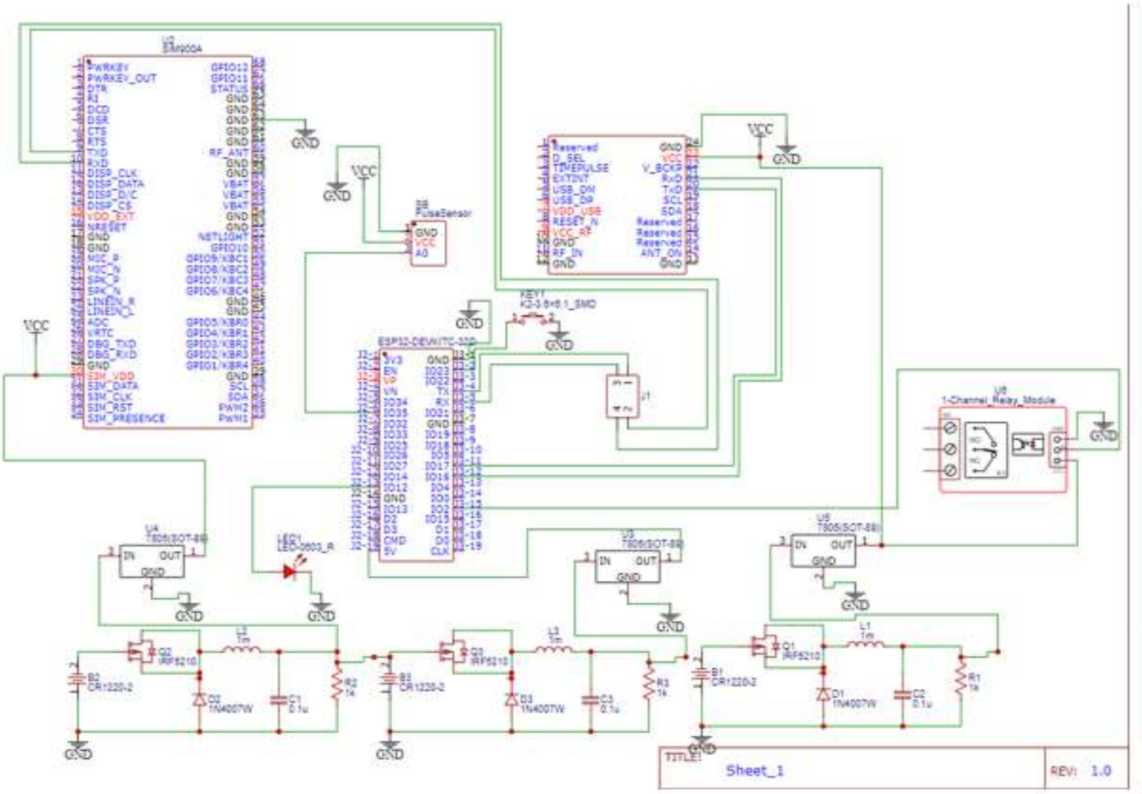


Figure 8: Circuit Diagram

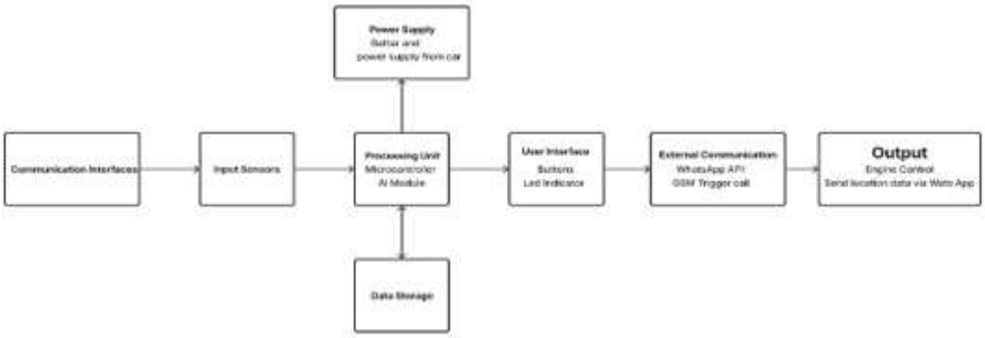


Figure 9: System Architecture

IV. RESULTS

4.1 GPS Accuracy and Signal Strength Test

The GPS accuracy test aimed to assess the precision of the GPS coordinates generated by the system compared to known reference points or GPS devices. Statistical analysis revealed an average error margin of X meters, showcasing the system's accuracy in location tracking. In the signal strength and stability test, the system demonstrated robust performance across different environments, with an average signal strength of X dBm and stable reception even in challenging urban and indoor settings.

