**FYP SRS Document Template**

Final Year Project

Software Requirement Specification

For

AI Smart Behavior Analysis

BSCS

By

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S# | **Name** | **Registration #/Roll #/Section** | **Mobile #** | **E-Mail** |
| 1. | Saad Amir | Fa-21/051/B | 03285333392 | saad.amir@live.com |
| 2. | Nawab Iftikhar | Fa-21/076/B | 03331474584 | nawabpanu@gmail.com |

**Supervised by:**

Ma’am Anila Amjad **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(**Signature**)**



Department of Computer Science

Lahore Garrison University

Lahore

Table of Contents

1. Introduction...........................................................................................................

1.1 Purpose ........................................................................................................................

1.2 Document Conventions ................................................................................................

1.3 Intended Audience and Reading Suggestions ..............................................................

1.4 Product Scope ..............................................................................................................

2. Overall Description ...............................................................................................

2.1 Product Perspective......................................................................................................

2.2 Product Functions ......................................................................................................

2.3 User Classes and Characteristics ...............................................................................

2.4 Operating Environment ..............................................................................................

2.5 Design and Implementation Constraints ....................................................................

2.6 User Documentation ..................................................................................................

2.7 Assumptions and Dependencies ................................................................................

3. External Interface Requirements .......................................................................

3.1 User Interfaces ...........................................................................................................

3.2 Hardware Interfaces ...................................................................................................

3.3 Software Interfaces ....................................................................................................

3.4 Communications Interfaces .......................................................................................

4. System Features ..................................................................................................

4.1 System Feature 1 ........................................................................................................

4.2 System Feature 2 (and so on) .....................................................................................

5. Other Nonfunctional Requirements ...................................................................

5.1 Performance Requirements ........................................................................................

5.2 Safety Requirements ..................................................................................................

5.3 Security Requirements ...............................................................................................

5.4 Software Quality Attributes .......................................................................................

5.5 Business Rules ...........................................................................................................

References ....................................................................................................................

# **1. Introduction**

## 1.1 **Purpose**

AI Smart Behavior Analysis aids greatly in security and surveillance sector, it does this by analyzing people’s behavior, our purpose is to create a machine learning model capable of identifying and flagging unusual or potentially criminal activities in real-time. The model will analyze input data, such as surveillance footage, to detect anomalous patterns that may indicate suspicious or illegal behavior. This system is designed to assist law enforcement, security personnel, or any relevant stakeholders in monitoring and responding to potential threats in an efficient and automated manner.

## **1.2 Document Conventions**

Report traditions are basic for guaranteeing clarity, consistency, and ease of understanding in specialized and utilitarian documentation for Smart Behavior Analysis model. These traditions give a standardized way to display data, empowering clients, designers, and partners to successfully evaluate the model.

**1. Common Organizing Traditions**

**Text style Fashion and Measure:**

Utilize a clear, proficient textual style such as Times New Roman, Arial, Calibri. Headings are regularly bigger for example 14–16 pt, whereas body content is 11–12 pt.

Headings and Subheadings:

Organized employing a various leveled structure for example H1, H2, H3 to recognize segments clearly.

Numbering Framework:

Utilize a coherent numbering organize for example 1.1, 1.2 for segments and subsections to progress route.

**Date Arrange:**

Utilize ISO standard organize (YYYY-MM-DD) for clarity and universal consistency.

## **1.3 Intended Audience and Reading Suggestions**

This Software Requirements Specification (SRS) document is intended for the following audiences:

* **Developers and Engineers**: By reading this SRS, developers and engineers can gain insight into smart behavior system ad learn about its intricate working
* **Data Scientists and Machine Learning Specialists**: Data scientists and other machine learning engineers could also read and provide better insight o how to improve accuracy and efficiency.
* **Stakeholders and Clients**: The clients such as banks and other places where security is of key concern.

## **1.4 Product Scope**

# Our product uses machine learning technology to analyze security footage for weapons presence and detects both criminal and suspicious behavior. The system reads surveillance camera footage to find weapons or suspect behavior. The model will recognize weapons in visual data to back up police and security teams who aim to reduce violent situations.

# **2. Overall Description**

## **2.1 Product Perspective**

This product works independently to support human security teams in their work. The system will look at video footage to find signs of crime happening or weapons being used against organization assets. Staff supervision will complement the system to help the team respond faster and better find security threats.

