Final Year Project Report

CRIME DETECTION & PREVENTION SYSTEM

Project Advisor:

SIR MUSTAHSAN HAMMAD NAQVI

Submitted By:

MUHAMMAD ARSHMAN NOOR (**21001376003**)
ARSHAD MEHMOOD (**21001376002**)
AHMED NADEEM BUTT (**21001376004**)

Session

Fall 2021-2025

UNIVERSITY OF MANAGEMENT AND TECHNOLOGY
SIALKOT

DEDICATION

We've had lots of people helping us out with our project, and we can't thank them enough. First off, we're grateful to God for giving us the strength and showing us how to make things better. Big shoutout to our folks too, who've been there for us through thick and thin, especially when this project got us feeling stressed.

And let's not forget our teachers! They've been like guiding stars, showing us new ways to do things and always cheering us on. We owe them a huge debt of gratitude for believing in us and keeping us on track.

FINAL APPROVAL

- **Head of Department** ________________________
  Department of AI
  School of Systems & Technology
  UMT Sialkot

- **Director (Final Year Projects-AI)** ________________________
  Department of AI.
  School of Systems & Technology
  UMT Sialkot

- **Supervisor** ________________________

  Department of AI.
  School of Systems & Technology
  UMT Sialkot

- **Co-Supervisor** ________________________

ACKNOWLEDGMENT

We are deeply grateful to God for blessing us with a beautiful life and granting us the wisdom and knowledge needed for this journey. A huge thank you to all the incredible teachers in the AI & CS department at UMT for being our guiding lights. Your support and dedication have shaped our learning experience and given us the opportunity to work on this project.

A special note of appreciation goes to Sir Hammad Naqvi. His unwavering guidance, encouragement, and support have been invaluable to us throughout this study, and we truly appreciate everything he has done.

Project Title:

Crime Detection & Prevention System

Undertaken by:

MUHAMMAD ARSHMAN NOOR (21001376003)

AHMED NADEEM BUTT (21001376004)

ARSHAD MEHMOOD (21001376002)

Supervised by:

Mr. Mustahsan Hammad Naqvi

Starting Date:

15 October 2024

Completion Date:

Tools Used:

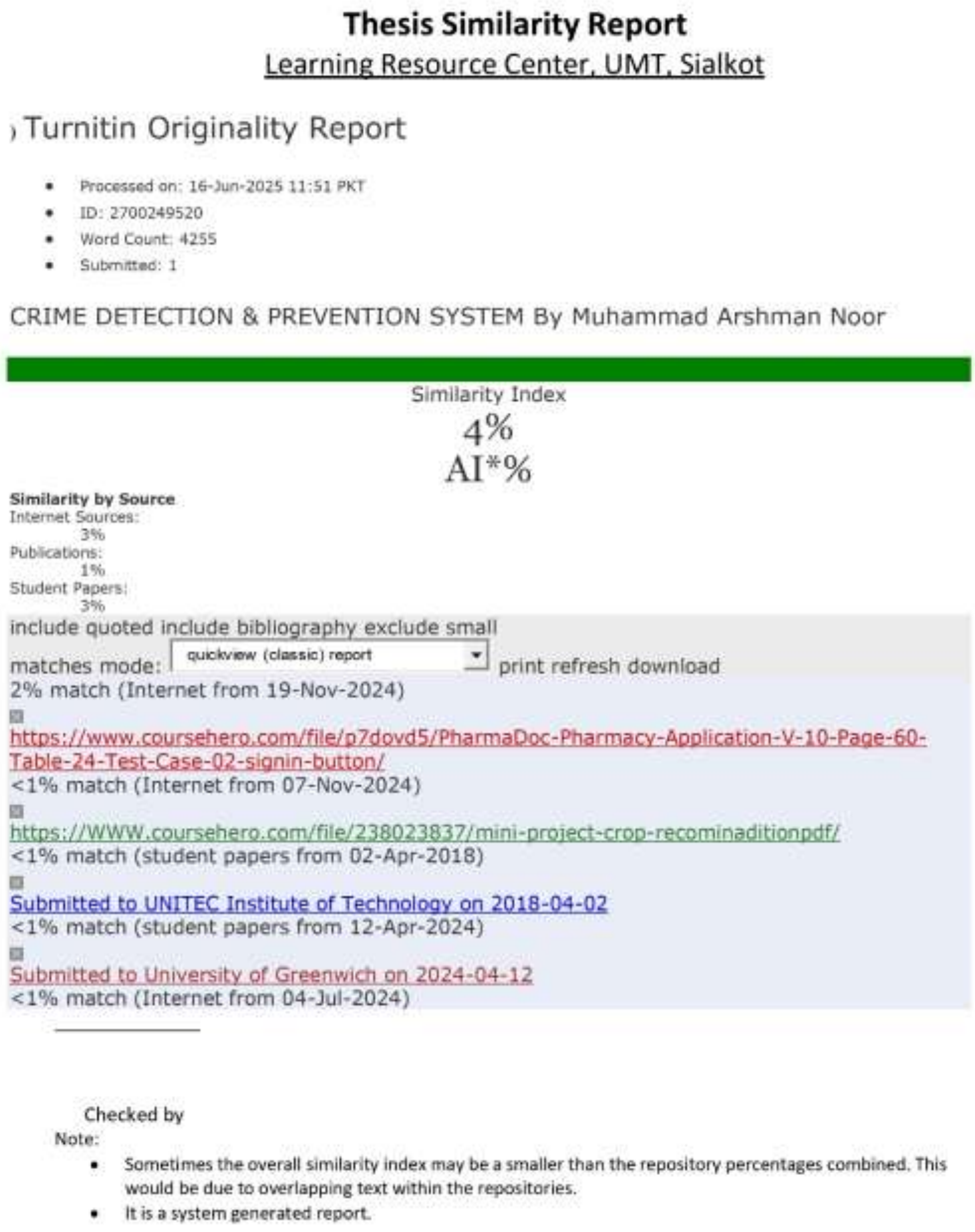
1. **Programming Languages:** Python
2. **AI Libraries/Frameworks:** TensorFlow, OpenCV, NLTK, Pytorch, scikit-learn etc
3. **Database:** sqlite3
4. **Version Control:** GitHub

Operating System:

Microsoft Windows

Android

PLAGIARISM REPORT



Thesis Similarity Report

Learning Resource Center, UMT, Sialkot

) Turnitin Originality Report

- Processed on: 16-Jun-2025 11:51 PKT
- ID: 2700249520
- Word Count: 4255
- Submitted: 1

CRIME DETECTION & PREVENTION SYSTEM By Muhammad Arshman Noor

Similarity Index

4%

AI*%

Similarity by Source

Internet Sources:
3%
Publications:
1%
Student Papers:
3%

include quoted include bibliography exclude small matches mode: quickview (classic) report print refresh download

2% match (Internet from 19-Nov-2024)

https://www.coursehero.com/file/p7dovd5/PharmaDoc-Pharmacy-Application-V-10-Page-60-Table-24-Test-Case-02-signin-button/

<1% match (Internet from 07-Nov-2024)

https://WWW.coursehero.com/file/238023837/mini-project-crop-recominaditionpdf/

<1% match (student papers from 02-Apr-2018)

Submitted to UNITEC Institute of Technology on 2018-04-02

<1% match (student papers from 12-Apr-2024)

Submitted to University of Greenwich on 2024-04-12

<1% match (Internet from 04-Jul-2024)

Checked by

Note:

- Sometimes the overall similarity index may be a smaller than the repository percentages combined. This would be due to overlapping text within the repositories.
- It is a system generated report.

ABSTRACT

Traditional crime detection and prevention methods rely on constant human surveillance, making them inefficient, costly, and prone to human error. The primary goal of this project is to reduce the need for continuous human monitoring by utilizing AI-powered automation. Our Crime Detection & Prevention System (CDPS) leverages machine learning, computer vision, and natural language processing (NLP) to analyze real-time surveillance feeds, detect suspicious activities, weapon detection and automatically alert monitoring personnel to specific cameras requiring attention. This ensures that human operators only review relevant, high-risk footage, significantly reducing workload while improving response times.

The system is designed to identify unusual behaviors, unauthorized access to restricted areas, and potential threats such as loitering, sudden movements, weapon detection or attempts to breach security zones. Once an anomaly is detected, an alert is instantly sent to the monitoring room, where personnel can verify the feed and deploy law enforcement teams as needed. This targeted approach not only enhances security efficiency but also prevents crimes before they escalate.

Additionally, an AI-driven chatbot is integrated to assist victims in reporting crimes securely, especially for those hesitant to speak directly to law enforcement. The system also supports automated alerts for red-alert license plates, ensuring rapid intervention when necessary.

By minimizing human workload, reducing monitoring fatigue, and enabling specific threat detection, CDPS enhances law enforcement capabilities and raises safer communities through intelligent, data-driven crime prevention.

REVISION CHART

Version	Primary Author(s)	Description of Version	Date Completed
Database & Research for Chatbot	Ahmed Nadeem	Started researching on chatbot and built the database schema.	12 February 2025
UI Design for Chatbot	Arshman Noor	Designed UI for Chatbot.	28 January 2025
Chatbot Development & AI Integration	Arshad Mehmood	Developed backend for chatbot and integrated database and API in it.	17 February 2025
Chatbot Frontend	Arshad Mehmood	Developed the frontend for Chatbot.	19 February 2025
Data Collection	Ahmed Nadeem	Collected data available over the internet for training	6 May 2025
Surveillance Development	Arshad Mehmood	Developed backend for surveillance system.	19 May 2025
Design Frontend	Arshman Noor	Designed Frontend Idea for surveillance system	22 May 2025
Surveillance Frontend	Arshad Mehmood	Developed frontend for surveillance system	27 May 2025
Data Collection	Ahmed Nadeem	Collected Data for testing	2 June 2025
Complete Documentation	Arshman Noor	Completed Documentation	14 June 2025

CONTENTS

LIST OF TABLES

LIST OF FIGURES

DEFINITIONS AND ACRONYMS

Table 1: Table of acronyms and definitions

ACRONYM	DEFINITION
CDPS	Crime Detection & Prevention System
UMT	University of Management and Technology
GUI	Graphic User Interface
ML	Machine learning
CV	Computer Vision
CNN	Convolutional Neural Networks
DNN	Deep Neural Network
FYP	Final Year Project
POF	Proof of Work
HOG	Histogram of Oriented Gradient
SLCV	Surveillance & logging Using Computer Vision
NLP	Natural Language Processing

1. INTRODUCTION

1.1 Motivations

The main motivation behind this project is to reduce crime rates by imposing artificial intelligence (AI) systems. This project aims to introduce an inventive solution which enhances the efficiency of crime detection and prevention through real-time alerts about anything suspicious. By automating the monitoring process, this system reduces the need for humans to observe each and every surveillance camera. AI generated alerts enable targeted monitoring of specific cameras which allow the quick verification through surveillance footage.