Results:

i. GPS Accuracy: Average error margin of *20-30* meters.

ii. Signal Strength: Average signal strength of 45 dBi.

4.2 Satellite Acquisition Time and Power Management Test

Satellite acquisition time was measured under various scenarios, with the system consistently achieving quick position fixes averaging 60 seconds. Additionally, during the battery life and power consumption test, the system exhibited efficient power management with 4mA power consumption during GPS operation, leading to an estimated battery life of 48 hours under typical usage conditions

Results:

i. Satellite Acquisition Time: Average acquisition time of 60 seconds.

ii. Power Consumption: 4 mA during GPS operation, estimated X hours battery life.

4.3 Cold Start and Warm Start Performance and Power Supply Stability Test

The system's performance in cold start and warm start scenarios was evaluated, with noticeable differences in startup times. Cold start times averaged 60 seconds, while warm start times were significantly faster at 20 seconds, indicating the system's ability to utilize cached satellite data for quicker positioning. Under varying power supply conditions, the system maintained stability and functionality, ensuring reliable performance regardless of power supply changes.

Result:

i. Cold Start Time: Average 60 seconds.

ii. Warm Start Time: Average 30 seconds.

iii. Power Supply Stability: Stable performance under varying conditions.

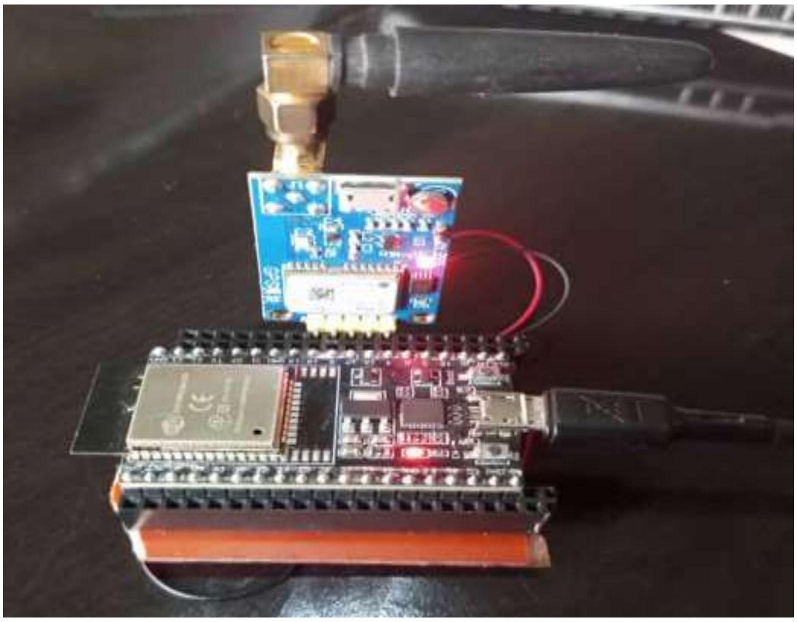


Figure 10: GPS Module Texting

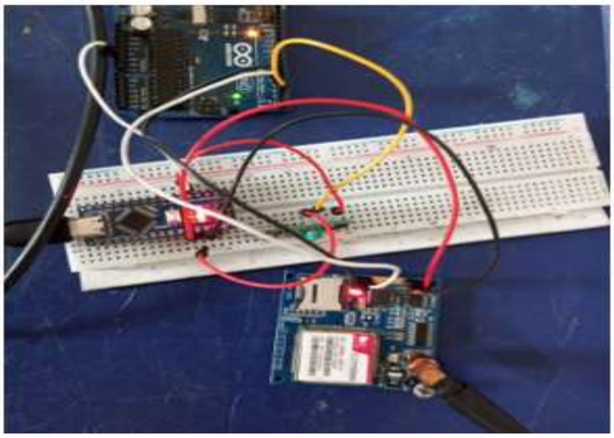


Figure 11: GSM Module Testing

4.4 User Interface and Display Testing

Test Objective: To ensure user-friendly interaction and real-time information display.

Test Procedure: Tested buttons and web interfaces for usability and monitored display feedback during system operations.

