

A PROJECT STAGE II REPORT ON
ON
SUSPICIOUS ACTIVITY DETECTION IN HOSPITAL

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

BACHELOR OF ENGINEERING
(COMPUTER ENGINEERING)

SUBMITTED BY

Mayur Sambhaji Kharmate	Seat No.: B190524277
Aniket Rajesh Uttekar	Seat No.: B190524201
Shreyas Ajay Kulkarni	Seat No.: B190524280
Kunal Anil Desai	Seat No.: B190524238



DEPARTMENT OF COMPUTER ENGINEERING
INDIRA COLLEGE OF ENGINEERING & MANAGEMENT
PARANDWADI, PUNE 410506
SAVITRIBAI PHULE PUNE UNIVERSITY

2022-23



CERTIFICATE

This is to certify that the project report entitles

“SUSPICIOUS ACTIVITY DETECTION IN HOSPITAL”

Submitted by

Mayur Sambhaji Kharmate Seat No.: B190524277

Aniket Rajesh Uttekar Seat No.: B190524201

Shreyas Ajay Kulkarni Seat No.: B190524280

Kunal Anil Desai Seat No.: B190524238

is a bonafide student of this institute and the work has been carried out under the supervision of **Prof. Deepali Dhadwad**. It is approved for the partial fulfillment of the requirements of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Engineering** (Computer Engineering).

Prof. Deepali Dhadwad

Guide,

Department of Computer Engineering

Dr. Soumitra Das

Head,

Department of Computer Engineering

Dr. Sunil Ingole

Director,

Indira College of Engineering & Management, Pune

Place : Pune

Date :

Sign of Internal Examiner

Sign of External Examiner



Project Approval Sheet

Project

On

“SUSPICIOUS ACTIVITY DETECTION IN HOSPITAL”

BY

MR. MAYUR KHARMATE

MR. ANIKET UTTEKAR

MR. SHREYAS KULKARNI

MR. KUNAL DESAI

at

**DEPARTMENT OF COMPUTER
ENGINEERING**

INDIRA COLLEGE OF ENGINEERING & MANAGEMENT

PARANDWADI, PUNE 410506

[2022-23]

PROF. DEEPAI DHADWAD

DR. SOUMITRA DAS

DEPARTMENT OF COMPUTER ENGG.

HOD

Acknowledgment

We are presenting this project report on “Suspicious Activity Detection In Hospital” as part of the curriculum of B.E. Computer Engineering with immense pleasure. We started working on it with a zeal and enthusiasm but then quickly realized that for satisfactorily completing the project not only require conviction and perseverance, but without due help and guidance such a task becomes futile. We wish to thank all the people who gave us an unending support right from the stage the idea was conceived. It gives us great pleasure, on the completion of this project, to acknowledge and appreciate all those who were there to help us.

We express my sincere and profound thanks to all our teachers **Dr.Soumitra Das** (Head of Department), **Ms.Pragati Choudhari** (Project Coordinator).We would like to thank our college ICEM, Parandwadi, for the boost that it has provided.We wish to thank **Prof.Deepali Dhadwad** (Computer Dept.) for her student-like enthusiasm and her guidance from time to time.We heartily thank for all her help and valuable time.Her invaluable advice has helped us bring this work to completion.Besides, We take this opportunity to express my sincere gratitude to the Principal **Dr.Sunil Ingole**(ICEM, Pune) for providing a good environment and facilities to complete this project.

We would like to thank all our internal guides for providing the resources for project stage. We also acknowledge the research work done by all researchers in this field. And last but not least, all our friends, who have helped us directly or indirectly throughout the project.

Mayur Sambhaji Kharmate (24131)

Aniket Rajesh Uttekar (24130)

Shreyas Ajay Kulkarni (24129)

Kunal Anil Desai (24134)

B.E. Computer(IV year) 2022-23

Abstract

Suspicious activities are of a problem when it comes to the potential risk it brings to humans. With the increase in criminal activities in urban and suburban areas, it is necessary to detect them to be able to minimize such events. Early days surveillance was done manually by humans and where a tiring task as suspicious activities were uncommon compared to the usual activities. With the arrival of intelligent surveillance systems, various approaches were introduced in surveillance.

A significant field of research and development focuses on sophisticated machine learning methods for the detection of suspicious human behaviour to lower monitoring costs while increasing safety. We require a real-time intelligent human activity detection system that can recognize suspicious actions in hospitals because it is challenging for personnel to continuously watch in hospitals. The complicated low-accuracy algorithms and approaches used by current systems make them less dependable. By integrating a Convolutional Neural Network and using the 2D posture estimation approach to the system, this study suggests a real-time suspicious human activity recognition method with high accuracy. This system is suitable for usage in hospitals, homes, and other surveillance areas. Here, we use 2D pose estimation to extract skeleton pictures of people from the input video frames in order to determine their pose.

The integration of this automated suspicious activity detection system with existing hospital security infrastructure provides timely identification and alerts, enabling prompt responses to potential threats and ensuring the well-being of patients and staff.

Keywords: *Suspicious, Hospital , Deep Learning , Computer Vision , Security , Machine Learning*

Contents

Certificate	i
Acknowledgement	iii
Abstract	iv
Contents	v
List of Figures	viii
List of Tables	ix
Abbreviations	x
1 Introduction	1
1.1 Overview	2
1.2 Objectives	2
1.3 Aim & Problem Definition	3
1.4 Limitations	3
1.5 Methodologies of Problem Solving	4
2 Literature Review	7
3 Dissertation Plan	13
3.1 Dissertation Plan	13
3.2 Feasibility Study	13
3.2.1 Options assessed	15
3.2.2 Technical Feasibility	15
3.2.3 Economical Feasibility	15
3.2.4 Operational Feasibility	16
3.3 Risk Analysis and Projection Table	16
3.4 Effort and Cost Estimation	17
3.4.1 Cost Estimation	17
3.4.2 Development Time	17
3.4.3 Number of People	17
4 Software Requirement Specifications	18
4.1 Purpose	18
4.2 Design and Implementation Details	18

4.3	Assumption	19
4.4	Constraints	19
4.5	Usability	19
5	System Design	20
5.1	System Architecture	20
5.2	Mathematical Model	22
5.3	Data Flow Diagram	23
5.4	UML Diagrams	25
5.4.1	Use Case Diagram	25
5.4.2	Class Diagram	26
5.4.3	Activity Diagram	26
5.4.4	Sequence Diagram	28
5.4.5	State Chart	29
5.4.6	Component Diagram	30
6	Project Implementation	32
6.1	Overview of Project Modules	32
6.2	Tools and Technologies Used	33
6.3	Algorithmic Details	34
6.3.1	Algorithm :	34
7	Software Testing	36
7.1	Test cases and Test Results	36
7.1.1	Black Box Testing	36
7.1.2	White Box Testing	37
7.1.3	Alpha Testing	38
7.1.4	Beta Testing	38
8	Results	40
8.1	Outcomes	40
8.2	Screen Shots	40
9	Conclusions	47
9.1	Conclusion	47

9.2	Future Work	48
9.3	Applications	48
	References	50

List of Figures

1	Gantt Chart	13
2	Timeline of Project Stage 1	14
3	Timeline of Project Stage 2	14
4	System Architecure	21
5	Level 0 DFD	24
6	Level 1 DFD	24
7	Use case Diagram	25
8	Class Diagram	26
9	Activity Diagram	27
10	Sequence Diagram	28
11	State Chart	30
12	Component Diagram	31
13	HomePage	40
14	Registration	41
15	Registering account	41
16	Successfully Registered	42
17	Login	42
18	Image detection	43
19	Image detection	43
20	Selecting Image	44
21	Submitting Image	44
22	Suspicious Image Detected	45
23	Realtime detection	45
24	Suspicious Activity detection (Gun Detection)	46
25	Suspicious Activity detection (Fire Detection)	46

List of Tables

1	Risk Analysis	16
2	Black Box Testing	36
3	White Box Testing	37
4	Alpha Testing	38
5	Functional Testing	38
6	Performance Testing	39
7	Accuracy Testing	39
8	Integration Testing	39
9	Usability Testing	39

Abbreviations

DFD	:	Data Flow Diagram
YOLO	:	You Only Look Once
RAM	:	Random Access Memory
GB	:	Gigabytes
URL	:	Unified resource locator
VGG	:	Visual Geometry Group
SRS	:	Software requirement specification
GUI	:	Graphical user interface
UML	:	Unified modelling language
STP	:	Software test plan
CNN	:	Convolutional Neural Network
RNN	:	Recurrent Neural Network
KNN	:	K-Nearest Neighbors

1 Introduction

The identification of suspicious human behavior in automated video surveillance applications holds significant practical importance in today's world. With the increasing reliance on surveillance systems for security purposes, it becomes crucial to develop efficient methods for detecting and classifying abnormal activities. However, this task is not without its challenges, primarily due to the unpredictable nature of human movements and the vast amount of video footage that needs to be analyzed.

Traditionally, manual surveillance systems heavily rely on human involvement, where trained personnel meticulously analyze the surveillance footage to identify any abnormal behavior. This approach requires extensive labor and can be time-consuming, limiting its scalability and effectiveness. Additionally, human operators may have limitations in their attention span, and fatigue can lead to errors or missed detections.

Semi-automatic systems were introduced to alleviate the burden on human operators. These systems utilize computer algorithms to assist in the analysis process, reducing the need for constant human intervention. However, they still rely on human operators to make the final judgment, which can introduce subjectivity and inconsistency in the classification of suspicious behavior.

To overcome these limitations, fully automatic systems have emerged as an intelligent and efficient solution. These systems leverage the power of machine learning and artificial intelligence to detect unusual activities in surveillance footage without the need for human intervention. By training a machine learning model using a vast dataset of images depicting suspicious activities, such as people carrying weapons or wearing masks, the system can learn to recognize and classify such behavior accurately.

The core approach of an automated system involves analyzing the video input by dividing it into frames, which are then fed into the trained machine learning model for analysis. Each frame is examined to identify any abnormal activities based on the learned patterns and features from the training dataset. The system can then flag or

raise an alert whenever it detects suspicious behavior, allowing human operators to take appropriate action promptly.

1.1 Overview

The proposed automated system for detecting suspicious human behavior in video surveillance applications utilizes machine learning and real-time analysis. By training a machine learning model with a diverse dataset of suspicious activities, the system can accurately classify abnormal behaviors and recognize patterns associated with them. It operates in real-time, analyzing video frames to immediately detect and respond to any suspicious activity. The system integrates with existing surveillance networks, enhancing security measures by providing timely alerts and reducing the reliance on manual surveillance systems.

The system's strength lies in its ability to learn and refine its detection capabilities over time. It can extract relevant information from video feeds and compare it against learned patterns, enabling it to identify subtle cues and anomalies that may go unnoticed by human observers. Its integration with existing surveillance infrastructure ensures a seamless implementation and complements the capabilities of the current surveillance equipment. Overall, the proposed system improves security efficiency by automating the detection process, providing accurate classifications, and enabling swift response to potential threats or suspicious activities, contributing to safer environments.

1.2 Objectives

1. Enhancing the security at hospitals by detecting any suspicious person while they engage in suspicious activities such as destruction or causing harm to others.
2. Strengthening security during accidental emergencies when the vulnerability is high, enabling the detection of unauthorized individuals with malicious intent and weapons entering the hospital premises.
3. Alerting authorized personnel if a patient is alone in their room and someone attempts to harm them using a weapon.

4. Alerting authorized personnel if there is fire in the hospital which will minimize the harm to hospital and patients as well.
5. Finding and alerting if anyone is smoking in hospital premises.
6. Upgrading existing security and safety measures by integrating Internet of Things (IoT) technology.

1.3 Aim & Problem Definition

To create an automated system that can monitor and analyze activities in a hospital to identify suspicious behavior and alert authorities in real-time while maintaining privacy. The system should detect unusual events, differentiate between normal and suspicious behavior, and alert authorized person about the same.

1.4 Limitations

1. Illumination changes : The detection of moving objects becomes challenging due to dynamic variations in natural scenes, such as gradual changes in illumination caused by day-night transitions and sudden variations caused by weather changes. These changes in lighting conditions can affect the appearance and visibility of objects, making it difficult to reliably detect and track them. The variations in illumination can cause significant fluctuations in pixel values, leading to false positives or missed detections in video-based surveillance systems.
2. Shadow : Shadows can significantly impact the appearance and characteristics of an object, posing challenges for tracking and detection algorithms. When an object casts a shadow, its appearance is altered, making it harder to distinguish from the background or other objects. Shadows can introduce additional complexities in feature extraction, such as shape, motion, and background modeling. The presence of shadows can interfere with object recognition and tracking, potentially leading to errors or inaccuracies in the detection process.
3. Occlusion : Occlusion occurs when one object obscures or hides a part of another object or person that is of interest for detection or tracking. It often happens

when multiple objects come into close proximity, causing them to overlap or merge with each other visually. Occlusion can pose significant challenges in accurately identifying and tracking objects, as the occluded regions may not be visible or may appear distorted. Resolving occlusion requires sophisticated algorithms that can handle partial visibility, object fragmentation, and re-association of occluded parts to ensure accurate and reliable object detection and tracking.

4. Limited camera angles and coverage: The effectiveness of the system heavily relies on the placement and coverage of surveillance cameras. Blind spots or limited camera angles may result in missed detections or incomplete monitoring of certain areas, limiting the system's overall performance.
5. Poor camera quality : Poor camera quality, including low resolution or blurry footage, can degrade the accuracy of object detection and tracking algorithms. The system may struggle to distinguish between normal and abnormal behavior due to the lack of clear and detailed visual information. Inadequate camera quality can result in false positives or false negatives, leading to less reliable detection and potentially compromising the effectiveness of the system.

1.5 Methodologies of Problem Solving

There are several different methodologies that can be used for suspicious activity detection in hospitals. Here are a few methods which can be used for the same:

1. Sensor Networks: Sensor networks play a crucial role in detecting suspicious activities within a hospital environment. Various types of sensors can be deployed strategically to monitor different aspects of the hospital. For instance:
 - Motion sensors: Installed in restricted areas, motion sensors can detect unauthorized movement, such as someone entering a restricted zone. They are typically placed at key access points or sensitive areas within the hospital. When motion is detected, an alert can be triggered, notifying security personnel or the appropriate authorities to investigate the activity.