This system will enhance efficiency, saves time, workforce required to monitor cameras and reduces human errors. Further, to support victims of crimes especially those who are not comfortable in talking or sharing consequences with authorities directly, integrating a chatbot. So, victims can communicate in a safer way and update the authorities about the situation.

This solution aims to create safer communities by timely detection of crime and compassionate victim support.

1.2 Project Overview

This project aims to introduce an inventive solution which enhances the efficiency of crime detection and prevention through real-time alerts about anything suspicious. By automating the monitoring process, this system reduces the need for humans to observe each and every surveillance camera. AI generated alerts enable targeted monitoring of specific cameras which allow the quick verification through surveillance footage. This system will enhance efficiency, saves time, workforce required to monitor cameras and reduces human errors. Further, to support victims of crimes especially those who are not comfortable in talking or sharing consequences with authorities directly, integrating a chatbot. So, victims can communicate in a safer way and update the authorities about the situation. This solution aims to create safer communities by timely detection of crime and compassionate victim support.

1.3 Problem Statement

Now a days crime has become a big problem to control, especially when it takes too long to detect and respond to it. In Traditional crime prevention methods authorities watch each & every security camera, which can be slow, costly, and sometimes human error can occur. If a crime is not detected on time, the police may take longer to respond, which makes harder to stop the situation in time.

To overcome this problem, we are introducing an AI-powered crime detection system that works in real-time. It uses security cameras to automatically spot suspicious activities and quickly alert the authorities by sending an alert in seconds. Further, to support victims of crimes especially those who are not comfortable in talking or sharing consequences with authorities directly, integrating a chatbot. So, victims can communicate in a safer way and update the authorities about the situation. By making crime detection faster, it reduces the human error and workforce required to monitor cameras, supporting victims resulting into a safer community.

1.4 Objectives

The main goal of CDPS is to detect & prevent crime on time which results into public safety, lowering the workforce cost, reducing human errors by surveillance monitoring and detecting anything suspicious like fire, weapon detection, gunshot, red alert number plates in real-time and sending an immediate alert to the authorities.

When the authorities receive an alert, an officer monitoring the screen check that specific camera for confirmation and after confirmation he will send the team at location to stop the crime, saving the victims and investigating the situation. In this way, CDPS helps the authorities to prevent the crime from happening or any big loss.

An AI Chatbot is also integrated with the system which help the victims, especially those who don’t feel comfortable in talking directly to a human. In this way, victims can talk about the situation, their feelings, what actually happened at the spot without communicate directly to a human.

In this way CDPS makes the community safer, reducing human errors, helping victims and lowering the cost.

2. Domain Analysis

2.1 Customer

The primary heirs of this project are government & private security organizations, law enforcement agencies and those individuals who want to secure their homes, buildings and private properties to enhance safety and security. Furthermore, this project offers a secure platform to hesitant victims to report crime and seek help without direct communication to any other human person.

2.2 Stakeholders

Table 2: list of stakeholders

Stakeholder	Role in System
Project development team	*A team of three members that are executing the development of the project*

2.3 Affected Groups with social or economic impact

1. **Law Enforcement Agencies:**

   The system enhances crime detection by reducing human errors, response time and optimize resource allocation.

2. **Private Security Firms:**

   Firms managing Large-Scale surveillance and responsible for any public, private security get advantage by reducing workforce and improved security operations.

3. **Crime Victims:**

   The Chabot provide a secure way of communication, helps in understanding the situation of victims.

4. **Business Owners & Institutions:**

   The system helps to prevent theft, vandalism and other crimes resulting fewer financial losses.

5. **Government & Policy Makers:**

   Crime detection system support better law enforcement strategies which improves the public safety.

2.4 Dependencies/ External Systems

This project relies on several external systems and technologies to function effectively:

1. **Surveillance Camera Systems:**

   For real-time monitoring CDPS requires an integration with existing surveillance cameras.

2. **AI and Machine Learning Models:**

   Advance AI & ML models are necessary for detecting something abnormal and generating real-time alerts

3. **Cloud Services:**

   Cloud based storage and processing power require for better data handling and remote access to surveillance feeds.

4. **Network Infrastructure:**

   A fast and stable internet connection is required for the transmission for video feeds, alerts and chatbot interaction.

5. **Law Enforcement Databases:**

   An access to criminal records and database may enhance he system efficiency and helps in detecting people, automobiles which are on red alert.

6. **Chatbot Frameworks:**

   The victim support chatbot relies on Natural Language Processing (NLP) technology for effective communication and responses.

7. **Mobile and Web Applications:**

   User-friendly interface is required for authorities and victims to interact with system efficiently.

2.5 Reference Documents

2.5.1 Related Projects

1. AI-Based Automatic Crime Detection System [1]
2. Chatbots for Crime Reporting [2]
3. AI-Driven Surveillance Systems [3]
4. AI-Powered Financial Crime Prevention [4]

2.5.2 Feature Comparison

Table 3: features comparison

SR NO.	Features	CDPS	AI-Based Automatic Crime Detection System	Chatbots for Crime Reporting	AI-Driven Surveillance Systems	AI-Powered Financial Crime Prevention	REMARKS
1	***Real-time Crime Detection***	*YES*	*YES*	*NO*	*YES*	*NO*	*Our AI-Powered Crime Detection System offers an efficient and victim centric approach compared to other existing solutions. Where most of the AI driven focus only on surveillance and law enforcement, our project provides real-time crime detection, analysis & an AI chatbot for victims. By automating alerts, it reduces human errors and workforce to monitor each & single surveillance cameras. In this way, CDPS reduces human error, workforce cost and improves efficiency.*
2	***Automated Alert System***	*YES*	*YES*	*NO*	*YES*	*YES*	
3	***AI Chatbot for Victims Assistance***	*YES*	*NO*	*YES*	*NO*	*NO*	
4	***Reduced Human Monitoring Effort***	*YES*	*YES*	*NO*	*YES*	*YES*	
5	***Integration with CCTV & Existing Systems***	*YES*	*YES*	*NO*	*YES*	*YES*	
6	***Facial & Behavioral Recognition***	*YES*	*YES*	*NO*	*YES*	*NO*	
7	***Crime Detection via AI Prediction***	*YES*	*NO*	*NO*	*NO*	*YES*	
8	***Cost & Workforce Efficiency***	*YES*	*YES*	*NO*	*YES*	*YES*	
9	***User Friendly Interface***	*YES*	*NO*	*YES*	*YES*	*NO*	

3. REQUIREMENTS ANALYSIS

3.1 Requirements

This section summaries the system's functional & non-functional requirements, capabilities and data handling specifications.

3.1.1 End Users, Operators, and Support Functions

- **End Users:**
  1. Law Enforcement Agencies.
  2. Victim Support Organizations.
  3. Security Agencies.
  4. Private Security Departments.

- **Operators:**
  1. System Administrators.
  2. AI System Managers.

- **Support & Integration Functions:**
  1. Automated Alerts.
  2. AI-driven Video Analysis.
  3. Chatbot for victim support.

3.1.2 Performance Requirements

1. Real-time processing of surveillance footage with an accuracy of 85%.
2. AI chatbot for victim support response time > 3 seconds per query.

3.1.3 Design Constraints

1. AI models should ensure minimal false positives/negatives.
2. Secure storage and processing of sensitive data.
3. System should be scalable for different crime detection scenarios.

3.1.4 Programming Language and Technologies

1. **Programming Languages:** Python
2. **AI Libraries:** TensorFlow, OpenCV, NLTK, PyTorch, scikit-learn
3. **Database:** Supabase with Postgre SQL
4. **Version Control:** GitHub

3.1.5 Interface Requirements

1. Web-based dashboard for law enforcement.
2. Mobile-friendly interface of Chatbot for victim support.
3. Integration with existing surveillance infrastructure.

Table 4: system functions

RID	Description	Category	Attribute	Details & boundary constraints
R1.1	***AI-based real-time crime detection through video surveillance***	*Functional*	*Response time*	*Anomaly detection in <5 seconds*
R1.2	***Automated alert system for suspicious activities***	*Functional*	*Notification speed*	*Alert generation <3 seconds*
R1.3	***AI chatbot for victim support***	*Functional*	*Response speed*	*Chatbot replies within 3 seconds*
R1.4	***Secure data storage***	*Non-functional*	*Compliance*	*Follows privacy regulations*

3.2 List of Actors

The actors represent users or external entities that will input data, receive alerts and interact with system.

Table 5: list of actors

Law Enforcement Officer	Monitors real-time crime alerts, verifies incidents, and takes necessary action.
Surveillance System Administrator	Manages the AI-powered smart surveillance system, including configuring camera feeds and monitoring analytics.
Crime Victim	Uses the AI chatbot for reporting crimes and receiving emotional or procedural support.
Security Personnel	Monitors private security infrastructure and receives alerts from the system for potential threats.
System Operator	Oversees the general system functionality, maintenance, and updates
External Law Enforcement Database	Provides historical crime records to enhance AI decision-making.
Public Safety Organization	Uses crime data to develop crime prevention strategies.
IT Administrator	Ensures the system remains functional, secure, and up-to-date.