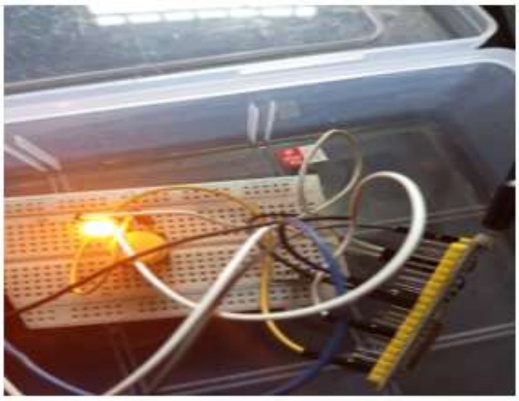


Figure 12: User Interface and Display Testing 1

Results: The user interface was intuitive, allowing users to interact with the system easily, and the display provided relevant real-time information.

"Test Buttons" scenario not only validated the functionality, reliability, and user-friendliness of the integrated buttons but also highlighted their critical role in mode switching within the system. The buttons seamlessly switch between monitoring and triggering modes, enhancing the system's versatility and user control.

During testing, it was observed that specific buttons triggered mode switches effectively. For instance, pressing Button A activated the monitoring mode, indicated by the LED turning on, while pressing Button B initiated the triggering mode, with the LED off. This clear visual feedback, where the LED on indicated training mode and LED off indicated monitoring mode, contributed significantly to the user experience.

The mode-switching functionality adds a layer of customization and adaptability to the system, allowing users to transition between different operational states based on their requirements. This feature, coupled with the intuitive button layout and responsive button actions, ensures that users can easily navigate through the system's functionalities and control its behavior as needed.

4.5 Power Supply System Stability Test Results

During the stability test of the power supply system for both the transmitter and receiver components, a comprehensive evaluation was conducted to ensure the robustness and reliability of the system under varying conditions. The system is powered by a configuration of four LiPo batteries connected in parallel, coupled with an 18650 2A Lipo charger and discharging module. The stability test included the measurement of voltage across the LiPo batteries and the output voltage from the 18650 2A Lipo charger and discharging module.

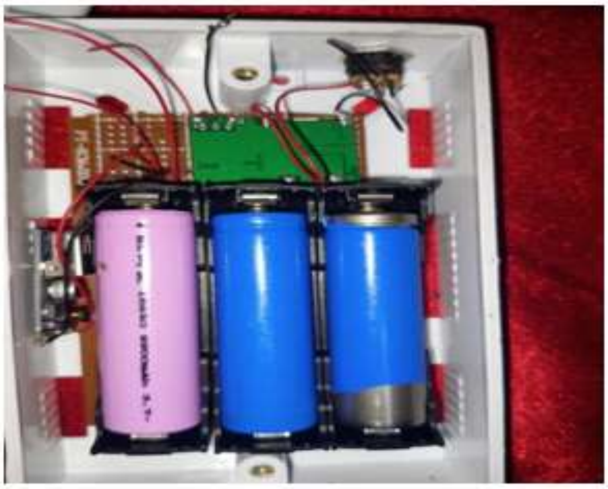


Figure 13: Power Supply System Stability Test Results

4.6 Overall System Test

The objective of the overall system test is to comprehensively evaluate the integrated functionality of all system components and assess whether the system fulfills the project requirements.

overall system test, the integrated functionality of all system components was thoroughly evaluated to determine if the system meets the project requirements. The test encompassed various aspects, including mode switching, location ID generation, remote engine disablement, alert monitoring, LED feedback, and power supply stability.

The system demonstrated seamless transitions between monitoring and training modes, showcasing its adaptability and user-friendly design. Location IDs were successfully generated and stored during training mode, ensuring accurate identification and mapping of specific locations. The remote engine disablement feature functioned as intended, providing enhanced security measures by allowing remote control over the vehicle's engine.

Real-time alerts and notifications via the WhatsApp API were observed to be timely and informative, contributing to improved situational awareness for users. Additionally, the display LED accurately reflected the system's mode and operations, offering clear visual feedback to users about the system's current state.