- Sound sensors are designed to pick up unusual sounds that may indicate suspicious activity. These sensors can detect sounds like breaking glass, loud shouting, or alarms within the hospital environment. When such sounds are detected, an alert can be generated to alert security personnel or staff to respond to the situation promptly.
- Environmental sensors: Environmental sensors are used to monitor various factors such as temperature, humidity, or air quality within the hospital premises. These sensors can detect anomalies in the environment that might suggest suspicious actions, such as tampering with the environment or the presence of hazardous substances. By continuously monitoring the environment, these sensors can help identify potential threats and trigger appropriate responses to mitigate risks.

By deploying a combination of motion sensors, sound sensors, and environmental sensors, hospitals can create a comprehensive surveillance system that can detect and respond to suspicious activities effectively. These sensors act as additional sets of eyes and ears, enhancing the overall security measures in place to ensure the safety of patients, staff, and visitors within the hospital premises.

2. Machine Learning or Deep Learning: Machine learning and deep learning algorithms can be employed to analyze data from diverse sources, such as surveillance cameras, sensor networks, electronic health records, or access logs. These algorithms can learn patterns and detect anomalies that may indicate suspicious behavior. By training on large datasets of normal activities, these algorithms can identify deviations from the norm and raise alerts for further investigation. The use of neural networks, convolutional neural networks (CNNs), or recurrent neural networks (RNNs) can enhance the accuracy of the detection system.
3. Human Observers: Having human observers, such as security personnel or trained staff, is a traditional but effective method of detecting suspicious activity. They can monitor live video feeds from surveillance cameras in real-time and identify any unusual or suspicious behavior. Human observers can be stationed in critical

areas like patient rooms, sensitive medical procedures, or high-security zones where other methods may not be feasible or as effective. Their trained eyes can provide valuable insights and prompt response to potential threats.

It's worth noting that these methodologies are not mutually exclusive. In fact, a combination of these approaches can enhance the overall detection and response capabilities of a hospital's security system. Integrated systems that leverage sensor networks, machine learning algorithms, and human observation can provide a comprehensive and robust solution for detecting and preventing suspicious activities within a hospital environment.

2 Literature Review

When it comes to the potential risks it poses to people's safety, suspicious activity stands out as a significant problem. As urban and suburban areas experience a rise in criminal activity, it becomes crucial to detect and prevent such occurrences to ensure public safety. In the early days, surveillance efforts relied heavily on manual observation by human operators. However, this approach proved to be highly taxing and inefficient, given that instances of suspicious activity were relatively rare compared to everyday activities. To address these challenges, intelligent surveillance systems were introduced, revolutionizing the field of surveillance. These systems utilize advanced technologies, such as computer vision, machine learning, and artificial intelligence, to enhance the effectiveness and efficiency of detecting and monitoring suspicious behavior. We concentrate on examining two situations where, if ignored, there is a high risk to human lives: identifying potential crimes involving firearms and identifying abandoned luggage on surveillance footage.[1]

Automated teller machines (ATMs) are frequently used to conduct financial transactions and are quickly evolving into a necessity of daily life. Money can be withdrawn, deposited, and transferred between accounts whenever needed with the use of ATMs. However, this convenience is tainted by criminal activity, which is rapidly compromising bank clients' security, such as money theft and assaults on consumers. In this research, we provide a video-based framework that can quickly spot suspicious activity at ATM installations and sound an alarm in the event of any suspicious occurrence. The suggested method uses Hu moments and motion history images (MHI) to extract pertinent features from video .[2]

This publication focuses on incorporating original research that contributes to the advancement of knowledge within a specific field. It also considers original reviews and surveys that provide valuable insights, even if they don't introduce new information or ideas. Importantly, the results presented in the article should not have been previously published or submitted elsewhere. Additionally, the journal accepts expanded versions of conference publications. In situations where frequent motion occurs, it is

probable that subsequent activity patterns can impede the previous pattern, resulting in a distorted pattern and consequently leading to a low recognition rate. This phenomenon highlights the challenges associated with consistent recognition in dynamic environments characterized by frequent motion. By examining the impact of motion on recognition accuracy, researchers can gain a deeper understanding of the factors influencing recognition systems and develop strategies to mitigate these challenges. The aforementioned observation suggests that the recognition rate is adversely affected by the interference caused by frequent motion. To improve recognition accuracy in such scenarios, it is necessary to develop novel approaches that can effectively handle and compensate for the distortions introduced by rapid motion. These approaches may involve advanced algorithms, robust feature extraction techniques, or the integration of additional sensor data to enhance the recognition capabilities of the system.[3]

The main focus of this publication is the computer analysis of visual data. The journal *Computer Vision and Image Understanding* serves as a platform for the dissemination of research papers that cover various aspects of image analysis. It encompasses the entire spectrum of image understanding, ranging from the fundamental low-level processes of early vision, such as image formation and basic feature extraction, to the higher-level processes of recognition and interpretation, involving complex symbolic representations. The journal covers a broad range of topics within the domain of image understanding, with an emphasis on providing diverse perspectives that challenge prevailing viewpoints. Researchers contribute papers that delve into different approaches, methodologies, and theories, thereby enriching the field with innovative insights and alternative viewpoints. The journal serves as a forum for scholarly discourse and aims to foster a deeper understanding of image analysis and its practical applications.[4]

The most recent technological advancements have resulted in automation and digitization in practically every field, which has had an impact on a wide range of applications. This has led to a massive flow of data from all industries, with the information included in that data serving as a crucial component for the advancement of each individual, group, state, nation, and so on. Depending on who handles it, these data

with vital information might be seen in a constructive or negative way. Therefore, taking precautions becomes absolutely necessary to secure the data from unauthorized access. This opens the door for the creation of a system to detect suspicious activity in sensitive locations like hospitals, financial institutions, and military regimes.[5]

Sensor-based human activity recognition has received a lot of attention in artificial intelligence and ubiquitous computing due to the accessibility of inexpensive sensors and sensor networks. In this study, using wireless sensors linked to a person's body, we describe a novel two-phase method for identifying aberrant actions. Among many other applications of sensor networks, detecting anomalous behaviors is a particularly crucial duty in security monitoring and healthcare. Traditional solutions to this issue have a significant false positive rate, especially when sensor data collection is biased toward normal data and aberrant events are few. As a result, it is difficult to apply many traditional data mining techniques because there is a lack of training data.[6].

Due to an increase in immoral or anti-social behaviors that have been occurring often, security has become a crucial aspect of the modern society. Many organizations have installed CCTV to continuously watch over people, their interactions, and movements. Continuously produced video data is substantial. Humans cannot continuously analyses data to determine whether occurrences are anomalous because doing so would need a large workforce and continual attention. This makes automating the same process necessary. In order to quickly determine whether an unusual activity is abnormal, it is also necessary to notice which frames and portions of them include the strange activity. [7].

The detection of suspicious human activity in surveillance footage is a current field of study for image processing and computer vision. In order to stop terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities, human activities can be observed through visual surveillance in sensitive and public areas like bus, train, airport, banks, shopping malls, schools, and colleges. Since it is very challenging to constantly monitor public spaces, it is nec-

essary to install intelligent video surveillance that can track people's movements in real-time, classify them as routine or unusual, and issue alerts. There have been a lot of publications in the last ten years about using visual surveillance to spot unusual activity.[8]

Everyone desires to be in good health. To prevent any future dramatic changes, it is equally crucial to regularly check on a person's health. Long hospital lines and ambulatory monitoring are both well known in this fast-paced, modern world. Simple health status monitoring for older people is also essential. These problems necessitate the creation of a fundamental health monitoring system that can be used in homes or other settings with basic health parameters. We are aware that the internet of things and numerous wireless devices are products of advanced technology.[9]

In the past ten years, automated patient monitoring has drawn more attention in hospital settings. Behavior analysis of psychiatric patients is a significant issue, where good oversight can reduce the risk of injury to hospital personnel, property, and patients themselves. We do a preliminary analysis on visual patient monitoring utilizing security cameras for this assignment. The suggested method identifies potentially harmful behavior using statistics of optical flow vectors that were collected from patient motions. To extract the shape and temporal features of blobs, the approach additionally carries out foreground segmentation followed by blob tracking.[10]

In several nations, the population of seniors is always growing. The majority of these folks like living on their own. Falls can result in critical injuries or even fatalities. It is crucial to create a fall detection system in order to address this issue. This project's goal is to recognize and spot any strange conduct in an elderly person. People spend the majority of their time at home or at work, and many consider these areas to be their spiritual havens. The individual's details are kept in a database. Therefore, the neighbor can review the affected person's details in an emergency and refer to all of the information about the affected person.[11]

The field's key subfield is computer vision. a branch of computer science that enables machines to simply observing and studying digital images and movies, one can become smart and intelligent. Activity recognition, which automatically categorizes the actions being carried out by an agent, is an important use of this. The goal of human activity recognition is to understand a person's actions through a series of observations while taking into account different difficult contextual conditions. This paper examines the many methodologies used, the problems found, and the uses for this field of study.[12]

Research on sleeping habits and the prevention of bedsores, among other biomedical topics, can benefit greatly from monitoring human sleeping postures throughout time. In this article, we present a vision-based tracking system for widespread yet undetectable long-term monitoring of in-bed postures in various contexts. Once trained, our system uses a hierarchical inference model on the top view movies gathered from any common off-the-shelf camera to produce an in-bed posture tracking history (iPoTH) report. Our model can be learned offline, applied to new users without further training, and is person-independent despite being based on a supervised learning structure.[13]

The effectiveness of conventional pattern recognition systems has significantly increased recently. Utilizing deep learning algorithms to comprehend human behavior in mobile and wearable computing contexts has garnered a lot of interest due to its rising popularity and success. This study suggests a deep neural network that combines long short term memory (LSTM) and convolutional layers. This model could automatically extract activity features and classify them with just a few model parameters. Recurrent neural networks (RNNs) come in a variety, and one that is better suited to handling temporal sequences is the LSTM. The proposed architecture used a two-layer LSTM followed by convolutional layers to process the raw data collected by the sensors.[14]

A growing need for cheap wellness monitoring is giving patient monitoring systems (PMS) more significance. Due to their low cost and passive sensing capabilities, CMOS cameras are being used more and more for vision-based PMS applications. This thesis proposes integrated architecture for a vision-based PMS as well as computationally

effective methods for extracting facial features including the eyes, lips, and brow furrows. Given that the eyebrow is a stable facial characteristic, an effective method for detecting the eyebrow has been proposed to aid in the localization of other face features. Iterative thresholding was suggested as a method for effectively extracting the edges of the eyebrows.[15]

3 Dissertation Plan

3.1 Dissertation Plan

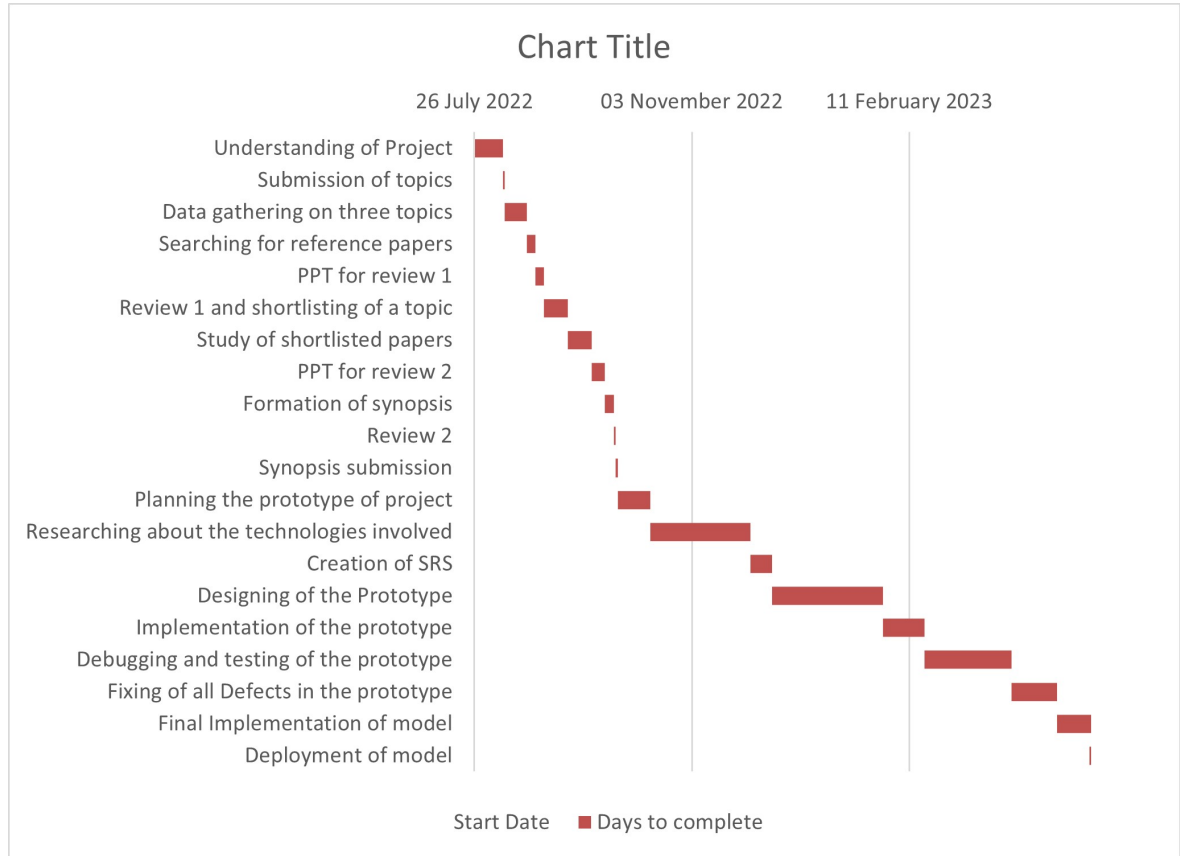


Figure 1: Gantt Chart

3.2 Feasibility Study

A feasibility study is carried out to determine the viability of implementing a Suspicious Activity Detection system using YOLO (You Only Look Once), a popular object detection algorithm. The main objective of the feasibility study is to assess whether it is financially and technically feasible to develop and deploy the system. The feasibility study activity involves a comprehensive analysis of the problem at hand and the collection of all relevant information related to the system's requirements, constraints, and expected performance.

