VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi – 590014.

Internship Project Report

On

"Smart Intrusion detection system"

By

1. MOHAMMED DHARVESH MOHIDEEN S (1AP21ISO20)
2. NITHIN (1AP21CS032)
3. SRUJAN U BHAT (1AP21CS045)

Under the guidance of:
SAI CHARAN TEJA

2024 - 2025

A P S COLLEGE OF ENGINEERING

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

Evaluation Sheet

Title of the Project: Smart Intrusion detection System

Name of the Students: **1. Mohammed Dharvesh Mohideen S**

2. Nithin

3. Srujan U Bhat

External Supervisor:

_____

Internal Supervisor:

_____

_____

Date:

Place:

Project Completion Certificate

I, **Mohammed Dharvesh Mohideen S** (Roll No:1AP21IS020), hereby declare that the material presented in the Project Report titled **"Smart Intrusion Detection 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:**10-12-2024** **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: **Dr.Shivamurthaiah** **Guide Name: Sai Charan Teja**

Advisor's Signature **Guide Signature**

Project Completion Certificate

I, **Nithin** (Roll No: **1AP21CS032**), hereby declare that the material presented in the Project Report titled **"Smart Intrusion Detection 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:**10-12-2024** **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: Dr.Shivamurthaiah **Guide Name: Sai Charan Teja**

Advisor's Signature **Guide Signature**

Project Completion Certificate

I, **Srujan U Bhat** (Roll No: 1AP21CS045), hereby declare that the material presented in the Project Report titled **"Smart Intrusion Detection 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: **10-12-2024** **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: Dr.Shivamurthaiah **Guide Name: Sai Charan Teja**

Advisor's Signature **Guide Signature**

TABLE OF CONTENTS

CHAPTER 1

ABSTRACT

This project aims to develop a robust and intelligent Intrusion Detection System (IDS) to enhance the security of residential, commercial, or restricted areas. The system will utilize a real-time surveillance camera integrated with advanced facial recognition technology to monitor and detect individuals entering the monitored space. A database of authorized individuals' facial data will be maintained, and the system will continuously compare real-time camera feed inputs against this dataset.

If an unidentified individual is detected, the system will classify them as an unauthorized entity and trigger an automated alert mechanism. Notifications will be sent to the property owner or relevant authority via Twilio, a cloud-based communication platform, to ensure real-time response to potential security breaches. Additionally, the system will include features to log intrusion events, providing a record of activity for future reference.

The project will employ machine learning algorithms for facial recognition, enabling high accuracy in identifying authorized individuals while minimizing false alarms. The design will be modular, allowing future scalability to include additional functionalities such as motion detection, night vision compatibility, and integration with smart home systems.

This IDS will serve as a proactive and reliable solution for modern security challenges, ensuring faster response times, enhanced safety, and peace of mind for users in an increasingly dynamic threat landscape.

CHAPTER 2

INTRODUCTION

2.1 Objectives

The primary goal of this project is to develop an intelligent Intrusion Detection System (IDS) that ensures enhanced security through real-time surveillance and automated alert mechanisms. The system will use advanced technologies such as facial recognition and cloud-based communication platforms to deliver a comprehensive and reliable security solution.

2.2 Problem Statement

1. **Inefficiency of Conventional Systems:** Existing security systems primarily rely on motion sensors or human monitoring, which can lead to operational inefficiencies and are prone to false alarms.

2. **Lack of Individual Identification:** Traditional systems fail to differentiate between authorized and unauthorized individuals, reducing their effectiveness in real-world scenarios.

3. **Susceptibility to Human Error:** Systems that depend on human monitoring introduce the possibility of oversight or delayed responses, compromising security.

4. **Absence of Real-Time Notifications:** Many current solutions do not provide instant alerts, leading to delays in detecting and responding to intrusions.

