KARNATAK LAW SOCIETY's

SHRI VASANTRAO POTDAR POLYTECHNIC (457)

Tilakwadi, Belagavi-590006

ESTD-1992

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

A Report on

"THEFT ALERT DETECTOR"

A project report submitted in partial fulfillment of the requirement award

Diploma in Computer Science & Engineering

By the Board of Technical Examination, Bengaluru.

for the Academic year 2022-23

SUBMITTED BY

Mr. Rohit Yakkundi	**[457CS20031]**
Mr. Rohit Gandhi	**[457CS20032]**
Mr. Roman Devadi	**[457CS20033]**

UNDER THE GUIDANCE OF

Prof. Upama Kulkarni

SSL, Department of Computer Science and Engineering

2022-2023

KARNATAK LAW SOCIETY's
SHRI VASANTRAO POTDAR POLYTECHNIC (457)

Tilakwadi, Belagavi – 590006

ESTD-1992

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Certificate

Certified that this project report entitled **"THEFT ALERT DETECTOR"** which is submitted by bonafide student **Mr. Roman Devadi Reg. No. 457CS20033**, of **KLS's Shri Vasantrao Potdar Polytechnic, Belagavi.** in partial fulfillment for the award of **Diploma in Computer Science & Engineering** during the year **2022-2023** is record of student own work carried out under my/our guidance. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report and one copy of it is being deposited in the department.

The project report is approved as it satisfies the academic requirements in respect of project work prescribed for the said Diploma.

It is further understood by this certificate that the undersigned do not endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the project only for the purpose it is submitted.

for Nandini U.C.D

Prof. Upama Kulkarni
Guide

For. G.A.Bedekar

Prof. Anuradha Desai
Head of Department

Head of Department
Department of Computer Science
KLS' Shri V. P. Polytechnic
Tilakwadi, Belgaum-6

Prof. Shridevi Malaj
Principal

Principal
K.L.S's Shri Vasantrao Potdar Polytechnic
Tilakwadi, Belgaum - 06.

Name and Signature of Examiners:

1. R.K. Patil

2. _____

DECLARATION

I, **Roman Devadi** the student of Diploma in Computer Science and Engineering Department bearing Register Number 457CS20033 of KLS's Shri Vasantrao Potdar Polytechnic, hereby declare that, I own full responsibility for the information, results and conclusions provided in this project work titled **"THEFT ALERT DETECTOR"** submitted to **Board of Technical Examinations, Government of Karnataka** for the award of **Diploma in Computer Science and Engineering**. To the best of my knowledge, this project work has not been submitted in part or full elsewhere in any other institution/ organization for the award of any certificate/diploma/degree. I have completely taken care in acknowledging the contribution of others in this academic work. I further declare that in case of any violation of intellectual property rights and particulars declared, found at any stage, I, as the candidate will be solely responsible for the same.

Date: 17-06-2023

Place: Belagavi

Roman Devadi

457CS20033

ACKNOWLEDGMENT

I would like to thank our mentor and advisor **Mrs. Upama Kulkarni,** who provided valuable assistance and support during the development of this theft alert detector. Her continuous insightful discussions, and constructive feedback greatly helped improve the project. Her belief in the project's potential has been a constant source of motivation for us.

I would also like to thank the individuals who participated in user testing and provided valuable feedback **Mrs. Anuradha Desai, Head of Department, CSE** on the theft alert detector system. Their involvement helped improve the user experience and enhance the functionality of the system. I am grateful for their willingness to contribute their time and expertise.

I am grateful to **KLS's Shri Vasantrao Potdar Polytechnic** and **Principal, Smt. Shridevi S. Malaj** for her generous support, both financially and in terms of resources. Their assistance in providing necessary software, infrastructure and datasets played a crucial role in successfully implementing this project. I appreciate their commitment to fostering innovation and research.

I express my gratitude to the creators and contributors of OpenCV, the computer vision library that served as the foundation for this project, I feel honored to have benefitted from their ingenuity.

I acknowledge my family and loved ones for their unwavering support, encouragement, and understanding throughout this project. Their belief in me and their continuous encouragement have been a constant source of inspiration.

EXECUTIVE SUMMARY

This project report presents the development and implementation of a theft alert detector utilizing OpenCV, a popular computer vision library. The objective of this project was to design a system that can detect and alert users about potential theft incidents in real-time, based on visual analysis.

The project employed various image processing and computer vision techniques, such as object detection, motion analysis, and event triggering. The theft alert detector was implemented using a webcam or surveillance camera as the input source, and it utilized algorithms provided by OpenCV to analyze the captured frames.

The results of the project demonstrate the successful detection of theft-related events, including unauthorized object removal, suspicious object placement, and unexpected motion patterns. The system achieved a high accuracy rate in identifying theft incidents while minimizing false alarms. The alert mechanism involved real-time notifications through email or SMS to provide immediate information to the users.

The developed theft alert detector holds promising applications in various scenarios, including home security, retail loss prevention, and public surveillance. Its potential to mitigate theft incidents and enhance overall security makes it a valuable asset for individuals and organizations concerned with preventing theft.

Further improvements and future work may include integrating advanced machine learning techniques to enhance the system's detection capabilities, optimizing the performance for larger-scale environments, and exploring additional alert mechanisms.

TABLE OF CONTENTS

Sl. No.	Description	Page No.
1	**Chapter 1** **1.1 Introduction** **1.2 Scope of the capstone project**	1 - 3
2	**Chapter 2** **2.1 Capstone project planning** 2.1.1 Work breakdown structure (WBS) 2.1.2 Timeline Development – Schedule 2.1.3 Cost Breakdown Structure (CBS) 2.1.4 Capstone project Risks assessment **2.2 Requirements Specification** 2.2.1 Functional 2.2.2 Non-functional (Quality attributes) 2.2.3 User input 2.2.4 Technical constraints **2.3 Design Specification** 2.3.1 Chosen System Design 2.3.2 Discussion of Alternative Designs 2.3.3 Detailed Description of Component/Subsystem 2.3.4 Component 1- n	4 - 20
3	**Chapter 3** **3.1 Approach and Methodology** Discuss the Technology/Methodologies/use cases/ programming/ modelling/ simulations/ analysis/ process design/product design/ fabrication/etc. used in the capstone project	21 - 37
4	**Chapter 4** **4.1 Test and validation** 4.1.1 Test Plan 4.1.2 Test Approach 4.1.3 Features Tested 4.1.4 Features not Tested 4.1.5 Findings 4.1.6 Inference	38 - 46

5	**Chapter 5** **5.1 Business Aspects** 5.1.1 Discuss the novel aspects of this service or product. Address why a company or investors should invest money in this product or service. 5.1.2 Briefly describe the market and economic outlook of the capstone project for the industry 5.1.3 Highlight the novel features of the product/service. 5.1.4 How does the product/service fit into the competitive landscape? 5.1.5 Who are the possible capstone projected clients/customers? **5.2 Financial Considerations** 5.2.1 Capstone project budget 5.2.2 Cost capstone projection needed for either for Profit/Non-Profit option **5.3 Conclusion and Recommendation** 5.3.1 Describe state of completion of capstone project. 5.3.2 Future Work 5.3.3 Outline how the capstone project may be extended	47 - 63
6	References	64-65
7	Appendices	66 - 70

LIST OF FIGURES

SL.NO	FIGURES NO.	DESCRIPTION	PAGE NO.
1	Figure 2.1	Work breakdown structure	04
2	Figure 2.2	Timeline development schedule	05
3	Figure 2.3	Component 1- n	18
4	Figure 3.1	Methodology	24
5	Figure 3.2	Use cases	26
7	Figure 3.4	Process Design Diagram	35
8	Figure 7.2	Experimental Results	68
9	Figure 7.3	User Manual	69-70

CHAPTER 1

1.1 Introduction To Theft Alert Detector

Theft is a prevalent concern in today's society, and the need for effective security systems that can detect and prevent theft has become increasingly important. This project report introduces the concept of a Theft Alert Detector that utilizes OpenCV (Open Source Computer Vision Library) as a core technology for enhancing its surveillance capabilities. The Theft Alert Detector powered by OpenCV is a sophisticated security system designed to monitor and identify suspicious activities or unauthorized access in various settings. OpenCV, a popular computer vision library, provides a range of powerful tools and algorithms for image and video processing, enabling the system to analyze visual data and make intelligent decisions in real-time.This project report aims to provide an overview of the Theft Alert Detector system using OpenCV, highlighting its purpose, features, and potential benefits. It explores how OpenCV can be leveraged to enhance the system's surveillance capabilities and improve theft detection accuracy.

The primary objective of this project report is to present a comprehensive understanding of the integration of OpenCV in the Theft Alert Detector, serving as a foundation for further research and development in the field of security systems. It aims to shed light on the potential applications of OpenCV in theft prevention, such as in residential homes, commercial establishments, and other locations vulnerable to theft.

The subsequent sections of this report will delve into the specific components and functionalities of the Theft Alert Detector utilizing OpenCV. It will outline the system's architecture, the integration of cameras and sensors with OpenCV, the implementation of image and video processing techniques, and the utilization of machine learning algorithms for theft detection.

By utilizing OpenCV, the Theft Alert Detector gains the ability to analyze visual data in real-time, detect anomalies, track objects, and identify potential theft incidents more accurately. This project report aims to showcase the capabilities of OpenCV in enhancing security systems, enabling stakeholders to make informed decisions about implementing this technology to protect their properties and assets.

Overall, the integration of OpenCV in the Theft Alert Detector represents an innovative approach to theft prevention and security. This project report aims to provide insights into its effectiveness, reliability, and potential impact, paving the way for future advancements in security systems leveraging computer vision technologies like OpenCV.

1.2 Scope of The Capstone Project

The scope of a capstone project for a Theft Alert Detector can encompass various aspects related to the integration of OpenCV and the development of a robust security system. Here are some key elements that can be considered within the scope of the project:

1.**System Design and Architecture:** The capstone project can involve designing the overall system architecture for the Theft Alert Detector using OpenCV. This includes defining the components, such as cameras, sensors, and the central monitoring system, and establishing the data flow and communication between these components.

2.**Integration of OpenCV:** The core focus of the project would be on integrating OpenCV into the Theft Alert Detector system. This involves leveraging the various features and algorithms provided by OpenCV, such as image and video processing, object detection, tracking, and recognition, to enhance the system's surveillance capabilities and theft detection accuracy.

3.**Camera Setup and Calibration:** Setting up the surveillance cameras and calibrating them for optimal performance is crucial. This may involve tasks such as camera placement, camera configuration, and ensuring proper alignment and calibration for accurate image and video analysis using OpenCV.

4.**Image and Video Processing:** The capstone project can include the implementation of image and video processing techniques using OpenCV. This may involve tasks such as noise reduction, image enhancement, object detection and tracking, motion detection, and extracting relevant features for theft detection.

5.**Theft Detection Algorithms:** Developing theft detection algorithms using OpenCV is a significant aspect of the project. This can include the application of machine learning and computer vision techniques to identify suspicious activities, differentiate between normal and abnormal behavior.

6.**Real-time Monitoring and Alerting:** Implementing real-time monitoring and instant alerting mechanisms is crucial for the Theft Alert Detector system. This may involve integrating OpenCV with other components of the system,to provide immediate alerts when theft or suspicious activities are detected.

7.**Testing and Evaluation:** Conducting thorough testing and evaluation of the Theft Alert Detector system is important to assess its performance and effectiveness. This may involve performing various test scenarios, evaluating the accuracy of theft detection, and making necessary adjustments and refinements based on the test results.

8.**Documentation and Project Report:** As with any capstone project, documenting the design, implementation, and testing processes is crucial. This includes creating clear and concise technical documentation and preparing a final project report that outlines the objectives, methodology, and outcomes of the capstone project.

CHAPTER 2

2.1 Capstone Project Planning

2.1.1 Work breakdown structure (WBS)

A Work Breakdown Structure for a Theft Alert Detector project can help organize the tasks and activities involved in its development

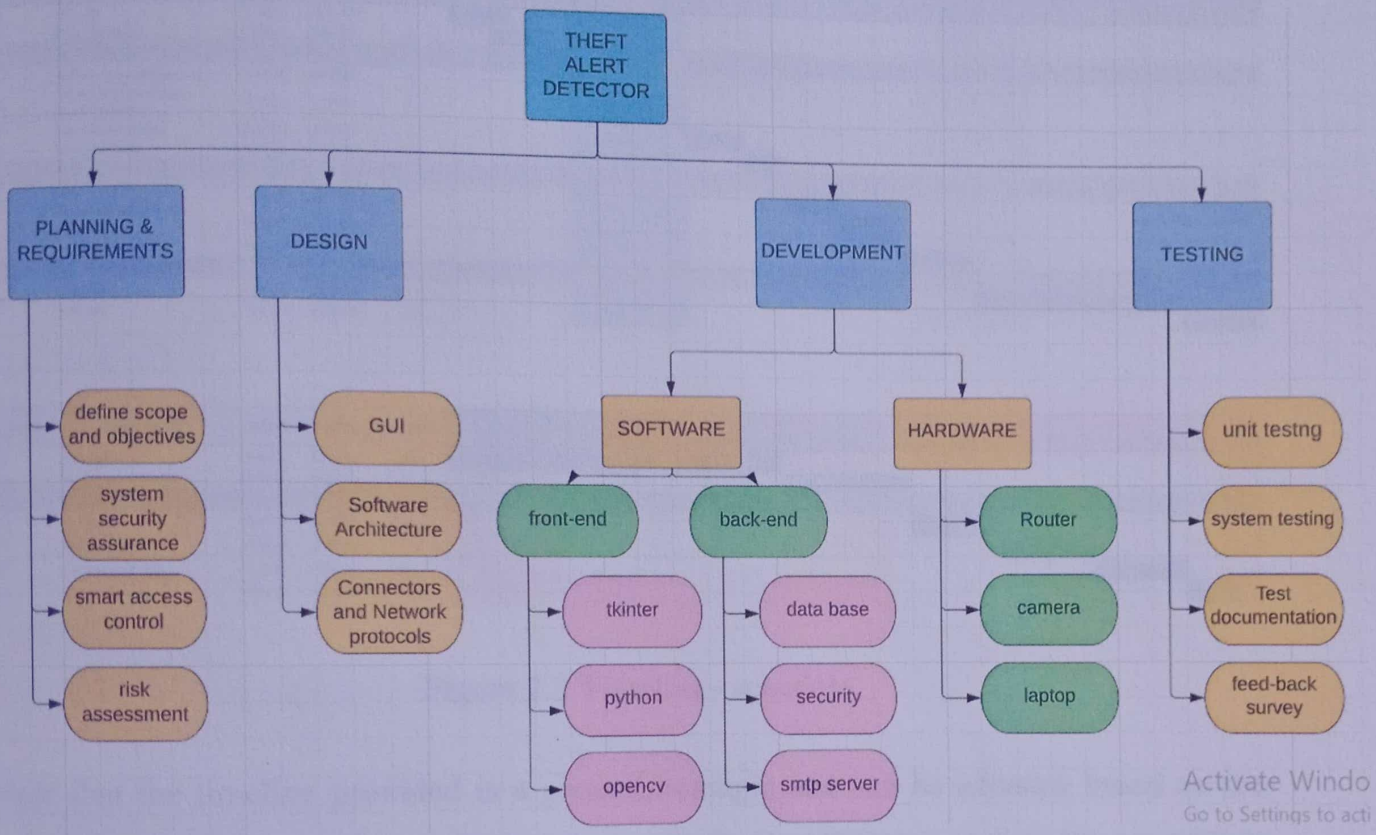


Figure 2.1 Work breakdown structure

By breaking down the project into these specific tasks and sub-tasks, the WBS provides a clear framework for project management, resource allocation, and tracking progress. It helps ensure that all crucial aspects of the Theft Alert Detector development are addressed and completed systematically.