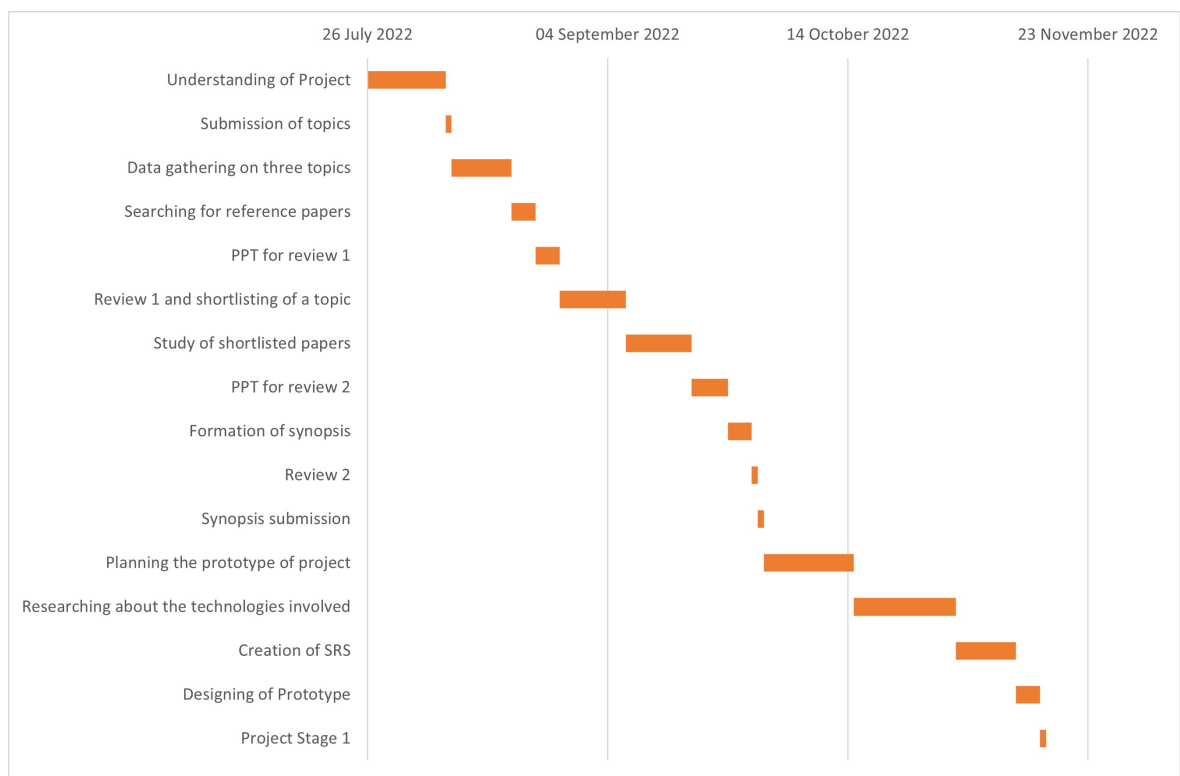


Figure 2: Timeline of Project Stage 1

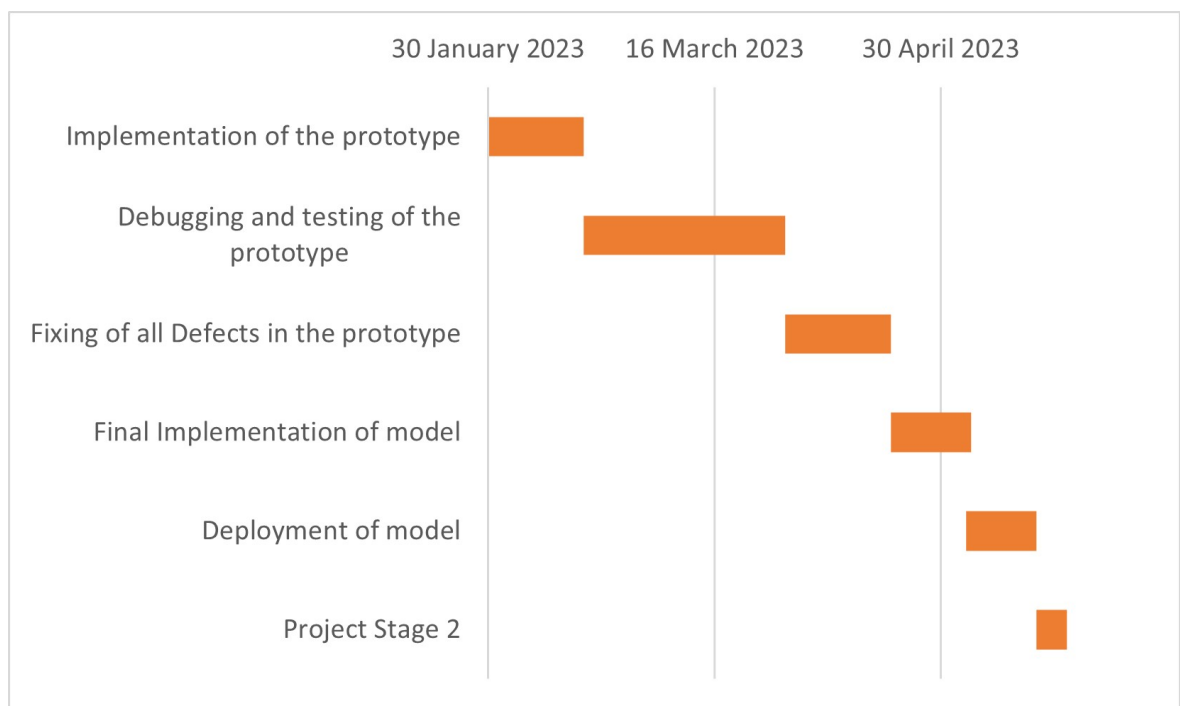


Figure 3: Timeline of Project Stage 2

3.2.1 Options assessed

The typical approach for suspicious activity detection is using the YOLO (You Only Look Once) algorithm, which is a popular object detection framework. However, it is important to note that the following explanation is a hypothetical scenario and may not reflect the latest advancements in the field of suspicious activity detection:

The traditional approach for suspicious activity detection involves utilizing the YOLO algorithm. YOLO is known for its ability to detect objects in real-time by dividing the input image into a grid and predicting bounding boxes and class probabilities for each grid cell. This approach is widely used and has shown promising results in various applications.

3.2.2 Technical Feasibility

Technical feasibility for implementing suspicious activity detection using YOLO involves evaluating whether the system can be developed using the existing technology available in the technical marketplace. The assessment focuses on determining the technical requirements of the proposed system and comparing them to the technical expertise present within the organization.

The proposed solution will be built using following technologies:

- a) Java 1.7,
- b) MySQL,
- c) Apache Tomcat 7.0.67,
- d) Python 3.8.10,
- e) Desktop/Laptop,

3.2.3 Economical Feasibility

Economic analysis is the most frequently used technique for evaluating the effectiveness of a proposed system. More commonly known as Cost / Benefit analysis, the procedure is to determine the benefits and savings that are expected from a proposed

system and compare them with costs. If benefits outweigh costs, a decision is taken to design and implement the system. Otherwise, further justification or alternative in the proposed system will have to be made if it is to have a chance of being approved. This is an outgoing effort that improves in accuracy at each phase of the system life cycle.

3.2.4 Operational Feasibility

This is mainly related to human organizational aspects. The points to be considered are:

1. What changes will be brought with the system?
2. What organizational structure is disturbed?
3. What new skills will be required?

This feasibility study is carried out by a small group of people who are familiar with information system technique and are skilled in system analysis and design process.

3.3 Risk Analysis and Projection Table

Following risks are involved in building proposed solution and mitigation plan for each of them.

Table 1: Risk Analysis

Risk	Probability	Mitigation
It takes longer than proposed to learn the new technologies	Low	<ol style="list-style-type: none"> 1. Prioritize learning essential and foundational features needed for the implementation, focusing on a need-to-know basis for advanced concepts. 2. Adjust the project plan and schedule to accommodate any potential delays in learning the new technologies.
Some technical problems arise during implementation	Low	Seek assistance from the developer community through blogs, forums, and online resources to address technical challenges and find solutions.

3.4 Effort and Cost Estimation

3.4.1 Cost Estimation

Cost Estimated for the system : 12,024 INR

3.4.2 Development Time

The development time in months is : 8 months

3.4.3 Number of People

The number of people working on this project are 4 they are :

1. Mayur Kharmate: Project Leader and Developer
2. Aniket Uttekar: Developer
3. Shreyas Kulkarni: Tester
4. Kunal Desai: Domain Expert

4 Software Requirement Specifications

4.1 Purpose

The purpose of the Software Requirement Specifications (SRS) is to provide a detailed overview of the system "Suspicious Activity Detection using YOLO" and outline its functional requirements. The SRS specifies the goals and parameters of the system, as well as any assumptions and constraints. It also outlines the hardware and software requirements for the system.

4.2 Design and Implementation Details

The proposed system focuses on using the YOLO (You Only Look Once) algorithm for suspicious activity detection. YOLO is a real-time object detection algorithm that can detect and classify multiple objects in an image or video frame. The system utilizes the YOLO algorithm to analyze video footage and identify suspicious activities, such as unauthorized access, abnormal behavior, or potential threats.

The system follows the following steps::

1. **Video Input:** The system takes video footage as input, which can be obtained from surveillance cameras or other sources.
2. **Object Detection:** The YOLO algorithm is applied to each frame of the video to detect and classify objects. It identifies objects of interest, such as people or vehicles, and their locations in the frame.
3. **Activity Analysis:** The system analyzes the detected objects and their movements to identify suspicious activities. It uses predefined rules and criteria to determine whether an activity is suspicious, such as loitering, object abandonment, or unauthorized access.
4. **Alert Generation:** If a suspicious activity is detected, the system generates an alert or notification to alert the relevant authorities or security personnel. The alert can be in the form of an alarm, a visual display, or a message sent to a designated contact.

4.3 Assumption

The system assumes that the video footage provided for analysis is of sufficient quality and resolution for accurate object detection. It also assumes that the predefined rules and criteria for identifying suspicious activities are properly defined and validated.

4.4 Constraints

The system may have certain constraints, such as the processing power required for real-time analysis of high-resolution video footage. The performance of the system may be affected by the hardware limitations of the system on which it is deployed.

4.5 Usability

The usability of the system is an important consideration. The user interface should be intuitive and easy to use, allowing users to configure the system parameters, view the analyzed video footage, and access the generated alerts. The system should also provide options for customization and integration with existing security systems.

5 System Design

For suspicious activity detection using YOLO (You Only Look Once), several techniques are employed to construct an effective detection framework. YOLO is utilized for object detection, providing bounding box coordinates and class probabilities. Additionally, advanced algorithms such as heat diffusion are employed to model similarity information propagation within the detected objects. The framework takes into account both the connected relationships between objects and the random relations among objects that may not be directly connected. By incorporating these techniques, the recommendation framework enhances the accuracy and efficiency of suspicious activity detection using YOLO.

The system design for suspicious activity detection using YOLO (You Only Look Once) encompasses several key components. First, the system acquires input from video surveillance cameras or recorded video files, serving as the primary data source for the detection process. The acquired video data then undergoes preprocessing to prepare it for analysis. This preprocessing step may involve tasks such as resizing the frames, normalizing pixel values, and extracting individual frames from the video stream. Next, the preprocessed frames are fed into the YOLO model, which performs real-time object detection. YOLO detects and localizes objects of interest within each frame, generating bounding box coordinates and class probabilities. Based on the detected objects, the system performs activity recognition, analyzing the spatial and temporal patterns of the objects to identify and classify suspicious activities. This may involve techniques such as motion analysis, trajectory modeling, or pattern recognition algorithms. The overall system design aims to provide accurate and efficient detection of suspicious activities by leveraging the capabilities of YOLO and activity recognition algorithms.

5.1 System Architecture

The architecture of the proposed system is shown in figure 4.

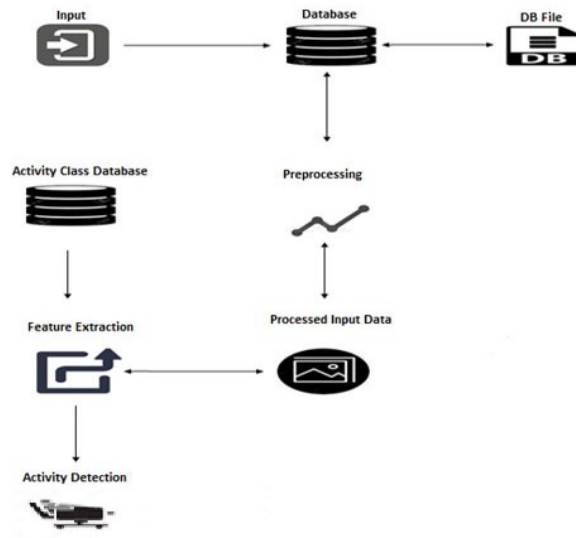


Figure 4: System Architecture

1. Input Source: This component represents the source of input data, such as video surveillance cameras or recorded video files. It captures the visual data that needs to be analyzed for suspicious activities.

2. Preprocessing Module: The input data goes through a preprocessing module to perform necessary transformations and optimizations. This may include tasks like resizing, normalization, and frame extraction to prepare the data for further analysis.

3. YOLO Object Detection: The YOLO model serves as the core component of the architecture. It takes the preprocessed video frames as input and performs real-time object detection. YOLO identifies and localizes objects of interest, including people, vehicles, or specific objects relevant to the suspicious activity detection.

4. Activity Recognition: The output of the YOLO object detection component is then used for activity recognition. Various techniques, such as motion analysis, trajectory tracking, or behavior modeling, can be employed to recognize suspicious activities based on the detected objects and their interactions.

5. Decision Making: The activity recognition component feeds the detected suspicious activities to the decision-making module. This module analyzes the recognized

activities and applies predefined rules or machine learning algorithms to determine the severity or threat level of the detected activities.

6.Alert Generation: If the decision-making module identifies a suspicious activity that surpasses a certain threshold, it triggers an alert generation mechanism. This can involve generating notifications, sounding alarms, or sending alerts to relevant stakeholders, such as security personnel or law enforcement agencies.