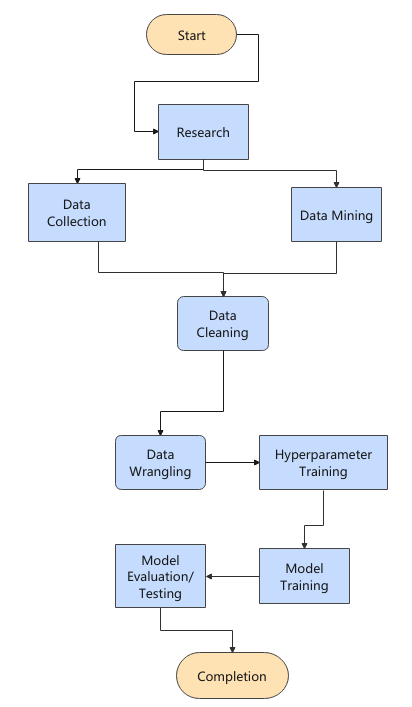
* Integration with Existing Systems: The ML model will be integrated with a web interface with access to live CCTV footage.
* **External Interfaces**: The system will alert the authorities as soon as something unusual is detected through the web interface
* **User Roles and Interactions**:
  + **Security Personnel**: The security guards will keep vigilant eye on the responses created by the system to ensure maximum accuracy and efficiency.