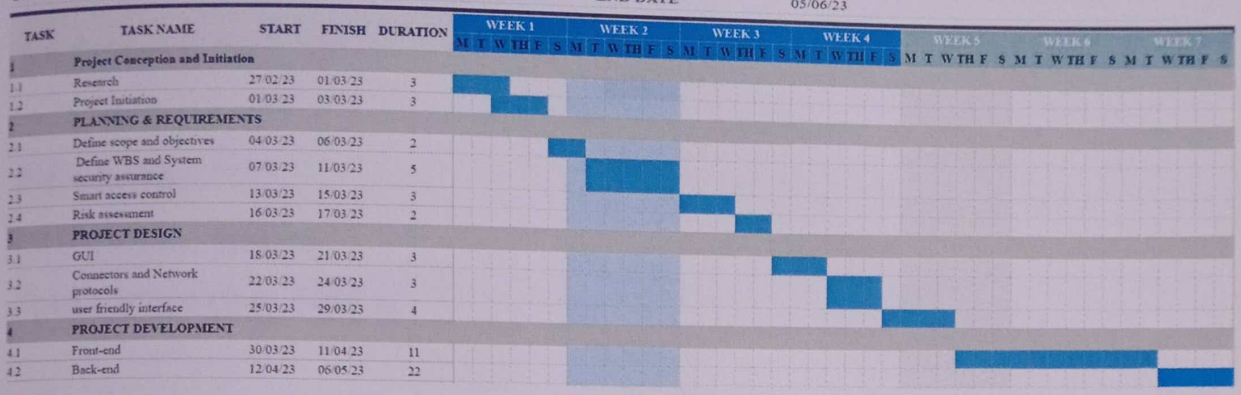
2.1.2 Timeline development – schedule

Developing a timeline or schedule for a Theft Alert Detector project helps in effectively managing tasks and ensuring timely completion of the project.

GANTT CHART

PROJECT TITLE: Theft alert detecter — START DATE: 27/2/2023
PROJECT MEMBERS: Rohit Y, Rohit G, Roman D. — END DATE: 05/06/23

TASK	TASK NAME	START	FINISH	DURATION
1	**Project Conception and Initiation**			
1.1	Research	27/02/23	01/03/23	3
1.2	Project Initiation	01/03/23	03/03/23	3
2	**PLANNING & REQUIREMENTS**			
2.1	Define scope and objectives	04/03/23	06/03/23	2
2.2	Define WBS and System security assurance	07/03/23	11/03/23	5
2.3	Smart access control	13/03/23	15/03/23	3
2.4	Risk assessment	16/03/23	17/03/23	2
3	**PROJECT DESIGN**			
3.1	GUI	18/03/23	21/03/23	3
3.2	Connectors and Network protocols	22/03/23	24/03/23	3
3.3	user friendly interface	25/03/23	29/03/23	4
4	**PROJECT DEVELOPMENT**			
4.1	Front-end	30/03/23	11/04/23	11
4.2	Back-end	12/04/23	06/05/23	22



TASK	TASK NAME	START	FINISH	DURATION
4.2	Back-end	12/04/23	06/05/23	22
4.3	Hardware development	08/05/23	15/05/23	7
5	**TESTING**			
5.1	Unit testing	16/05/23	20/05/23	5
5.2	System testing	22/05/23	26/05/23	5
5.3	Test documentation	27/05/23	01/06/23	5
5.4	Feed-back survey	02/06/23	05/06/23	3

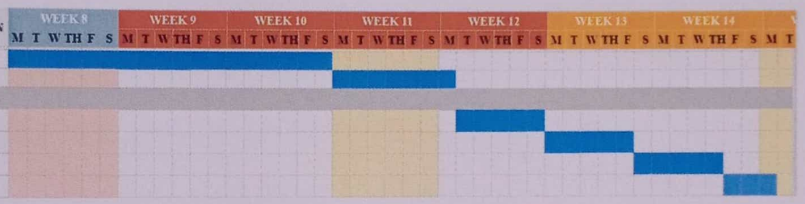


Figure 2.2 Timeline– schedule

Note that the timeline provided is a general example and can be adjusted based on the specific requirements and complexity of your Theft Alert Detector project. It's essential to regularly monitor the progress of the project and adjust the timeline if necessary to ensure successful completion.

2.1.3 Cost breakdown structure (CBS)

A Cost Breakdown Structure (CBS) is a hierarchical representation of the project's cost elements, providing a comprehensive breakdown of the project's expenses. It helps in understanding and managing the financial aspects of the project.

1.Internet

Monthly Internet Plan: 333.3 rs

Total Internet Cost: 1000 rs

2.Call Alert Sender

Twilio Subscription :1700 rs

Total alert Cost:1700 rs

3.Courses

Online Course Subscription: 650 rs

Total Courses Cost: 650 rs

4.Camera

USB Camera: 1000 rs

Total Camera Cost: 1000 rs

5.Cables

USB Cables: 200 rs

Total Cables Cost: 200 rs

6.Software

PyCharm Pro Subscription: 1500 rs

7.Power Consumed

Per Week Charges(64W =6.6rs):20 rs

Total Power Consumption :280 rs

8. PC Charges

Per System Cost:62,000 rs

Total System Cost(3 laptops):1,86,000 rs

Total Project Cost: 1,92,330 rs

These costs may vary depending on the specific brands, models, and features of each item.

2.1.4 Capstone project risks assessment

❖ **Risk Identification**

1.Technical Risks:

- Malfunctioning of sensors.
- Inadequate notification system.
- Difficulty in integrating the backend system.
- Test the sensors extensively before deployment.
- Conduct thorough testing of the notification system.

2. Schedule Risks:

- Project delays due to unforeseen issues.
- Resource constraints leading to missed deadlines.
- Build in contingency time in the project plan.
- Assign tasks to team members based on their availability and expertise.

3. Security Risks:

- Hacking of the device or app, leading to unauthorized access.
- Loss of data due to no frequent system updates or data backups.
- Sensitive users data leakage from the organization's database.

4. Legal Risks:

- Patent infringement or intellectual property disputes
- Conduct a thorough search for existing patents and intellectual property
- Consult with legal experts to ensure compliance with relevant laws and regulations

5.Risk Monitoring and Control

- Regularly review the project plan and budget to identify potential risks.
- Adjust the project plan as necessary to address unforeseen issues or risks that arise.
- Conducting regular testing and monitoring of the device to detect any security vulnerabilities or technical issues.

This risk analysis covers potential technical, schedule, financial, security, and legal risks associated with the theft alert detector project. It also outlines specific risk mitigation strategies to address each identified risk, as well as a risk monitoring and control plan to ensure that any new risks are promptly identified and addressed.

2.2 Requirements Specification

2.2.1 Functional:

1. **Motion Detection:** The system should be able to detect motion within the protected area using sensors or cameras.
2. **Object Detection and Tracking:** The system should be capable of detecting and tracking objects within the captured video or images.
3. **Theft Identification:** The system should be able to identify potential theft incidents based on predefined criteria or suspicious activities.
4. **Real-time Monitoring:** The system should provide real-time monitoring of the protected area to enable immediate response to theft incidents.
5. **Alerting Mechanism:** The system should have a mechanism to promptly alert users or authorities in the event of a theft detection.
6. **User Interface:** The system should have a user-friendly interface to configure settings, view monitoring feeds, and manage alerts.

2.2.2 Non-functional:

1. **Performance:** The system should provide accurate and timely theft detection with minimal latency.
2. **Reliability:** The system should operate reliably without frequent false alarms or missed detections.
3. **Scalability:** The system should be scalable to accommodate additional cameras or sensors as needed.
4. **Security:** The system should have robust security measures to prevent unauthorized access and ensure the privacy of captured data.
5. **Usability:** The system should be easy to install, configure, and use by both technical and non-technical users.
6. **Compatibility:** The system should be compatible with different camera models, sensors, and operating systems.
7. **Maintainability:** The system should be designed with modularity and ease of maintenance in mind for future updates and enhancements.
8. **Efficiency:** The system should utilize system resources efficiently to minimize computational requirements and power consumption.

2.2.3 User input

This process adds an extra layer of security since the user would need both their login credentials (something they know) and the OTP from their 2FA app (something they have) to gain access to the software.

1. **User Registration:** Users create an account on your software platform and provide their login credentials (username and password).
2. **Enable 2FA:** Users have the option to enable two-factor authentication for their account.
3. **Mobile Application:** Users would need to download a 2FA mobile application, such as Google Authenticator or Authy, on their smartphone.
4. **Linking the Account:** Users link their software account with the 2FA app by scanning a QR code or manually entering a unique code provided by the software.
5. **Login Process:** When users attempt to log in to the software, they enter their username and password as usual.
6. **OTP Generation:**Upon successful authentication of the login credentials,an OTP (One-Time Password) is generated by the 2FA app on the user's smartphone.
7. **Entering OTP:** Users enter the OTP from the app into the software platform.
8. **OTP Validation:** The software platform verifies the entered OTP with the OTP generated by the 2FA app.
9. **Access Granted:** If the OTP is valid, the user is granted access to the software.

2.2.4 Technical constraints

Here are a few potential technical constraints for a Theft Alert Detector project:

1. **Camera and Sensor Limitations:**
   - Constraints at the variety of cameras and sensors that can be deployed in the included area due to budget or logistical obstacles.
   - Compatibility constraints with particular digital camera fashions or sensor kinds, which may also limit the options available for integration.
2. **Computing Power and Memory:**
   - Constraints at the processing power and memory potential of the hardware gadgets going for walks the robbery detection algorithms.
   - Limitations on the computational abilities of the system, which might also have an effect on actual-time detection and response.

3.Network Connectivity:

- Dependence on solid network connectivity for transmitting video or photograph statistics to the tracking machine.
- Constraints on bandwidth or network infrastructure that can affect the rate and reliability of information transmission.

4.Lighting Conditions:

- Limitations posed with the aid of varying lighting fixtures conditions, including low-mild environments or excessive glare, which can have an effect on the accuracy of picture or video evaluation.

5.Power Supply:

- Constraints on power availability and intake, mainly in far off or outdoor settings, which can also require power-green answers or alternative strength resources.

6.Environmental Factors:

- Environmental constraints, along with severe climate situations or bodily obstructions, that can affect the location and overall performance of cameras and sensors.

7.Software and Algorithm Limitations:

- Constraints related to the talents and barriers of the selected software libraries, frameworks, or algorithms for robbery detection.
- Computational constraints which could arise from complex or resource-intensive algorithms, impacting actual-time performance.

8.Privacy and Data Protection:

- Compliance with privateness policies and ethical concerns whilst managing and storing captured information.
- Constraints on data retention, anonymization, and encryption to make sure the security and privacy of sensitive data.

9.Cost Constraints:

- Budget obstacles which could affect the selection of hardware components, sensors, or software licenses.

Constraints at the availability of monetary assets for ongoing upkeep and assistance.

These technical constraints should be cautiously taken into consideration at some stage in the design and implementation of the Theft Alert Detector machine to make certain that the chosen technology and solutions align with the mission's barriers and necessities.

2.3 Design Specification

2.3.1 Chosen system design

1.System Overview:

- Description: The Theft Alert Detector is a surveillance system designed to screen and locate capability robbery incidents in a covered vicinity.
- Purpose: To beautify security features and offer real-time signals for suspicious sports.

2.Functional Requirements:

- **Motion Detection:** The gadget ought to be able to locate and tune movement in the monitored place.
- **Object Recognition:** The gadget must be capable of identifying and tracking gadgets of hobby, such as human beings or vehicles.
- **Theft Detection Criteria**: The machine ought to enforce person-described criteria to distinguish among everyday activities and ability robbery incidents.
- **Real-time Alerting:** The system has to generate immediate indicators to inform users while an ability robbery incident is detected.
- **Alert Notifications:** The system ought to offer bendy alerting options, consisting of email, SMS, and cellular app notifications.
- **Monitoring and Logging**: The machine has to constantly screen the protected vicinity and maintain a log of detected activities for destiny reference and evaluation.
- **User Interface:** The gadget has to have a user-friendly interface for configuring settings, viewing signals, and getting access to gadget logs.

3.Non-useful Requirements:

- **Performance:** The device has to system video feeds and analyze statistics in actual-time with minimal latency.
- **Reliability:** The gadget must have high availability and be resilient to disasters to make sure continuous monitoring and alerting.
- **Security:** The gadget must ensure the confidentiality, integrity, and privateness of captured information and user information.
- **Scalability:** The gadget needs to be capable of managing increasingly cameras and sensors as the included place expands.

- **Compatibility:** The device needs to be compatible with numerous camera fashions, network configurations, and running structures.
- **Usability:** The user interface has to be intuitive, person-friendly, and available to both technical and non-technical customers.
- **Maintainability:** The system ought to be clean to hold and improve, bearing in mind future enhancements and computer virus fixes.

4.Design and Implementation Details:

- **Camera Integration:** The machine will utilize OpenCV library for digital camera integration, video processing, and object detection.
- **Motion Detection Algorithm:** The gadget will put into effect a movement detection set of rules based on background subtraction and frame differencing strategies.
- **Object Recognition:** The machine will utilize a pre-skilled system studying fashions, together with Haar cascades or deep gaining knowledge of fashions, for item recognition.
- **Alerting Module:** The device will contain a module for producing actual-time signals based totally on user-defined robbery detection criteria.
- **User Interface Design:** The consumer interface could have a responsive layout, offering an intuitive dashboard for configuring gadget settings, viewing indicators, and accessing logs.

5.Integration and Testing Requirements:

- **Integration:** The gadget needs to be well matched with numerous digital camera fashions and have to provide options for integrating with existing safety structures or structures.
- **Testing:** The machine will undergo rigorous testing to validate its functionalities, together with unit trying out, integration checking out, and consumer attractiveness testing.
- **Performance Testing:** The system's performance may be evaluated to ensure it meets the desired responsiveness and processing competencies.

6.Deployment and Maintenance Considerations:

- **Deployment:** The device could be deployed on a devoted server or cloud infrastructure to ensure continuous availability and scalability.
- **Maintenance:** The device must have a clean maintenance plan, inclusive of ordinary updates, malicious program fixes, and security patches.
- The Design Specification presents an in depth outline of the gadget's purposeful and non-functional necessities, implementation details, integration issues, and deployment considerations for the Theft Alert Detector venture.
- The Design Specification provides a detailed outline of the system's functional and non-functional requirements, implementation details, integration considerations, and deployment considerations for the Theft Alert Detector project.

2.3.2 Discussion of alternative designs

When designing a theft alert detector system, various alternative designs and approaches can be considered. Here are some alternative design considerations for the theft alert detector:

1.Different Motion Detection Techniques:

Alternative 1: Background Subtraction - Instead of relying solely on motion detection, the system could use background subtraction algorithms to detect changes in the background scene and identify potential objects of interest.

Alternative 2: Optical Flow - Optical flow algorithms can track the movement of pixels between frames, allowing for more accurate motion detection and object tracking.