3.3 List of use cases

Table 6: list of usecase

Use Case ID	Use Case Name	Description
UC-1	**Crime Detection & Alerting**	AI system monitors surveillance feeds & detect abnormal activities.
UC-2	**Automated Alert Notification**	When any criminal activity detected, real-time alert will send to the law enforcement officers.
UC-3	**Victim Crime Reporting**	Victims can use Chatbots to report crime securely without interacted to any human being.
UC-4	**User Authentication**	To access system functionalities, a login is required of law enforcement and administrators.
UC-5	**System Configuration**	Surveillance administrators can adjust AI parameters, monitoring rules and sensitivity.
UC-6	**Data Storage & Retrieval**	For future references, stores reported crimes and evidence securely.
UC-7	**Surveillance Feed Monitoring**	Users can review live surveillance footage manually alongside AI detected alerts for confirmation.
UC-8	**Chatbot Assistance**	Provides support to victims and collect necessary information.
UC-9	**Integration with Law Enforcement Database**	Connection with external crime databases to increase AI accuracy and crime pattern recognition.
UC-10	**User Role Management**	Administrator can assign different roles, boundaries and permissions for different types of users.
UC-11	**System Maintenance & Updates**	Administrator can monitor system health, updates and resolve technical issues.

3.4 System use case diagram

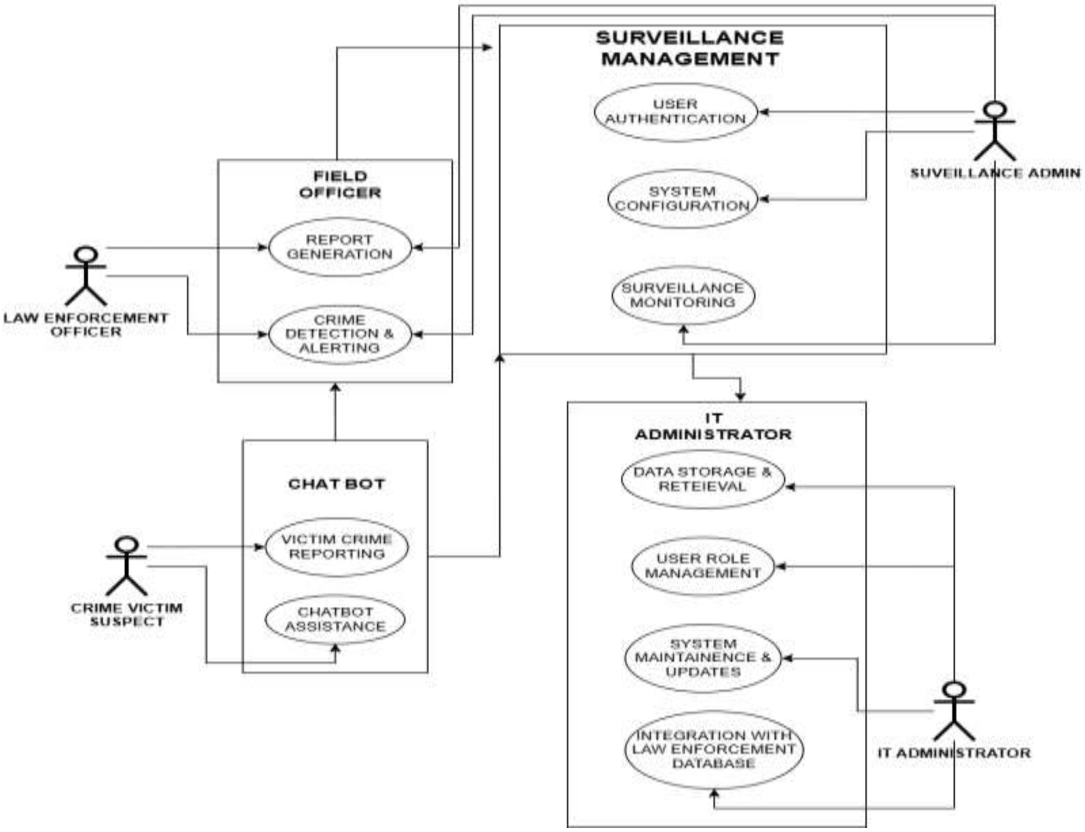


Figure 1: use case diagram

3.5 Extended use cases

Table 7: extended usecase CDPS-UC-1.1

Use Case ID:	CDPS-UC-1.1		
Use Case Name:	Detect and Alert Suspicious Activities		
Created By:	Arshman Noor	**Last Updated By:**	Arshman Noor
Date Created:	19 January, 2025	**Last Revision Date:**	18 February, 2025
Actors:	Law Enforcement Officer, System Administrator		
Description:	The AI system analyzes live footage of surveillance using advanced pattern recognition to detect abnormal activities. An alert will automatically be generated including timestamp, location, camera number, and a classification of the threat/crime and sent to law enforcement officers or headquarters on the detection and identification of a threat. This enables rapid assessment and response by authorities. The system logs all the detected incidents in a safe and secure database for future needs, contributing to improve prevention strategies and more efficient law enforcement operations.		
Trigger:	The AI system continuously cans surveillance feeds, recognizing patterns and detecting abnormalities that may specify criminal activities, which then triggers an alert for further investigation.		
Preconditions:	1. Surveillance cameras should be active and connected to the system. 2. AI model must be trained and operational.		

	3. For real-time processing system must have stable and high speed network connectivity. 4. Law enforcement workforce must be registered and authenticated in the system. 5. An access to historical crime database for AI pattern analysis.
Post conditions:	1. An alert is generated and forwarded to headquarters and law enforcement officers. 2. Surveillance feed is stored for future needs. 3. A report generated and made available to law enforcement. 4. Surveillance feed stored which may help in further investigation.
Normal Flow:	1. The system continuously processes live feeds. 2. Based on predefined patterns, AI detects abnormal activity. 3. On detecting abnormal activities, the system generates an alert and notifies the headquarters. 4. Officers verifies the alert and responds accordingly.
Alternative Flows:	**AF1: False Positive Detection** 1. If an alert is determined to be a false positive, the officer marks it as resolved. 2. The AI model is retrained to improve accuracy. **AF2: Low Confidence Alert** 1. In step 3 of the normal flow, if the AI system is unsure about an alert, it sends it for manual review. 2. A human operator validates or dismisses the alert before notifying law enforcement. **AF3: High-Priority Incident** 1. In step 3 of the normal flow, if a detected activity matches a high-priority crime pattern, an urgent alert is sent. 2. Law enforcement receives immediate notifications with live video feed access. **AF4: System Downtime** 1. If the system goes offline, an automatic alert is sent to the IT administrator. 2. The system attempts to restart, and a backup mode is activated for basic surveillance. **AF5: Restricted Area Breach** 1. If AI detects unauthorized access to a restricted area, a specific security protocol is triggered. 2. Security personnel are alerted, and automated lockdown procedures may be initiated.
Exceptions:	1. The system logs an error and sends a system health alert if the surveillance system gets offline. 2. An emergency mode with human monitoring activated if AI fails to process video feeds due to any error like poor image quality and connection error. 3. The system forwards an alert to higher authorities if the alert is not acknowledged within a set time. 4. Alerts and logs will store temporarily in a local backup in case of database inaccessibility. 5. If the chatbot fails to interpret victim input correctly, it redirects to a human operator for assistance.
Includes:	User Authentication (UC-4), Data Storage & Retrieval (UC-6)
Frequency of Use:	Continuous operation.

Special Requirements:	Real-time processing, Stable Network, High computational power, Access to Law enforcement database.
Assumptions:	The AI model is accurate enough to minimize false positives and false negatives.
Notes and Issues:	What is the threshold for detecting suspicious activities?

Table 8: extended usecase CDPS-UC-2.1

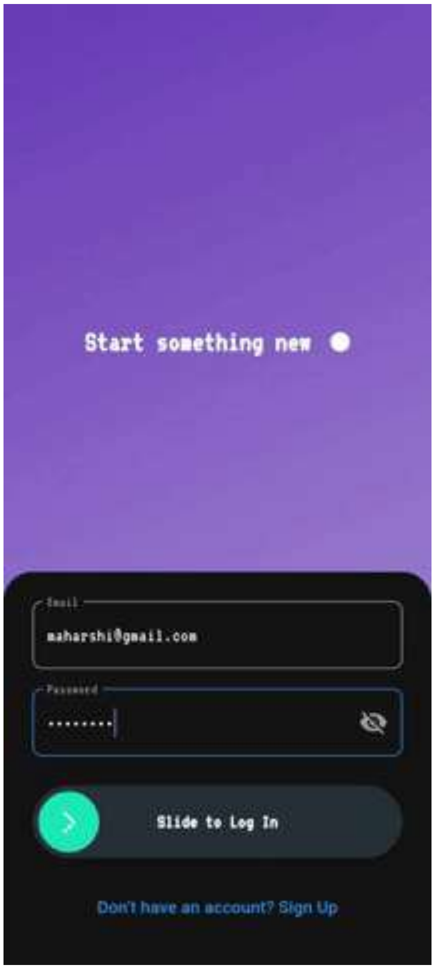
Use Case ID:	CDPS-UC-2.1		
Use Case Name:	Report Crime via Chatbot		
Created By:	Arshman Noor	**Last Updated By:**	Ahmed Nadeem
Date Created:	3 February, 2025	**Last Revision Date:**	19 February, 2025
Actors:	Crime Victim (Primary), Law Enforcement Officer (Secondary)		
Description:	The AI chatbot offer user-friendly interface for a victim to report a crime and talks about the situation to authorities without direct human interaction. It systematically collects the details like location, time, type of crime, and any relevant evidence before filing the report. The system verifies the provided data, cross-referencing it with existing records for accuracy and consistency. After verification, the report is forwarded to law enforcement with the categorization tags, sensitivity level and relevant data. This ensures fast and secure communication and help those victims who don't feel comfortable in talking to an officer or human being directly.		
Trigger:	A victim starts communication with Chatbot to report a crime.		
Preconditions:	1. The chatbot must be active and operational. 2. The victim must have an internet access and compatible device to start chat with chatbot. 3. Law enforcement officer's registration is required for receiving reports. 4. A secure data storage must be available to log crime reports. 5. AI chatbot must be trained to interpret different types of crime reports.		
Post conditions:	1. The system has successfully recorded the crime report. 2. The victim is provided with emergency contacts or appropriate guidance. 3. Law enforcement is informed of pertinent case information. 4. A preliminary criminal report is created by the system for a further inquiry. 5. An officer is tasked with following up with the victim if required.		
Normal Flow:	1. The victim uses his mobile app or website to access the chatbot. 2. The chatbot prompts the victim for crime details, location and urgency. 3. The victim provides details about the crime. 4. The system verifies and logs the crime details into the database. 5. Law enforcement is notified and assigned to review the report. 6. The chatbot provides further assistance, such as legal advice or emergency numbers.		
Alternative Flows:	**AF1: Victim Disconnects Before Completing Report** 1. The chatbot saves important details for future sessions. 2. The chatbot resumes the report from the last recorded step on the return of victim. **AF2: Emergency Case Detection** 1. The chatbot immediately directs the victim to emergency services if it identifies an emergency (e.g., ongoing assault). 2. For immediate response a high-priority alert will be sent to law enforcement.		
Exceptions:	1. The victims are redirected to an alternative manual reporting method if chatbot service is offline. 2. The chatbot requests clarification or offers human assistance if the victim provides unclear responses. 3. The system forwarded the report if the law enforcement fails to acknowledge		