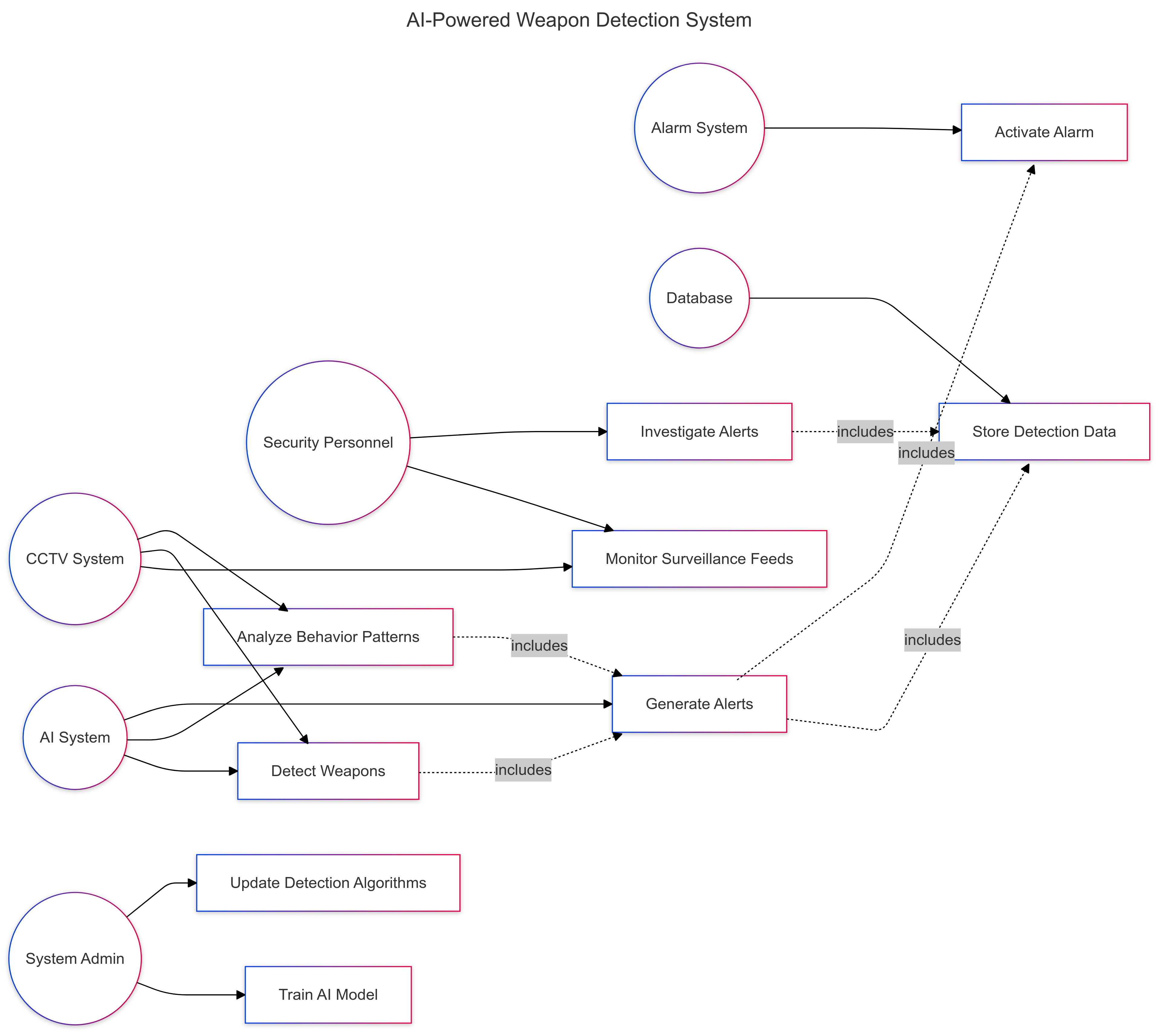
Production Position

This machine learning based detection model will provide enhanced situational awareness by detecting unusual behavior and the presence of a weapon, thus reducing the need of excessive security personnel and improving the speed of threat identification. It will be beneficial in environments where security and continuous monitoring are critical, such as:

* **Public Places**: Airports, train stations, malls, or large public events, where detecting weapons and suspicious activities can help prevent violent incidents.
* **Retail Environments**: Stores and warehouses, where the system can prevent theft, violence, and detect any concealed or openly carried weapons.
* **Critical Infrastructure**: High security areas such as banks, government buildings, military installations, or private facilities that need to detect weapons and criminal behavior in real time.

Time line Flowchart:



**Working Flow Chart:**

## 

## **2.2 Product Functions**

The system is designed to detect unusual behavior, identify weapons, and recognize an ongoing robbery. It uses machine learning and computer vision techniques to analyse real time video feeds. The system's functions are outlined as follows:

2.2.1 Real Time Behavior Analysis

* **Function**: The system will monitor and analyze human behavior in real time, using input from security cameras. It will detect unusual or criminal activity based on predefined behavioral patterns.
* **Inputs**: Real time video feed from surveillance cameras.
* **Outputs**: Behavioral status report, real time alert or notification.

2.2.2 Weapon Detection

* **Function**: The system will detect and identify weapons in real time using computer vision techniques, analyzing both objects and gestures that may indicate weapon possession.
* **Inputs**: Video feed from surveillance cameras, images from public and private spaces.
* **Outputs**: Alerts for weapon detection, weapon identification.

2.2.3 Robbery Detection

* **Function**: The system will detect potential robbery events based on certain behavioral and environmental factors commonly associated with robbery scenarios.
* **Inputs**: Real time video feed from surveillance cameras.
* **Outputs**: robbery detection, weapon detection and alert.

## **2.3 User Classes and Characteristics**

The system will serve security personnel in monitoring and safe guarding precious assets by continuously monitoring the environment; moreover it will also be able to serve law enforcement agencies in general public safety:

2.3.1 Security Personnel

* **Description**: Security personnel are the primary users responsible for monitoring and responding to security threats. They are typically employed by businesses, bank, facilities, or public spaces and are tasked with ensuring the safety of the environment.
* **Characteristics**:
  + **Experience Level**: Intermediate to expert knowledge of security systems and incident response.
  + **Primary Functions**:
    - Monitor alerts generated by the system for suspicious activity.
    - Respond to detected threats. View real time video feeds and analyse detected behaviors or threats.
    - Review and analyze generated reports on security events.
  + **Access Level**: Access to real-time alerts, video feeds, behavior analysis data, and incident reports. Permissions to interact with the system’s alerts and integrate with other security systems such as alarms, locks.

2.3.2 Law Enforcement Agencies

* **Description**: Law enforcement agencies are users responsible for investigating potential criminal activities flagged by the system. They may be external or internal users who act upon more serious threats or incidents.
* **Characteristics**:
  + **Experience Level**: Expert in law enforcement procedures and criminal investigation.
  + **Primary Functions**:
    - Review detailed incident reports and alerts to determine further investigation or action.
    - Access to historical data and crime prediction analysis for ongoing investigations.
    - Collaboration with security personnel to assess crime scenarios and respond appropriately.
    - Trigger external actions, such as notifying authorities.
  + **Access Level**: Access to detailed incident reports, weapon detection data, predictive analysis, and historical event data. Limited control over system settings or configurations.
  + **Device Usage**: Desktop or Laptop application with law enforcement-specific interfaces for deeper investigation into flagged events.