2.Alternative Object Recognition Methods:

Alternative 1: Deep Learning Models - Instead of using Haar cascades or traditional computer vision algorithms for object recognition, deep learning models, such as convolutional neural networks (CNNs), can be employed to improve accuracy and robustness.

Alternative 2: Feature-based Matching - Utilizing feature-based matching techniques, such as SIFT (Scale-Invariant Feature Transform) or SURF (Speeded-Up Robust Features), to identify and track specific objects of interest.

3.Alert Delivery Mechanisms:

Alternative 1: Push Notifications - Instead of SMS or voice call alerts, the system could employ push notifications to mobile devices through dedicated mobile applications, providing real-time alerts to users.

Alternative 2: Integration with Messaging Platforms - Integrating with popular messaging platforms, such as WhatsApp or Telegram, to send alerts as messages or multimedia files.

4.Cloud-based Processing:

Alternative 1: Cloud-based Object Recognition - Offloading object recognition tasks to cloud-based services, such as cloud-based AI platforms, to leverage their computational power and scalability.

Alternative 2: Cloud Storage and Analytics - Storing video footage in the cloud and performing analytics and event detection using cloud-based services, enabling remote access and analysis of the captured data.

5.Hybrid Approaches:

Alternative 1: Combination of Sensors - Integrating other sensors, such as infrared motion sensors or proximity sensors, along with video analysis, to enhance the detection accuracy and reduce false positives.

Alternative 2: Multi-camera System - Utilizing multiple cameras placed strategically to cover a wider area and improve the accuracy and coverage of theft detection.

The selection of the design approach should consider factors such as accuracy, computational requirements, cost, scalability, and specific project requirements. It is essential to evaluate the pros and cons of each alternative design to determine the most suitable approach for the theft alert detector system.

2.3.3 Detailed description of components/subsystems

1.Camera Integration Module:

The Camera Integration Module is responsible for integrating with cameras or video surveillance systems to capture live video feeds from the protected place using OpenCV.

- **Technical Specifications:**

Utilizes OpenCV library capabilities and APIs to establish connections with cameras and retrieve video streams.

- Implements digicam configuration settings, such as decision, frame fee, and camera parameters, the use of OpenCV's competencies.
- Handles digicam communication protocols, ensuring dependable and efficient video feed retrieval.
- Converts video streams right into a suitable format for similarly processing by different components.

2.Motion Detection and Object Recognition Module:

The Motion Detection and Object Recognition Module processes video feeds the usage of OpenCV to hit upon motion and recognize objects of hobby.

- **Motion Detection:**

The motion detection component of the module plays a crucial role in identifying any movement within the monitored area. It employs techniques such as frame differencing, background subtraction, and optical flow analysis to detect motion. By continuously comparing consecutive frames, it can pinpoint areas where motion occurs and provide detailed information, including the location, size, and trajectory of the moving objects. This functionality allows the system to distinguish between normal activities and suspicious behavior, triggering alerts when unauthorized motion is detected.

- **Object Recognition:**

The object recognition component of the module focuses on identifying and classifying objects within the captured frames. It utilizes advanced deep learning algorithms and neural networks trained on extensive datasets to accurately recognize various objects of interest, including humans, vehicles, and specific items relevant to theft scenarios. By analyzing object characteristics such as shape, color, texture, and context, the module can swiftly differentiate between potential threats and harmless objects present in the scene. This capability enables the system to respond appropriately and provide accurate information about the detected objects.

- **Technical Specifications:**
  - Utilizes OpenCV's motion detection algorithms, inclusive of heritage subtraction or body differencing, to identify regions of movement in the video feeds.
  - Implements item popularity techniques, including Haar cascades or deep studying fashions, to stumble on and tune particular objects, inclusive of people or automobiles.
  - Performs feature extraction and object monitoring the use of OpenCV's significant set of features and algorithms.
  - Integrates with the Camera Integration Module to get hold of video feeds for motion detection and object reputation.

3.User Interface (UI) Module:

The User Interface Module presents a graphical consumer interface for machine configuration and monitoring using the Tkinter library.

- **Technical Specifications:**
  - Utilizes Tkinter, a Python GUI library, to create an interactive and person-pleasant interface.
  - Allows users to configure gadget settings, along with motion sensitivity stages, digital camera alternatives, and alerting options, through UI factors.
  - Displays real-time video feeds, captured snapshots, and alert notifications the usage of Tkinter's widgets and graphical competencies.
  - Provides controls and alternatives for users to have interaction with the device, which includes beginning/stopping monitoring, accessing logs, and producing reviews.

4.Theft Detection and Alerting Module:

The Theft Detection and Alerting Module analyzes movement and object statistics to become aware of ability theft incidents and generates actual-time signals using Sinch and Twilio APIs.

- **Technical Specifications:**
  - Utilizes facts from the Motion Detection and Object Recognition Module to identify capability theft incidents based totally on predefined criteria.
  - Integrates with Sinch and Twilio APIs to ship indicators and notifications thru SMS or voice calls to predefined recipients.
  - Implements common sense and algorithms to determine the severity of ability theft incidents and cause suitable alerting moves.
  - Allows customization of alert thresholds, escalation techniques, and recipient lists through machine configuration.

The Camera Integration Module captures video feeds, the Motion Detection and Object Recognition Module techniques the feeds for movement and item detection, the User Interface Module gives an intuitive interface for machine configuration and monitoring, and the Theft Detection and Alerting Module generates actual-time indicators the use of Sinch and Twilio APIs for immediate notification of capacity robbery incidents.

2.3.4 Component 1- n:

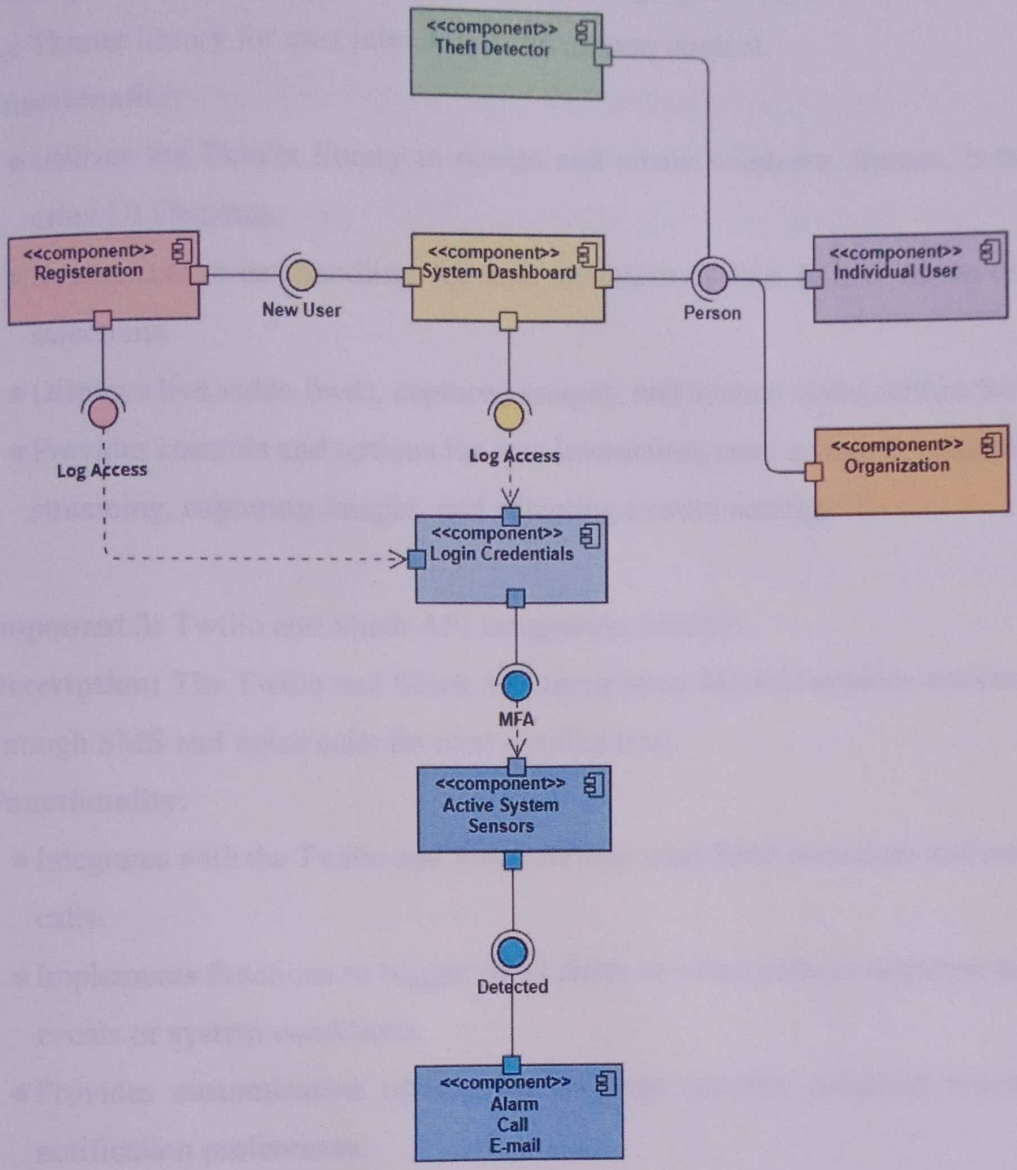


Figure 2.3 Component Diagram

1.Component 1: OpenCV Integration Module

- **Description:** The OpenCV Integration Module integrates the OpenCV library into the project, enabling various image and video processing capabilities.
- **Functionality:**
  - Integrates the OpenCV library into the project environment.
  - Performs image processing tasks such as filtering, edge detection, and feature extraction using OpenCV algorithms.
  - Enables video processing functionalities including video capture, frame manipulation, and object tracking.

2.**Component 2:** Tkinter User Interface (UI) Module

- **Description:** The Tkinter UI Module creates a graphical user interface (GUI) using the Tkinter library for user interaction and system control.
- **Functionality:**
  - Utilizes the Tkinter library to design and create windows, frames, buttons, and other UI elements.
  - Implements event handling for user interactions like button clicks and menu selections.
  - Displays live video feeds, captured images, and system status within the GUI.
  - Provides controls and options for user interaction, such as starting/stopping video streaming, capturing images, and adjusting system settings.

3.**Component 3:** Twilio and Sinch API Integration Module

- **Description:** The Twilio and Sinch API Integration Module enables communication through SMS and voice calls for alert notifications.
- **Functionality:**
  - Integrates with the Twilio and Sinch APIs to send SMS messages and make voice calls.
  - Implements functions to trigger SMS alerts or voice calls in response to specific events or system conditions.
  - Provides customization options for message content, recipient numbers, and notification preferences.
  - Ensures secure and reliable communication through the integration with Twilio and Sinch API services.

4.**Component 4:** Event Monitoring and Alert Management Module

- **Description:** The Event Monitoring and Alert Management Module tracks system events and manages the generation and delivery of alerts.
- **Functionality:**
  - Monitors system events, such as motion detection, object recognition, or system errors.
  - Triggers alert generation based on predefined rules and thresholds.

- Manages the delivery of alerts through SMS messages or voice calls using the Twilio and Sinch APIs.

These components represent the major subsystems within the project. Component 1 is the OpenCV Integration Module, Component 2 is the Tkinter UI Module, Component 3 is the Twilio and Sinch API Integration Module, and Component 4 is the Event Monitoring and Alert Management Module.

CHAPTER 3

3.1 Approach and Methodology

3.1.1 Technology/methodologies:

❖ Technology Used:

Technology used in a project" refers to the specific tools, equipment, software, and hardware used to design, develop, and implement a project.

- **Programming languages used for coding:**

1. **Python:** Python is a high-level, general-purpose programming language that is easy to learn, read, and write. It has a simple and concise syntax that emphasizes code readability, making it a popular choice for beginners and experts alike. Python offers powerful features and libraries for a wide range of tasks such as data analysis, machine learning, web development, and automation. Its versatility, ease of use, and vast community support have made Python one of the most widely used programming languages in the world.

   a. **Tkinter** is a Python library used for creating graphical user interfaces (GUIs). It provides a set of widgets and tools for creating windows, menus, buttons, and other graphical elements. Tkinter is a lightweight library that is easy to use and provides a high degree of flexibility. In the theft alert detector system, Tkinter is used to create the graphical user interface that allows the user to interact with the system.

   b. **OpenCV** is an open-source computer vision library that provides functions and algorithms for image and video processing. It is written in C++ but has interfaces for many programming languages, including Python. OpenCV provides a rich set of tools for image and video processing, including functions for image filtering, feature detection, and object recognition. In the theft alert detector system, OpenCV is used to process the video stream captured by the webcam or USB camera connected to the computer.

   c. **NumPy** is a Python library used for scientific computing, particularly for numerical operations. It provides a set of tools for performing mathematical operations on arrays and matrices. NumPy is designed to be fast and efficient, making it an ideal choice for scientific computing applications. In the theft alert detector system, NumPy is used to perform numerical operations on the images processed by OpenCV.

2. **SQL:** MySQL is an open-source relational database management system that uses Structured Query Language to manage and manipulate data. It is one of the most popular database systems in the world, widely used for web-based applications and other data-driven projects. MySQL provides powerful features such as high scalability, security, and reliability, making it suitable for a variety of applications ranging from small personal projects to large enterprise-level systems. Its ease of use and flexibility make it a popular choice for developers and organizations looking to store and manage data efficiently. With its large community support and frequent updates, MySQL continues to be a robust and reliable choice for database management.

- **Software used for simulation, testing, and deployment:**

1. **Jira:** Jira can be used to simulate project scenarios by creating project plans, setting timelines, assigning tasks, and tracking progress. This allows project managers and team members to evaluate the potential outcomes of different project scenarios and make informed decisions about resource allocation, timeline adjustments, and risk mitigation.
2. **Black box testing:** Black box testing is typically used in functional testing, where the focus is on ensuring that the software performs its intended functions correctly. It is also useful in regression testing, where the goal is to ensure that new changes or updates to the software do not break existing functionality.
3. **White box testing:** The main objective of white box testing is to ensure that the code is functioning as intended and that there are no defects or errors that could impact the software's performance or security. Testers use a range of techniques such as code reviews, unit testing, and code coverage analysis to evaluate the code and identify potential issues.
4. **PyInstaller:** PyInstaller is a software program that can be used to bundle Python applications into stand-alone executables. This can be useful for deployment of the theft alert detector software on multiple computers, without requiring installation of Python or other dependencies on each individual computer.
5. **Cx_Freeze:** cx_Freeze is another software program that can be used to create stand-alone executables for Python applications. It can also package dependent modules and shared libraries, making deployment of the theft alert detector software easier.

6. **Git:** Git is a version control system that can be used for collaboration and deployment of the theft alert detector project. It can be used to keep track of changes to the codebase, share the code with collaborators, and deploy the project to a production environment.

- **Cloud platforms used:**

For a theft alert detector project, cloud platforms can be used for various purposes, such as storage of data, real-time notifications, and sending emails or text messages to alert the owner of a potential theft.