	the report.
Includes:	User Authentication (UC-4), Data Storage & Retrieval (UC-6)
Frequency of Use:	On demand.
Special Requirements:	For data privacy use secure encryption, for better accessibility it should be multilingual.
Assumptions:	Victims will provide honest and accurate crime reports.
Notes and Issues:	1. How will the system ensure chatbot responses remain sensitive and accurate? 2. What measures are in place for false reports or misuse of the chatbot?

3.6 User interfaces (mock screens)

1. **Crime Reporting Chatbot (P1)**

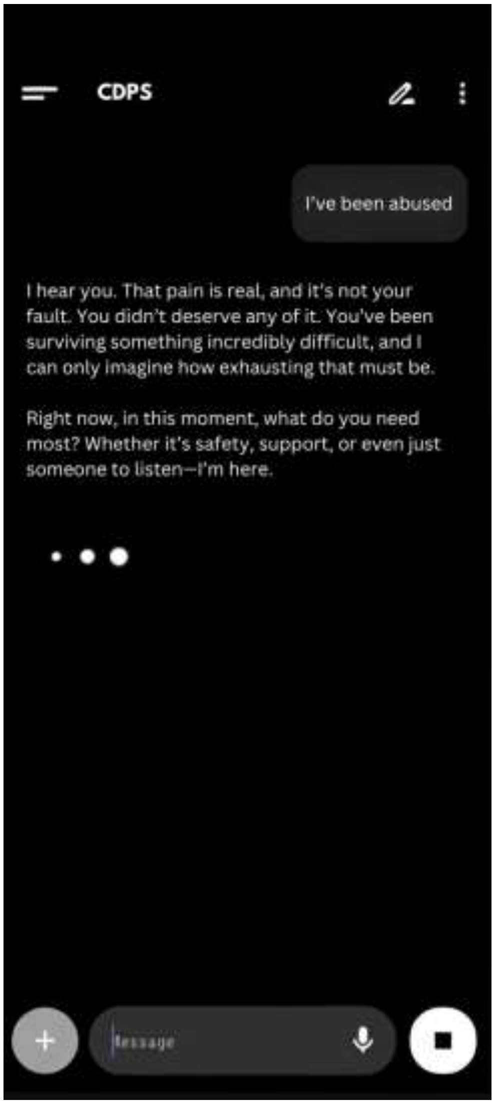
Victims interact with AI powered Chatbot.



Email: maharshi@gmail.com

Password: ••••••••

Prototype 1: Login Screen



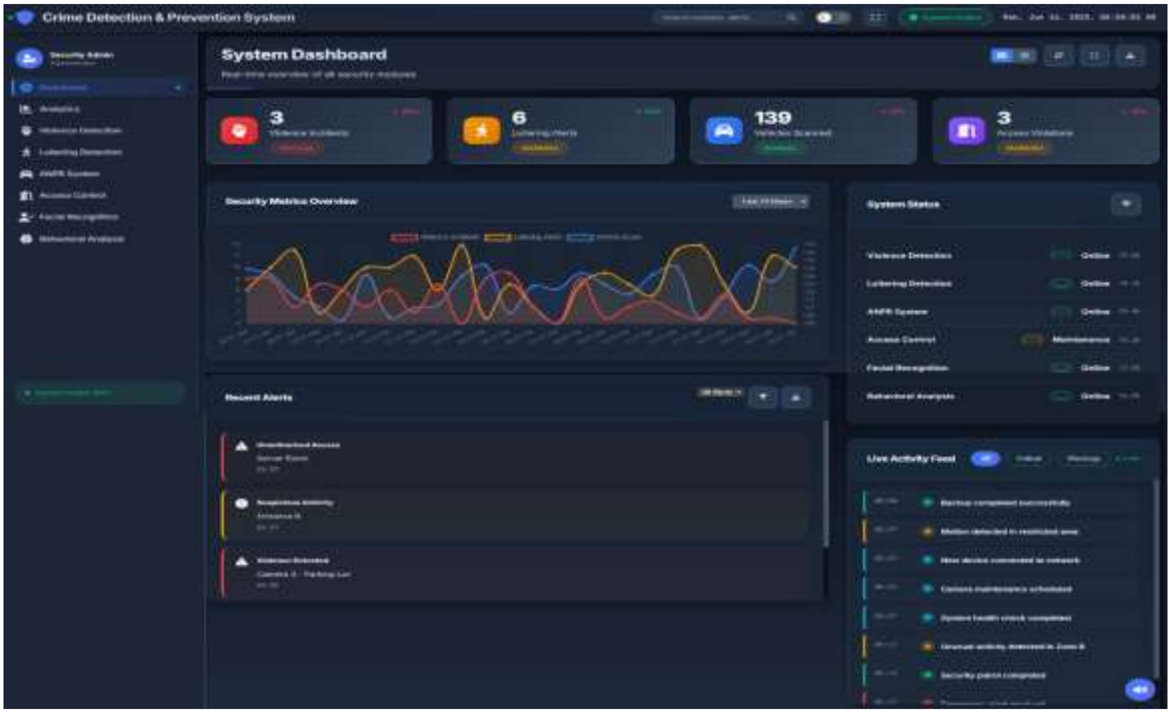
I've been abused

I hear you. That pain is real, and it's not your fault. You didn't deserve any of it. You've been surviving something incredibly difficult, and I can only imagine how exhausting that must be.

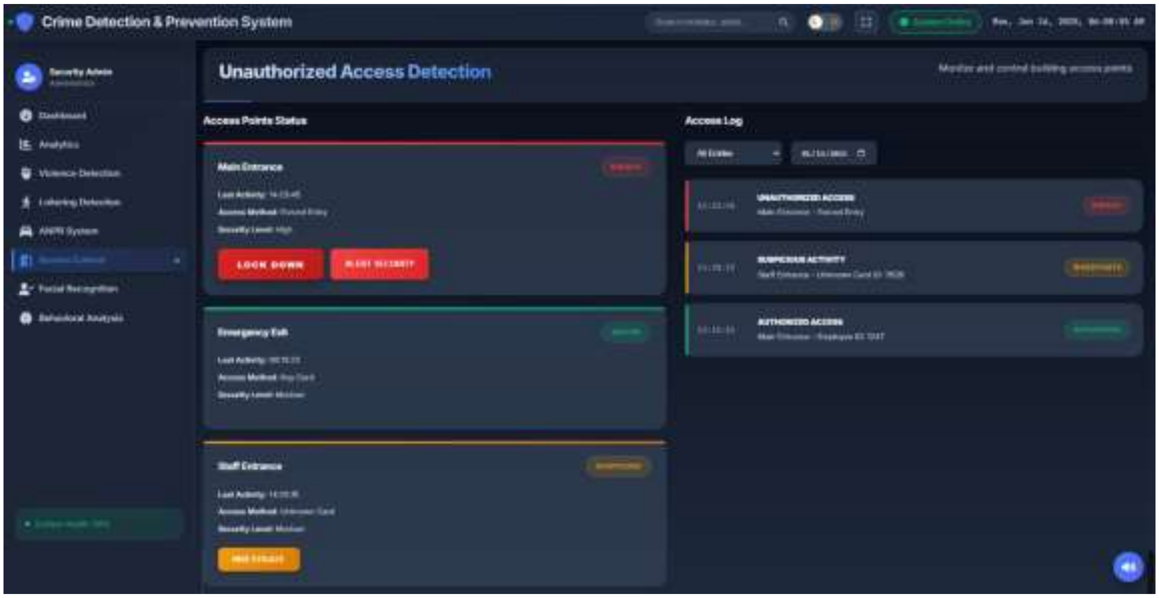
Right now, in this moment, what do you need most? Whether it's safety, support, or even just someone to listen—I'm here.