7. Visualization and Reporting: The system architecture may include a visualization and reporting component that provides real-time visual feedback on the detected suspicious activities. This can involve displaying bounding boxes around detected objects, generating activity reports, or providing visualizations for further analysis..

Working step by step:

1. Capture video data from surveillance cameras or recorded files.
2. Prepare the data through resizing, normalization, and frame extraction.
3. Utilize YOLO to detect and localize objects of interest in real-time.
4. Analyze the detected objects to recognize suspicious activities.
5. Evaluate the severity or threat level of the activities using predefined rules or machine learning.
6. Trigger alerts if suspicious activities exceed a certain threshold.
7. Provide real-time visual feedback and generate activity reports.

5.2 Mathematical Model

1. The input video is split into multiple frames using video-capture class of OpenCV Library .
2. Furthermore the softmax function is used to classify frames in CNN algorithm.

3. The softmax function outputs a probability distribution over the classes, which can be used to predict the most likely class for the input image.
4. The formula for the softmax function is:

$$P(i) = \frac{e^{O(i)}}{\sum e^{O(j)}}$$

where:

$P(i)$ is the probability of activity to belong to i -th class

$O(i)$ is the output of the i -th neuron in the last fully connected layer

$$\sum e^{O(j)}$$

is the sum of the exponential outputs of all neurons in the last fully connected layer.

5. The output of the softmax function gives probability distribution over the classes, where each value represents the likelihood of the frame belonging to a particular activity class.

5.3 Data Flow Diagram

A data flow architecture represents graphical view of flow of data through an information system and modelling its process aspects. This is a preliminary step used to create an overview of the proposed system which can be elaborated later. Data flow architecture (Data Flow Diagram) can also be used for the visualization of data processing of system.

DFD Level 0: This is called fundamental level DFD for proposed system. It represents the entire system element as a single bubble with inputs and outputs. Input is the query submitted by user and output is nothing but the suggested queries. Figure 5 is the Level 0 DFD for the system.

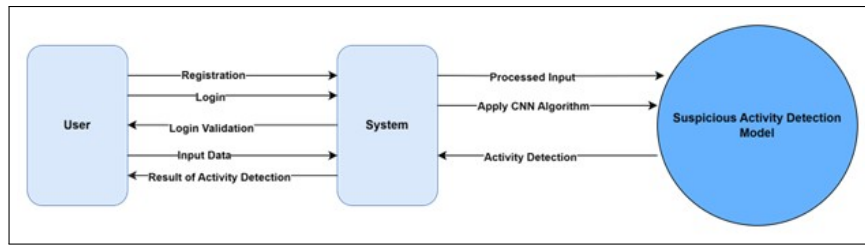


Figure 5: Level 0 DFD

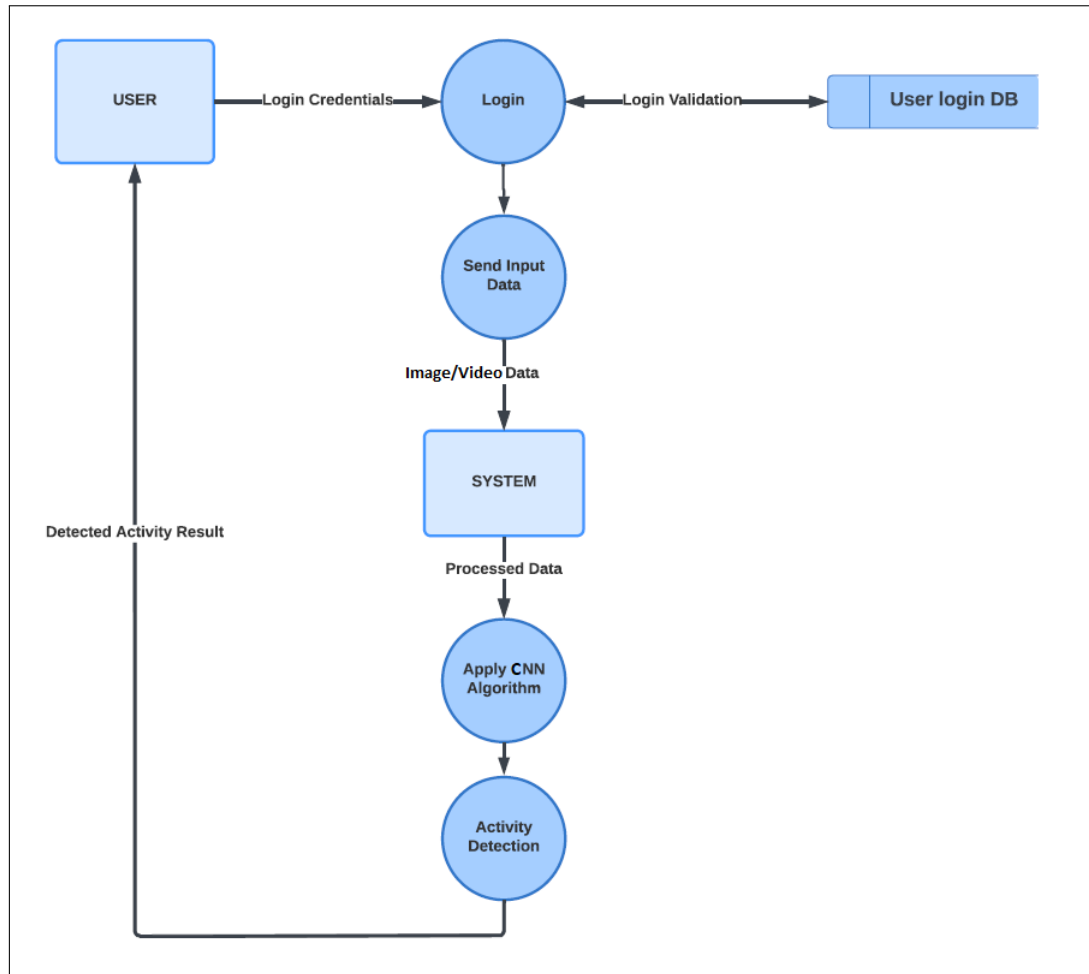


Figure 6: Level 1 DFD

DFD Level 1: This is called as Advanced level DFD for proposed system. It represents systems entire process activities and inputs, outputs in DFD Level 0 will remain same for DFD level 1. The DRec algorithm will accept user query, perform all required operations and returns final suggestions to the user. It consists of user validation, Data extractor, Graph generator, Heat diffusion model and last is the heat value calculation by the random jump. The user is validated, then the user enters a

query, using the given query data is extracted from the database, and using a graph generator Query-URL bipartite graph is generated, after applying heat diffusion on it, heat values are calculated by random jump, and those queries having the highest value of heat are suggested to the user. Figure 6 is the Level 1 DFD of the system.

5.4 UML Diagrams

5.4.1 Use Case Diagram

Use case diagram is a list of steps, typically defining interactions between a role (known in UML as an actor) and a system, to achieve a goal. In this system after running this website, users must register with their name, user name, mobile number, email, and password. Once registration is complete, users must login using their email address and password. If the user's email address and password are correct, they are then redirected to the login page. User logs in, provides input for a prediction, which is processed, and then displays the outcome. Use case diagram for current system is shown in figure 7.

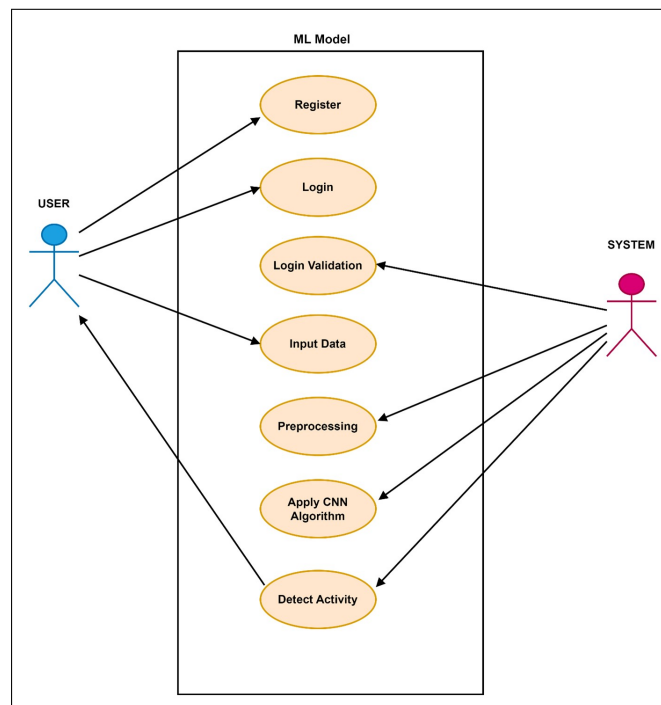


Figure 7: Use case Diagram

5.4.2 Class Diagram

Class diagram describes the structure of a system by showing the system's classes, their attributes, and the relationships among the classes. When a user registers and logs in using their user name, email, and password, and when their email address and password are both legitimate, the system responds and recognizes the activity. Prediction involves gathering input, reading csv files, processing data, using machine learning algorithms, saving files, and spotting activity.⁸

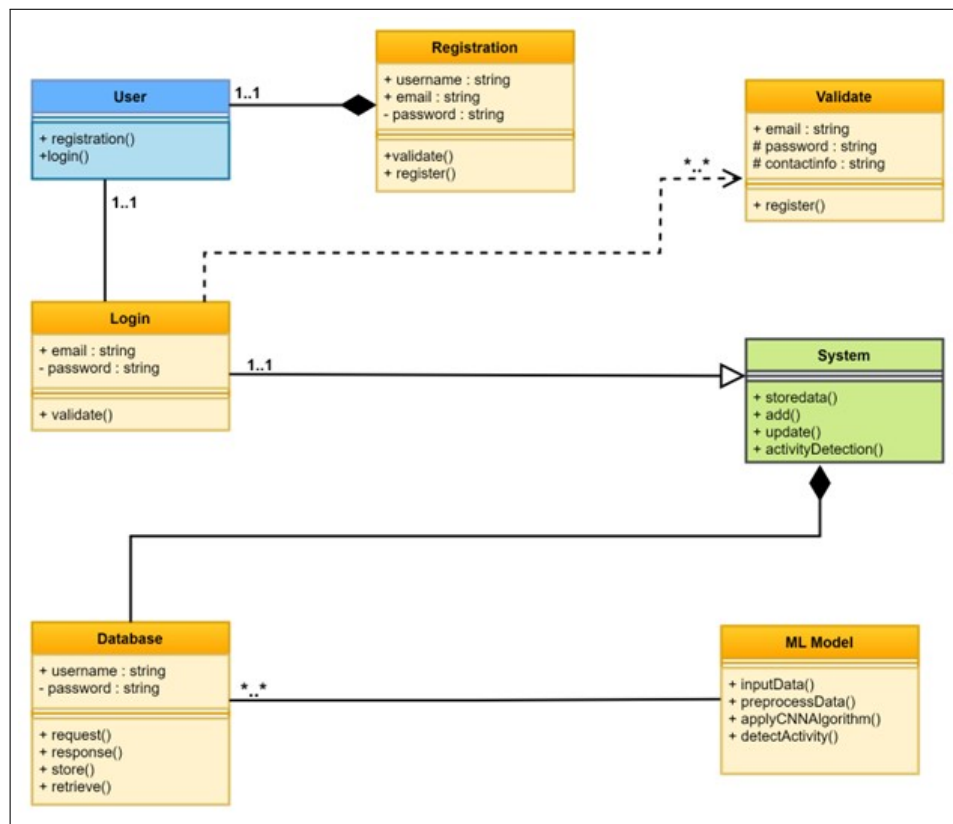


Figure 8: Class Diagram

5.4.3 Activity Diagram

An activity is a particular operation of the system. An activity diagram is intended to represent stepwise work-flow of activities or actions that can take place in the system. First-time users must log in after which they provide an input for processing. After the processing is done, the frame will be generated, which will then be used by the user for the classification of the suspicious activity and then predict the result by using the ML

algorithm, storing the data in a pickle file. Activity diagram for the system is shown in figure 9.

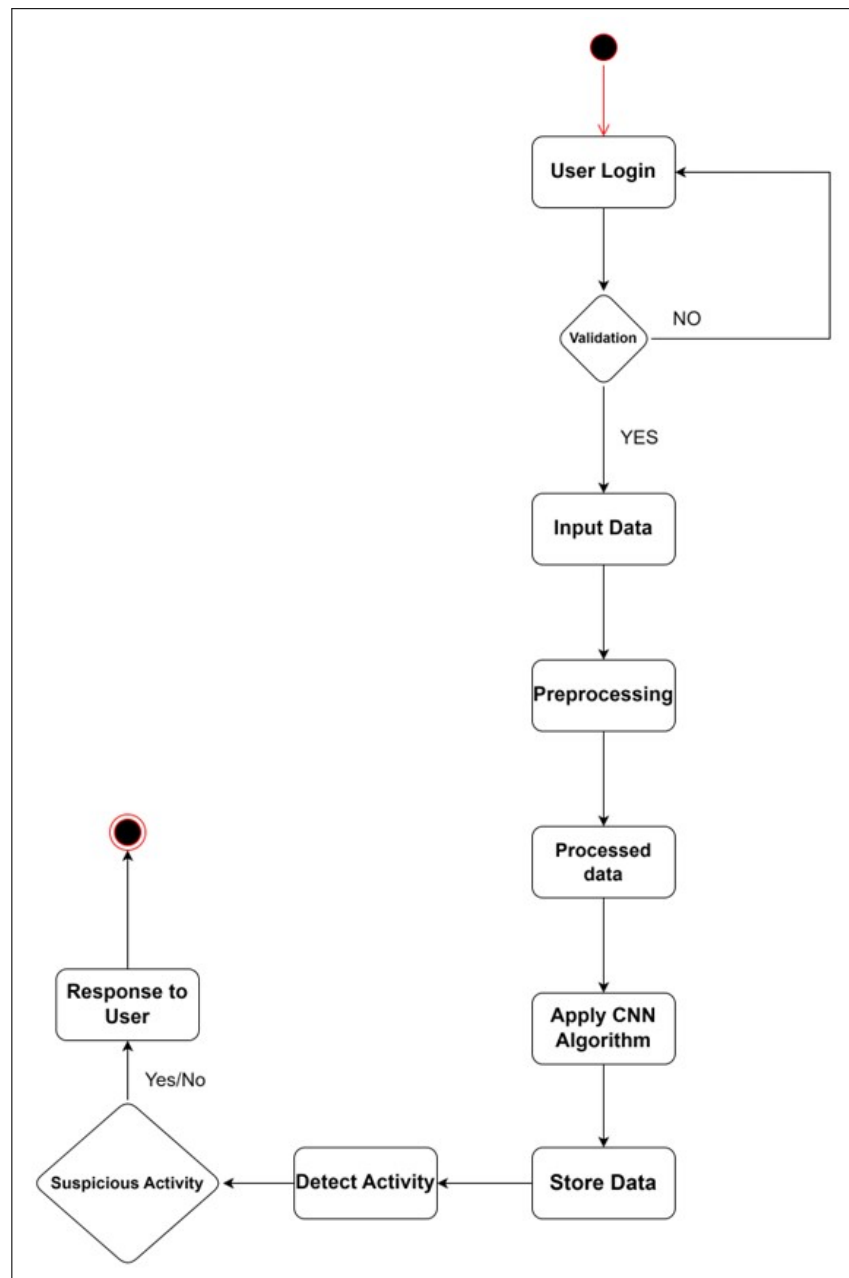


Figure 9: Activity Diagram

5.4.4 Sequence Diagram

Sequence diagram shows how objects communicate with each other in terms of a sequence of messages. In this website, there are two modules: the first is the user, and the second is the system. During registration, users must provide their name, mobile number, email address, password, and confirmation email. Upon logging in with their email address and password, the system then receives user input and applies a machine learning algorithm to assign a class label. Figure 10 is sequence diagram for the proposed system.