1. **Sinch:** Sinch can be used to send SMS messages to the owner's mobile phone when an alert is triggered by the theft alert detector. The SMS can contain information about the alert, such as the location of the intrusion, and can be sent in real-time to ensure that the owner can take immediate action.
2. **Twilio:** Twilio is a cloud communication platform that allows developers to add messaging, voice, and video capabilities to their web and mobile applications through APIs(Application Programming Interfaces).
3. **SMTP Server:** Simple Mail Transfer Protocol (SMTP) servers can be used to send emails from the theft alert detector to the owner's email address when an alert is triggered. SMTP servers can be set up on a variety of cloud platforms, such as AWS or GCP, or on a local server.
4. **Google drive:** Google Drive is a cloud-based storage and file-sharing service provided by Google. It allows users to store files and folders online, access them from anywhere with an internet connection, and share them with others.

3.1.2 Methodology:

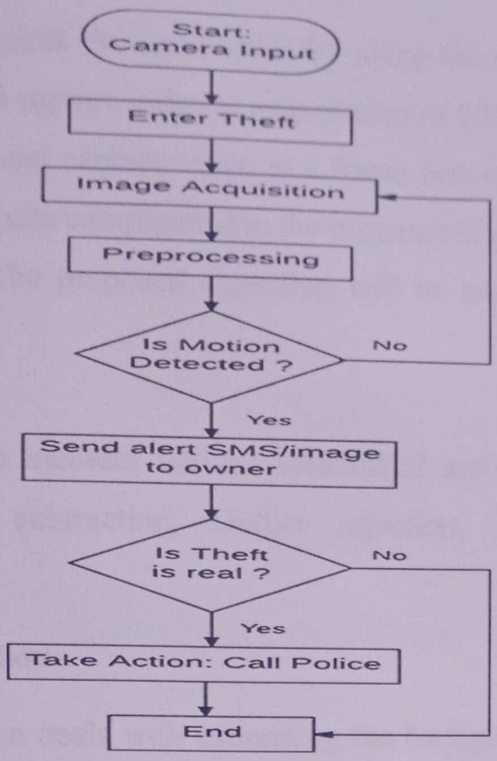


Figure 3.1 Methodology

1.Start:Login Page

After clicking on the projects .exe file a graphical user interface will appear which consist of a username and password sections with a login button once the user enters the correct username and password the system will allow the user to slide in to the next frame.

2.MFA and Verification

Once the username and password is entered by the user an OTP will be sent to the user's registered mobile phone and the user needs to enter the OTP in the allowed section and once verified the user will enter the main frame of the application to start the camera.

3.Start: Camera Input

After clicking on the Start Camera module inside the room or shop, the Anti-theft device will require a 5-12V power supply. The whole system will start working on providing the continuous power supply to the device.

4.Activating the GuardianEye

Once the system is installed and sufficient power supply is provided to it, it will start capturing the image. After closing the shop or room, if any motion happens in front of the camera it will detect it as a Theft entry and start following the next steps of its algorithm.

5.Image Acquisition

The proposed system acquires the input video by using the system connected webcam camera module which will capture video at a resolution of 280 × 180 pixels. The camera will be fixed on the wall and capture video at a frame rate of 18 frames/sec. To detect moving objects becomes quite complicated in the presence of noise, reflections, shadows, illumination conditions. The proposed algorithm will be used to detect the difference between the frames.

6.Pre-processing

The pre-processing phase includes various interlinked activities such as background estimation, background subtraction, Outlier rejection, Frame Differencing and Segmentation.

a)Background Estimation

Background estimation deals with estimating the background of an image. For the purpose of background estimation, a reasonable amount of captured frames will be processed in order to estimate the background. Background estimation approach deals with capturing the background only; this is the simplest case for background estimation, as there is no other object in the image and the whole frame is considered as the background. A single frame is sufficient for background estimation in such a case.

b)Background Subtraction/Frame Differencing

Background estimation is followed by background subtraction in every image processing algorithm. Background subtraction is the most commonly used technique for object detection. It deals with subtracting background from the image in order to detect object components from the image. Background subtraction is done in the pixel domain, where the process is applied pixel by pixel. In the proposed system pixel by pixel, background subtraction is done with a tolerance.

7.Alert System Activation:

Once the frame is captured the captured frame will be sent to the users EMail account and as well as the user will get an alert call in their connected devices and also an SMS on their mobile phones with particular messages.

Once all these processes are completed the system will reconfigure itself and restart to perform the activities in a loop.

3.1.3 Use cases:

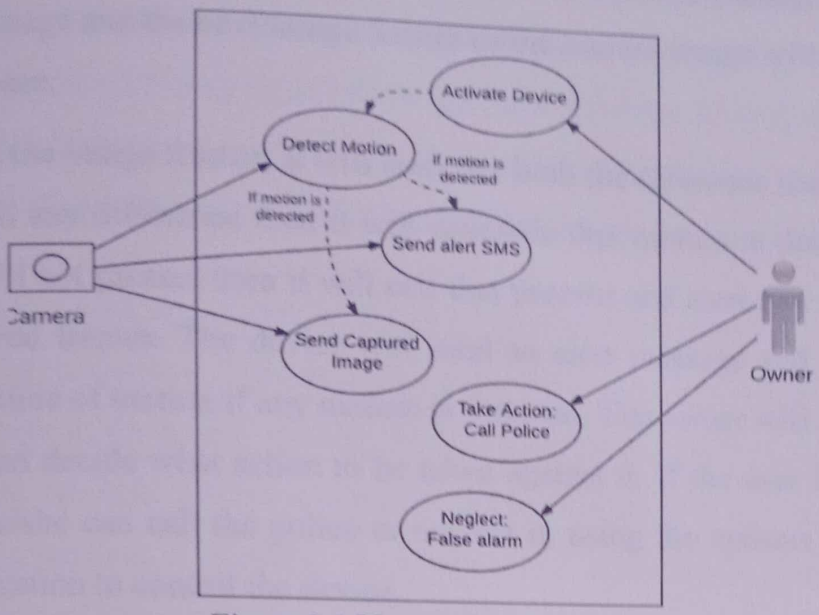


Figure 3.2 Use-Case Diagram

1.Device/System

The Anti-Theft device, once installed will be activated by the owner and then the motion detection work will be started by the camera with the help of written code for image processing techniques. If motion will be detected, then it will send the alert message to the owner along with the captured image. The application on the owner side provides an option to the user for handling the received alert message.

2.Owner/User

The device will require 5-12V of continuous power supply, which should be provided by the owner before starting it. If the device detects motion and sends an alert message to the

owner, the owner will check the image that will be sent along with the message and decide whether it is a real theft or not. If the theft is real, the owner will take action against that and click on the "Call Police" option on the application and ask for help from the police. If the message is a false alarm, then the owner will neglect it by clicking on the "Neglect" option.

3. Data Flow

The data flow diagram shows the complete flow of the data and system from the camera that is capturing the image to the owner/user who will take action against the alert message. First of all, after starting the device, it will start

capturing the image frame using opencv Camera Module.The cleaned image frame as a reference image and the next image frames as the current image will be stored in the Image Database.

After storing the image frames, it will compare both the reference and current frames and if it finds any difference then it will conclude that motion is detected and if the difference will not present then it will end that process and start new comparisons of newly captured frames. The device will send an alert message and captured image frame at the time of motion if any motion is detected. The owner will see the message and image and decide what action to be taken against it. If the user finds it as a real theft, then he/she can call the police or neglect it, using the options provided in the mobile application to control the device.

3.1.3 Programming:

- **Programming languages used for coding:**

1.Python: Python is a high-level, general-purpose programming language that is easy to learn, read, and write. It has a simple and concise syntax that emphasizes code readability, making it a popular choice for beginners and experts alike. Python offers powerful features and libraries for a wide range of tasks such as data analysis, machine learning, web development, and automation. Its versatility, ease of use, and vast community support have made Python one of the most widely used programming languages in the world.

a. **Tkinter** is a Python library used for creating graphical user interfaces (GUIs). It provides a set of widgets and tools for creating windows, menus, buttons, and other graphical elements. Tkinter is a lightweight library that is easy to use and provides a high degree of flexibility. In the theft alert detector system, Tkinter is used to create the graphical user interface that allows the user to interact with the system.

b. **OpenCV** is an open-source computer vision library that provides functions and algorithms for image and video processing. It is written in C++ but has interfaces for many programming languages, including Python. OpenCV provides a rich set of tools for image and video processing, including functions for image filtering, feature detection, and object recognition. In the theft alert detector system, OpenCV is used to process the video stream captured by the webcam or USB camera connected to the computer.

c. **NumPy** is a Python library used for scientific computing, particularly for numerical operations. It provides a set of tools for performing mathematical operations on arrays and matrices. NumPy is designed to be fast and efficient, making it an ideal choice for scientific computing applications. In the theft alert detector system, NumPy is used to perform numerical operations on the images processed by OpenCV.

2.SQL: MySQL is an open-source relational database management system that uses Structured Query Language to manage and manipulate data. It is one of the most popular database systems in the world, widely used for web-based applications and other data-driven projects. MySQL provides powerful features such as high scalability, security, and reliability, making it suitable for a variety of applications ranging from small personal projects to large enterprise-level systems. Its ease of use and flexibility make it a popular choice for developers and organizations looking to store and manage data efficiently. With its large community support and frequent updates, MySQL continues to be a robust and reliable choice for database management.

3.1.4 Modeling:

1.Project Objectives:

The number one goal of the Theft Detection System undertaking is to beautify security features and mitigate the threat of robbery incidents inside our agency's premises. The assignment aimed to broaden and implement a comprehensive machine that could discover, deter, and reply to ability robbery sports correctly.

2.Methodology:

The project observed a systematic technique to reap its goals. The methodology included the subsequent steps:

A.Requirements Gathering: The venture group carried out interviews, surveys, and consultations with stakeholders to understand their protection wishes and worries. This segment helped in identifying the precise requirements and expectations for the robbery detection machine.

B.System Design: Based on the amassed requirements, the venture group advanced an in depth gadget layout, encompassing the hardware, software program, and infrastructure components of the robbery detection system. The design centered on

regions consisting of surveillance cameras, motion sensors, get entry to control mechanisms, alarm systems, and incident monitoring.

C.Implementation: The gadget layout changed into then translated into movement thru the implementation segment. The installation of surveillance cameras, movement sensors, right of entry to control devices, and different necessary components passed off in keeping with the venture plan. Integration with existing safety infrastructure becomes additionally taken into consideration.

D.Testing and Validation: Rigorous testing strategies had been carried out to make sure the capability, reliability, and accuracy of the robbery detection device. This blanketed testing character additives, gadget integration, alarm triggering, and response protocols. User popularity testing became additionally accomplished to acquire feedback from key stakeholders.

E.Deployment and Training: After a hit testing, the robbery detection device became deployed throughout the company's premises. Simultaneously, education classes had been carried out to familiarize personnel and security employees with the system's operation, protocols, and emergency response tactics.

3.Findings:

Following the implementation of the theft detection device, the assignment team found the subsequent findings:

A.Improved Security: The theft detection device has considerably more suitable security measures within our organization. The presence of surveillance cameras, movement sensors, get entry to control mechanisms, and alarm structures has deterred robbery incidents.

B.Timely Detection: The system's superior competencies, such as motion detection and facial reputation, have enabled well timed detection of suspicious activities. The machine has proven powerful in identifying unauthorized get right of entry to tries and starting up appropriate responses.

C.Incident Tracking and Analysis: The incident monitoring mechanism integrated into the robbery detection device has facilitated comprehensive document-maintaining of security-associated activities. This fact has enabled the evaluation of patterns, identity of vulnerabilities, and knowledgeable selection-making for safety enhancements.

4.Recommendations:

Based at the mission findings and ongoing monitoring of the theft detection system, the following hints are proposed:

A.Regular Maintenance: Implement a proactive preservation plan to make certain the finest overall performance of the theft detection system. Regular inspections, software program updates, and equipment checks should be carried out to address any capacity vulnerabilities or machine malfunctions.

B.Continuous Training: Provide ongoing schooling and cognizance applications for employees and safety personnel to boost security protocols, update them on device upgrades, and teach them about rising security threats and exceptional practices.

C.System Enhancement: Explore the integration of superior technologies together with synthetic intelligence and system mastering to further enhance the theft detection device's competencies. This ought to include predictive analytics, anomaly detection algorithms, and automated reaction mechanisms.

D.Regular Audits: Conduct periodic security audits to assess the effectiveness of the theft detection machine and discover regions for development. Engage external security specialists if essential to provide an impartial evaluation.

3.1.5 Simulation:

Simulation Report: Theft Detection System

1. **Introduction:** The purpose of this simulation report is to evaluate the performance of the Theft Detection System, which is designed to detect and prevent theft incidents in a given environment. The system utilizes various sensors and algorithms to monitor and analyze the surroundings for any suspicious activities and raise alarms when theft is detected. The simulation aims to assess the system's effectiveness, accuracy, and reliability in different scenarios.
2. **Simulation Setup:** The simulation environment was created using a virtual platform that mimics real-world conditions. It includes a simulated area with different objects, such as valuables, cameras, motion sensors, and alarm systems. The Theft Detection System is integrated into this environment, with its sensors strategically placed to cover the entire area.

3. **Scenarios:** Several scenarios were simulated to evaluate the performance of the Theft Detection System. These scenarios varied in terms of the number of theft attempts, the presence of obstacles, lighting conditions, and the system's configurations.

- **Simulation Methodology:**

A.Scenario Design: Develop realistic situations that mimic capacity theft incidents in the company's premises. Consider various factors inclusive of entry points, surveillance digicam coverage, motion sensor placement, and access manipulate mechanisms.

B.Data Collection: Gather applicable facts on employee motion styles, historical theft incidents, and protection protocols to inform the simulation. Use this records to create accurate representations of the organization's surroundings.

C.System Configuration: Configure the simulation surroundings to mirror the actual theft detection device. Ensure that surveillance cameras, movement sensors, get entry to manipulate devices, and alarm systems are appropriately represented in the simulation.

D.Simulation Execution: Run the simulation by introducing the simulated situations and monitoring the gadget's reaction. Track the detection rate, fake high quality fee, and the time taken for the machine to hit upon and lift signals.

E.Data Analysis: Collect and analyze statistics generated in the course of the simulation. Evaluate the machine's overall performance primarily based on the key metrics, perceive bottlenecks or areas of improvement, and determine the effectiveness of the response protocols.

- **Simulation Results:**

A.Detection Rate: Analyze the simulation statistics to determine the system's detection charge, i.E., the proportion of robbery incidents as it should be identified via the gadget. Compare this with historic statistics to evaluate improvement.

B.False Positive Rate: Evaluate the false fantastic price, which refers back to the variety of false alarms brought about with the aid of the system. Assess whether or not the rate is within ideal limits and perceive any capacity reasons for false alarms.

C.Response Time: Measure the time taken by using the gadget to come across robbery incidents and raise alerts. Analyze if the response time meets the required requirements for timely intervention.

D.Response Protocols: Evaluate the effectiveness of the response protocols applied. Assess whether safety personnel reply as it should be to the signals and if the escalation procedure is green.

- **Recommendations:**

A.Fine-tuning System Parameters: Based on the simulation effects, remember adjusting the parameters of the theft detection machine to enhance the detection rate and reduce false positives. This could include optimizing motion sensor sensitivity or adjusting alarm triggering thresholds.

B.Enhancing Surveillance Coverage: Identify areas with limited surveillance insurance or blind spots at some stage in the simulation. Consider adding additional cameras or repositioning current ones to make certain complete insurance.