Prototype 2: Asking a query

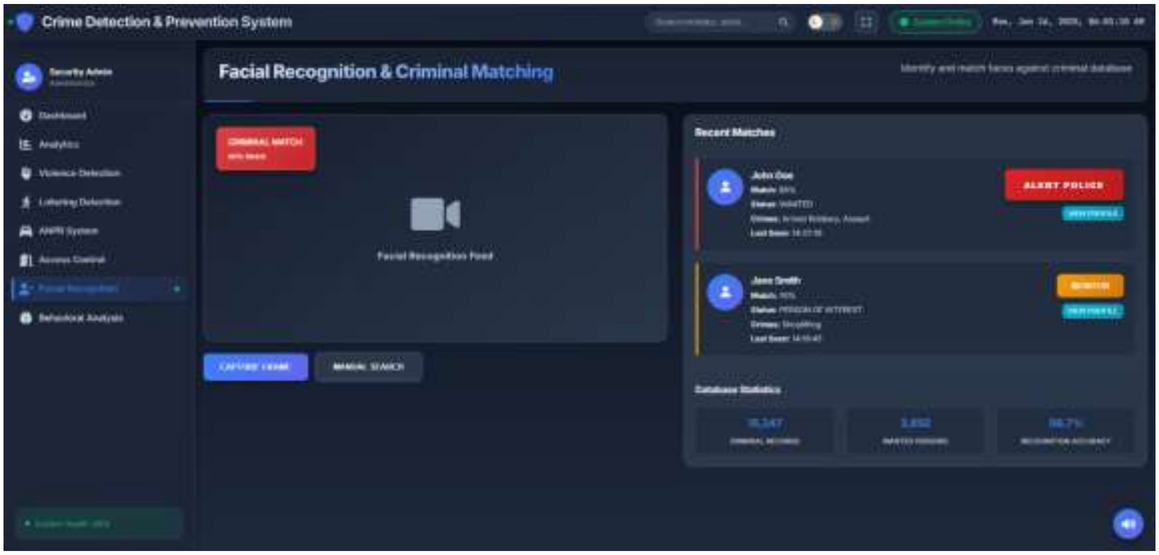
2. **Surveillance System (P2):**



Prototype 3: Admin Dashboard



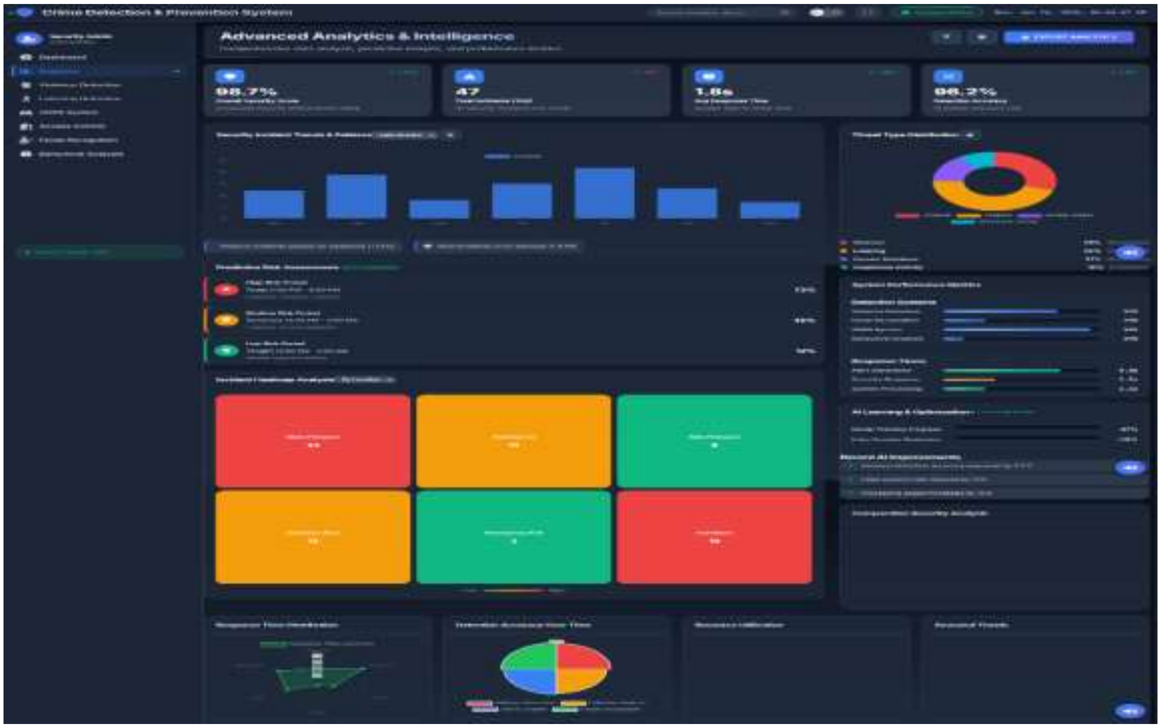
Prototype 4: Access Control



John Doe
Status: WANTED
Crimes: Armed Robbery, Assault

Jane Smith
Status: PERSON OF INTEREST
Crimes: Shoplifting

Prototype 5: Facial Recognition


Crime Detection & Prevention System
Advanced Analytics & Intelligence
98.7%
47
1.8s
96.2%
Security Incident Trends & Patterns
Threat Type Distribution
Predictive Risk Assessment
Incident Heatmap Analysis
System Performance Metrics
AI Learning & Optimization
Response Time Distribution
Detection Accuracy Over Time
Resource Utilization
Seasonal Trends