5. **Inadequate Response Mechanisms:** Conventional systems lack automated mechanisms to alert property owners or authorities, limiting their ability to mitigate threats swiftly.

6. **Poor Scalability:** Traditional security solutions often lack modularity, making it difficult to adapt them for diverse environments, such as homes, offices, or public spaces.

7. **High False Alarm Rates:** Motion sensors and basic surveillance systems frequently generate false positives, causing unnecessary disruptions and reducing trust in the system.

8. **Need for Integration with Modern Technology:** Many existing solutions do not leverage advanced technologies such as facial recognition and cloud-based communication for enhanced functionality.

CHAPTER 3

APPLICATION

The Smart Intrusion Detection System (SIDS) is a versatile and practical solution with applications across a wide range of sectors. Its ability to identify unauthorized individuals and send real-time alerts makes it indispensable in enhancing security. The following are detailed use cases of the system:

Residential

The system provides homeowners with a reliable way to monitor their property, particularly during times when they are away. It acts as an early warning mechanism, preventing break-ins and trespassing by instantly alerting homeowners to the presence of unknown individuals. This feature is particularly beneficial for ensuring the safety of families with vulnerable members, such as young children or elderly individuals, who may be unable to respond quickly to potential threats.

Commercial

In offices and business settings, the IDS offers an efficient method to control access to sensitive areas while monitoring employees and visitors. By integrating with additional security measures such as automated locks and access control systems, it ensures a layered approach to protection. It enhances employee safety and protects valuable assets, making it a vital tool for ensuring business continuity.

Restricted

The IDS is highly suitable for securing restricted zones such as research laboratories, data centers, and military installations, where access must be strictly regulated. Its real-time identification of unauthorized individuals and the ability to log intrusion attempts make it an effective tool for maintaining the integrity of these critical spaces. The system ensures that any security breach is detected immediately, enabling swift action to mitigate risks.

Educational

The IDS offers a proactive way to enhance security in schools, colleges, and universities by monitoring and identifying unknown visitors on campus. This added layer of security helps safeguard students, faculty, and staff, fostering a safer learning environment. The system is

particularly valuable during events or periods when campuses experience higher foot traffic, ensuring that only authorized individuals are allowed in.

Healthcare

Hospitals and healthcare center benefit from the IDS by restricting access to sensitive areas like operation theaters, intensive care units, or pharmaceutical storage rooms. It ensures that only authorized medical personnel or staff members can enter, thus protecting patient privacy and valuable medical resources.

Retail And Commercial Space

For retail outlets and shopping malls, the IDS provides a way to monitor customer and staff activity. It can deter shoplifting or other criminal activities while also ensuring the safety of customers and employees. By integrating with existing security systems, it enhances the overall safety of these establishments.

Smart Homes And IoT-Enabled Environments

The system integrates seamlessly with other IoT devices in a smart home environment, providing a centralized platform for security. It can trigger additional responses, such as locking doors, activating alarms, or contacting emergency services, ensuring a comprehensive approach to safeguarding the home.

Industrial And Warehouse Facilities

In industrial setups, the IDS monitors unauthorized access to areas housing expensive equipment or hazardous materials. It ensures the safety of both personnel and assets by detecting and alerting against any intrusion attempts.

CHAPTER 4

COMPONENTS

Hardware Components

1. **Raspberry Pi**: Raspberry Pi is a small, affordable single-board computer used for a variety of projects, including automation, education, and IoT applications. It features a versatile ARM processor, GPIO pins for hardware interfacing, and supports various operating systems, primarily Linux-based. Its compact size and low cost make it an ideal platform for prototyping and learning about computing and electronics.

Acts as the central processing unit for the smart home system.

2. **Ultrasonic Sensor (HC-SR04)**: The Ultrasonic Sensor (HC-SR04) is a distance-measuring sensor that uses sound waves to detect objects and measure their distance. It consists of two components: a transmitter that emits ultrasonic waves and a receiver that listens for the echo. It is commonly used in robotics and automation projects for obstacle detection and range measurement.