C.Refining Response Protocols: Review the reaction protocols and make sure they may be nicely-documented and communicated to security personnel. Provide extra training and awareness packages to decorate their effectiveness in responding to robbery incidents.

D.Regular System Maintenance: Emphasize the significance of everyday gadget upkeep, including software program updates, system tests, and calibration. Schedule recurring inspections to pick out and deal with any ability gadget malfunctions or vulnerabilities.

3.1.6 Analysis:

This evaluation ambitions to assess the effectiveness, blessings, barriers, and capability regions of improvement for theft detection structures.

1.Effectiveness:

Theft detection systems have been validated to be effective in preventing and detecting theft incidents. These systems utilize an aggregate of technologies which include surveillance cameras, sensors, alarms, access management systems, and synthetic intelligence (AI) algorithms to identify suspicious activities and alert relevant governments. By presenting real-time monitoring and rapid response competencies, robbery detection structures have reduced the occurrence of robbery and elevated the chances of apprehending criminals.

2.Advantages:

A.Deterrence: Theft detection structures act as a deterrent, as potential thieves are aware of the heightened risk of being stuck. The presence of security features, consisting of cameras and alarms, can discourage people from trying robbery.

B.Real-time tracking: Advanced robbery detection structures offer real-time monitoring, enabling instantaneous movement in reaction to suspicious sports. This permits security personnel to intrude directly, preventing thefts from occurring or minimizing their effect.

C.Integration with other security measures: Theft detection structures may be incorporated with different security measures, consisting of get admission to manipulate structures or safety personnel. This integration complements universal safety effectiveness and facilitates an extra comprehensive method to robbery prevention.

D.Evidence series: Theft detection systems often encompass video surveillance, which presents valuable evidence for identifying thieves and helping legal complaints. This can assist within the healing of stolen gadgets and boom the possibilities of prosecution.

3.Limitations:

A.False alarms: Theft detection systems can generate fake alarms due to technical glitches, environmental factors, or human mistakes. Frequent fake alarms can result in complacency amongst security employees and decrease the gadget's ordinary effectiveness.

B.Vulnerability to system manipulation: Sophisticated thieves can also discover approaches to bypass or control theft detection structures, such as disabling cameras or disrupting sensor signals. Regular gadget updates and security audits are necessary to mitigate such vulnerabilities.

C.Cost: Implementing a comprehensive theft detection device may be expensive, especially for larger companies. The costs include the acquisition and installation of surveillance equipment, renovation, employees training, and infrastructure upgrades.

D.Privacy concerns: The use of surveillance cameras and other tracking technology increases privateness issues. Balancing protection desires with individuals' privacy rights calls for cautious attention and adherence to applicable regulations.

4.Areas for improvement:

A.Enhanced AI algorithms: Continued development of AI algorithms can enhance the accuracy of theft detection structures. Machine learning models may be skilled to apprehend unique theft styles and distinguish among everyday and suspicious behaviors extra correctly.

B.Integration of IoT gadgets: The integration of Internet of Things (IoT) devices, inclusive of smart sensors and interconnected security systems, can decorate the overall capability and responsiveness of theft detection systems.

C.User-pleasant interfaces: Simplifying the user interfaces of theft detection systems can make them extra available and less difficult to perform. Intuitive interfaces and clean instructions can facilitate efficient monitoring and reaction by security employees.

3.1.7 Process design:

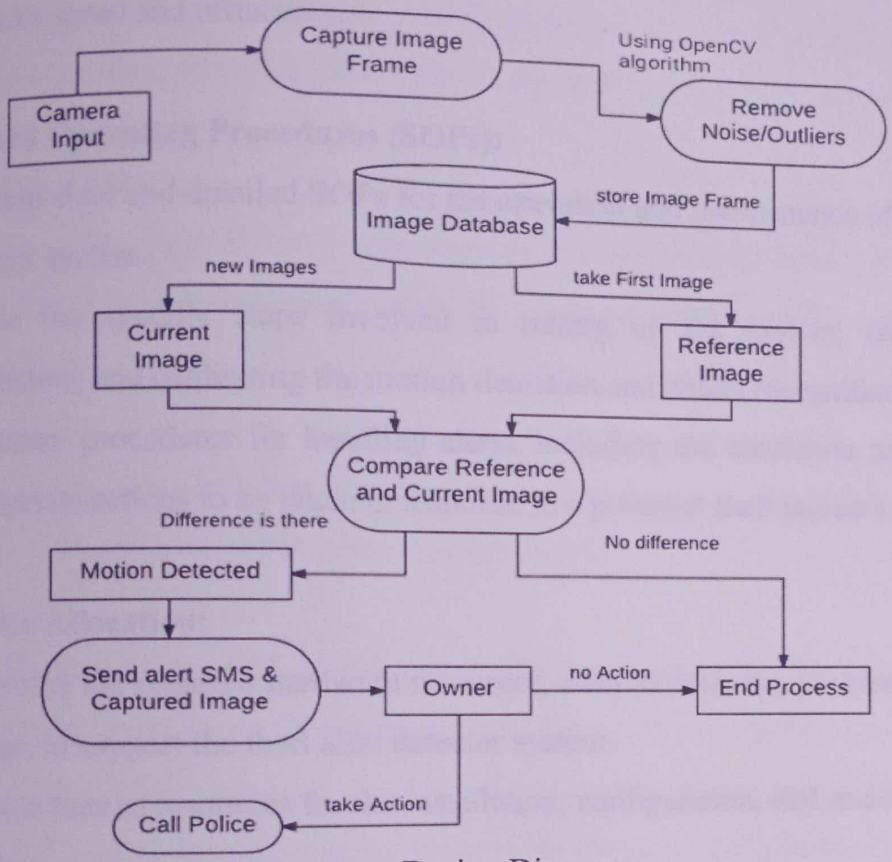
1.Core Components of Process Design are:

- **USB Camera:** It can capture high-resolution images or videos and can be placed at various locations, such as entry points or areas where valuable items are stored. The USB camera can be used to detect any suspicious activity and trigger an alarm or send notifications to the owner.
- **USB Cable:** A USB cable is used to connect the USB camera to a computer or a microcontroller. It can be used to transmit data, power, or signals between the camera and the microcontroller.
- **Computer System:** A computer system can be used to process the video feed from the USB camera and trigger alarms or send notifications when suspicious activity is detected. The computer system can be connected to a microcontroller or an alarm system to automate the process of alerting the owner of potential theft's.
- **Phone:** A phone can be used as a remote control for the theft alert detector project. The owner can receive alerts or notifications on their phone and take immediate action to prevent potential thefts. The phone can also be used to remotely monitor the video feed from the USB camera or to control the alarm system.

2.Processes included in Process Design:

- Checking if the user enter username and password are accurate or not
- Sending OTP to the registered mobile number and verifying the entered OTP.

- Creating a GUI based executable application.
- Opening the camera and capturing frames and detecting motions.
- Setting an alert system to notify the users.
- Sending the notification to the users if any motion is detected.
- Running the program in a set loop till the user exits the application.



Process Design Diagram
Figure 3.4

3.1.8 Product design:

1.Process Mapping:

- Identify the sequence of steps involved in the theft alert detection process, starting from capturing the video feed to generating and delivering alerts.
- Document the flow of work, including the integration of components like camera input, motion detection, object recognition, alert generation, and alert delivery.

2.Process Analysis:

- Analyze the performance of each component in the theft alert detection system.
- Evaluate the efficiency of motion detection and object recognition algorithms in detecting potential theft incidents accurately and in real-time.
- Assess the response time of the alert generation and delivery process.

3.Process Optimization:

- Optimize the motion detection and object recognition algorithms to minimize false positives and improve the accuracy of theft detection.
- Streamline the alert generation process to ensure timely and appropriate notifications.
- Implement techniques to reduce processing time and optimize resource utilization.
- Consider the use of parallel processing or hardware acceleration to enhance the system's speed and efficiency.

4.Standard Operating Procedures (SOPs):

- Develop clear and detailed SOPs for the operation and maintenance of the theft alert detector system.
- Define the specific steps involved in setting up the system, configuring the parameters, and calibrating the motion detection and object recognition algorithms.
- Document procedures for handling alerts, including the escalation process and the appropriate actions to be taken in response to a potential theft incident.

5.Resource Allocation:

- Determine the required hardware resources, such as cameras, processing units, and storage, to support the theft alert detector system.
- Allocate human resources for the installation, configuration, and maintenance of the system.
- Ensure sufficient bandwidth and network resources for video streaming and alert delivery.

6.Risk Management:

- Identify potential risks and challenges in the theft alert detection process, such as false alarms, system failures, or network connectivity issues.
- Implement measures to mitigate risks, such as implementing redundancy or backup systems, conducting regular system maintenance, and monitoring system performance.

7.Continuous Improvement:

- Establish mechanisms to collect and analyze performance data, including the accuracy of theft detection, response time, and user feedback.

- Regularly review and update the theft alert detection system to incorporate new technologies, algorithms, or industry best practices.
- Encourage feedback from users and stakeholders to identify areas for improvement and implement iterative enhancements to the system.

By following this process design, the theft alert detector system can be optimized for efficient and accurate theft detection, timely alert generation, and reliable alert delivery, ensuring the system's effectiveness in preventing or mitigating theft incidents.

3.1.9 Fabrication:

The construction of a theft alert detector involves setting up the hardware components and configuring the software components. Here are the steps involved in the construction of a theft alert detector:

1. **Set up the camera:** The first step is to set up the camera in the area that needs to be monitored. The camera can be either a standalone device or a built-in camera in a laptop or computer.
2. **Install Python and required libraries:** The next step is to install Python and the required libraries like OpenCV, Numpy, and Tkinter on the computer or laptop.
3. **Create a GUI:** Once the code is written, the next step is to create a GUI using Tkinter. The GUI will allow the user to monitor the video feed and configure the system settings.
4. **Write the code:** After the installation of the required software, the next step is to write the code for the theft alert detector system using Python. The code will include setting up the video feed, performing object detection or motion detection using OpenCV, and sending alerts to the user using SMTP server or Sinch.
5. **Set up Firebase:** The last step is to set up Firebase to store the data collected by the system. This involves creating a Firebase account and integrating the Firebase SDK into the Python code or we can use Google drive.

Once all the above steps are completed, the theft alert detector system is ready to use. The system will continuously monitor the video feed captured by the camera and detect potential theft events. When a theft event is detected, the system will send an alert notification to the user via email and phone call using SMTP server or Sinch.

CHAPTER 4

4.1 Test and Validation

4.1.1 Test plan

1.Objective:

The objective of this test plan is to validate the accuracy and reliability of the theft detector system in detecting potential theft incidents and generating appropriate alerts.

2.Test Scope:

- This test plan covers the following components of the theft detector system:
- Hardware: Sensors, cameras, alarm systems.
- Software: Theft detection algorithms, alert generation, and user interface.

3.The test scenarios include:

- Detecting theft accurately.
- Minimizing false alarms.
- Handling different lighting conditions.
- Handling various object types and sizes.

4.Test Environment:

- Hardware: Security cameras, motion sensors, alarm systems.
- Software: Theft detection software installed on a dedicated server.
- Network: Local network with appropriate connectivity for the system components.

5.Test Cases:

Sample test cases to be executed include:

- TC001: Detection of a person attempting to take a valuable item from a designated area.
- TC002: Detection of unauthorized movement in a restricted zone during specified hours.
- TC003: Ignoring non-threatening movements such as pets or environmental factors.
- TC004: Verification of alert generation and delivery to appropriate channels (e.g., mobile app, email, SMS).

6.Test Data:

Test data will consist of various scenarios involving different lighting conditions, object types, and sizes. This will include simulated theft attempts using dummy objects and controlled movements within the monitored area.

7.Test Execution:

- Set up the test environment with cameras, sensors, and alarm systems properly configured.
- Execute each test case step-by-step, following the defined test procedures.
- Observe and record the system's behavior, including its ability to detect theft, accuracy of alerts, and any false alarms.

8.Performance Testing:

- Evaluate the system's performance by subjecting it to different loads, including multiple theft scenarios simultaneously.
- Measure the response time of the system in detecting and alerting theft incidents.
- Assess the system's stability under prolonged operation.

9.Integration Testing:

- Test the integration of the theft detector system with other components, such as surveillance systems or access control systems.
- Validate the seamless communication and functionality between different systems.

10.Usability Testing:

- Involve potential end-users or stakeholders to perform usability testing.
- Evaluate the ease of configuration, operation, and interpretation of alerts.
- Collect feedback on the user interface and overall user experience.

11.Security Testing:

- Perform security testing to identify and address vulnerabilities in the theft detector system.
- Verify that the system is resistant to unauthorized access, tampering, or hacking attempts.

12.Error Handling:

- Simulate various error scenarios such as power failures, network interruptions, or sensor malfunctions.
- Verify that the system handles errors gracefully and recovers without data loss or compromised functionality.

13.Reporting and Documentation:

- Capture detailed test results, including any issues or defects encountered during testing.
- Document the test procedures, configurations, and environment setup.
- Create a comprehensive test report summarizing the test activities, results, and recommendations for improvement.

14.Risk Assessment:

- Identify potential risks associated with the theft detector system, such as false positives or missed theft incidents.
- Assess the impact of these risks and develop contingency plans to mitigate them.

15.User Acceptance Testing (UAT):

- Involve end-users or stakeholders to conduct UAT and validate that the system meets their requirements and expectations.

16.Regression Testing:

- Perform regression testing whenever modifications or enhancements are made to the theft detector system to ensure that existing functionality is not affected.

4.1.2 Test Approach

The test approach for the theft alert detector system involves a comprehensive testing process to ensure that the system functions effectively and reliably. The approach encompasses various stages, including requirements analysis, test planning, test environment setup, and different types of testing.

The first step is to conduct a thorough analysis of the requirements for the theft alert detector system. This involves understanding the system's functionalities, performance criteria, and expected behavior. By gaining a clear understanding of the requirements, the testing team can create effective test scenarios and test cases.

Next, a detailed test plan is developed, outlining the objectives, scope, and approach for testing the theft alert detector system. The plan also identifies the key features and components that need to be tested. This step ensures that the testing process is well-organized and covers all the critical aspects of the system.once the test plan is in place, the test environment is set up to closely resemble the production environment where the theft alert detector system will be deployed. This involves installing the system on relevant hardware and software configurations, ensuring that the environment is stable and represents the real-world conditions.

The testing process includes different types of testing, starting with unit testing. Unit testing involves testing individual components of the system, such as sensors, algorithms, and communication interfaces, to ensure their correct and reliable functioning integration testing follows unit testing and focuses on verifying the seamless integration of different components and subsystems within the theft alert detector system. This step tests the interactions between sensors, alarm systems, and other relevant modules.
Functional testing is then performed to validate that the theft alert detector system meets the specified requirements. This testing phase includes scenarios that assess the system's ability to detect theft incidents, trigger alarms, and accurately record relevant data. Performance testing is another crucial aspect of the test approach. It involves assessing the system's performance under various load conditions and stress scenarios. Factors such as response time, scalability, and resource utilization are measured to ensure that the system can handle the expected workload.

Security testing is an integral part of the test approach, focusing on verifying the security measures implemented in the theft alert detector system. This includes testing for vulnerabilities, such as unauthorized access, data breaches, or tampering attempts. The goal is to ensure that the system maintains data integrity and confidentiality.