Prototype 6: Analytics

4. SYSTEM DESIGN

4.1 System Architecture Diagram

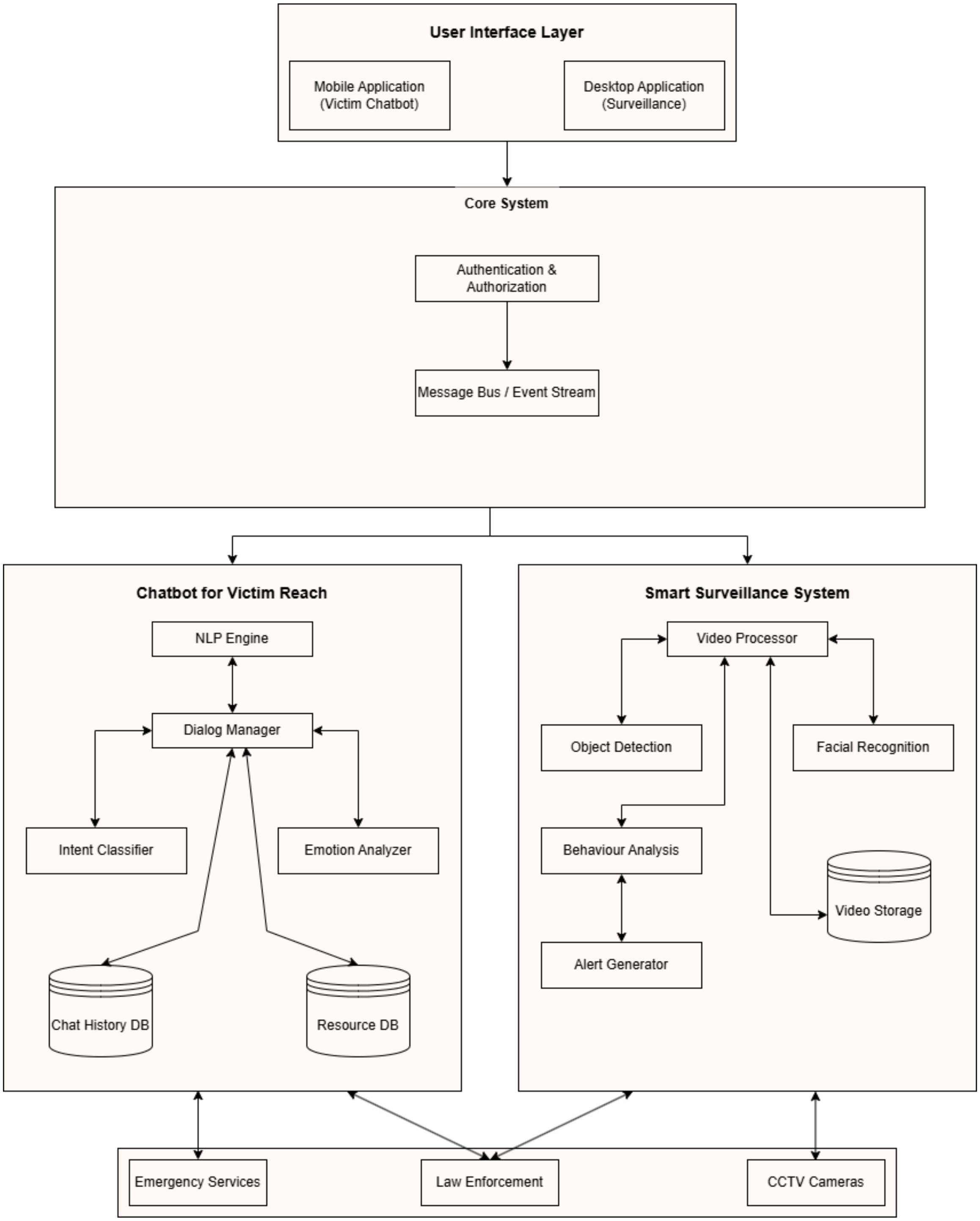


Figure 2: system architecture diagram

4.2 Class Diagram

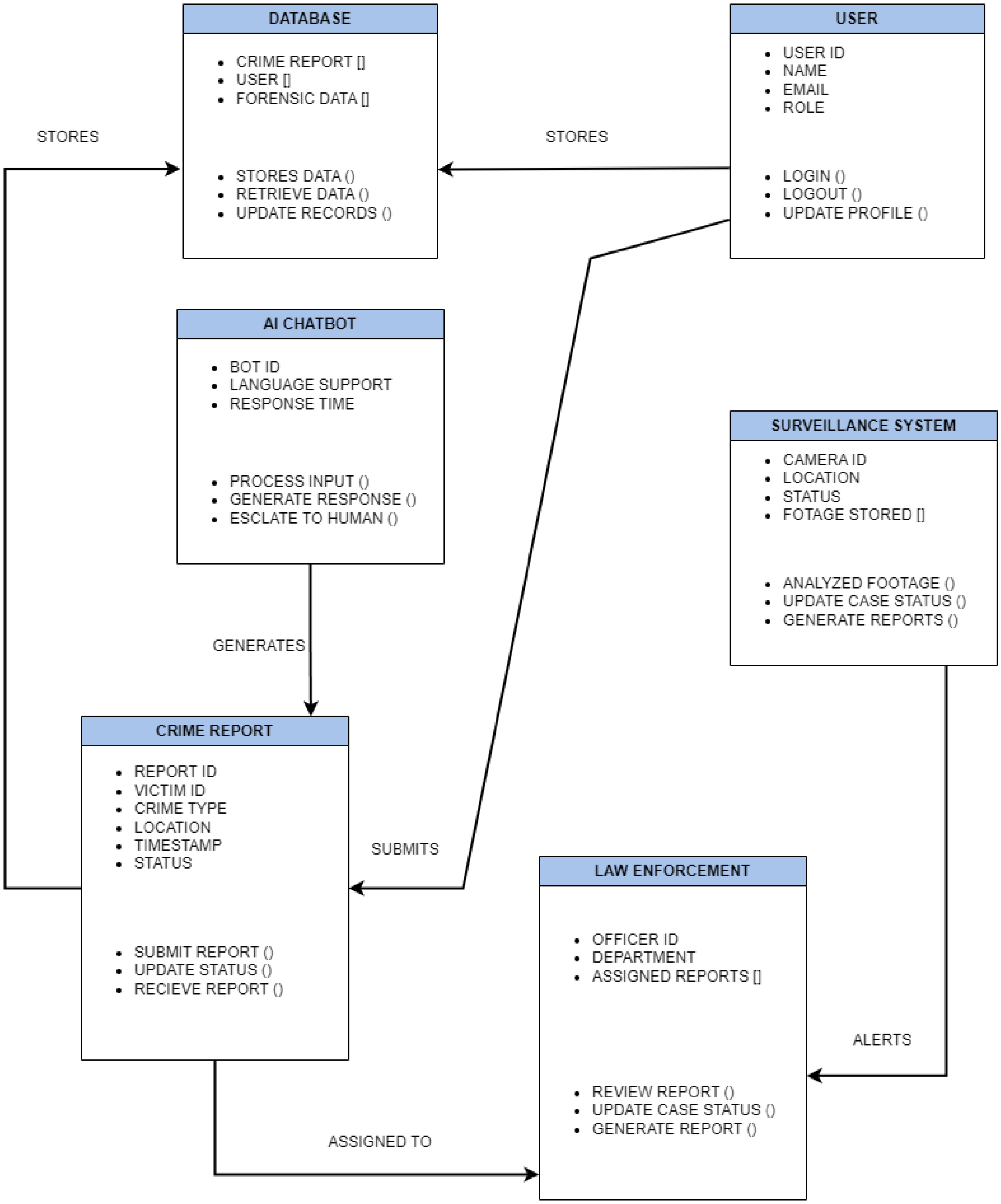


Figure 3: class diagram

4.3 Sequence Diagrams

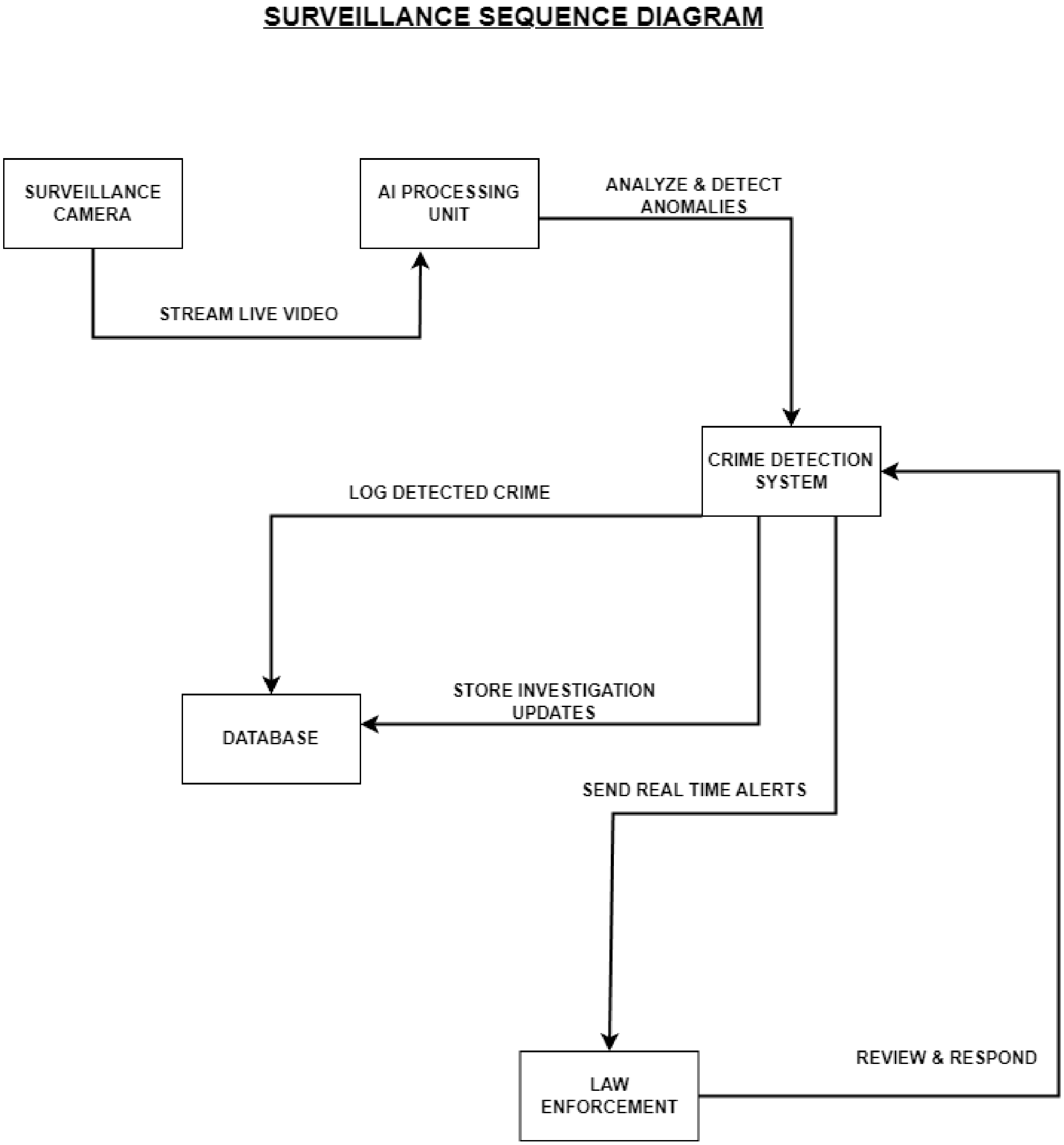


Figure 4: surveillance sequence diagram

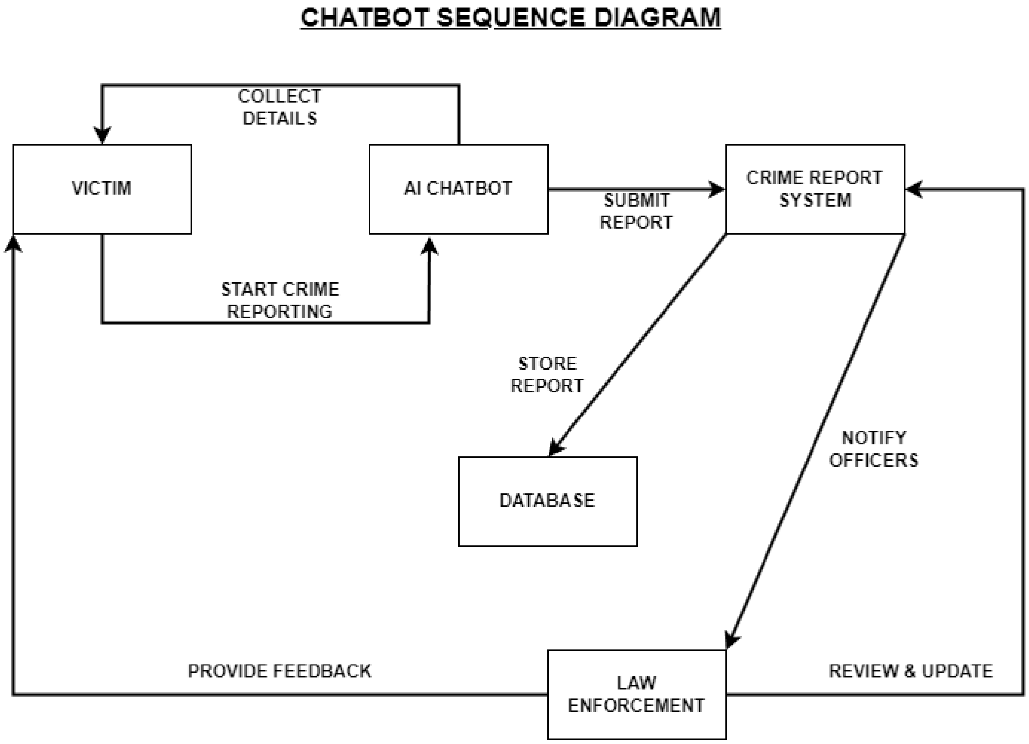


Figure 5: chatbot sequence diagram

4.4 Collaboration Diagrams

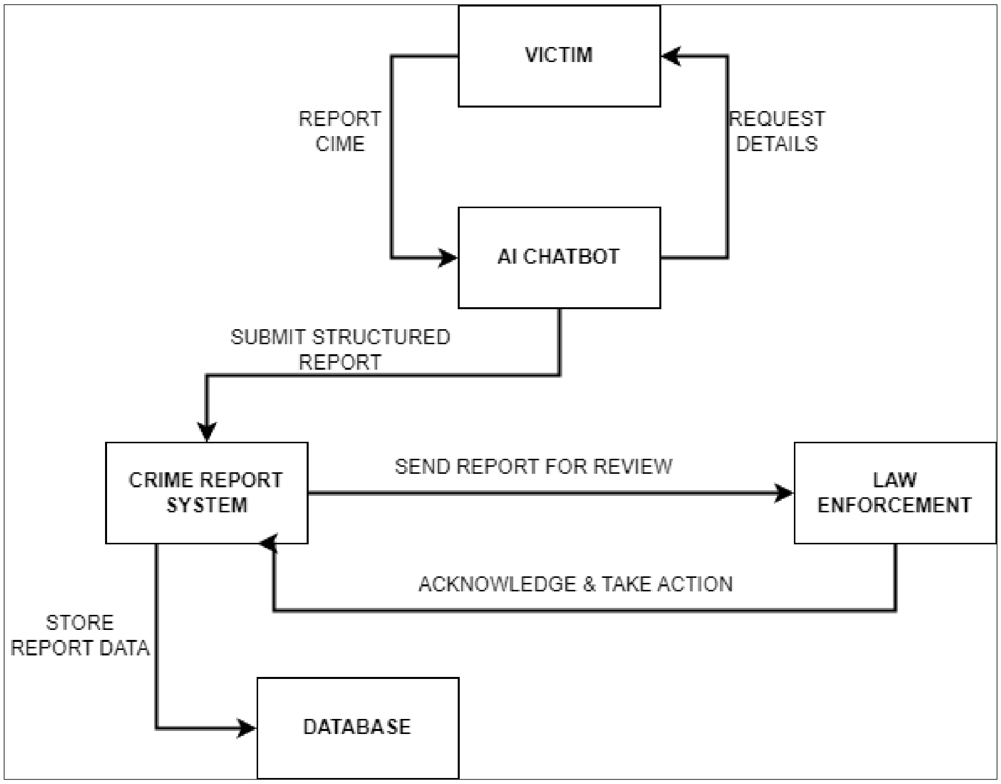


Figure 6: chatbot collaboration diagram

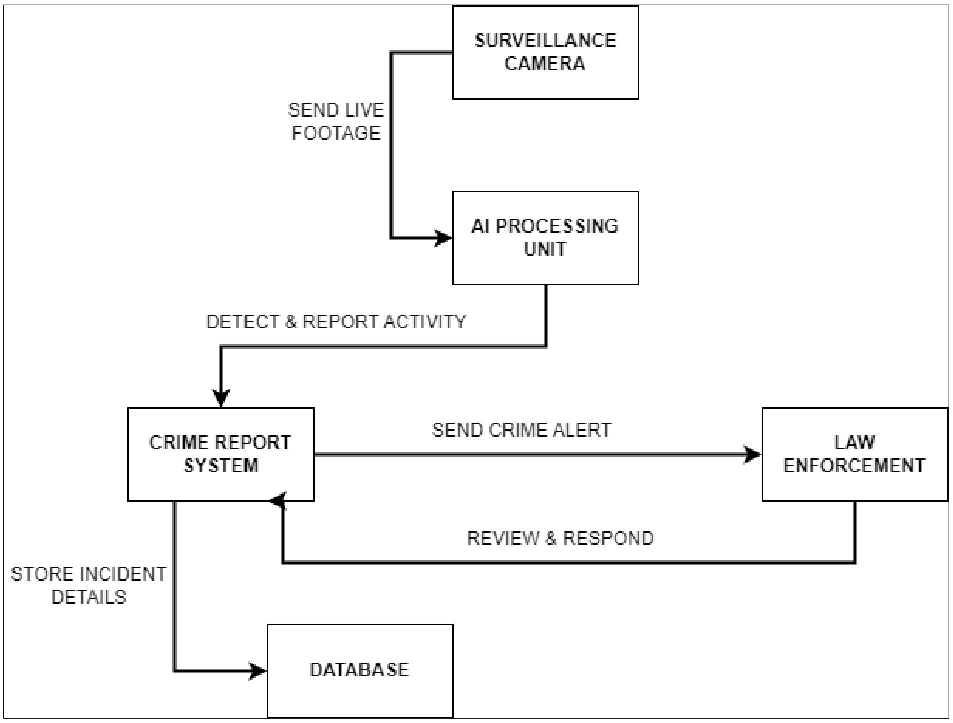


Figure 7: surveillance collaboration diagram

4.5 Other UMLs

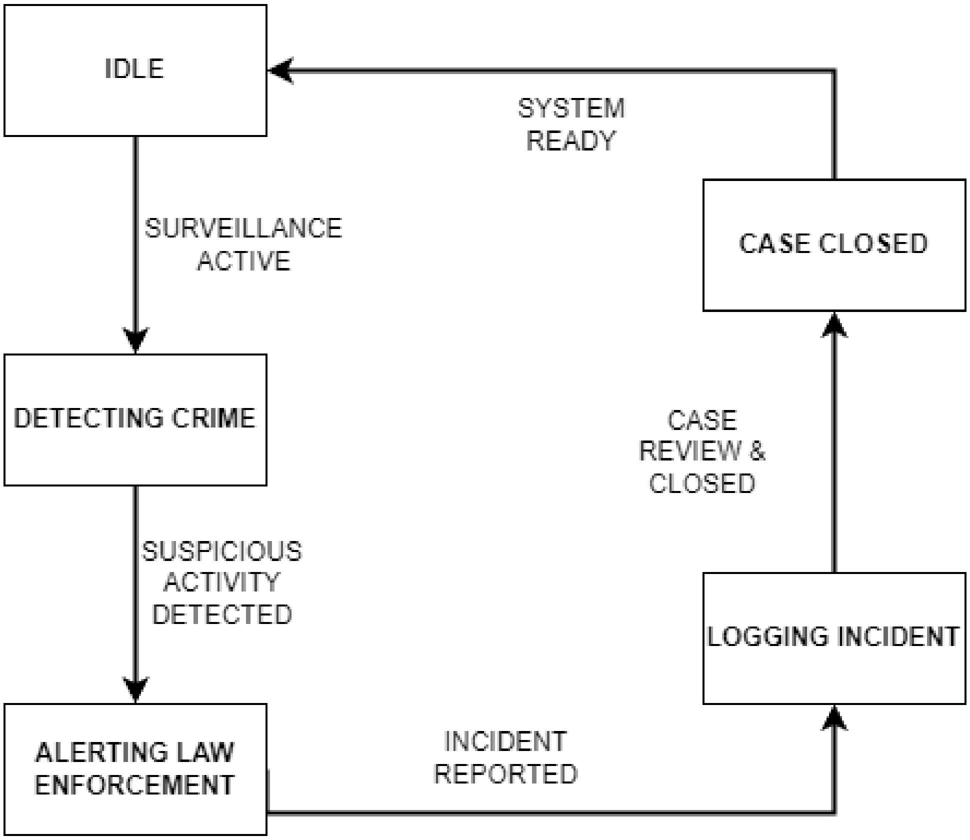


Figure 8: surveillance system uml

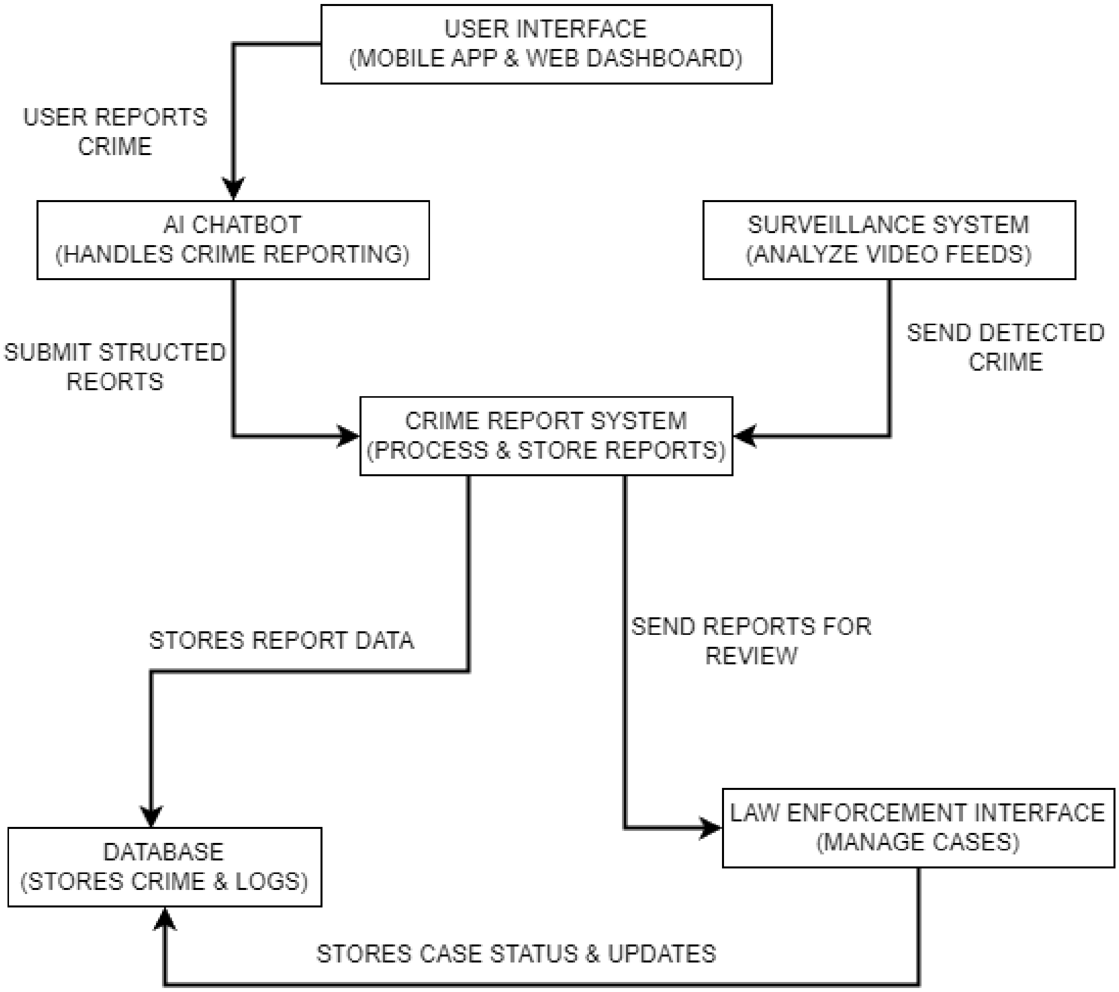


Figure 9: component diagram

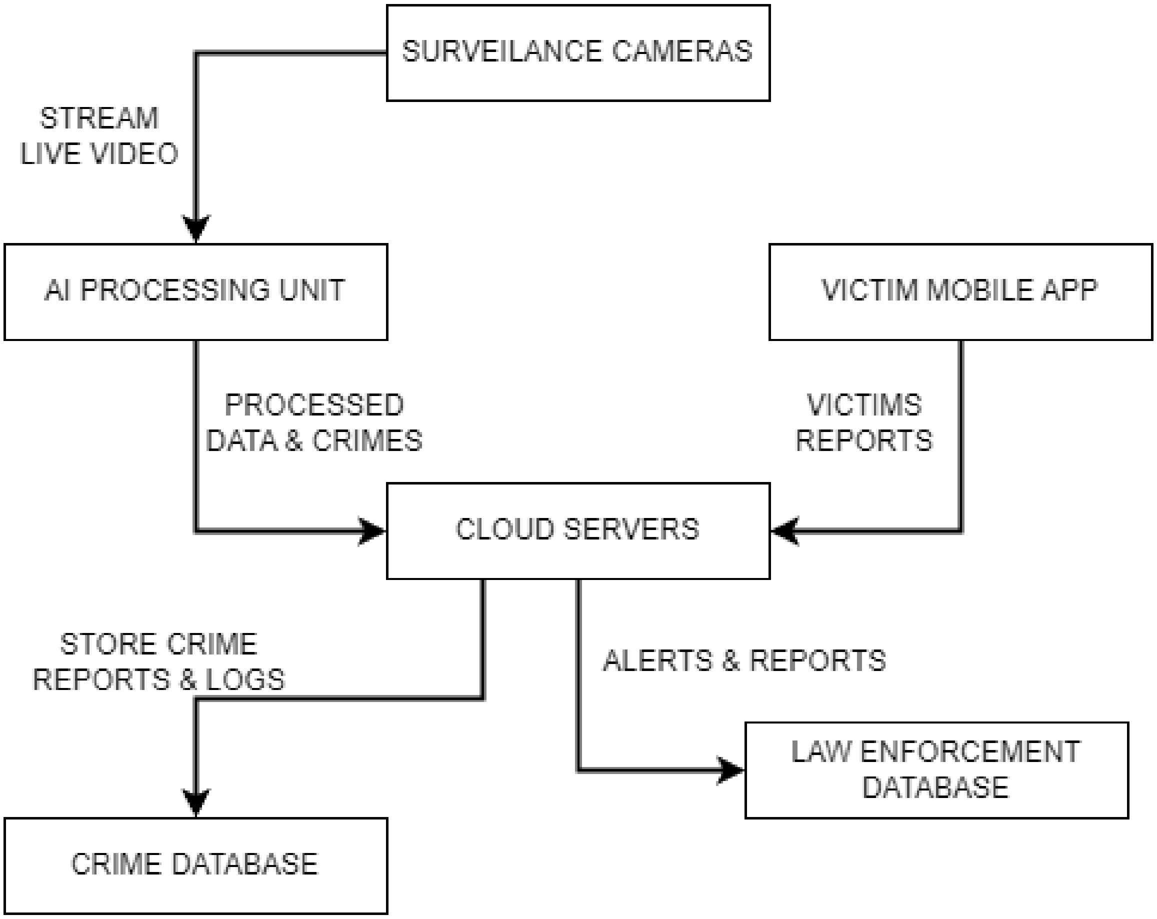


Figure 10: deployment diagram

4.6 ERD

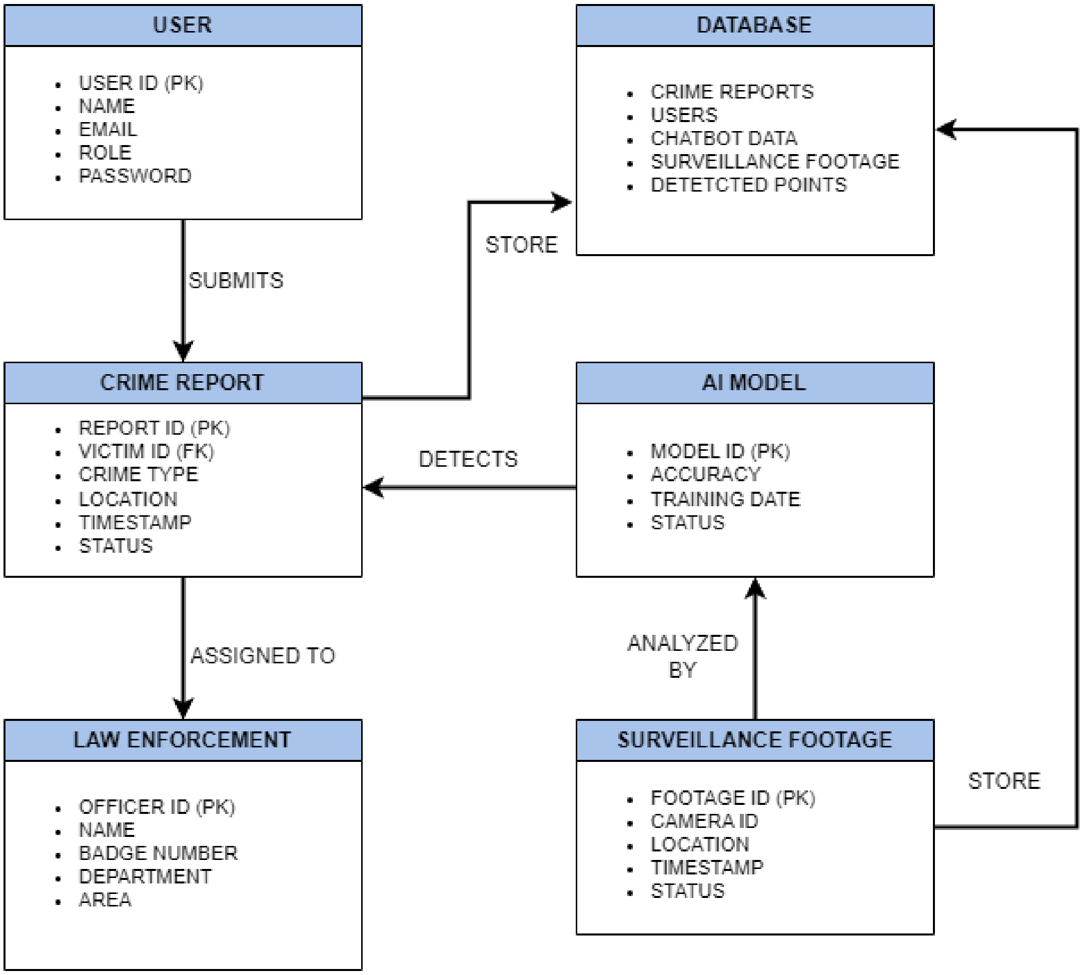


Figure 11: erd diagram

4.7 Data Dictionary

Table 9: data dictionary

Element Name	Type	Validation	Mandatory	Remarks