Measures proximity to detect objects near the door.

3. **Power Supply:**

Provides power to all components.

4. **Camera:** The camera is used to continuously monitor the area for detecting individuals. It captures real-time video footage, which is processed by the facial recognition software to identify known and unknown faces. The camera serves as the primary input device for triggering the security alerts when an unknown person is detected.

Used for continuous monitoring and capturing real-time video feeds for facial recognition.

5. **Wi-Fi Module (built-in or external):** The Wi-Fi module enables wireless communication between the Raspberry Pi and the cloud for real-time notifications. It allows the system to send alerts and communicate with the Twilio platform for instant owner notifications.

Enables communication with the cloud for notifications and remote monitoring.

6. **Laptop Hardware:**

Serves as a development and testing platform for coding, training facial recognition models, and integrating the system components.

Software Components

1. **Flask Framework**:

   For building the web application.

2. **Twilio API:**

   Sends SMS alerts to the user.

3. **Python(3.10+)**:

   Implements the logic for hardware interaction and web application functionalities.

4. **OpenCV:**

   Utilized for real-time image processing, including capturing video feeds and preprocessing facial data.

5. **face_recognition:**

   Python library used for facial recognition tasks, including encoding and comparing faces to identify known and unknown individuals.

CHAPTER 5

FLOWCHART

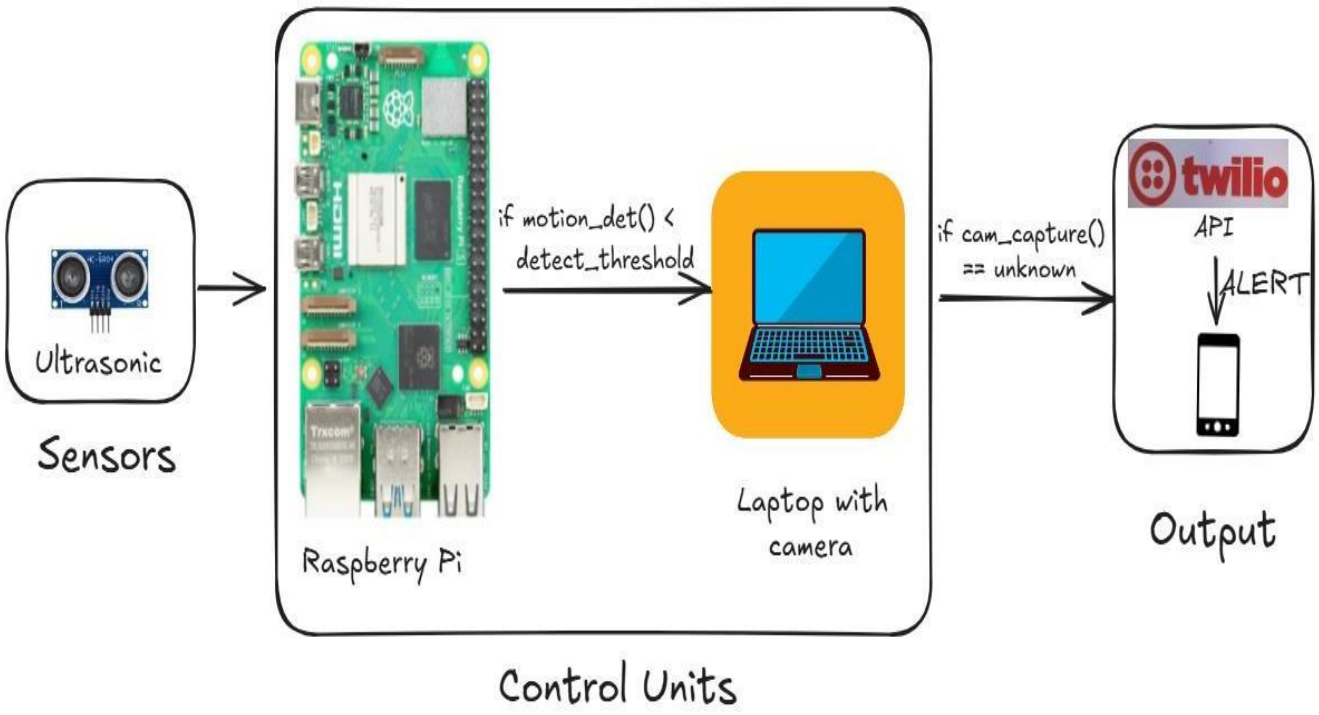

FIGURE : The flow of the SID system

CHAPTER 6

FUTURE WORK

1. **Integration with IoT Devices:** Extend the system to connect with IoT-enabled devices such as smart locks, lights, and alarms to automate additional security measures.

2. **Enhanced Facial Recognition:** Improve the facial recognition model's accuracy using advanced machine learning techniques to better handle varying lighting, angles, and occlusions.

3. **Night Vision Capability:** Incorporate infrared cameras to enable effective monitoring and detection in low-light or nighttime conditions.

4. **Multi-Camera Support:** Expand the system to support multiple cameras for monitoring larger areas or different locations simultaneously.

5. **Mobile Application Development:** Create a dedicated mobile app to provide users with real-time alerts, live video feeds, and control over system settings.

6. **Edge Computing:** Implement edge computing techniques to process data locally on the hardware, reducing dependency on cloud services and ensuring faster detection.

