VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi – 590014.

Internship Project Report

On

"Anti-Theft Password-Based Ignition Lock"

Submitted in partial fulfillment of the requirement for the award of 7th SEM

of

BACHELOR OF ENGINEERING

In

INFORMATION SCIENCE & ENGINEERING

&

COMPUTER SCIENCE & ENGINEERING

By

SUMAN NAIDU R	**(1AP21IS036)**
BIDHAN GOPE	**(1AP21CS011)**
SANDEEP J	**(1AP22CS405)**

2023 - 2024

DEPARTMENT OF
INFORMATION SCIENCE AND ENGINEERING
&
COMPUTER SCIENCE AND ENGENERRING

A P S COLLEGE OF ENGINEERING

Anantha Gnana Gangothri,
NH-209, Kanakapura Road, Somanahalli, Bengaluru-560116.

Project Completion Certificate

I, **Suman Naidu R** (USN: 1AP21IS036), hereby declare that the material presented in the Project Report titled **"Anti-Theft Password-Based Ignition System"** represents original work carried out by me in the **Department of Information Science and Engineering at** the **APS college of Engineering, Bangalore** during the tenure **2 October, 2024 – 12, December, 2024**.

With My signature, I certify that:

- I have not manipulated any of the data or results.
- I have not committed any plagiarism of intellectual property and have clearly indicated and referenced the contributions of others.
- I have explicitly acknowledged all collaborative research and discussions.
- I understand that any false claim will result in severe disciplinary action.
- I understand that the work may be screened for any form of academic misconduct.

Date: **Student Signature**:

In my capacity as the supervisor of the above-mentioned work, I certify that the work presented in this report was carried out under my supervision and is worthy of consideration for the requirements of the B.Tech. Internship Work.

Advisor's Name: **Guide Name:**

SAI CHARAN TEJA

Advisor's Signature **Guide Signature**

Project Completion Certificate

I, **Sandeep J** (USN: 1AP22CS405), hereby declare that the material presented in the Project Report titled **" Anti-Theft Password-Based Ignition System "** represents original work carried out by me in the **Department of Computer Science and Engineering** at the **APS college of Engineering, Bangalore** during the tenure **2 October, 2024 – 12, December, 2024**.

With My signature, I certify that:

- I have not manipulated any of the data or results.
- I have not committed any plagiarism of intellectual property and have clearly indicated and referenced the contributions of others.
- I have explicitly acknowledged all collaborative research and discussions.
- I understand that any false claim will result in severe disciplinary action.
- I understand that the work may be screened for any form of academic misconduct.

Date: **Student Signature**:

In my capacity as the supervisor of the above-mentioned work, I certify that the work presented in this report was carried out under my supervision and is worthy of consideration for the requirements of the B.Tech. Internship Work.

Advisor's Name: **Guide Name:**

SAI CHARAN TEJA

Advisor's Signature **Guide Signature**

Project Completion Certificate

I, **Bidhan Gope** (USN: 1AP21CS011), hereby declare that the material presented in the Project Report titled **" Anti-Theft Password-Based Ignition System "** represents original work carried out by me in the **Department of Computer Science and Engineering** at the **APS college of Engineering, Bangalore** during the tenure **2 October, 2024 – 12, December, 2024**.

With My signature, I certify that:

- I have not manipulated any of the data or results.
- I have not committed any plagiarism of intellectual property and have clearly indicated and referenced the contributions of others.
- I have explicitly acknowledged all collaborative research and discussions.
- I understand that any false claim will result in severe disciplinary action.
- I understand that the work may be screened for any form of academic misconduct.

Date: **Student Signature**:

In my capacity as the supervisor of the above-mentioned work, I certify that the work presented in this report was carried out under my supervision and is worthy of consideration for the requirements of the B.Tech. Internship Work.

Advisor's Name: **Guide Name:**

SAI CHARAN TEJA

Advisor's Signature **Guide Signature**

Evaluation Sheet

Title of the Project: Anti-Theft Password-Based Ignition System

Name of the Students: Suman Naidu R

Sandeep J

Bidhan Gope

External Supervisor:

_____

Internal Supervisor:

_____

_____

Date:

Place:

Table of Contents

ABSTRACT **2**

INTRODUCTION **3**

OBJECTIVE 3

PROBLEM STATEMENT 3

APPLICATIONS **4**

COMPONENTS **5**

FLOWCHART **6**

CONCLUSION **7**

FUTURE WORK **8**

APPENDIX **9**

PSEUDO CODE 9

ABSTRACT

The **Anti-Theft Password-Based Ignition System** is an advanced security solution aimed at enhancing the safety of two-wheelers by integrating cutting-edge facial recognition technology with a reliable password-based fallback mechanism. This system employs a Raspberry Pi as the core controller and a Flask-based server to manage facial authentication. By utilizing powerful image processing libraries such as OpenCV and FACE_RECOGNITION, it provides a robust and user-friendly authentication process.