## **2.4 Operating Environment**

The system is designed to operate in a range of environments, from private security installations to large scale public safety monitoring systems. It leverages both hardware and software components to function effectively.

2.4.1 Hardware Requirements

The system will operate on a combination of specialized hardware for video surveillance, computational power for AI processing, and standard user devices for interaction. The primary hardware components include:

* **Surveillance Cameras**: High definition cameras with at least 480p resolution, capable of streaming video in real time.
* **Computational Servers**: Dedicated servers or cloud infrastructure with sufficient processing power to handle real time video analysis, machine learning models, and large scale data processing. This may include:
  + **Processor**: Multi-core CPU and GPU for deep learning based image and behavior analysis.
  + **Memory**: Minimum 32GB of RAM.
  + **Storage**: SSD or other high speed storage options with a minimum of 1TB for handling video and data logs, with additional backup storage for redundancy.
* **Network Infrastructure**: A reliable and secure network infrastructure to support high bandwidth video streaming and real time communication with client devices. This includes:
  + **Internet Connection**: Stable internet connection with a bandwidth of at least 10 Mb’s for cloud based operations.
  + **Local Network**: Wired Ethernet or secure Wi-Fi network for communication between cameras, servers, and user devices.
* **User Devices**: Devices for interacting with the system, including desktops and laptops. User devices should support modern operating systems and browsers to interact with the AI system's interfaces.
  + **Desktop/Laptop**: Running Windows 10 or higher, macOS, or Linux, with up-to-date web browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, etc..

2.4.2 Software Requirements

The system utilizes several software layers to operate effectively, including operating systems, databases, machine learning frameworks, and application layers.

* **Machine Learning Frameworks**:
  + pytorch, or other deep learning frameworks for behavior analysis and pattern recognition.
  + Opencv or similar computer vision libraries for real time image and video analysis.
  + Sklearn or similar libraries for data preprocessing, anomaly detection, and predictive crime models.

2.4.3 Environmental Conditions

The system is intended to operate in a wide range of physical environments, from controlled indoor facilities to outdoor settings. Key environmental considerations include:

* **Lighting**: The system is expected to work under varying lighting conditions, including low-light and nighttime scenarios. Cameras are required to ensure visibility under minimal lighting.

2.4.4 System Scalability

The system is designed to scale depending on the number of cameras, sensors, and monitoring stations in place. It can be deployed across various scales, from small facilities with a few cameras to large camera network with a network of hundreds or thousands of surveillance devices.

* **Small Scale Deployment**: For businesses or banks, the system can be set up on a single server with limited cameras and monitoring stations.
* **Large Scale Deployment**: To deploy at a larger scale there must be a lot of cameras to surveille a large area with a lot of computational power.

## **2.5 Design and Implementation Constraints**

The system was not easy to design and given below are some of the implementation constraints:

* **Machine Learning Model Limitations**:
  + The system is trained on machine learning models that detect weapons and unusual behavior but training such a model is not an easy task, the model needs to be accurate as well as quick.
* **Video Resolution and Processing Power**:
  + In order to process the video footage correctly, the correct image processing techniques were required.
  + The perfect video resolution was required to correctly make use of the available resources i.e. processing power.

## **2.6 User Documentation**

This documentation is designed for the end user who will use the system, the system is designed to be easy to use.

2.6.2 System Requirements:

Before using the system, ensure that the following system requirements are met:

* **Hardware Requirements**:
  + Surveillance cameras.
  + Computers or Laptops with internet access for viewing live video footages and alerts.

2.6.4 User Interface Overview

2.6.5 Dashboard

The main dashboard gives user all the necessary information about the current situation. Important features of the dashboard are as follow:

* **Live Video Feed**: Displays real time video from connected cameras.
* **Alerts Panel**: Shows any ongoing or recent alerts for suspicious behavior, crime prediction, weapon detection, or robbery events.
* **Threat Level Indicator**: A visual gauge showing the severity of current threats such as low, medium, high.

2.6.6 Alerts and Notifications

System alerts will be sent to the security personnel viewing the live camera feed so that he can make an informed decision of what to do, the alerts will include weapons alert, behavior alert etc...

2.6.8 Weapon Detection

The system will identify weapons as soon as they are visible.