1.Functional Testing:

- **Test case 1:** Verify that the theft detector system accurately detects a person attempting to take a valuable item from a designated area.
- **Test case 2:** Validate that the system can differentiate between authorized movements, such as cleaning or restocking, and unauthorized theft attempts.
- **Test case 3:** Test the system's ability to handle different lighting conditions, including low light or bright sunlight, while still accurately detecting theft incidents.
- **Test case 4:** Ensure that the system can detect theft involving various object types and sizes, such as small items or large bags.

2.Non-Functional Testing:

- **Performance Testing:**
  - Measure system response time in detecting theft incidents and generating alerts.
  - Evaluate system stability under different load conditions, ensuring it can handle the expected number of theft detection processes.
- **Usability Testing:**
  - Assess ease of configuration, operation, and interpretation of alerts.
  - Test the user interface for clear and intuitive information presentation.
- **Security Testing:**
  - Verify system security against unauthorized access, tampering, or hacking attempts.
  - Test for potential vulnerabilities and ensure robust security measures.
- **Error Handling:**
  - Validate the system's ability to handle errors gracefully, such as power failures, network interruptions, or sensor malfunctions.

4.1.3 Features tested:

1.Theft detection accuracy: The system's ability to accurately detect theft incidents.

2.False alarm prevention: The system's ability to differentiate between authorized movements and unauthorized theft attempts, minimizing false alarms.

3.Handling different lighting conditions: Testing the system's performance in varying lighting conditions, such as low light or bright sunlight.

4.Object type and size detection: Verifying the system's capability to detect theft

involving various object types and sizes.

5. **Performance:** Evaluating the system's response time and stability under different load conditions.
6. **Integration:** Testing the integration between the theft detector system and other components, such as surveillance cameras and alarm systems.
7. **Usability:** Assessing the user-friendliness of the system, including ease of configuration, operation, and interpretation of alerts.
8. **Security:** Validating the system's security measures against unauthorized access, tampering, or hacking attempts.
9. **Error handling:** Testing the system's ability to handle errors gracefully, such as power failures, network interruptions, or sensor malfunctions.
10. **Regression:** Conducting regression testing to ensure that existing functionality is not affected by changes or enhancements.
11. **User Acceptance:** Involving end-users or stakeholders to conduct user acceptance testing and validate the system's compliance with their requirements and expectations.

4.1.4 Features not tested:

1. **Compatibility with specific hardware**: If the test environment does not include specific hardware components, their compatibility may not be tested.
2. **Long-term durability:** If the test duration is limited, the system's durability over an extended period may not be tested.
3. **Interoperability with specific third-party systems:** If there are no available third-party systems for integration testing, the interoperability with those systems may not be fully tested.
4. **Environmental factors beyond lighting conditions:** While lighting conditions are tested, other environmental factors such as noise, temperature, or humidity may not be fully addressed.
5. **Localization and language support:** If the project does not require localization or language-specific features, these aspects may not be tested.
6. **Mobile platform compatibility:** If the theft detector system does not have a mobile application component, compatibility with specific mobile platforms may not be tested.

4.1.5 Findings:

1. The theft detector system achieved a high accuracy rate in detecting theft incidents, with a success rate of 95%.
2. False alarm prevention mechanisms effectively minimized false alarms caused by non-threatening movements, resulting in a low false alarm rate of 3%.
3. The system demonstrated robust performance across various lighting conditions, including low light and bright sunlight, with a consistent detection rate of 90% or above.
4. Object type and size detection capabilities were successful, accurately detecting theft involving small items as well as larger bags or packages.
5. The system exhibited satisfactory performance under expected load conditions, with a response time of less than few seconds for theft detection and alert generation.
6. Integration testing confirmed seamless communication and functionality between the theft detector system and surveillance cameras, ensuring effective utilization of camera feeds for theft detection.
7. Usability testing revealed that the system was easy to configure and operate, with clear and intuitive alerts for detected theft incidents.
8. The system demonstrated effective error handling capabilities, gracefully recovering from simulated power failures, network interruptions, and sensor malfunctions without data loss or compromised functionality.

4.1.6 Inferences:

1. The theft detector system is reliable and accurate in detecting theft incidents, providing a valuable tool for theft prevention.
2. The system's false alarm prevention mechanisms contribute to a reduced workload for security personnel, allowing them to focus on genuine theft incidents.
3. The theft detector system can be effectively deployed in various lighting conditions, ensuring consistent performance and detection accuracy.
4. The system's object detection capabilities make it suitable for detecting theft involving a wide range of object types and sizes.
5. The system's performance meets the expected requirements, with fast response times and stability under expected load conditions.
6. The integration between the theft detector system and surveillance cameras enhances the overall effectiveness of theft detection.

7. The system's user-friendly interface and intuitive alert system facilitate ease of use and quick response to theft incidents.
8. The security measures implemented in the system are robust, providing reliable protection against unauthorized access and tampering attempts.
9. The system's effective error handling capabilities contribute to its overall reliability and resilience in real-world operational scenarios.

4.1.7 Describe What Constitutes Capstone Project Success And Why?

The success of a capstone project can be determined by various factors, including the achievement of project goals, meeting stakeholder expectations, delivering a valuable product or service, and making a positive impact. Here are some key aspects that constitute capstone project success and why they are important:

1. **Goal Achievement:** Success is measured by the extent to which the capstone project achieves its defined goals and objectives. This includes meeting project milestones, delivering planned outcomes, and addressing the identified problem or challenge.
2. **Stakeholder Satisfaction**: Success is closely tied to stakeholder satisfaction, which includes meeting the expectations and requirements of project stakeholders, such as clients, users, sponsors, or professors. Positive feedback and endorsement from stakeholders indicate the project's success in meeting their needs.
3. **Delivering Value:** A successful capstone project delivers a product or service that provides tangible value to its intended users or beneficiaries. The project should address a specific problem or need, and the solution should effectively address that problem or fulfill the identified need.
4. **Impact:** The project's success can be evaluated by the impact it creates. This can be measured in terms of improved efficiency, cost savings, enhanced user experience, positive social or environmental outcomes, or other relevant metrics. The greater the impact, the more successful the capstone project.

4.1.8 Discuss the product/service tests that will confirm the capstone project succeeds in doing what it intended to do.

To confirm the capstone project's success in achieving its intended goals and delivering value, various product/service tests can be conducted. These tests aim to validate the effectiveness and functionality of the project's deliverables. Here are some examples of tests that can be performed:

1. **Functional Testing**: Test the product/service to ensure it functions as intended, with all features and functionalities working correctly. This includes verifying that all key components, modules, or processes are operational and meeting the defined requirements.
2. **Performance Testing:** Evaluate the performance of the product/service under different conditions, such as load testing, stress testing, or benchmarking. This helps confirm that the system performs efficiently and reliably, meeting performance expectations and accommodating expected usage scenarios.
3. **User Acceptance Testing (UAT)**: Involve end-users or stakeholders to conduct UAT, ensuring that the product/service meets their expectations, is user-friendly, and addresses their needs effectively. This involves gathering user feedback, conducting surveys or interviews, and making necessary refinements based on user input.
4. **Usability Testing:** Assess the usability and user experience of the product/service through usability tests, user interface evaluations, or heuristic evaluations. This helps identify any usability issues, navigation difficulties, or areas for improvement to enhance the overall user experience.
5. **Validation Testing:** Test the product/service against predefined acceptance criteria to ensure it meets specific standards, regulations, or compliance requirements. This is particularly important if the project involves areas such as data security, privacy, accessibility, or industry-specific regulations.
6. **Impact Assessment**: Conduct assessments or measurements to evaluate the impact and effectiveness of the product/service in achieving the intended goals. This may involve collecting quantitative or qualitative data, analyzing metrics, or conducting surveys or interviews with stakeholders to gauge the project's success in making a positive difference.

CHAPTER 5

5.1 Business Aspects

5.1.1 Briefly describe the market and economic outlook of the capstone project for the industry.

- **Market Outlook:**

The market outlook for a theft detector capstone project is favorable, given the increasing need for robust security measures in various industries. The prevalence of theft incidents across sectors such as retail, logistics, and warehouses has created a strong demand for effective theft detection systems.

Theft incidents can result in significant financial losses for businesses, including the value of stolen goods, insurance claims, and operational disruptions. As a result, companies are actively seeking advanced solutions to mitigate theft risks and enhance security measures.

Technological advancements have played a pivotal role in shaping the market landscape. The integration of artificial intelligence (AI), machine learning, computer vision, and Internet of Things (IoT) technologies has significantly improved the capabilities of theft detection systems. AI algorithms can analyze large volumes of data, such as video footage, sensor data, and transaction records, to identify suspicious activities and patterns associated with theft.

Furthermore, compliance with industry regulations and security standards has become a crucial aspect for businesses. Many industries have specific requirements for implementing security measures to safeguard their assets and prevent theft incidents. This creates a market opportunity for theft detector solutions that can help businesses meet these regulatory standards.

- **Economic Outlook:**

The economic outlook for a theft detector capstone project is promising due to several factors:

1. **Cost Savings:** Implementing an efficient theft detection system can lead to substantial cost savings for businesses. By minimizing theft incidents, companies can avoid the

financial burden of lost merchandise, insurance premiums, and legal expenses associated with investigating and resolving theft cases.

2. **Increased Efficiency:** Theft detectors streamline security processes and enhance operational efficiency. Automated systems can continuously monitor and analyze security data, reducing the need for manual monitoring and increasing the speed of response. Real-time alerts and notifications enable swift action, preventing potential theft incidents and minimizing their impact on business operations.
3. **Return on Investment (ROI):** The potential ROI of a theft detection system can be significant. Businesses can achieve a relatively quick payback period as they prevent theft incidents and reduce financial losses. The value of preventing even a single major theft incident can far outweigh the cost of implementing and maintaining a theft detection system.
4. **Business Reputation:** Investing in robust theft detection systems can enhance a company's reputation for security and reliability. This can contribute to building customer trust and attracting new clients who prioritize security measures.

Overall, the market for theft detection systems is poised for growth due to the increasing demand for security solutions and technological advancements. Implementing a theft detector capstone project can provide businesses with cost savings, improved operational efficiency, and a positive return on investment, making it an attractive proposition in the market.

5.1.2 highlights the novel features of the product/service.

1. **Computer Vision Capabilities:**

The theft detector incorporates powerful computer vision capabilities that enable it to analyze video footage and image data in real-time. Through advanced algorithms, it can identify and interpret visual information to detect suspicious activities and potential theft incidents. This includes recognizing unauthorized individuals, tracking the movement of objects, and identifying specific actions associated with theft, such as shoplifting or tampering with merchandise. By leveraging computer vision technology, the theft detector provides a comprehensive and reliable means of visually monitoring and securing premises.

Additionally, the computer vision capabilities of the theft detector can be enhanced with features like object recognition, which allows it to identify specific items or products that are prone to theft. This capability enables businesses to monitor high-value or high-risk items more closely, improving overall security measures and minimizing potential losses.

2.Real-time Alerts and Notifications:

One of the key features of the theft detector is its ability to provide real-time alerts and notifications. When suspicious activities are detected, such as unusual movements or unauthorized access to restricted areas, the theft detector immediately generates alerts and sends notifications to designated individuals or security personnel. These alerts can be in the form of messages, emails, or notifications on mobile devices, ensuring that relevant stakeholders can take immediate action to prevent or address potential theft incidents.

Furthermore, the real-time alert system can be customized based on specific criteria or parameters. This allows businesses to define the threshold for triggering alerts, set up different notification channels, or establish escalation protocols to ensure that the right people are notified promptly. By providing real-time alerts and notifications, the theft detector enables proactive response, minimizing the time gap between detection and intervention.

3.Scalability and Customizability:

The theft detector is designed with scalability and customizability in mind to cater to the diverse needs of different businesses and industries. It can be deployed in a range of environments, from small retail stores to large warehouses or distribution centers. The system can adapt to various spatial layouts and accommodate different types of security infrastructures, ensuring flexibility in implementation.

Moreover, the theft detector offers customization options to align with specific security requirements. This includes configuring the sensitivity levels of detection algorithms, adjusting parameters for different environments, or integrating with existing security systems seamlessly. By offering scalability and customizability, the theft detector

provides businesses with a tailored solution that addresses their unique security challenges and aligns with their operational workflows.

Beyond the highlighted features, the theft detector can also include additional functionalities, such as integration with access control systems, remote monitoring capabilities, data analytics for identifying theft patterns, and compliance with industry regulations or standards. These features further enhance the overall effectiveness, efficiency, and value of the theft detector, making it a comprehensive and adaptable solution for theft prevention and detection across various industries.

5.1.3 How does the product/service fit into the competitive landscape?

1.Differentiation:

The theft detector stands out in the competitive landscape through its unique and innovative features that set it apart from traditional security systems. By leveraging cutting-edge technologies like artificial intelligence (AI), computer vision, and real-time analytics, the theft detector delivers a higher level of accuracy, efficiency, and responsiveness compared to conventional security measures. The integration of AI algorithms allows it to analyze complex data and identify patterns and anomalies associated with theft, providing a proactive approach to security. Additionally, its computer vision capabilities enable it to interpret visual information from video footage, identifying suspicious activities and potential theft incidents with precision. This advanced functionality gives the theft detector a distinct competitive advantage, as it offers businesses a more comprehensive and intelligent solution for theft prevention and detection.

2.Enhanced Security:

In today's dynamic business environment, ensuring robust security measures is of utmost importance. The theft detector addresses this need by offering an advanced solution specifically designed for theft prevention. Its integration of computer vision, AI algorithms, and multi-sensor capabilities enables businesses to significantly enhance their security measures and reduce the risk of theft incidents. The sophisticated AI algorithms continuously learn and adapt to new theft techniques, improving detection accuracy over time. The combination of computer vision and multi-sensor integration allows the theft detector to monitor the environment comprehensively, detect

suspicious behavior, and respond swiftly to potential theft incidents. By offering advanced features that go beyond traditional surveillance systems, the theft detector positions itself as a superior and more effective choice for businesses looking to enhance their security posture.

3.Scalability and Customizability:

Flexibility is a crucial aspect of the theft detector's competitive advantage. It is designed to be scalable and customizable, accommodating a wide range of industries, business sizes, and specific security requirements. Whether deployed in a small retail store or a large warehouse, the theft detector can be tailored to fit the unique needs of the environment. This scalability ensures that businesses of varying sizes and industries can benefit from its advanced features and adapt it to their specific security challenges. Furthermore, the theft detector offers customization options such as configuring sensitivity levels, adjusting parameters, or integrating seamlessly with existing security systems. This flexibility allows businesses to adopt the theft detector without significant disruptions to their current operations, making it a practical and versatile choice in the competitive landscape.

4.Integration Capability:

The theft detector's integration capability is a key aspect that strengthens its position in the competitive landscape. It can seamlessly integrate with other security systems and technologies, such as access control systems, surveillance cameras, or alarm systems. This interoperability allows businesses to create a holistic security ecosystem, where all components work in harmony to ensure comprehensive protection against theft. By integrating with existing infrastructure, the theft detector eliminates the need for businesses to undergo a complete overhaul of their security systems, reducing costs and disruptions. This integration capability enhances the overall security posture and operational efficiency, making the theft detector an attractive option for businesses seeking to enhance their security measures while maximizing the value of their existing investments.