The primary security layer relies on facial recognition. Authorized users can unlock the vehicle's ignition by simply scanning their faces, ensuring a seamless and convenient user experience. In cases where the facial recognition system fails to identify a user, a secondary layer of protection is activated through a password-based authentication system. This ensures that only legitimate users can gain access to the vehicle.

To further strengthen the system, a locking mechanism is implemented to temporarily disable the system after multiple failed authentication attempts. This feature significantly reduces the risk of unauthorized access. Additionally, the system includes an emergency shutdown option and a reset mechanism, allowing users to quickly recover from accidental lockouts or critical situations.

The hardware setup of the system is designed to deliver reliable performance. It incorporates a relay to control the ignition lock, an LCD to display real-time status updates, and GPIO-interfaced switches and a buzzer to provide user feedback and alerts. The integration of these components ensures a responsive and interactive user experience.

This project demonstrates the powerful combination of IoT, artificial intelligence, and embedded systems to address real-world security challenges. Its modular design not only provides robust two-wheeler security but also allows for future enhancements, such as GPS tracking and remote vehicle control. This innovative solution showcases the potential of technology to revolutionize everyday safety measures.

INTRODUCTION

Vehicle theft remains a significant issue, particularly for two-wheelers with limited security features. The Anti-Theft Password-Based Ignition System addresses this by integrating facial recognition and password authentication for enhanced protection.

The system uses a Raspberry Pi as the controller and a Flask server to process facial recognition via OpenCV and FACE_RECOGNITION. Authorized users can unlock the ignition through facial authentication, while a password serves as a fallback mechanism. To prevent unauthorized access, the system locks after multiple failed attempts and includes emergency reset and shutdown options.

With hardware components like relays, an LCD, switches, and a buzzer, the system offers a secure, user-friendly solution. This project combines IoT and AI to provide a scalable and robust approach to vehicle security.

Objective

- Develop a dual-layer authentication system using facial recognition and password verification to prevent unauthorized access.
- Provide a seamless and user-friendly experience by replacing traditional keys with advanced authentication methods.
- Include system locking, emergency shutdown, and reset functionalities to ensure reliability and adaptability in various scenarios.

Problem Statement

Two-wheeler theft is a common issue due to the lack of advanced security mechanisms in traditional ignition systems, which primarily rely on physical keys or basic password protection. These methods are prone to theft through duplication or unauthorized access. There is a need for a robust and user-friendly security system that integrates advanced technologies to prevent unauthorized use, ensure vehicle safety, and enhance the overall user experience. Key issues include:

1. Traditional ignition systems relying on keys or simple passwords are vulnerable to theft and unauthorized access.
2. Absence of dual-layer authentication, such as facial recognition and password fallback, increases security risks.
3. Most systems do not provide features like automatic locking, emergency shutdown, or reset options, leading to reduced reliability.

This project seeks to address these challenges by developing a comprehensive and reliable system.