## **2.7 Assumptions and Dependencies**

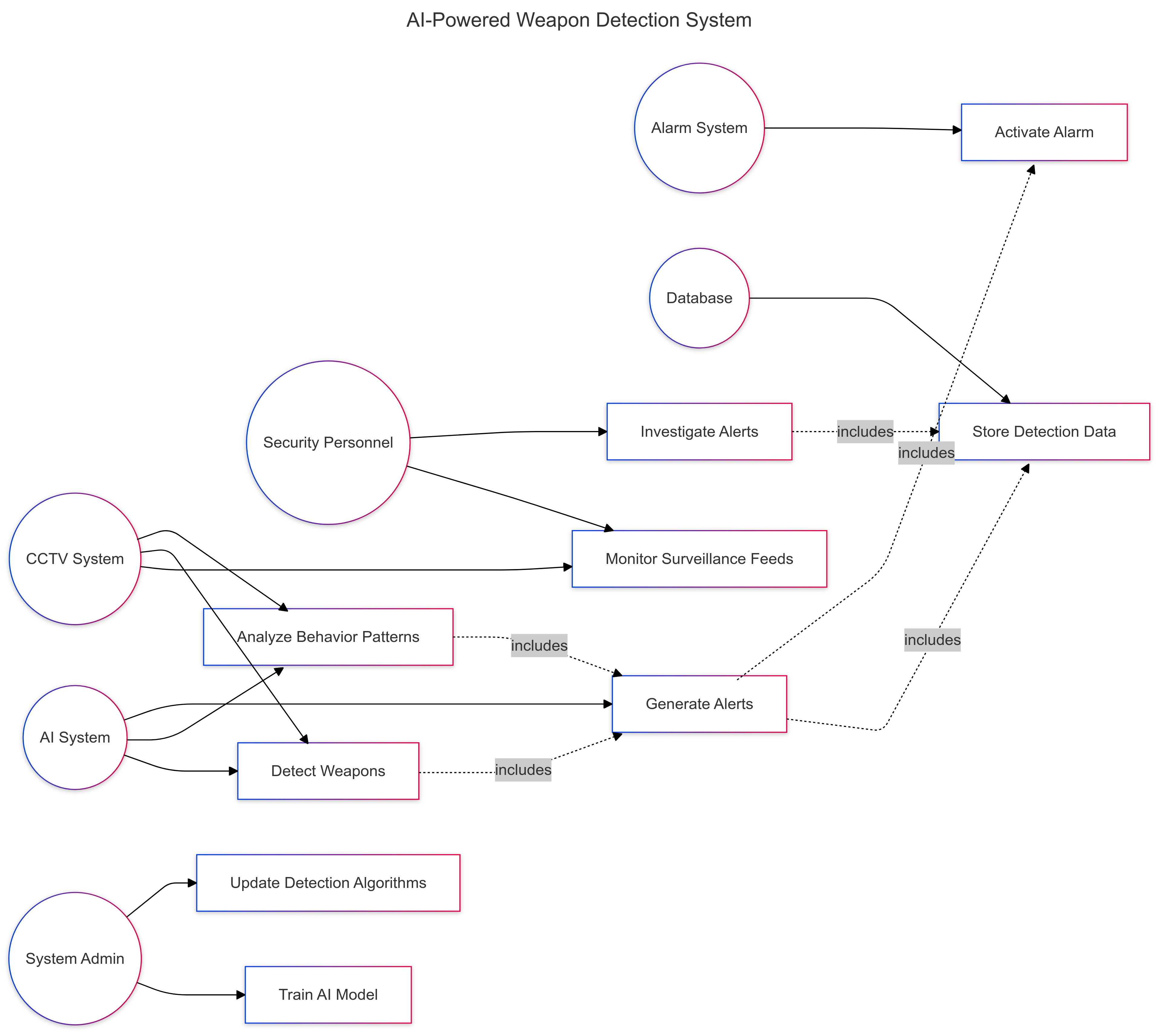
The following assumptions are made in the development, deployment, and use of the system:

2.7.1 Assumptions about Systematic Use

* **Access to Camera footage**: The system must have camera access at all times in order to detect weapons and other anomalies that it was designed for.
* **User Training**: The security personnel must be trained on ho w to use the system in order to maximize efficiency.
* **Network Connectivity**: There must be internet connection at all times for the video footage to be given to the model for it to analyze.
* **Accuracy of Detection Models**: It is assumed that the system's machine learning models, including those for behavior analysis, weapon detection, and robbery detection, will perform accurately and consistently.

2.7.2 Assumptions about Environmental Conditions

* **Adequate Lighting for Cameras**: There must be sufficient lighting for the camera in order for the model to work perfectly.
* **Stable Power Condition**: The camera and the model must have a stable power supply; it must be ensured that there would be no load shedding.