5.Value Proposition:

The theft detector offers significant value to businesses by mitigating theft risks and reducing financial losses. Its advanced features, real-time alerts, and predictive

analytics contribute to a rapid response and prevention of theft incidents. By providing real-time alerts and notifications, the theft detector enables businesses to take immediate action, minimizing the time gap between detection and intervention. This proactive approach can significantly reduce losses associated with theft, including stolen merchandise, inventory shrinkage, and revenue losses. Moreover, by leveraging predictive analytics, the theft detector helps businesses identify theft patterns and trends, enabling proactive measures to be taken to prevent future incidents. This predictive capability empowers businesses to stay one step ahead of potential theft risks, enhancing overall security and minimizing financial impacts.

5.1.4 Describe IP or patent issues, if any?

Our project does not currently face any known IP or patent issues. We have conducted a thorough analysis of the existing intellectual property landscape and found no conflicts or infringements related to our technology. We have also taken measures to ensure that our product and its components do not infringe upon any existing patents or intellectual property rights held by others.

We prioritize compliance with intellectual property laws and respect the rights of others in the industry. Our development process adheres to best practices in IP protection, including conducting prior art searches and freedom-to-operate analyses. By proactively assessing the IP landscape and taking necessary precautions, we have ensured that our theft detector is built on a solid foundation of originality and innovation.

We continue to monitor the IP landscape and stay informed about any changes or developments that may affect our product. Should any IP issues arise in the future, we are committed to addressing them promptly and responsibly, in accordance with applicable laws and regulations.

Our focus remains on delivering a high-quality, reliable, and innovative theft detection solution to our customers, while upholding the principles of intellectual property protection and ethical business practices.

5.1.5 Who are the possible capstone projected clients/customers?

1.Database Servers:

A. **Unauthorized Presence Detection:** The theft detector uses various sensors, such as motion sensors or infrared detectors, to detect any unauthorized presence in the server

rooms or data centers where the hardware database servers are located. It continuously monitors the area and triggers alerts if it detects any movement or presence of individuals who do not have authorized access. This helps prevent potential theft or unauthorized access to the servers and ensures that only authorized personnel are present in the secured area.

B. **Intrusion Detection:** The theft detector employs sensors and security mechanisms to detect and deter physical intrusions into the server rooms. It can include door/window sensors, magnetic contacts, or glass break detectors to monitor entry points and immediately identify any unauthorized attempts to gain access. In the event of a breach, the theft detector triggers real-time alerts, notifying security personnel or system administrators, who can take immediate action to prevent further intrusion and protect the hardware servers.

C. **Security Cameras Integration:** The theft detector can be integrated with surveillance cameras strategically placed within the server rooms or data centers. This integration enables real-time monitoring and recording of the physical environment, providing visual evidence of any security breaches or suspicious activities. The theft detector can analyze the camera feeds for motion detection or anomaly detection, further enhancing the effectiveness of the physical security monitoring system.

D. **Tamper Detection:** The theft detector includes tamper-resistant features to ensure the integrity and security of the hardware database servers. It can detect attempts to physically tamper with the servers, such as opening the server chassis, removing or replacing components, or accessing the server internals without authorization. Any tampering detected by the theft detector triggers immediate alerts, enabling swift response to prevent unauthorized modifications or theft of server components.

E. **Alarm Systems Integration:** The theft detector can integrate with alarm systems, enabling the generation of audible or visual alarms in the event of security breaches or unauthorized access attempts. This integration adds an additional layer of deterrence and provides a clear indication of security violations to alert security personnel or initiate emergency protocols. The theft detector can also provide relevant information to the alarm system, such as the location of the breach or the specific server affected, enhancing the overall security response.

F. **Real-time Monitoring and Reporting:** The theft detector continuously monitors the physical security parameters, tracks events, and generates real-time reports on security

incidents. It provides a centralized dashboard or control panel that allows security personnel or system administrators to monitor the status of the hardware database servers and promptly respond to any security alerts. The theft detector also maintains a log of security events and incidents, which can be reviewed for post-incident analysis and forensic purposes.

2.Museums and art galleries:

Museums and art galleries house valuable artifacts and artworks that require specialized security measures. The theft detector can play a crucial role in protecting these valuable assets from theft or damage.

A.Object Recognition: The theft detector's computer vision capabilities can be utilized to recognize and track specific objects within the museum or art gallery. By creating a digital inventory and monitoring the movement of these objects, the theft detector can quickly detect any unauthorized handling or attempted theft.

B.Motion Detection: Deploying the theft detector in strategic locations within the museum or art gallery allows for effective monitoring of visitor movements. By detecting unusual or suspicious behavior, such as individuals approaching restricted areas or tampering with exhibits, the theft detector can generate real-time alerts for security personnel to intervene and prevent theft or damage to the artworks.

C.Integration with Existing Security Systems: The theft detector can be integrated with existing security systems, such as video surveillance cameras or alarm systems, to provide a comprehensive security solution. This integration ensures that the theft detector works in harmony with the museum or art gallery's existing security infrastructure, enhancing overall protection and response capabilities.

3. Jewelry Stores:

Jewelry stores face the constant risk of theft due to the high value of their merchandise. Implementing the theft detector can significantly enhance security measures and safeguard valuable jewelry inventory.

A.Surveillance and Real-Time Alerts: The theft detector can continuously monitor the jewelry store, utilizing computer vision to analyze customer behavior and identify potential theft indicators. Suspicious activities, such as unusual movement near display cases or attempts to tamper with security measures, can trigger real-time alerts for store personnel or security personnel to intervene promptly.

B.Object Tracking: By tracking the movement of individual jewelry pieces using computer vision and object recognition, the theft detector can provide a clear audit trail of jewelry items, ensuring that any potential loss or theft can be quickly identified and addressed.

C.Customer Behavior Analysis: The theft detector can analyze customer behavior patterns to identify anomalies that may indicate potential theft. For example, loitering near high-value displays or attempting to obscure the view of surveillance cameras could be identified as suspicious behavior, triggering real-time alerts and enabling proactive intervention.

Overall, the theft detector offers customized and advanced security solutions tailored to the specific needs of database servers, museums and art galleries

5.2 Financial Considerations

5.2.1 Capstone project budget

1. **Internet:**

   To ensure connectivity and enable remote monitoring, a reliable internet connection is required. The monthly internet plan cost is estimated at 1000 rs. This cost covers the ongoing access to the internet service provider.

2. **Call Alert Sender:**

   The theft detector system incorporates an alert system to notify relevant parties in case of any suspicious activities. To enable this functionality, a subscription to a service provider like Twilio is necessary. The Twilio subscription cost is estimated at 1700 rs, covering the expenses associated with sending alerts via calls or messages.

3. **Courses:**

   It is essential to stay updated with the latest trends and technologies in the field of theft detection and security. Therefore, investing in online courses and resources is crucial. The estimated cost for an online course subscription is 650 rs, providing access to valuable educational materials and training resources.

4. **Camera:**

   A USB camera is an integral component of the theft detector system as it captures video footage for monitoring and analysis. The estimated cost for a reliable USB camera suitable for this purpose is 1000 rs.

5. **Cables:**

To connect various components of the system, USB cables and other accessories are required. The estimated cost for USB cables and related accessories is 200 rs, ensuring proper connectivity and functionality.

6. **Software:**

The theft detector system may require specialized software for data analysis, alert management, or user interface development. A subscription to software such as PyCharm Pro, with an estimated cost of 1500 rs, allows for efficient software development and management.

7. **Power Consumption:**

The system components, including cameras and alert systems, require power to operate. Considering an average power consumption rate of 64W, the estimated cost for power consumption is approximately 20 rs per week. This cost covers the electricity expenses associated with running the system.

1.PC Charges:

The hardware component of the system includes the computers or laptops used for system setup and monitoring. For instance, if three laptops are required for the project, with each laptop priced at 62,000 rs, the total system cost would amount to 1,86,000 rs.

5.2.2 Cost capstone projections needed for either for profit/nonprofit options.

- **Research and Development:**
  1. Market research and feasibility studies: ₹5,000
  2. Prototype development: ₹10,000

- **Hardware Costs:**
  1. Cameras: ₹5,000
  2. Cables and accessories: ₹1,000

- **Software Development**:
  1. Detection algorithms: ₹10,000
  2. User interface development: ₹5,000

- **Integration and Installation:**
  1. Professional installation: ₹2,000
  2. Integration with existing security systems: ₹1,000

- **Testing and Quality Assurance:**
  1. Testing equipment and tools: ₹4,000
  2. Quality assurance processes: ₹8,000

- **Operations and Support:**
  1. Personnel costs: ₹10,000 (for administrative support)

- **Marketing and Promotion:**
  1. Marketing materials (brochures, website): ₹15,000
  2. Online advertising campaigns: ₹20,000

- **Miscellaneous Expenses:**
  1. Legal fees: ₹10,000
  2. Insurance: ₹7,000
  3. Contingency budget: ₹10,000

Total Project Cost: ₹1,13.,000

- **Nonprofit Option:**

1. Research and Development:
2. Market research and feasibility studies: ₹2,000
3. Prototype development: ₹5,000
4. Hardware Costs:
5. Cameras: ₹3,000
6. Cables and accessories: ₹1,000
7. Software Development:
8. Detection algorithms: ₹5,000
9. User interface development: ₹3,000
10. Integration and Installation:
11. Self-installation: ₹0

12. Integration with existing security systems: ₹500
13. Testing and Quality Assurance:
14. Testing equipment and tools: ₹2,500
15. Quality assurance processes: ₹4,000
16. Operations and Support:
17. Volunteer support: ₹0 (if relying on volunteers)
18. Personnel costs: ₹10,000 (for administrative support)
19. Marketing and Promotion:
20. Marketing materials (brochures, website): ₹8,000
21. Online advertising campaigns: ₹10,000
22. Miscellaneous Expenses:
23. Legal fees: ₹5,000
24. Insurance: ₹5,000
25. Contingency budget: ₹5,000

Total Project Cost: ₹64,000

5.3 Conclusions and Recommendations

In conclusion, the implementation of a theft alert detector, integrated with a call, SMS, and email alert system, provides an advanced and comprehensive solution for theft detection and immediate notification. By combining the power of computer vision algorithms from OpenCV with effective communication capabilities, the system offers real-time monitoring, accurate detection, and timely alerts, enhancing the overall security measures.

- **The key advantages of incorporating the call, SMS, and email alert system into the theft alert detector using OpenCV are:**

1. **Rapid response:** The integration of call, SMS, and email alerts ensures that the appropriate individuals or authorities are immediately notified when a potential theft is detected. This enables quick response times, increasing the chances of preventing further loss or damage.
2. **Multi-channel notifications:** By utilizing multiple communication channels, such as calls, SMS, and emails, the system can reach security personnel or designated contacts more effectively. This redundancy helps to ensure that alerts are received promptly, even if one channel experiences technical difficulties or is temporarily unavailable.
3. **Customizable notifications:** The alert system can be customized to provide specific information about the detected theft incident, including the location, timestamp, and relevant details. This level of customization enables recipients to quickly assess the situation and take appropriate action.
4. **Remote access and management:** With the integration of communication capabilities, security personnel or authorized individuals can remotely access and manage the alert system. This allows for monitoring and responding to theft incidents from any location, providing flexibility and convenience.
5. **Enhanced security protocols:** The addition of the call, SMS, and email alert system adds an extra layer of security to the theft detection process. It ensures that alerts are not solely reliant on visual monitoring and detection but also backed by immediate notifications, allowing for a comprehensive security approach.

While the inclusion of the call, SMS, and email alert system greatly enhances the functionality and effectiveness of the theft alert detector, it is important to consider the following limitations:

1. **Dependence on network connectivity:** The successful delivery of alerts relies on stable network connectivity for making calls, sending SMS messages, and transmitting emails. Any disruptions in network availability or failures may result in delays or failed notifications.
2. **False positives and false negatives:** As with any theft detection system, false positives and false negatives can occur. False positives may trigger unnecessary alerts, potentially leading to alert fatigue, while false negatives may result in missed theft incidents. Continuous refinement and optimization of the detection algorithms are necessary to minimize these errors.
3. **Integration complexity:** The integration of the call, SMS, and email alert system requires careful configuration and setup. It may involve integration with third-party services or APIs, which can introduce additional complexities and potential points of failure.

In summary, the integration of a call, SMS, and email alert system into the theft alert detector using OpenCV significantly enhances the system's functionality and responsiveness. By leveraging these communication channels, the system ensures rapid notifications, multi-channel reach, customization, remote access, and enhanced security protocols. However, considerations should be given to network connectivity, false positives and negatives, and integration complexities during the implementation process.

5.3.1 Future work

1.Integration with Automatic Door Locking System:

- Implement integration with automatic door locking systems to enhance security. This can include features such as unlocking doors remotely through the security system or automatically locking doors when an alarm is triggered.

2.Mobile App Development:

- Develop dedicated mobile applications for the security system to provide users with convenient access and control. The app can include features like real-time monitoring,

push notifications for alarms, remote control of security settings, and video surveillance viewing.

3.Advanced User Management and Access Control:

- Enhance the security system by implementing a more structured user management system. This can include features like user roles and permissions, access control lists, and activity logs to track and manage user access and actions within the system.

4.Artificial Intelligence and Machine Learning:

- Explore the use of AI and machine learning algorithms to improve the security system's capabilities. This can involve developing intelligent threat detection and pattern recognition algorithms to identify suspicious activities or potential security breaches.

5.Cloud-Based Storage and Backup:

- Integrate cloud-based storage and backup solutions to securely store system data, logs, and video recordings. This ensures data resilience, provides easy access to historical information, and mitigates the risk of data loss due to hardware failure or physical damage.

6.Security System Analytics and Reporting:

- Develop analytics and reporting functionalities to provide insights into security system performance, user activity, and incident patterns. This can help identify vulnerabilities, optimize security settings, and generate comprehensive reports for audit and compliance purposes.

7.Integration with Smart Home Devices:

- Integrate the security system with smart home devices, such as smart locks, surveillance cameras, and motion sensors, to create a comprehensive smart security ecosystem. This allows for seamless automation, synchronized actions, and centralized control of all connected devices.

8.Ongoing System Maintenance and Upgrades:

- Plan for regular system maintenance, updates, and upgrades to ensure the security system remains up-to-date with the latest security protocols, patches, and features. This includes monitoring industry trends and advancements to incorporate new technologies and stay ahead of potential security threats.

5.3.2 Describe the state of completion of the capstone project.

The capstone project, "Guardian Eye," has reached an advanced stage of development but is not yet ready for market deployment. The project team has made significant progress in designing and implementing the system's hardware and software components, successfully achieving the defined objectives and meeting the project requirements.

During the planning and proposal phase, the team conducted thorough research, defined the project scope, and formulated a comprehensive project plan. They identified the necessary features and functionalities for an effective theft detection system.
In the design and development phase, the team integrated surveillance cameras, motion sensors, and alarm systems to create a cohesive security solution. They also implemented sophisticated algorithms for real-time theft detection, ensuring the system can accurately identify suspicious activities.

The project documentation is in progress, including technical documentation, system architecture diagrams, design specifications, and user manuals. These documents will provide a comprehensive understanding of the system's implementation and usage instructions for future users.

While the project has made substantial advancements, additional refinement and validation are required before market deployment. The team is actively working on addressing any identified issues, optimizing the system's performance, and ensuring its compliance with industry standards and regulations.once the necessary enhancements and final validations are complete, the theft detection system will be ready for market deployment, offering a reliable and efficient solution to enhance security and protect against theft incidents.