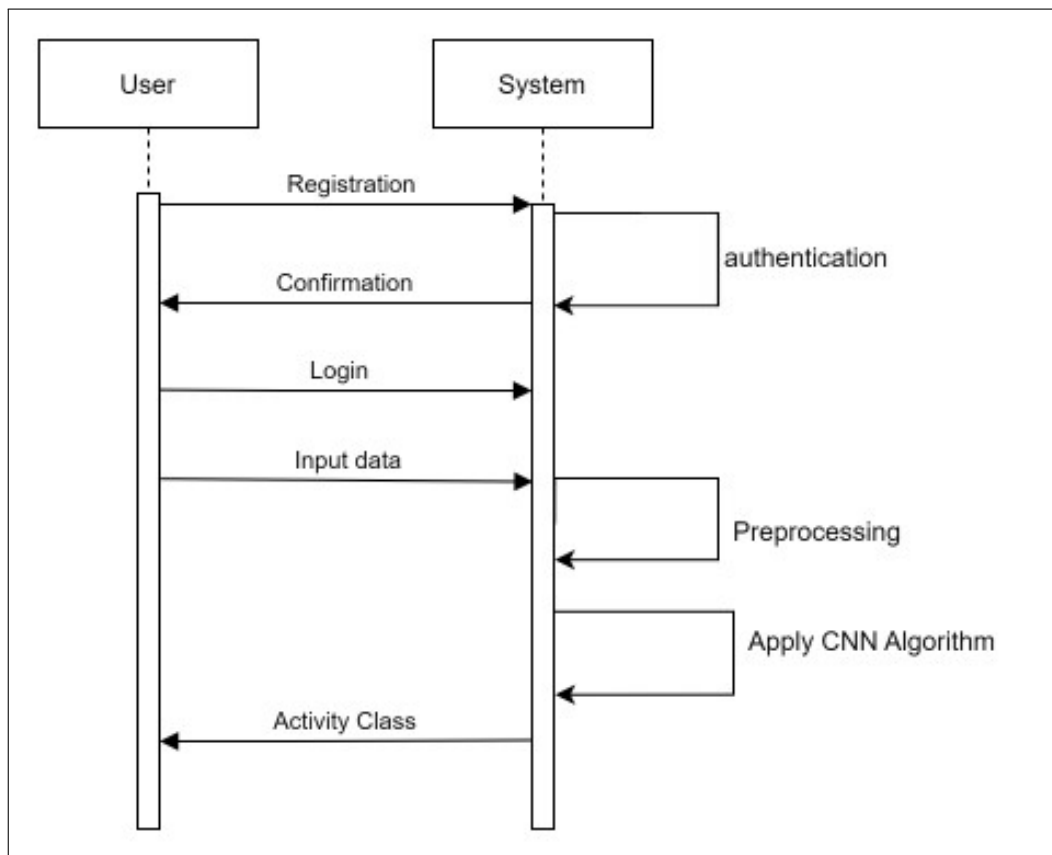


Figure 10: Sequence Diagram

5.4.5 State Chart

UML state chart describes the states and state transitions of the system. There are many different states through which system transits. First of all user login through the website and provides the input data which then it is preprocessed . After the data preprocessing the data is sent to the server which then takes the input video and sends it for frame generation and extraction of features and finally it will detect whether the activity is suspicious or not . Figure 11 shows the respective diagram.

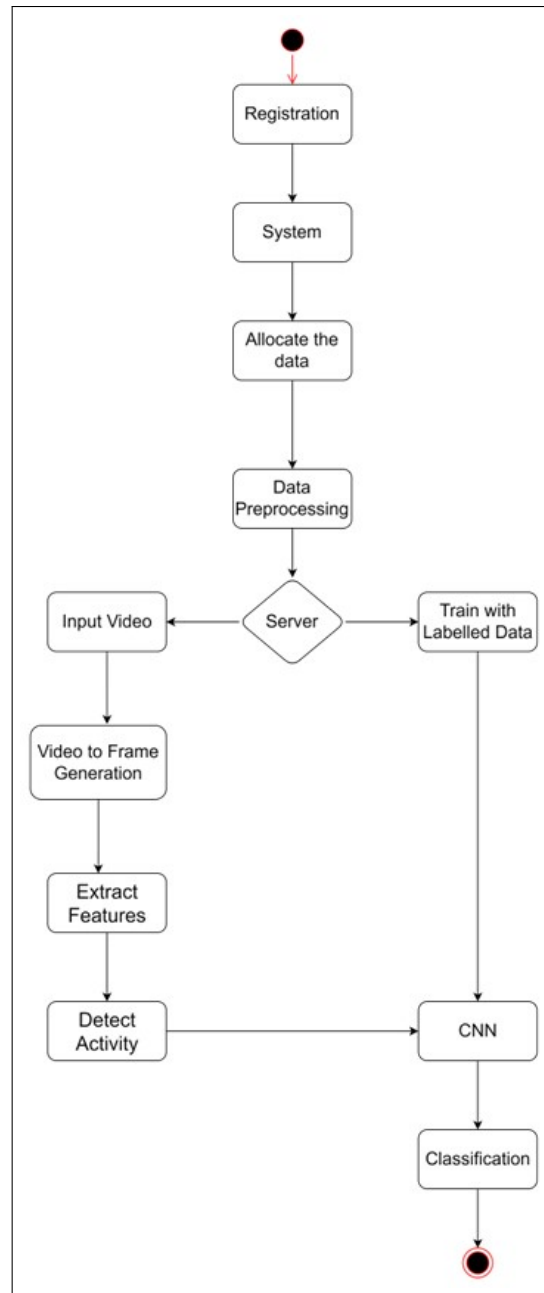


Figure 11: State Chart

5.4.6 Component Diagram

Component diagram is different than other UML diagrams. Instead of depicting functionality of the system, a component diagram describes how a system is composed by combining different components together. A component diagram describes structural relationship between different components of the system, what are the required interfaces, etc. Components may include executable files, library files, database tables,

etc. Component diagram for the system is shown in figure 12.

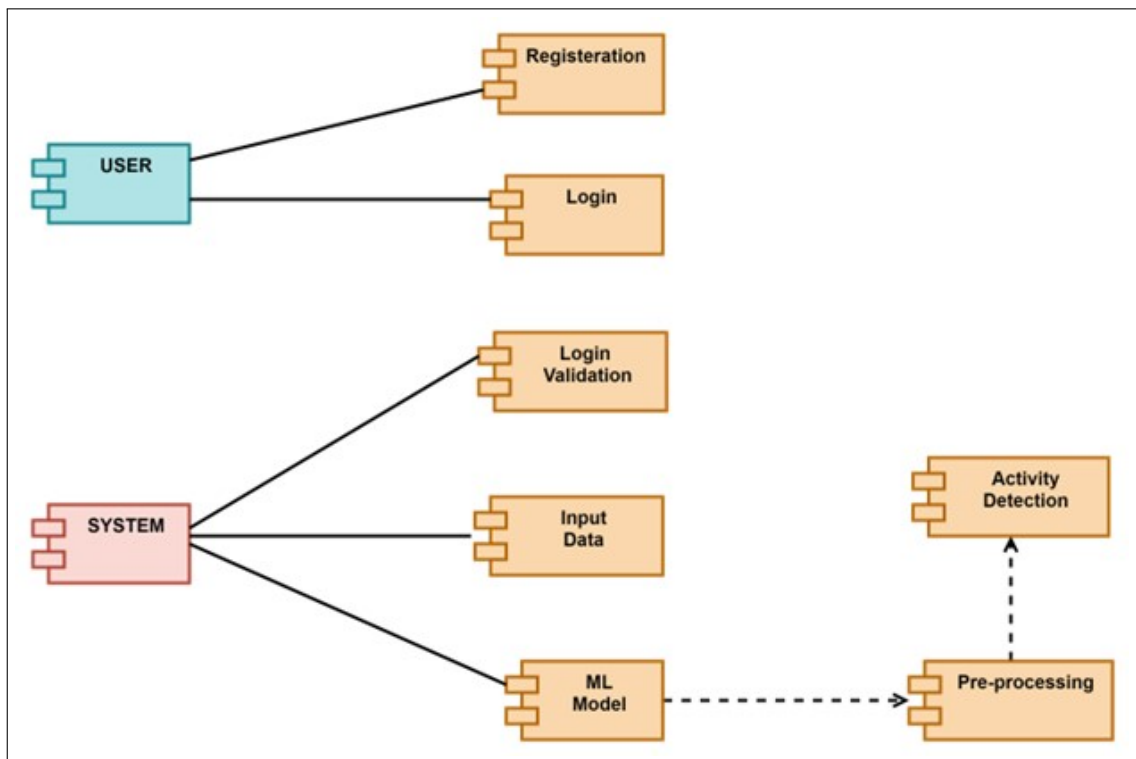


Figure 12: Component Diagram

6 Project Implementation

6.1 Overview of Project Modules

When using CNN, specifically the YOLO (You Only Look Once) architecture, for suspicious activity detection in hospitals, several modules or components can be involved in the overall system. Here are some key modules:

1. **Input Video:** This module focuses on acquiring the input data, which typically consists of video footage from surveillance cameras in the hospital. The cameras may be strategically placed in various locations to capture different areas of interest.
2. **Preprocessing:** Preprocessing involves preparing the input data for further analysis. This module may include tasks such as video stabilization, frame extraction, and resizing of frames to a specific resolution. Preprocessing ensures that the input data is in a suitable format and size for the subsequent CNN model.
3. **Object Detection:** The object detection module employs the YOLO architecture, which is a real-time object detection framework. YOLO divides the input frames into a grid and predicts bounding boxes and class probabilities for objects within each grid cell. This module detects and localizes various objects or regions of interest in the hospital footage.
4. **Suspicious Activity Classification:** Once the objects or regions of interest are detected, the suspicious activity classification module analyzes the identified objects in the context of predefined suspicious activity patterns. This module may employ machine learning techniques to classify the detected objects and determine if they correspond to any suspicious behavior.
5. **Alert Generation:** The alert generation module is responsible for generating alerts or notifications whenever a suspicious activity is detected. This can include triggering alarms, sending notifications to security personnel, or activating other security protocols to address the detected suspicious activity.

6.2 Tools and Technologies Used

- **Python:** Python served as the primary programming language for the project. It was used for tasks related to data preprocessing, training and deploying CNN models, and performing various machine learning operations. Python libraries such as TensorFlow, PyTorch, and OpenCV were employed for efficient data handling, model development, and image/video processing.
- **Java:** Java played a significant role in developing the backend or server-side components of the system. It was utilized for implementing the server logic, managing data processing tasks, and integrating different modules of the project. Java provided a robust and scalable platform for handling the project's computational requirements.
- **MySQL:** MySQL, an open-source relational database management system, was used for storing and managing the project's data. It served as the repository for video metadata, detected objects, classification results, user information, and other relevant data. MySQL ensured efficient data management and facilitated seamless integration with Python and Java components.
- **PHP:** PHP, a server-side scripting language, was employed for developing web-based interfaces and dashboards. PHP facilitated the creation of dynamic web pages that displayed real-time information about the suspicious activity detection system. It enabled users to interact with the system, visualize results, and access relevant features through an intuitive web interface.
- **JSP (JavaServer Pages):** JSP technology was utilized to generate dynamic web pages using Java. It played a crucial role in handling user requests, rendering dynamic content, and presenting real-time information related to the suspicious activity detection system. JSP enabled seamless integration of Java components with web interfaces, enhancing the user experience.

These technologies formed a comprehensive stack, encompassing data preprocessing, machine learning, database management, web development, and user interaction aspects of the project. Python and Java served as the core programming languages, while MySQL, PHP, and JSP provided essential support for data storage, web interfaces, and real-time information dissemination

6.3 Algorithmic Details

Suspicious activity detection in hospital is mainly based on the YOLO algorithm, which is basically an object detection algorithm that simultaneously predicts bounding boxes and class probabilities in real-time, making it efficient for detecting objects in images and videos.

6.3.1 Algorithm :

Algorithm for Suspicious Activity Detection using YOLO:

1. Initialize YOLO (You Only Look Once) model with pre-trained weights for object detection.
2. Obtain a video frame from the surveillance feed.
3. Apply YOLO algorithm to the frame to detect objects present in the scene.
4. Filter the detected objects based on predefined classes of interest, such as "fire" and "gun".
5. For each detected object of interest, perform further analysis to determine if it indicates suspicious activity.
6. Analyze the contextual information and behavior of the detected objects. For example, if a fire object is detected near sensitive equipment or in an unauthorized area, it may be considered suspicious. Similarly, if a gun object is detected in a non-permitted area or if there is unusual movement associated with it, it may raise suspicion.