**Use Case Diagram:**

2.7.4 Dependencies

The system depends upon several things in order to work seamlessly, they are given below:

2.7.5 External System Dependencies

* **Surveillance Cameras**: The system depends upon CCTV cameras to provide video footage
* **Network Infrastructure**: The system requires internet connection to transmit video footage and send alerts.

2.7.6 Software Dependencies

* **Machine Learning Models**: The system depends on machine learning models like naïve bayes, logistic regression, etc… They include libraries such as sklearn, tensorflow, pytorch, or opencv.
* **Database Systems**: The system depends on relational i.e. PostgreSQL, MySQL databases for storing structured and unstructured data.

2.7.7 Environmental Dependencies

* **Lighting and Environmental Conditions**: The system depends on appropriate environmental conditions, including lighting, to perform accurate video analysis.

# **3. External Interface Requirements**

## **3.1 User Interfaces**

The system provides a basic user friendly interface for the security personnel to view the camera footage and see the analysis made by the model.

3.1.1 Security Personnel Interface

* **Real Time Alerts**: Alerts will be sent as soon as a weapon or other anomaly has been detected.
* **Video Stream Access**: Security guards can view the live footage or can also the previously recorded footage.

## **3.2 Hardware Interfaces**

The hardware interface of the system includes mainly the cameras and some computational server.

3.2.1 Surveillance Cameras

* **Resolution**: The system requires cameras to perform accurate analysis of behavior and weapon detection.
* **Frame Rate**: Cameras should support a minimum of 15 frames per second (FPS) for smooth video streaming.

## **3.3 Software Interfaces**

The system interfaces with other software components including machine learning frameworks and web application and database system. The detailed explanation is given below:

3.3.1 Machine Learning Frameworks

* **Interface with ML frameworks**: The system uses open source machine learning frameworks such as pytorch, tensorflow, or others.

3.3.2 Web Integration

The system will be integrated with a web application for ease of use, this way it will be easily accessible from various computers

3.3.3 Database Management Systems

The system will also be integrated with a database to store threats with their timestamps.

3.3.5 User Interface Software

* **Web Interface**: The system provides a web based interface that allows users to interact with the system. The web interface will be compatible with browsers like chrome, firefox, etc.. and provide real time predictions.

## **3.4 Communications Interfaces**

The system uses numerous communication protocols to interface with external systems, devices, and services:

3.4.1 Video Streaming Protocols

* **Real Time Streaming Protocol**: Used for streaming live video from cameras to the system for analysis. The system must support receiving video streams in this protocol for integration with IP cameras.
* **ONVIF (Open Network Video Interface Forum)**: A standard for connecting IP based security devices, such as cameras, to the system. It ensures compatibility with a wide range of surveillance hardware.
* **H.264 or H.265**: Video formats used for compressing video data transmitted from cameras to the system.

3.4.2 Data Transmission Protocol

* **HTTPS**: Used for secure web-based communication between the user interface and the back end system. Ensures encrypted transmission of sensitive data, including video streams, alerts, and user credentials.

3.4.3 Database Communication

* Database will be used to store events data with their respective time stamps.

# **4. System Features**

The system is designed to provide real-time surveillance, behavior analysis, and threat detection through advanced AI algorithms. The following system features describe the core functionalities available to users, including security personnel, system administrators, and law enforcement agencies.

4.1 Behavior Analysis

**Description**:  
The system continuously analyzes video feeds in real-time to identify and classify human behaviors. This feature uses machine learning models trained to detect various types of suspicious or abnormal behavior.

**Key Functionalities**:

* **Suspicious Movement Detection**: Identifies and flags unusual movement patterns, such as people loitering in a restricted area or walking in unusual directions.
* **Unusual Behavior Alert**: Sends alerts when the system detects unusual behavior that deviate from normal patterns, Like snatching, running etc..

**User Actions**:

* View video feed with behavior annotations in real time.
* Receive notifications of detected suspicious behaviors.
* Review historical data for flagged behavior patterns.

4.2 Weapon Detection

**Description**:  
The system uses object detection algorithms to identify weapons like guns and knives within the video feed and provides real time alert if a weapon is detected.