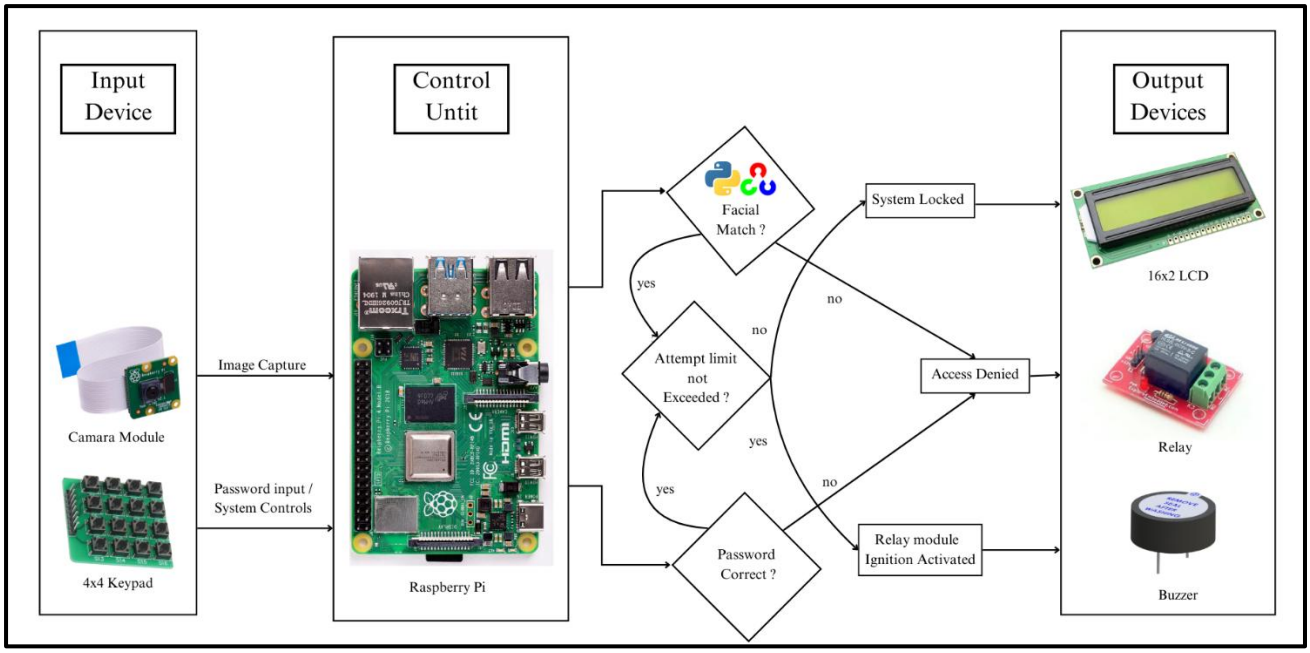
APPLICATIONS

1. **Two-Wheeler Security**: Enhances vehicle safety by preventing unauthorized ignition access through facial recognition and password authentication.
2. **Fleet Management:** Ideal for rental or shared vehicles to ensure only registered users can operate the vehicle.
3. **Personal Vehicles:** Provides individual vehicle owners with advanced security features against theft.
4. **IoT-Based Systems:** Demonstrates the application of IoT in real-world security scenarios, integrating hardware and software seamlessly.
5. **Smart Transportation:** Can be integrated into broader smart city initiatives for secure and automated transportation systems.
6. **Scalable Solutions:** The modular design allows scalability to other vehicles, such as cars or bicycles, and integration with GPS tracking systems.
7. **Customizable Access:** Useful for multi-user access, where different users can be granted permission through facial recognition.
8. **Educational Use:** Serves as a practical demonstration of IoT, AI, and embedded systems for academic and research purposes.

COMPONENTS

1. **Camera Module**: Captures images for facial recognition authentication.
2. **Relay Module**: Controls the ignition system by enabling or disabling the circuit.
3. **LCD Display**: Provides real-time status updates to the user, such as authentication success or failure.
4. **Raspberry Pi**: Acts as the central controller to manage system operations and run the authentication logic.
5. **Push Buttons/Switches**: Used for user inputs, such as entering the password or triggering emergency actions.
6. **Buzzer**: Alerts the user in case of failed attempts, system lock, or emergency shutdown.
7. **Power Supply Unit**: Powers the Raspberry Pi and other connected components.
8. **Python Programming**: Used for implementing facial recognition, password authentication, and system logic.
9. **Flask Framework**: Creates a lightweight server for handling facial recognition and API requests.
10. **OpenCV and face_recognition Libraries**: Perform image processing and facial authentication.
11. **GPIO Library**: Interfaces the Raspberry Pi with hardware components like relays, switches, and buzzer.

FLOWCHART



The flowchart illustrates the operation of the Anti-Theft Password-Based Ignition System, where input devices (camera and keypad) send data to the control unit (Raspberry Pi). The Raspberry Pi processes inputs using facial recognition and password verification. If the facial recognition fails, the system checks the password and monitors the attempt limit. Successful authentication activates the relay to unlock the ignition, while failed attempts trigger the buzzer or lock the system. Output devices like the LCD display show system status, the relay controls ignition, and the buzzer alerts unauthorized access. This ensures a secure and efficient anti-theft mechanism.

CONCLUSION

The **Anti-Theft Password-Based Ignition System** provides an innovative and secure solution to prevent unauthorized access to two-wheelers. By integrating technologies such as facial recognition, password authentication, and control mechanisms via Raspberry Pi, the system ensures a robust anti-theft framework. The use of a relay module for ignition control, coupled with an LCD display and buzzer for real-time feedback, enhances both functionality and user experience. This project demonstrates how modern technology can be effectively utilized to address security challenges, offering reliability, ease of use, and scalability for future enhancements such as AI integration.

FUTURE WORK

The **Anti-Theft Password-Based Ignition System** has significant potential for future enhancements to improve its functionality and scalability. Some key areas for future work include:

1. **Integration of AI-Based Security**: Incorporating advanced AI algorithms for improved facial recognition accuracy and real-time anomaly detection to identify suspicious activities around the vehicle.
2. **Biometric Authentication**: Adding features like fingerprint or voice recognition for multi-layered authentication to enhance security.
3. **Mobile Application Support**: Developing a mobile app for remote system control, notifications, and real-time monitoring of the vehicle's status.
4. **GPS and GSM Module Integration**: Enabling vehicle tracking and sending alerts via SMS in case of unauthorized access or theft attempts.
5. **IoT Connectivity**: Leveraging IoT to connect the system to a cloud server for data logging, analytics, and remote management.
6. **Battery Management**: Enhancing power efficiency to ensure the system operates effectively even during low-battery conditions.
7. **Vehicle Compatibility**: Expanding the system's compatibility to work with a variety of vehicles, including cars and electric bikes.
8. **Emergency Protocols**: Adding emergency features like panic buttons or automated calls to authorities in case of security breaches.

APPENDIX

PSEUDO CODE