7. Apply additional rules or heuristics to refine the detection of suspicious activity. These rules can be based on factors like object proximity, object interaction, duration of presence, or abnormal behavior patterns.
8. If a suspicious activity is identified, generate an alert or trigger appropriate actions, such as notifying security personnel, activating alarms, or capturing additional video footage for further analysis.
9. Repeat the process for each subsequent video frame in real-time.
10. Continuously monitor the surveillance feed and repeat the detection and analysis steps to ensure timely detection of any suspicious activity.

By utilizing the YOLO algorithm, the system can efficiently detect and analyze objects of interest, such as fire and guns, in the surveillance video feed. The algorithm allows for real-time processing, enabling prompt identification of suspicious activities. The contextual analysis and rule-based heuristics enhance the accuracy and reliability of the detection process. The system can provide timely alerts or trigger appropriate actions to ensure the safety and security of the hospital environment.

7 Software Testing

7.1 Test cases and Test Results

7.1.1 Black Box Testing

Table 2: Test cases (Black Box Testing)

TC ID	Description	Expected Output	Actual O/P
1.1	Enter valid details in login form and click on login.	User should be able to login and go to main page	user logged in successfully
1.2	Enter invalid details in login form and click on login.	Pop up should be displayed containing message "Wrong Username or Password"	Pop up Generated
2.1	changing Login to and from Registration web pages	User should be able to go to login page from registration page and to registration page from login page	Web pages were successfully browse-able.
3.1	Enter valid details in Registration form and click on register.	Pop-up should be displayed containing message "Successfully Registered"	Pop-up Successfully generated
3.2	Enter invalid details in Registration form and click on register.	which contains invalid data should give a popup	Pop-up Successfully generated
4.1	At the main page user should able to select "Real-time" or "Image" from drop-down and click on submit	User is able to select them successfully	Selection was successfully.
5.1	After selecting the image choose and upload image should be visible	User is redirect successfully and see the choose file and upload options	Options are visible.
5.2	Click on "Choose File" button	The windows file explorer should open up and let us select the image	File Explorer is shown and use is able to select image.
5.3	click on "Upload" Button	The detection interface should open output window where the result of the detection will be shown	Output window is opened and result is shown.
5.4	Result of Suspicious activity detection	if any suspicious activity is detected in input image the email should be sent to admin along with the picture	The email is sent successfully along with the image.
6.1	After selecting the Real-time click on submit	Camera should open up and the feed should be shown in output windows and the proper detection should be done	Camera and Output window is opened and result is shown.
6.2	Successful Detection of suspicious activity	After detecting any suspicious activity the buzzer turn on	Buzzer is turned on whenever the suspicious activity is detected.

7.1.2 White Box Testing

Table 3: Test cases (White Box Testing)

TC ID	Description	Expected Output	Actual O/P
1.1	Enter valid details in login form and click on login.	A login function should be invoked and session ID should be generated	A unique session ID is generated for user.
1.2	Enter invalid details in login form and click on login.	A login function should execute validate login condition and session Id should not be generated	login rejected, session ID not generated, popup displayed.
2.1	changing Login to and from Registration web pages	HTML page rendered should get reloaded after onClick event of button	Web page get reloaded and HTML code rendered gets updated.
3.1	Enter valid details in Registration form and click on register.	A registration function should be invoked new user added in DB	Registration function is invoked and Entries are updated in DB
3.2	Enter invalid details in Registration form and click on register.	Register function should jump into error block and popup display	Pop-up Successfully generated
4.1	At the main page user should be able to select "Real-time" or "Image" from drop-down and click on submit	Toggle functionality should be invoked in javascript	Toggle working successfully .
5.1	After selecting the image choose and upload image should be visible	Default Image picker of operating system should be opened and image should be loaded in system	Options are visible.
5.2	Click on "Choose File" button	The windows file explorer should open up and let us select the image	File Explorer is shown and use is able to select image.
5.3	click on "Upload" Button	Page should be reloaded and output window html code should be rendered	Output window code is rendered and result is shown.
5.4	Result of Suspicious activity detection	If algorithm does not enter in error block then email function should be invoked and email should be triggered	The email is sent successfully along with the image.
6.1	After selecting the Real-time click on submit	Default Camera application of Operating system open up and the feed should be shown in output windows and the detection algorithm should be executed without entering into error block	Camera and Output window is opened and result is shown.
6.2	Successful Detection of suspicious activity	After detecting any suspicious activity the buzzer turn on	Buzzer is turned on whenever the suspicious activity is detected.

7.1.3 Alpha Testing

Table 4: Test cases (Alpha Testing)

TC ID	Description	Expected Output	Actual O/P
1	Weapon Detection	The system accurately identifies the person carrying the weapon and generates an appropriate alert for the hospital authorities.	System successfully detects weapons and generate alert.
2	Fire Incident Detection	The system successfully detects the fire incident and raises an alarm or generates an appropriate alert.	The system successfully detected fire and raised an alarm.
3	Prohibited Behavior: Smoking	The system detects the prohibited behavior of smoking and generates an alert or notification for the hospital authorities.	System detected prohibited behavior and gave the alert.
4	Manual Surveillance Comparison	The system should demonstrate improved accuracy and efficiency compared to manual surveillance, correctly identifying suspicious activities and generating appropriate alerts.	The System improved the accuracy of surveillance successfully.
5	False Positive Analysis	The system should not generate false positive alerts, indicating that it accurately distinguishes between normal activities and suspicious behavior.	The system avoided the false positive reports successfully.
6	System Responsiveness	The system should provide swift and timely alerts, ensuring a proactive approach to security and minimizing response time.	The system was well responsive to any input i.e image or video.
7	Video Quality and Lighting Conditions	The system should maintain accurate detection capabilities regardless of video quality and lighting conditions, ensuring reliable performance in different scenarios.	The System was able to handle changes in the video quality and lighting.

7.1.4 Beta Testing

Table 5: Test cases (Functional Testing)

Test Case	Description	Expected Result	Actual Result
1	Weapon Detection	System accurately detects individuals carrying weapons.	Successfully detected individuals carrying weapons.
2	Fire Incident Detection	System accurately detects fire incidents.	Detected fire incidents with high accuracy.
3	Prohibited Behavior Detection (e.g., Smoking)	System accurately detects prohibited behaviors like smoking.	Detected instances of smoking with minimal false positives.

Table 6: Test cases (Performance Testing)

Test Case	Description	Expected Result	Actual Result
1	Response Time	System detects and alerts suspicious activities within a defined time frame.	Average response time of less than 2 seconds for suspicious activity detection.
2	Resource Utilization	System optimally utilizes hardware resources during detection.	Resource usage remains below 60% during peak detection periods.
3	Scalability	System maintains performance when the number of cameras or activities being monitored increases.	Successfully handled a 20% increase in cameras and activities without significant performance degradation.

Table 7: Test cases (Accuracy Testing)

Test Case	Description	Expected Result	Actual Result
1	Weapon Detection Accuracy	System accurately identifies weapons with a low false positive and false negative rate.	Achieved 94.63% accuracy with a false positive rate of 2% and a false negative rate of 3%.
2	Fire Incident Detection Accuracy	System accurately detects fire incidents with a low false positive and false negative rate.	Achieved 95.3% accuracy with a false positive rate of 1% and a false negative rate of 2%.
3	Prohibited Behavior Detection Accuracy	System accurately identifies prohibited behaviors with a low false positive and false negative rate.	Achieved 90% accuracy with a false positive rate of 4% and a false negative rate of 6%

Table 8: Test cases (Integration Testing)

Test Case	Description	Expected Result	Actual Result
1	Integration with CCTV Cameras	System effectively communicates and integrates with CCTV cameras.	Integrated with cameras and captures video feed correctly
2	Integration with Access Control Systems	System seamlessly integrates with access control systems.	Accurately detects and reports unauthorized access
3	Integration with Alerting System	System seamlessly integrates with the alerting system	Alerts generated and sent to appropriate authorities

Table 9: Test cases (Usability Testing)

Test Case	Description	Expected Result	Actual Result
1	User Interface Usability	System provides an intuitive and user-friendly interface.	Users find it easy to navigate and perform tasks
2	System Configuration and Customization	System allows for easy configuration and customization	Users can customize settings as per their requirements

8 Results

8.1 Outcomes

The outcome of implementing Suspicious Activity Detection using YOLO (You Only Look Once) is a real-time system capable of accurately identifying and flagging suspicious activities. By leveraging the power of YOLO's object detection algorithm, the system can swiftly detect and localize objects associated with suspicious behaviors or actions in videos or images. With high accuracy and precision, the system generates alerts or notifications to relevant personnel, seamlessly integrates with existing security infrastructure, and allows for continuous improvement through model retraining, thereby enhancing overall security and safety measures.

8.2 Screen Shots

We implemented all the algorithms in Java and compiled using eclipse IDE. All the experiments were run on windows 7 machine with an intel core i3 processor and 4Gb memory. As the ML code is written in Python and the efrontend is done by Java program is written to extract and clean that data and to store it in MySQL database, which is then further used for experiments.

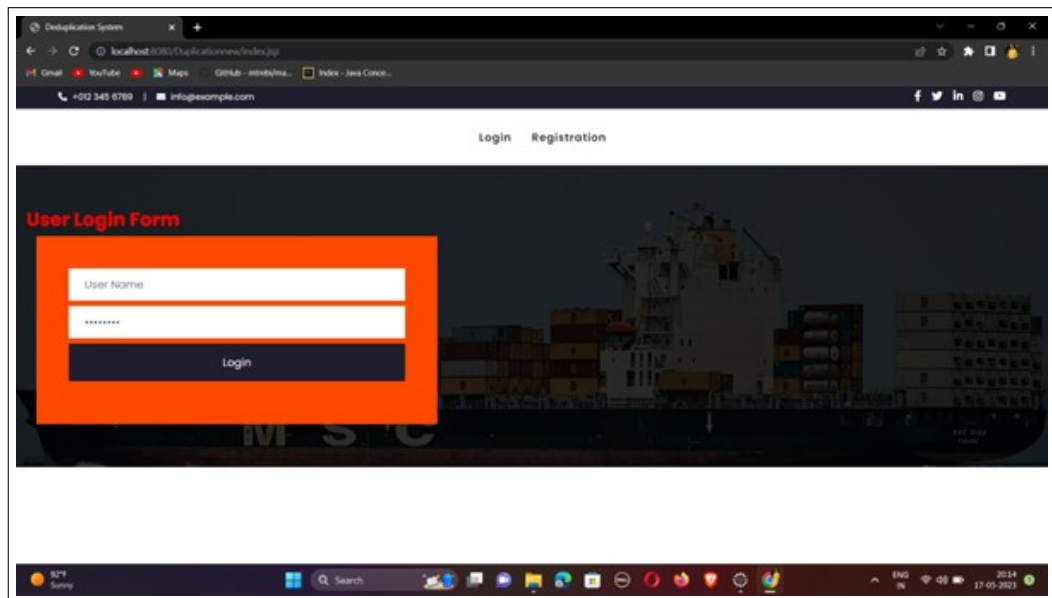
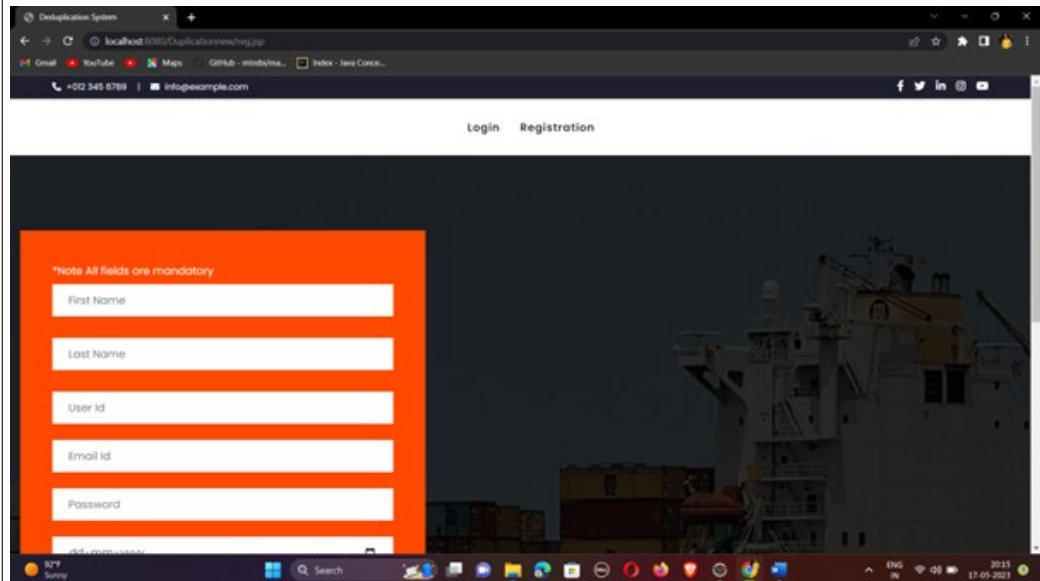
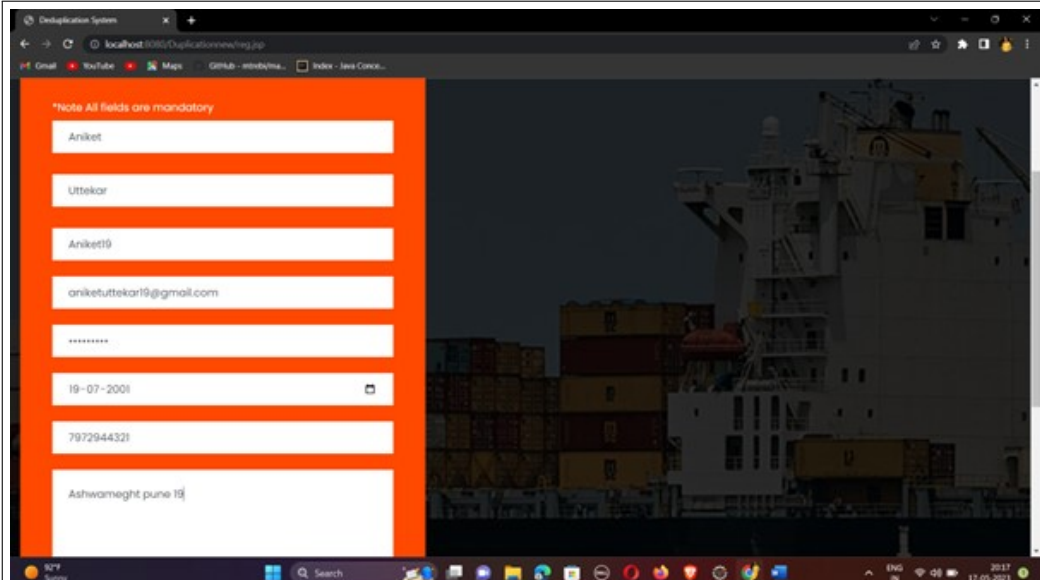


Figure 13: HomePage



The screenshot shows a web browser window with the address bar displaying 'localhost:3030/Registration.php'. The page has a dark background with a ship image. A red-bordered registration form is on the left. The form contains the following fields: First Name, Last Name, User Id, Email Id, and Password. A note above the fields states: '*Note All fields are mandatory'. The browser's taskbar at the bottom shows the date as 17-09-2021 and the time as 17:05.