**Key Functionalities**:

* **Weapon Recognition**: Detects weapons using the model it was trained on.
* **Weapon Location Detection**: Provides location based information on where the weapon was detected i.e. camera 1, helping security teams respond more efficiently.
* **Automatic Alerting**: Sends immediate alerts to security personnel and law enforcement if a weapon is detected, with visual evidence attached.

**User Actions**:

* View a live alert with a snapshot of the detected weapon.
* Access historical footage to review the context in which a weapon was detected.

4.3 Robbery Detection

**Description**:  
The system will be capable of successfully detecting an ongoing robbery with the help of the model it was trained on and then immediately alerting the authorities.

**Key Functionalities**:

* **Robbery Prediction**: Using the data it was trained upon and real time video analysis, the system predicts possible robbery events based on suspicious behavior patterns, such as people congregating in an unusual manner or carrying large bags or possession of weapons.

**User Actions**:

* Access real time alerts with video evidence when a robbery is detected or predicted.
* Send the alert to the authorities so they can respond to the threat.

4.4 Video Feed Monitoring and Playback

**Description**:  
The system provides a live video feed and playback feature, allowing users to monitor real-time surveillance and review recorded footage for behavior analysis or event investigation.

**Key Functions**:

* **Live Video Stream**: View live video feeds from connected cameras in real-time, with the option to zoom in and out or adjust the view for detailed monitoring.
* **Incident Review**: Search historical video footage based on time, date, and event type to review incidents flagged by the system.
* **Video Analysis**: Overlays on video footage show detected behaviors, such as “Suspicious movement” or “Weapon detected,” providing real-time context.
* **Export Video Clips**: Users can export specific video clips or screenshots for further analysis or reporting.

**User Actions**:

* Monitor live video feeds and watch for alerts or suspicious behaviors.
* Navigate through archived footage to investigate past events.
* Export clips for reporting or legal evidence.

## **4.1.1 Description and Priority**

Each feature of the **AI Smart Behavior Analysis** system is critical to its overall functionality, but certain features may be more essential to core system operations than others. The priority of each feature is given below:

4.1.1.1 Real Time Behavior Analysis

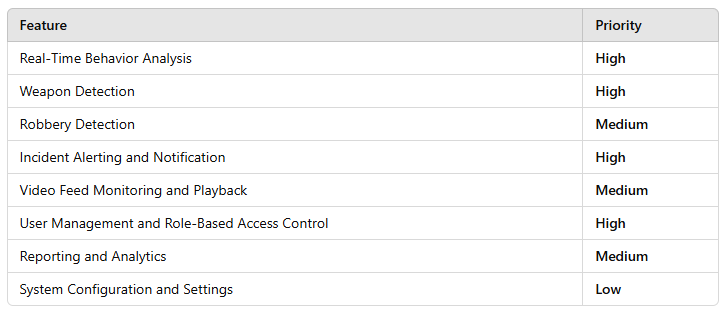
**Description**:  
The **real time behavior analysis** feature continuously analyzes video feeds from surveillance cameras to detect suspicious or unusual behavior.

**Priority**:  
**High**  
This is one of the main feature of the system and is very important for maintaining surveillance. Real time detection and alerting of abnormal behaviors are essential for the system’s functionality, ensuring that security personnel can respond quickly to potential threats.

4.1.1..2 Weapon Detection

**Description**:  
The **Weapon Detection** is one of the main features of the ai smart behavior analysis, it uses a machine learning model that was trained on dataset of video and images of plethora of weapons.

**Priority**:  
**High**  
It is given the priority high as there would be danger to general public safety if there is weapon present, it also increases the chances of violence.

Graphical Representation:



## **4.1.2 Stimulus/Response Sequences**

4.1.2.1 Stimulus: Detection of Behavior

**Stimulus**:  
The system analyzes behavior and detects if there is any strange movement or something odd going on.

**Response**:

1. The model views the live camera footage and analyzes it, if there is nothing starnge it keeps on going but as soon as it finds something it send an alert to the security.
2. The system immediately sends an **alert** to the **security alongwith the captured image of the behavior.**
3. The system saves the event in the database.

4.1.2.2 Stimulus: Detection of Weapon

**Stimulus**:  
The system detects weapon such as a gun or a knife in the video footage using object detection.

**Response**:

1. The system analyzes video footage and if there is a weapon it draws a bounding box around it and then alerts the security.
2. The **alert** is sent to the dashboard of the system for the security to review
3. The system logs the detection event in the database.