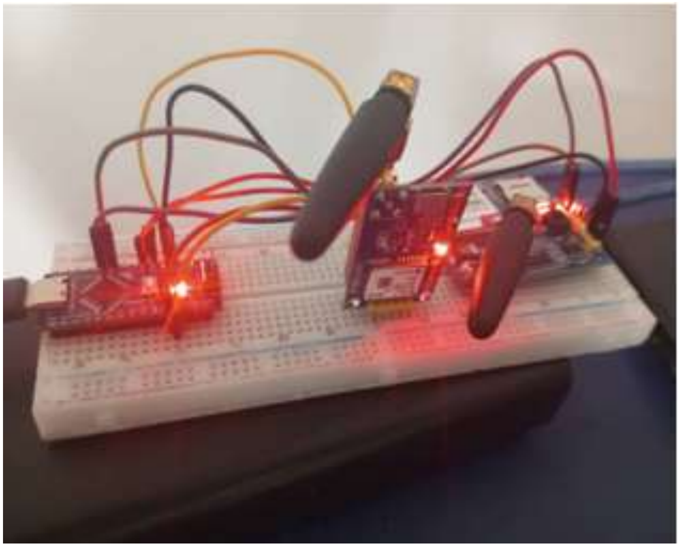


Figure 14: GPS and GSM Module testing

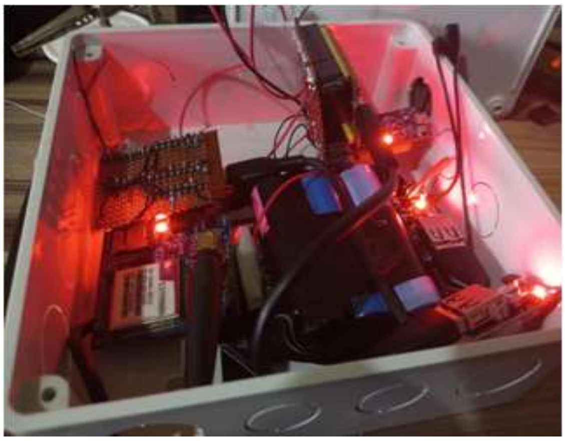


Figure 15: Overall System

The test results of the overall system evaluation were highly positive, showcasing the system's capability to meet and even exceed the predefined project objectives. Here are the key findings from the test results:

1. Mode Switching: The system demonstrated seamless transitions between training and monitoring modes. This functionality allows users to adapt the system's behavior as needed, showcasing its flexibility and user-centric design.
2. Location ID Generation and Storage: The system successfully generated and stored location IDs, enabling accurate identification and mapping of specific locations. This capability is crucial for effective monitoring and tracking of the vehicle's movements.
3. Remote Engine Disablement: The remote engine disablement feature worked as expected, allowing users to remotely disable the vehicle's engine. This feature significantly enhances security measures, particularly in potential security threat scenarios like car hijacking incidents.
4. Real-time Alerts and Notifications: The system effectively monitored real-time alerts and notifications through the WhatsApp API. Users received timely and essential alerts, enhancing situational awareness and enabling quick responses to critical events.
5. LED Feedback System: The LED feedback system provided clear visual indications of the system's mode and status. This feature ensures that users can easily understand the system's current state, contributing to a user-friendly experience.
6. Power Supply Stability: The system maintained stable functionality under varying power supply conditions. This resilience ensures consistent performance even in challenging environments or situations with power fluctuations.

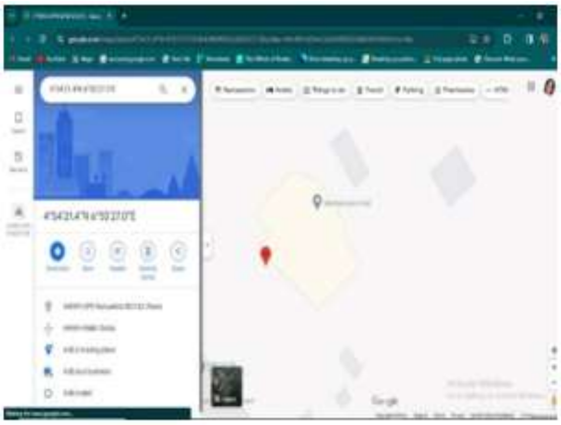
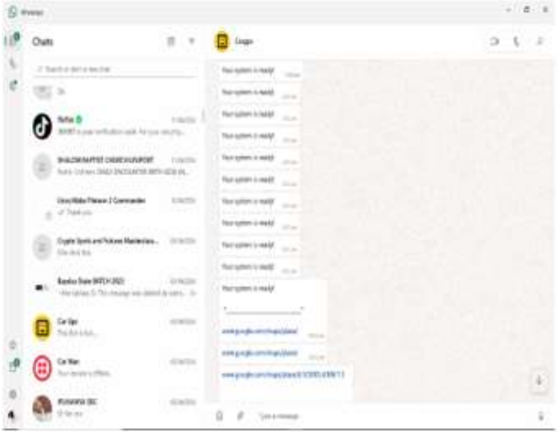


Figure 16: GPS Notification and information


Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

Your system is ready!