7. **Intruder Behavior Analysis:** Introduce behavior analysis algorithms to predict potential threats based on movement patterns or other characteristics.

8. **Integration with Law Enforcement:** Develop an optional feature to alert local authorities in case of persistent or severe intrusion attempts.

9. **Scalability for Public Spaces:** Adapt the system for use in public spaces such as airports, stadiums, or city surveillance to enhance safety at a larger scale.

10. **Voice-Based Authentication:** Add voice recognition as an additional layer of authentication for identifying authorized individuals.

CHAPTER 7

CONCLUSION

The project successfully demonstrated a practical, real-time security solution using facial recognition technology. We developed a system that utilized a camera to monitor an area, with known faces stored in a dataset for comparison. When an unknown person was detected by the camera, the system recognized them and sent a warning notification to the owner via Twilio, ensuring prompt alerts.

Through this project, we addressed the limitations of traditional security systems such as motion sensors and manual monitoring by creating a more reliable and automated solution. By utilizing OpenCV and the face_Recognition library, we achieved accurate facial identification and rapid detection. Twilio's integration allowed for instant communication, ensuring that the owner was immediately informed of any unauthorized access.

The system minimized false alarms and human errors, making it a dependable security solution for various environments, including residential properties, businesses, and public spaces. We also designed the system to be modular and scalable, allowing for potential future improvements, such as adding night vision, supporting multiple cameras, and integrating with IoT devices. This project provided a solid foundation for developing a more advanced, future-proof security system.

CHAPTER 8

APPENDIX

8.1 Pseudo Code

BEGIN Smart Intrusion Detection System

1. Initialize System:
   LOAD known faces, CONFIGURE sensors and webcam, SET up Twilio API.

2. Monitor Motion:
   WHILE active, IF motion detected, CALL trigger_webcam().

3. Trigger Webcam:
   CAPTURE image, CALL recognize_faces(image).

4. Face Recognition:
   DETECT faces, COMPARE with known faces.
   IF unknown, CALL send_alert("Unknown face detected").
   ELSE, LOG recognized face activity.

5. Send Alert:
   SEND message using Twilio API.

6. Log Activity:
   SAVE data, UPDATE web interface.

7. Terminate:
   WHEN system off, TERMINATE processes.

END Smart Intrusion Detection System

8.2 Pseudocode Flow Diagram