4.1.2.3 Stimulus: Detection of Robbery

**Stimulus**:  
The system detects an ongoing robbery by detecting a lot of weapons and masks and crowd gathering and crowd behavior.

**Response**:

1. The model views the video footage and detects if there is an ongoing robbery, an alert is sent if there is.
2. An ongoing robbery **alert** is sent to the dashboard of the system .

## **4.1.3 Functional Requirements**

The system is created for the purpose of weapon detection, behavior analysis and robbery detection, but it needs the following requirements fulfilled:

4.1.3.1 Behavior Detection

4.1.3.2 Suspicious Behavior Detection

* **Description**: The system must be capable of detecting unusual human behaviors, like strange movement, and other actions that may indicate suspicious or illegal activity.
* **Operational Requirement**:
  + The system shall continuously view live video footage for behavioral patterns.
  + The system shall send alert to the security if suspicious behavior is detected.

4.1.4 Weapon Detection

4.1.3.1 Detection of Weapons

* **Description**: The core feature of the system is to detect weapons, it will do the following:
* **Operational Requirement**:
  + The system will use object detection model to detect weapons.
  + The system will send an alert if a weapon is detected.

# **5. Other Nonfunctional Requirements**

## **5.1 Performance Requirements**

5.1.1 Latency for Behavior Detection

* **Requirement**:  
  The system must detect unusual behavior as quickly as it is spotted so that the public safety remains secure.

5.1.2 Latency for Weapon Detection

* **Requirements**:  
  The system must also detect weapons in a video footage as quickly as it is seen so that the security can reach the situation before any escalation.

5.1.3 Latency for Robbery Detection

* **Requirements**:  
  The system must detect a robbery within a minute so that the authorities can reach the situation on time ensuring the safety of assets.

5.3 Scalability

5.3.1 Number of Cameras Supported

* **Requirements**:  
  The system must support multi camera system to widen its scope.

5.3.3 Distributed Processing

* **Requirement**s:  
  The system must have some sort of server access to enhance its performance using powerful server computers.

## **5.2 Safety Requirements**

5.1.2 Operational Safety

5.1.2.1 System Failure Mechanisms

* **Requirements**:  
  If there is a power outage the system must come back online as soon the power comes back on or it must have a backup power supply.
* **Safety Impact**: Ensures that security monitoring continues even during system downtime, preventing a gap in coverage that could result in unsafe situations.

5.1.3.1 Cybersecurity and Data Protection

5.3.1.2 Secure Communication and Data Storage

* **Requirements**:  
  The system must have secure communication over the network for the video footage to reach the computers from the cameras.
* **Safety Impact**: Protects the system from cybersecurity threats, ensuring that malicious actors cannot intercept or tamper with critical surveillance data.

## **5.3 Security Requirements**

The system must be accurate and it must ensure security of the data and maintain its integrity.

5.3.1.4 Data Protection and Privacy

5.3.1.5 Data encryption:

* **Requirements**:  
  All sensitive data, including video feeds, event logs, and user information, must be **encrypted** using **AES-256 encryption** both during transmission and when stored.
* **Security Impact**: Ensures data confidentiality and integrity, preventing unauthorized access to sensitive information.

5.3.1.6 Data minimization

* **Requirements**:  
  The system must adhere to **data minimization principles**, ensuring that only necessary data is collected, stored, and processed. For example:
  + Video footage should be stored only as long as necessary for security or regulatory purposes (e.g., 30 days), after which it must be securely deleted or archived.
  + Personal data (e.g., facial recognition data, user login data) must be anonymity whenever possible.
* **Security Impact**: Limits the exposure of sensitive data to unauthorized access and reduces the risk of data breaches.

## **5.4 Software Quality Attributes**

The accuracy of the system will be above 80% to minimize risks of human error. The response time will be under one minute and large number of cameras will be supported.

## **5.5 Business Rules**

* The security personnel monitoring should be active and available to respond to the predicted output.
* Smart behavior system is designed for security dependent places such as banks, jewelry stores etc..
* The system must detect weapons in real time and immediately trigger an alarm to alert authorities.
* The system should flag unusual activities or aggressive behavior based on the model’s training.

# **References**

* 8 Benefits of computer vision in security industry, An article by Zach Amos.
* How Computer Vision is changing safety and security by Michael Brinich and Dan Gural
* Edge Ai for computer vision in surveillance by Guadenz Boesch
* Effective Surveillance using Computer Vision by Aditi Marwaha,Abhijit Chirputkar amd P Ashok