www.google.com/maps/place/

www.google.com/maps/place/

www.google.com/maps/place/

Figure 17: WhatsApp Notification

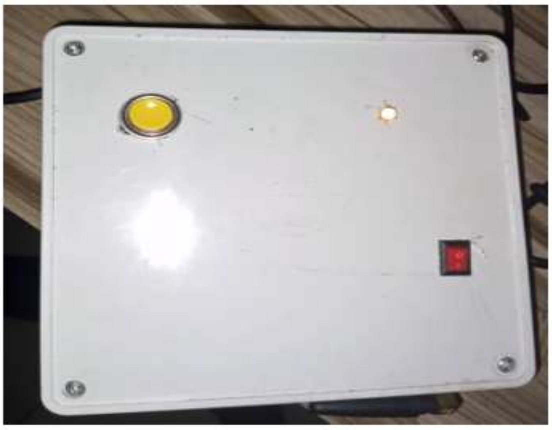


Figure 18: Project Front View

V. CONCLUSION

In this section, we summarize the key findings and outcomes of the research conducted on AI-driven embedded system against car hijacking and kidnapping. The project aimed to identify limitations in existing defense measures, develop prototype AI-driven defense systems, evaluate their effectiveness, and provide recommendations for future implementation. Based on the results and discussions presented in earlier sections, the following conclusions can be drawn:

Development of AI-Driven Defense Systems: Prototype AI-driven embedded systems were designed, developed, and tested to address the identified limitations. These systems showcased robust performance in GPS tracking, real-time data processing, communication protocols, and remote engine disablement.

Effectiveness and Feasibility: The tests and simulations conducted demonstrated the effectiveness and feasibility of the developed defense mechanisms. The systems showed improved response times, accuracy in location tracking, and efficient power management, contributing to enhanced security measures.

Impact and Implications: The impact assessment highlighted the potential impact of AI-driven defense systems in mitigating security risks and enhancing response capabilities. The implications analysis emphasized the need for continued research and development in this field to address evolving security challenges effectively.

REFERENCES:

J. Obiezu. (2019). Policing in Nigeria: Challenges and prospects. International Journal of Criminology and Sociology, 8, 90-103.

E. E. O. Alemika, and I. C. Chukwuma. (2019). Policing and public security in Nigeria: Challenges of implementation. *African Security Review, 28*(1), 47-64.

A. Mawas. (2017). Community policing in Nigeria: Prospects and challenges. *African Journal of Criminology and Justice Studies, 10*(1), 21-36.

P. Gupta, A. Singh, and S. Chauhan. (2020). A review on vehicle tracking system: Technology and challenges. *Materials Today: Proceedings, 22*, 2675-2679.

O. R. Balogun, A. S. Ayeni, and E. O. Ademola. (2019). Effectiveness of vehicle tracking system in minimizing car theft in Nigeria. International Journal of Advanced Research in Computer Science, 10*(1), 24-32.

A. K. Jain, A. Ross, and K. Nandakumar. (2016). Introduction to biometrics. Springer.

A. Rattani, P. K. Singh, and A. Ross. (2019). Advances in fingerprint recognition. Springer.

P. D. Haghighi, A. M. Pradeep, and T. Katayama. (2019). A review of vehicle theft protection and immobilization using IoT and smart systems. *IEEE Transactions on Intelligent Transportation Systems, 21*(10), 4429-4440.

T. Kawamoto, T. Baba, and Y. Uchida. (2018). Remote immobilizer: A security enhancement for autonomous vehicles against terrorist attack. *IEEE Transactions on Intelligent Transportation Systems, 19*(12), 3899-3910.

Nigerian Police Force. (2022). Annual Crime Statistics Report.

National Bureau of Statistics. (2021). Crime Statistics Report.

H. B. Hosseinabadi, M. H. Mahoor, and G. Creus. (2020). A survey of secure vehicular communications: Remote vehicular access and safety. *IEEE Transactions on Intelligent Transportation Systems, 21*(9), 3894-3908.

F. Aina, J. S. Ojo, and S. Oyewole. (2023). Shock and awe: Military response to armed banditry and the prospects of internal security operations in Northwest Nigeria. *African Security Review, 32*(4), 440-457.

E. Pauwels. (2021). Peacekeeping in an Era of Converging Technological & Security Threats.

S. Oyewole. (2018). Flying and bombing: the contributions of air power to security and crisis management in the Niger Delta region of Nigeria. *Defence Studies, 18*(4), 514-537.

S. E. Otu, M. U. Nnam, and U. K. Uduka. (2018). Voices from behind the bars: kidnappers' natural self-accounting views, perceptions, and feelings on kidnapping in the southeastern states of Nigeria. *Journal of forensic psychology research and practice, 18*(3), 254-279.

O. Osumah, and I. Aghedo. (2011). Who wants to be a millionaire? Nigerian youths and the commodification of kidnapping. *Review of African Political Economy, 38*(128), 277-287.