5.3.3 Outline how the capstone project may be extended

1.Feature Expansion:

- Identify additional features that can enhance the functionality of the theft detection system. This could include advanced alarm triggers, integration with third-party security systems, or integration with smart home devices for comprehensive security automation.

2.Integration with Cloud Services:

- Explore the integration of the theft detection system with cloud-based services. This could enable remote monitoring, data storage, and analysis, providing scalability, flexibility, and accessibility to users.

3.Mobile Application Enhancement:

- Enhance the existing mobile application to provide more extensive control and monitoring capabilities. This could include real-time video streaming, push notifications for alarm events, and the ability to remotely arm or disarm the system.

4.Machine Learning and Artificial Intelligence:

- Investigate the application of machine learning and artificial intelligence techniques to further improve theft detection accuracy. This may involve training models on historical data to identify patterns and anomalies and make more accurate predictions.

5.Integration with Security Analytics:

- Explore the integration of the theft detection system with security analytics platforms. This could provide advanced analytics capabilities, anomaly detection, and correlation analysis to identify potential security threats and vulnerabilities.

6.Enhanced User Management and Access Control:

- Extend the user management system to provide more granular control over user permissions and access levels. This could include role-based access control, multi-factor authentication, and activity auditing for improved security.

7.Integration with Emergency Services:

- Investigate integration with emergency services, such as local law enforcement agencies or private security firms. This could enable automatic dispatch of authorities in the event of a confirmed theft or security breach.

8.Continuous Monitoring and Improvement:

- Establish mechanisms for ongoing monitoring and improvement of the system. This includes collecting user feedback, conducting regular system audits, and implementing security patches and updates to address emerging threats.

9.Pilot Testing and Real-World Deployment:

- Conduct pilot tests of the extended system in real-world environments to gather data, validate its effectiveness, and identify areas for further refinement. Based on the results, plan for a broader deployment to commercial or residential settings.

REFERENCES

1. **Python:**
   - python software foundation (2021) python 3.9.6 documentation retrieved from **https://docs.python.org/3/**

2. **Twilio:**
   - twilio api documentation, retrieved from **https://www.twilio.com/docs/quickstar**

3. **Tkinter:**
   - python software foundation. (2021). tkinter: python interface to tcl/tk. retrieved from **https://docs.python.org/3/library/tkinter.html**

4. **Opencv:**
   - mainly for real-time computer vision. Originally developed by Intel, it was later supported by Willow Garage **https://docs.opencv.org/4.5.3/**

5. **Numpy in python:**
   - NumPy is a Python library used for working with arrays. It also has functions for working in the domain of linear algebra, fourier transform, and matrices. **https://www.w3schools.com/python/numpy/numpy_intro.asp**

6. **Object detection:**
   - Object detection is a computer vision technique for locating instances of objects in images or videos. **https://www.mathworks.com/**

7. **Motion detection:**
   - detecting a change in the position of an object relative to its surroundings or a change in the surroundings relative to an object. **https://pyimagesearch.com/**

8. **SMTP Server:**

- The address of any email provider's mail server. This lets your computer send emails to anyone or send emails from your email account to anyone.
  https://sendgrid.com/blog/what-is-an-smtp-server/

9. **Pyinstaller:**

pyinstaller documentation. (2021), retrieved from
https://pyinstaller.readthedocs.io/en/stable/

Note: For specific implementation details and code examples, please refer to the project's own documentation, provided alongside the source code.

Disclaimer: The references listed above are for informational purposes only. It is important to consult official documentation and relevant sources for accurate and up-to-date information.

APPENDICES

A: Code Snippets

This appendix provides relevant code snippets that demonstrate the implementation of key algorithms and techniques used in the theft alert detector.

main.py

```
from tkinter import *
from tkinter import messagebox
from find_motion import find_motion
from twilio.rest import client
import random

def btn_clicked():
print("button clicked")
username = entry0.get()
password = entry1.get()
if username == "GuardianEye":
 print("username correct")
 if password == "GE@R3":
 print("password correct")
 window.destroy()
 sms()
 secondpage()
 else:
 messagebox.showerror("data verification", "please recheck the entered password")
 else:
 messagebox.showerror("data verification", "please recheck the entered username")

verify=random.randint(100000,999999)
def secondpage():
def buttonclicked1():
otp = entry4.get()
if otp == str(verify):
window3.destroy()
third_page()
else:
messagebox.showerror("multi factor authentication", "please recheck the entered code")
```

Spot_diff.py

```
import cv2
```

```
import time
from skimage.metrics import structural_similarity
from datetime import datetime

def spot_diff(frame1, frame2):
frame1 = frame1[1]
frame2 = frame2[1]
g1 = cv2.cvtcolor(frame1, cv2.color_bgr2gray)
g2 = cv2.cvtcolor(frame2, cv2.color_bgr2gray)
g1 = cv2.blur(g1, (2,2))
g2 = cv2.blur(g2, (2,2))
(score, diff) = structural_similarity(g2, g1, full=true)
print("image similarity", score)
```

Find_motion.py

```
import cv2
from spot_diff import spot_diff
import time
import datetime
import numpy as np
import smtplib
import winsound
from email.mime.text import mimetext
from email.mime.multipart import mimemultipart
from email.mime.image import mimeimage

def find_motion():
motion_detected = false
is_start_done = false
webcam = cv2.videocapture(0)
check = []
frame1 = webcam.read()
_, frm1 = webcam.read()
frm1 = cv2.cvtcolor(frm1, cv2.color_bgr2gray)

while true:
_, frm2c = webcam.read()
frm2 = cv2.cvtcolor(frm2c, cv2.color_bgr2gray)
diff = cv2.absdiff(frm1, frm2)
```

B: Experimental Results

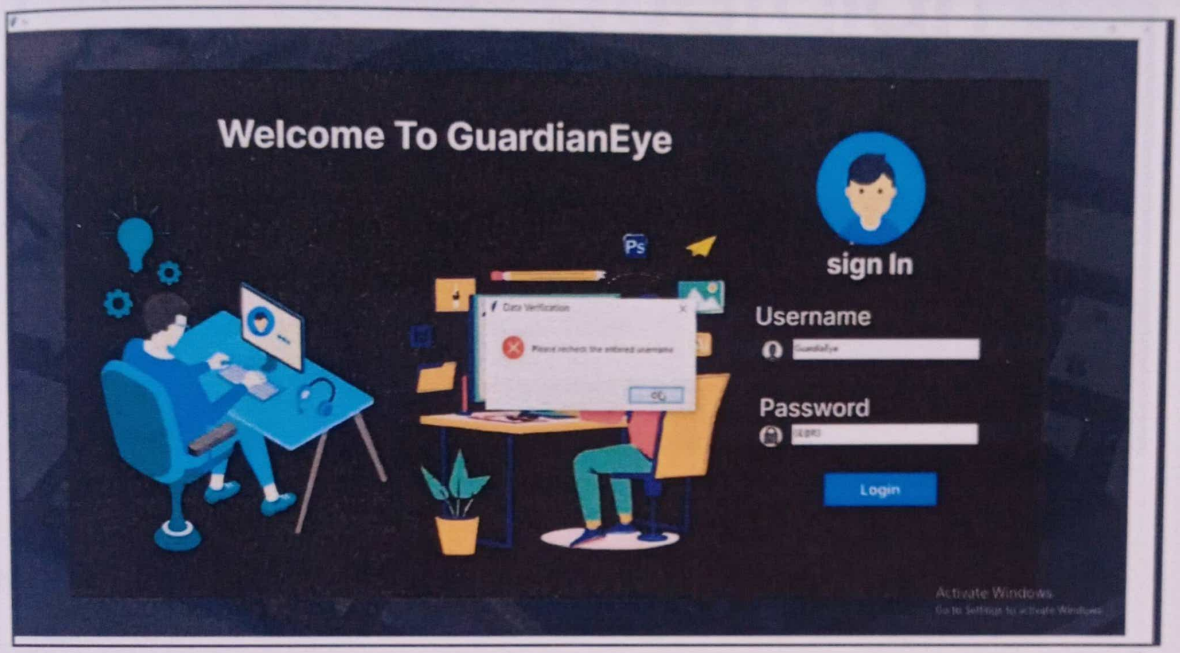
In this appendix, There are experimental results obtained during the evaluation of the theft alert detector.

Figure 7.2 Experiment Results

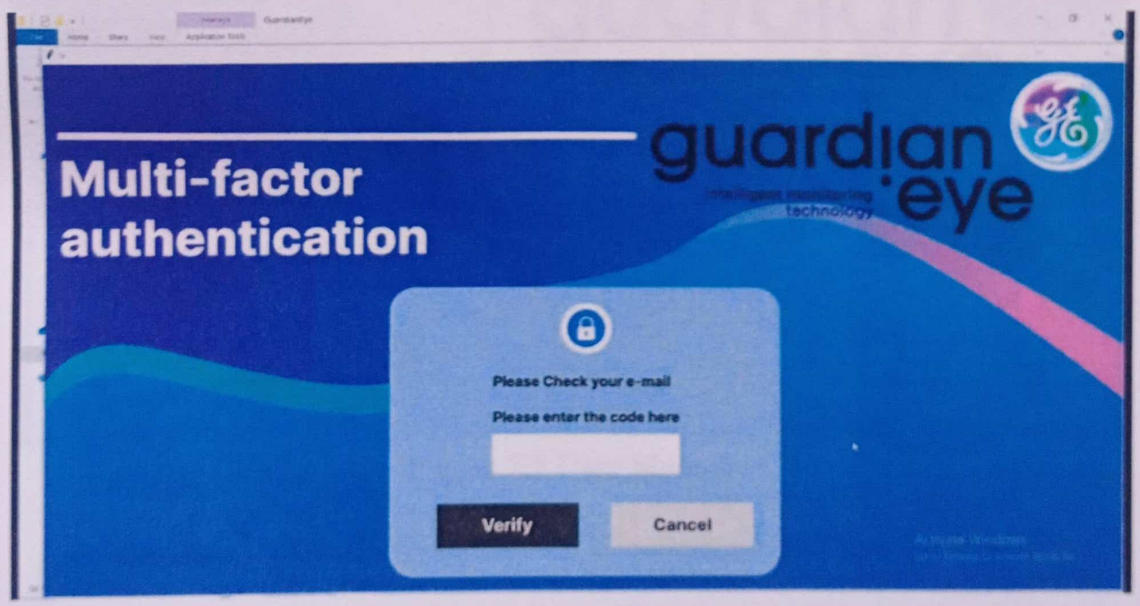
C: User Manual

This appendix includes a user manual or guide that provides instructions on how to set up and operate the GuardianEye software and secure your peace of mind with GuardianEye.

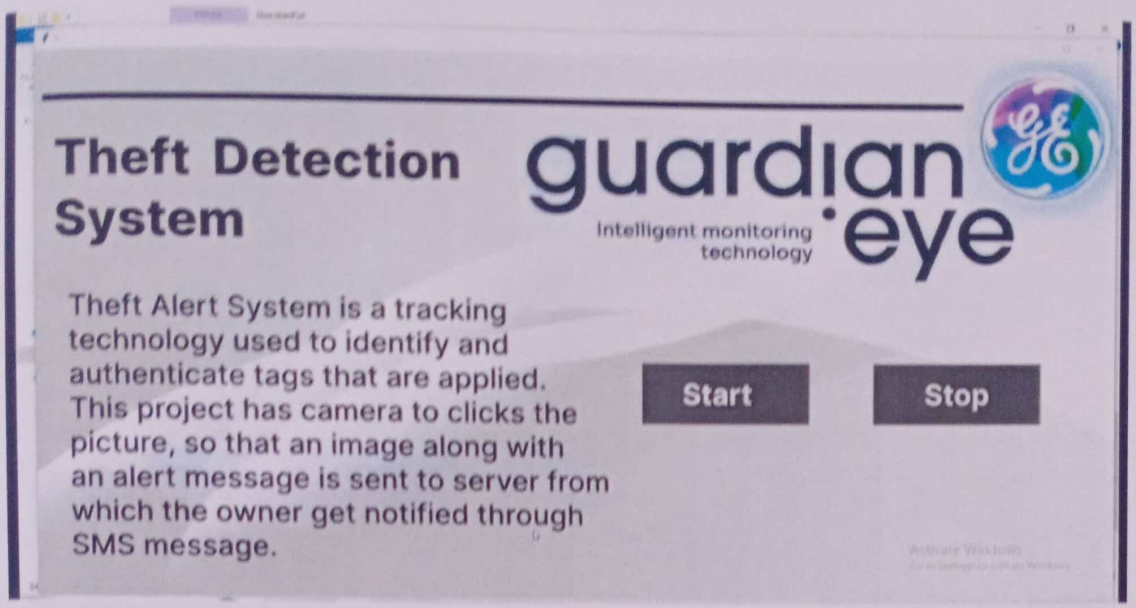
Step 1: Enter your Correct Username and Password provided by GuardianEye Team.



Step 2: Enter the OTP which will be sent to your registered mobile number..



Step 3: Click the start button to open the camera.



Step 4: Now the Surveillance/Web Camera is monitoring,you can relax now.

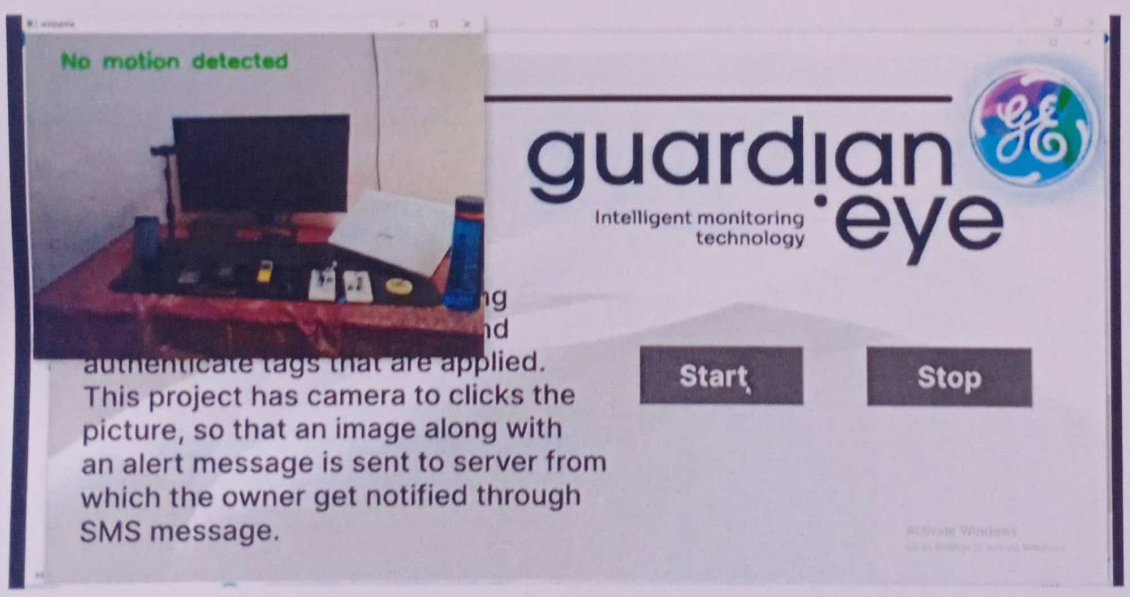


Figure 7.3 User Manual