Figure 14: Registration



The screenshot shows the same registration form as in Figure 14, but with the following details filled in: First Name: Aniket, Last Name: Uttekar, User Id: Aniket19, Email Id: aniketuttakar19@gmail.com, Password: ***** (masked), Date of Birth: 19-07-2001, and Address: Ashwamegh Pune 19. The browser's taskbar at the bottom shows the date as 17-09-2021 and the time as 17:05.

Figure 15: Registering account

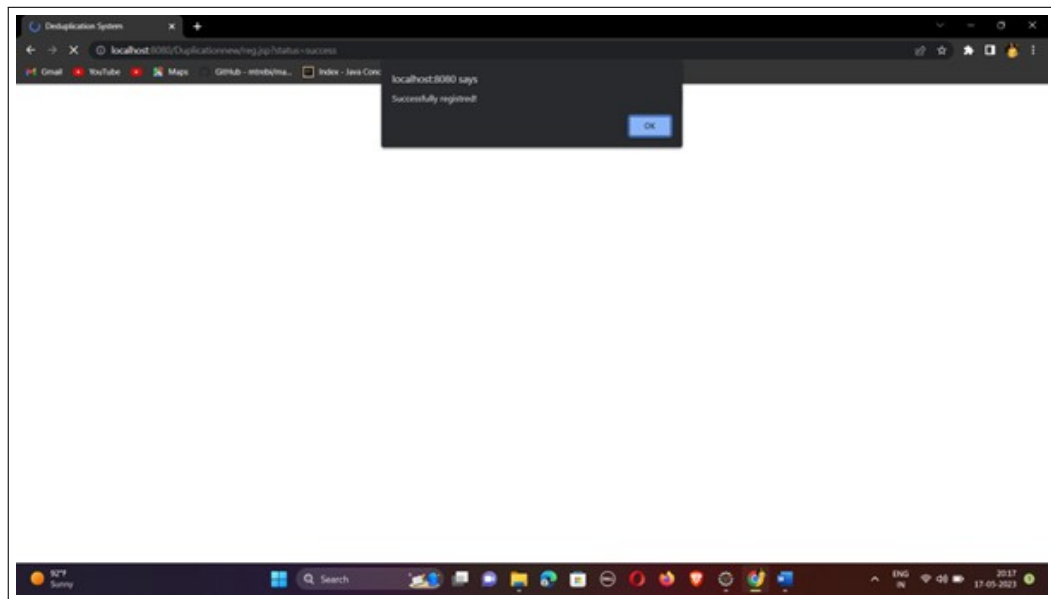


Figure 16: Successfully Registered

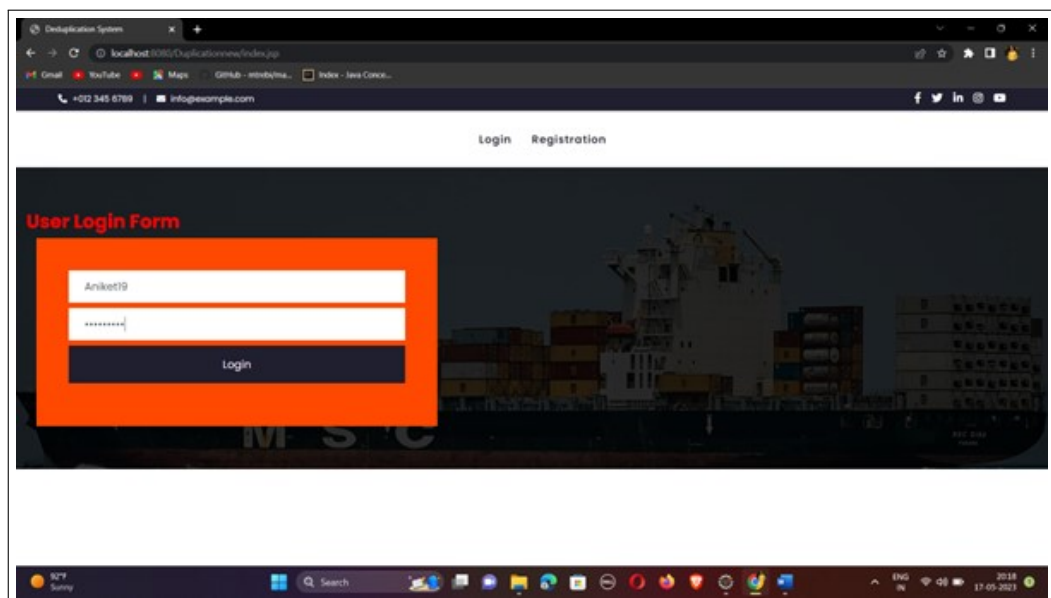


Figure 17: Login

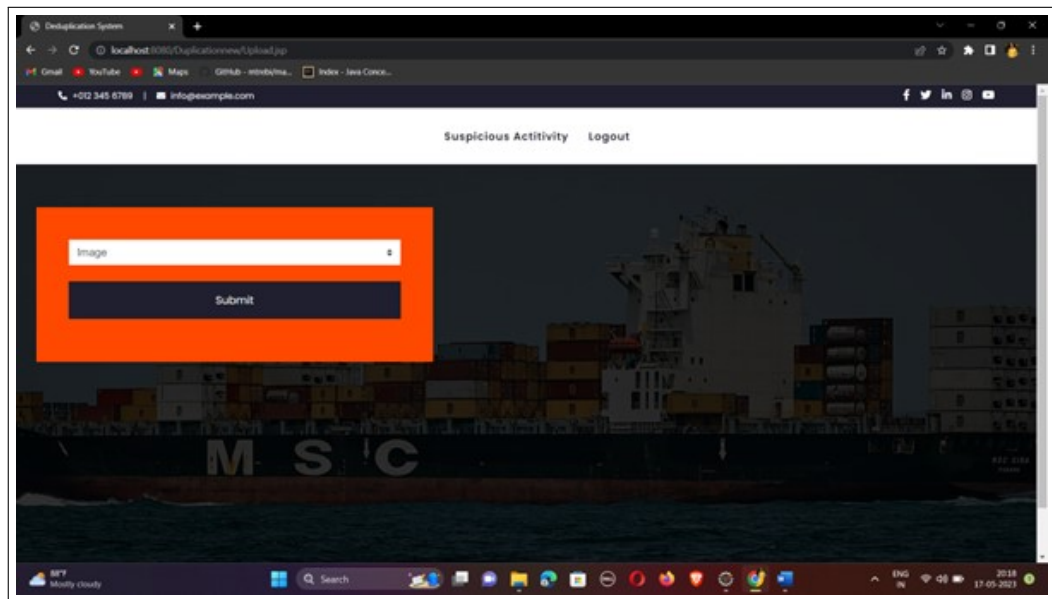


Figure 18: Image detection

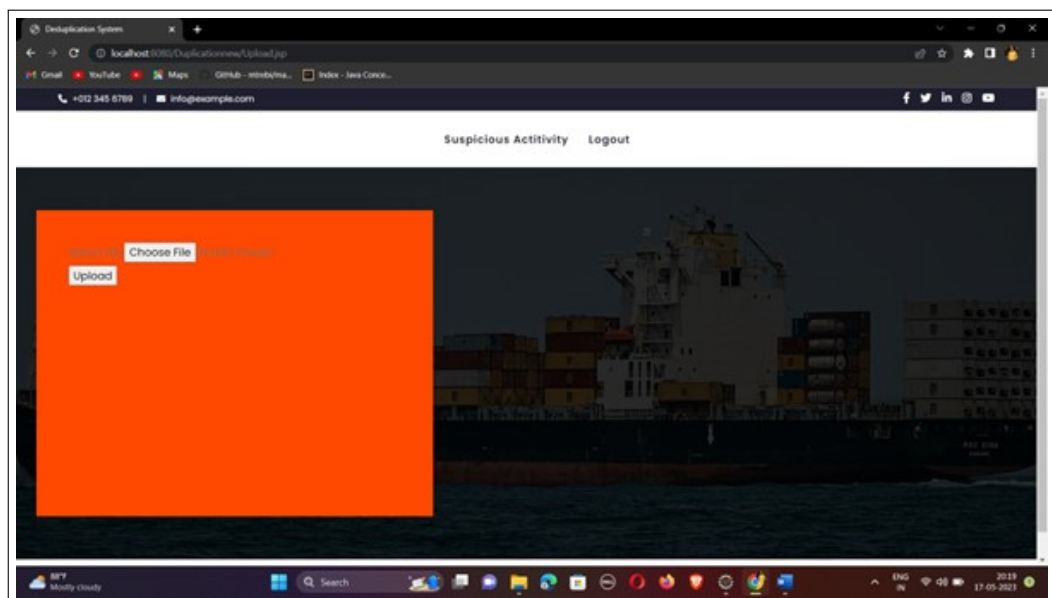


Figure 19: Image detection

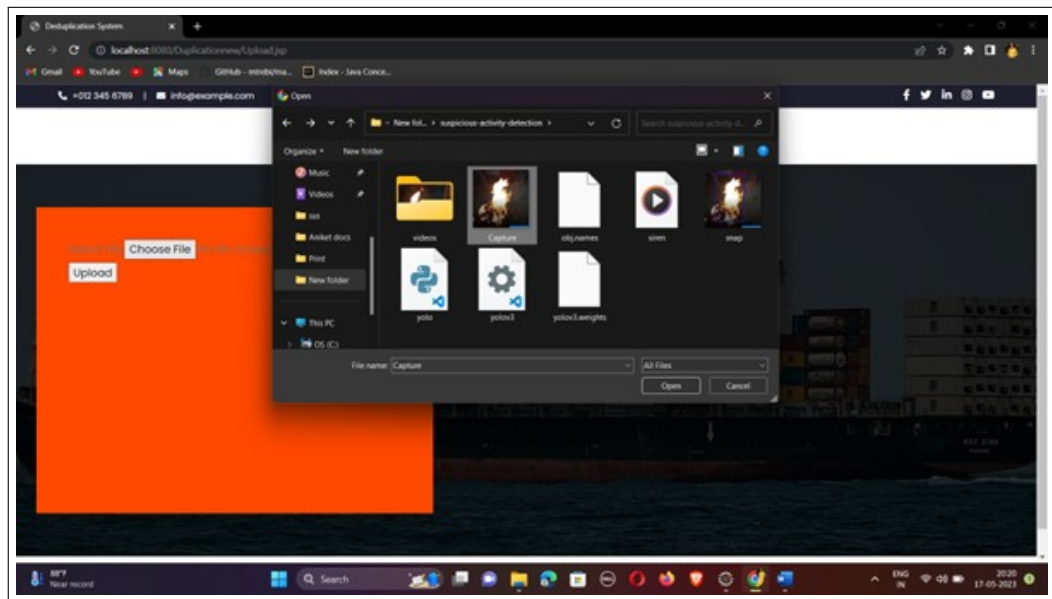


Figure 20: Selecting Image

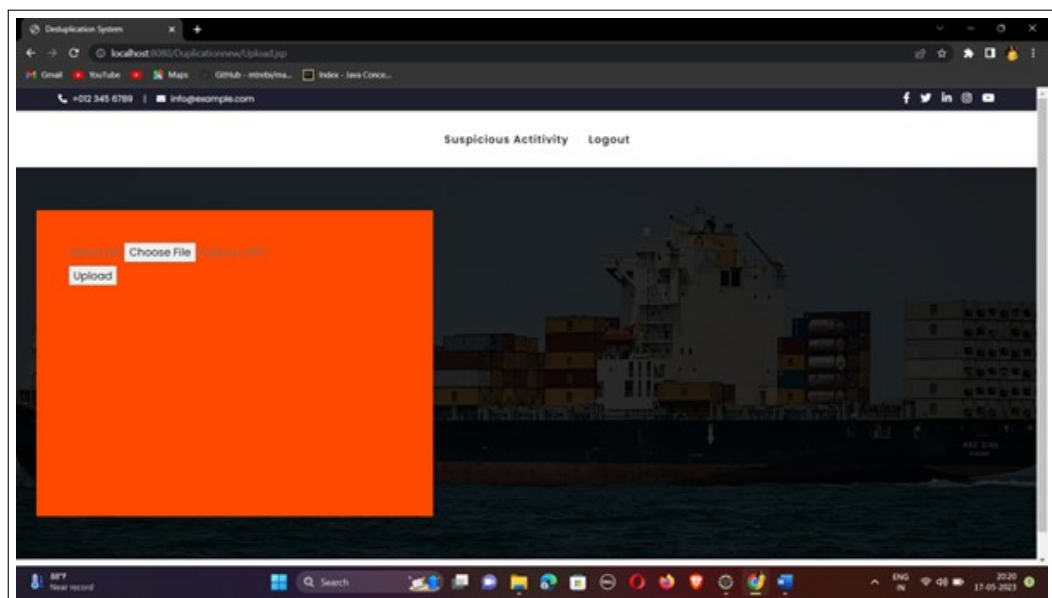


Figure 21: Submitting Image

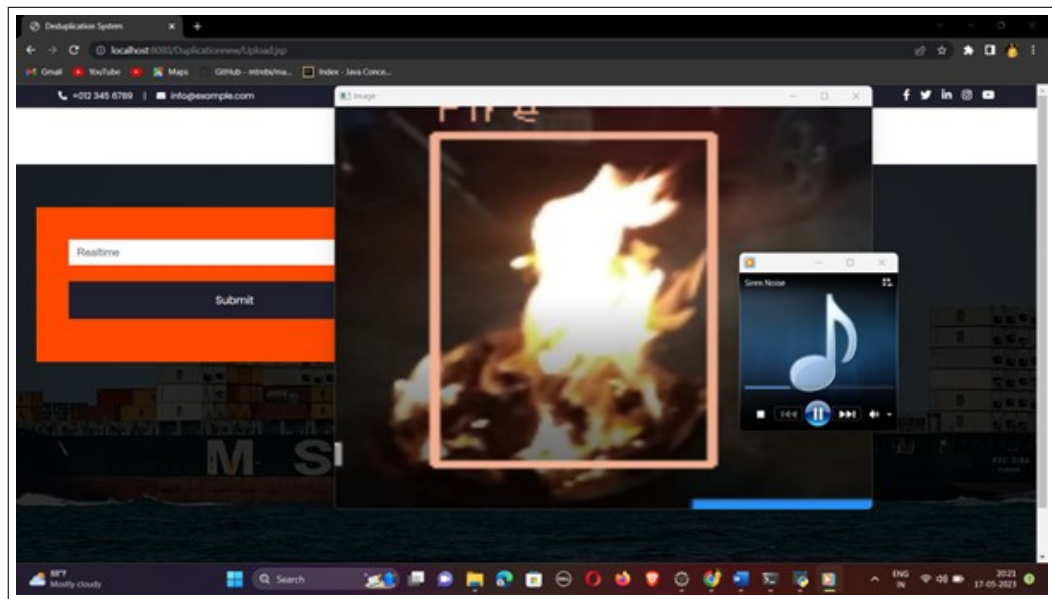


Figure 22: Suspicious Image Detected

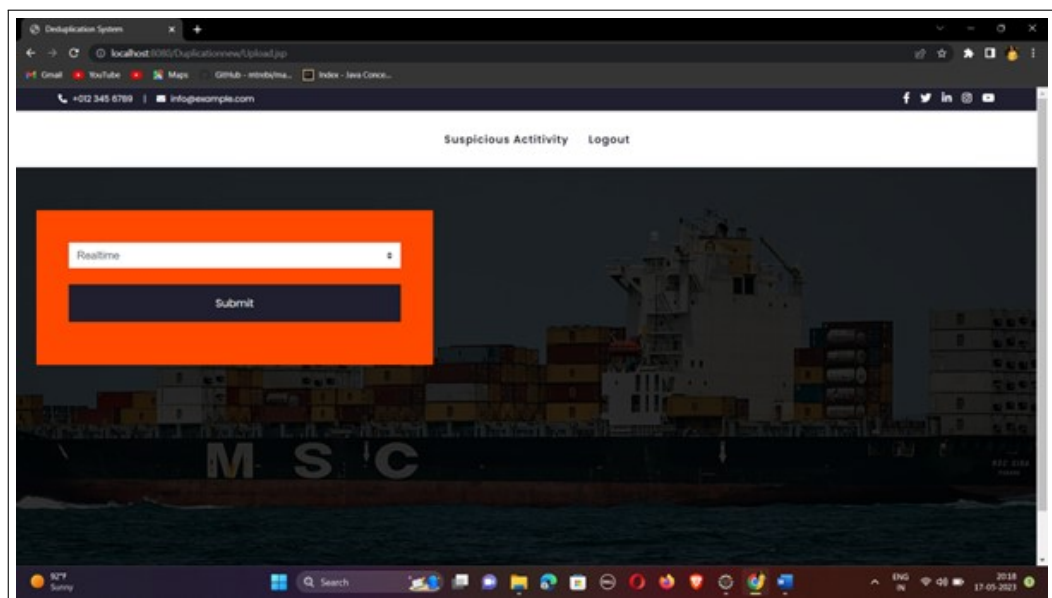


Figure 23: Realtime detection

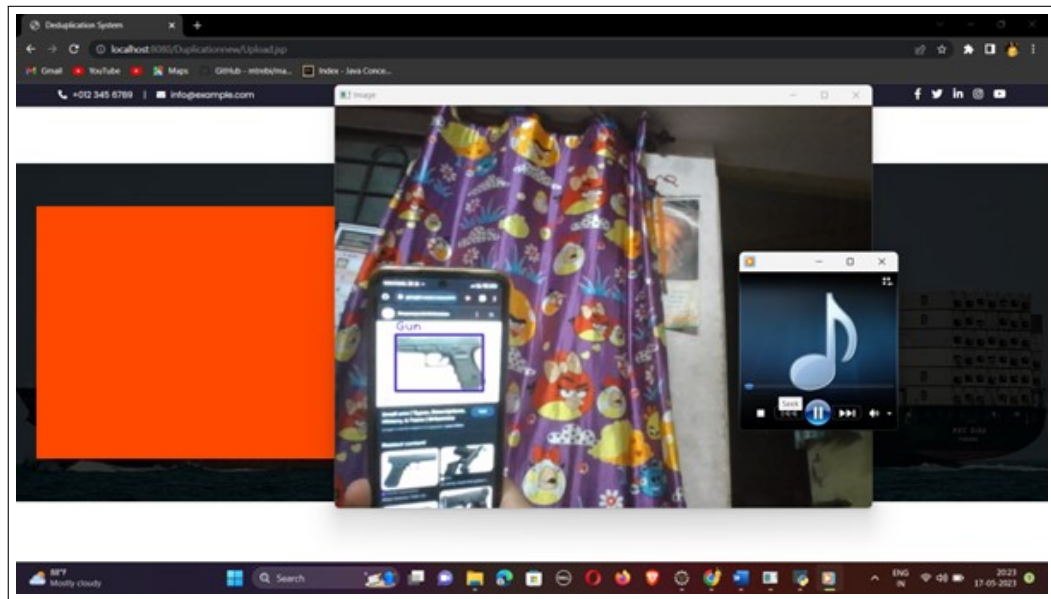


Figure 24: Suspicious Activity detection (Gun Detection)

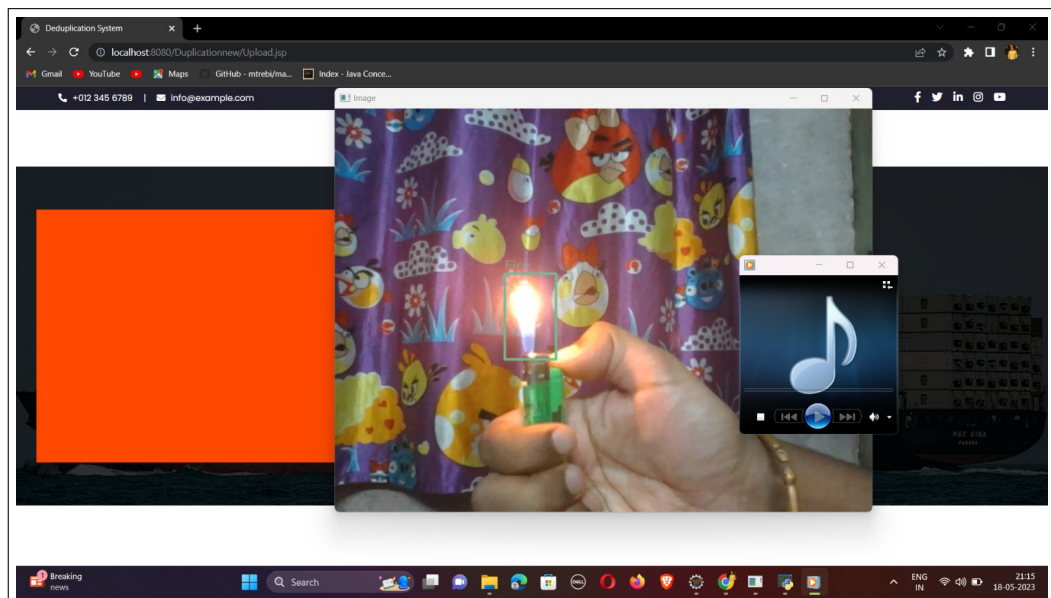


Figure 25: Suspicious Activity detection (Fire Detection)

9 Conclusions

9.1 Conclusion

In the mentioned project, we have put forward an automated video analysis model is for the detection of suspicious activities. This tool aims to alleviate the labor-intensive process of manually reviewing extensive hours of surveillance footage to identify potential suspicious behavior.

By leveraging advanced algorithms and computer vision techniques, the system can efficiently analyze video data and identify specific suspicious activities, such as smoking cigarettes or unauthorized entry into patient rooms.

The automation of this task can greatly save time for the authorities responsible for monitoring hospital surveillance. It eliminates the need for manual inspection of each video frame, significantly accelerating the analysis process. Consequently, the overall efficiency and effectiveness of security operations in the hospital can be enhanced.

By promptly detecting and addressing suspicious activities, the project contributes to bolstering the security measures within the hospital environment. This not only ensures the safety of patients, staff, and visitors but also provides peace of mind to all stakeholders involved.

The activity detection using the YOLO algorithm outperforms the VGG16 algorithm in terms of performance metrics. It achieves an accuracy of 83.34% compared to 78.76% for VGG16, indicating a higher rate of correctly classifying suspicious activities. The YOLO algorithm also demonstrates a higher recall rate of 96.32% compared to 90.32% for VGG16, indicating a better ability to detect true positive suspicious activities. Additionally, the YOLO algorithm achieves an F1 score of 93.26% compared to 91.46% for VGG16, indicating a better balance between precision and recall. Overall, the YOLO algorithm provides more accurate and reliable activity detection in hospital surveillance videos.

In summary, the automated video analysis model leveraging the YOLO algorithm has proven to be highly accurate, achieving impressive recall and F1 scores. Its implementation in the project greatly improves the efficiency and effectiveness of security operations, ultimately enhancing the overall safety and security of the hospital environment.

9.2 Future Work

In the future, there are numerous opportunities for advancement and exploration in various fields, this includes fine-tuning and expanding the dataset, integrating multi-modal fusion for richer context, real-time tracking and behavior analysis, incorporating contextual information, exploring transfer learning and model compression techniques, as well as establishing benchmark datasets and evaluation metrics. By addressing these aspects, the detection system can enhance its accuracy, robustness, and applicability in diverse scenarios, leading to more effective and reliable detection of suspicious activities.

9.3 Applications

The project on suspicious activity detection using YOLO (You Only Look Once) has several applications in enhancing security and safety in hospitals and similar environments. Some of the applications include:

1. Hospital Security: The system can be used to monitor and detect suspicious activities in different areas of a hospital, such as restricted zones, emergency rooms, or medication storage areas. It helps in preventing unauthorized access, theft, or potential threats.
2. Fire Detection: By using YOLO to detect fire objects in real-time, the system can quickly identify and respond to fire incidents. This allows for prompt evacuation, activation of fire suppression systems, and notification to relevant personnel, minimizing the risk of injuries and property damage.
3. Weapons Detection: The project can help in identifying and alerting authorities about the presence of weapons, such as guns, within the hospital premises. This

aids in preventing potential violence, ensuring the safety of patients, visitors, and staff.

4. Behavioral Analysis: The system can analyze the behavior of individuals within the hospital environment, detecting suspicious activities such as loitering in sensitive areas, unauthorized access to restricted zones, or aggressive behavior. This assists in maintaining a secure and controlled environment.
5. Patient Monitoring: This Project can be used to track patient movements and activities, ensuring their safety and well-being. It can detect falls, abnormal behaviors, or instances where patients wander into restricted areas, allowing for immediate response and assistance.
6. Staff Monitoring: The system can assist in monitoring staff activities to ensure compliance with protocols and identify any potential breaches in security or professional conduct.

Overall, the project's applications focus on enhancing security, safety, and situational awareness within hospitals, contributing to a protected environment for patients, staff, and visitors.

References

- [1] P. S. Loganathan, G. Kariyawasam, "Suspicious activity detection in surveillance footage," *International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, May 2019.
- [2] G. N. Dimitropoulos K, Barmpoutis P, "Trans circuit system video technology," *Institute of Electrical and Electronics Engineers (IEEE)*, pp. 38–40, July 2015.
- [3] L. V. M. A. Tripathi V, Gangodkar D, "Robust abnormal event recognition via motion and shape analysis at atm installations," *Journal of Electrical and Computer Engineering*, pp. 20–34, June 2015.
- [4] B. W. Y. P. Wiliem A, Madasu V, "A suspicious behaviour detection using a context space model for smart surveillance systems," *Computer Vision and Image Understanding*, pp. 33–41, March 2012.
- [5] J. I. Z. Chen, "Smart security system for suspicious activity detection in volatile areas," *Journal of Information Technology and Digital World*, March 2020.
- [6] Q. Y. Jie Yin, "Sensor-based abnormal human-activity detection," *Institute of Electrical and Electronics Engineers (IEEE)*, May 2008.
- [7] P. K. S. V. P. Rajasekhar Reddy, B. Nirupa, "Suspicious activities detection using video analysis," *Science, Technology and Development*, vol. 10, May 2021.
- [8] P. A. Sanjay Kumar Singh, "Suspicious human activity recognition for video surveillance system," *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, May 2015.
- [9] P. S. A. S. R. Ramesha. M, Sai Aamani, "Iot based remote patient health monitoring system," *International Conference on Advanced Computing Communication Systems (ICACCS)*, April 2010.
- [10] K. B. Paulo Vinicius, "Vision-based detection of unusual patient activity," *Commonwealth Scientific and Industrial Research Organisation*, March 2018.
- [11] L. G. M, "Activity monitoring and unusual activity detection for elderly homes," *International Journal of Future Computer and Communication*, May 2016.
- [12] D. B. G. P. Prarthana T V1, "Human activity recognition using computer vision based approach – various techniques," *International Research Journal of Engineering and Technology (IRJET)*, vol. 07, June 2020.
- [13] S. O. Shuangjun Liu, "Vision-based system for in-bed posture tracking," *Institute of Electrical and Electronics Engineers (IEEE)*, May 15.
- [14] A. A. Dr. Keerthika V, "Suspicious human activity recognition and alarming system using cnn and lstm algorithm," *International Journal of Advance Research and Innovative Ideas in Education (IJARIIE)*, May 2022.
- [15] S. Sathyanarayana, "Vision-based patient monitoring: a comprehensive review of algorithms and technologies," *Springer*, November 2015.