Username	Text Field	Must be a valid email format (user@example.com)	*Yes*	For Authentication
Password	Password Field	Minimum 8 characters, at least one digit and special character	*Yes*	Encrypted for security
Login Button	Button	Enable only if fields are valid	*Yes*	Initiates authentication process
Crime Type	Dropdown	Predefined categories (e.g., Theft, Assault, Fraud)	*Yes*	Helps in classification of crimes
Location	Text Field	Must be valid address or GPS coordinates	*Yes*	Autofill (if GPS enabled)
Incident Timestamp	Date / Time Picker	Must be a valid date-time format	*Yes*	Captures exact time of incident reporting
Upload Evidence	File Upload	Accepts images, videos (50 MB, JPG, PNG, MP4, MOV)	*No*	Optional but helps in investigation
Submit Report	Button	Enabled if mandatory fields are filled	*Yes*	Sends crime report to database
Chatbot Input	Text Field	No offensive words allowed	*No*	Auto-correct enabled for user clarity
AI Alert Notification	Pop-Up	Displays real-time alerts	*Yes*	Visible to only Authorized users
Law Enforcement Dashboard	Ui Panel	Displays reports, alerts & crime analytics	*Yes*	Only accessible to authorized users
System Logs	Hidden Field	Stores user actions & timestamps	*Yes*	For security monitoring
Case Status	Dropdown	Open, Under Investigation, Closed	*Yes*	Helps to track progress of case reported
Suspect Description	Text Field	Minimum 5 characters requires	*No*	Provide details of suspects
Emergency Contact	Text Field	Must be a valid phone number (e.g., +92 304 9990123)	*No*	To enable quick communication with victims
AI Crime Prediction	System Output	Uses past data to predict crime trends	*No*	Helps law enforcement in crime prevention

Incident Report ID	Auto-generated	Unique identifier for each crime report	*Yes*	Automatically assigned upon report submission
Case Assignment	Dropdown	List of officers assigned to the case	*Yes*	Ensures accountability and tracking
Evidence Review	UI Panel	Allows law enforcement to view submitted evidence	*Yes*	Used for validation and case building
User Role Management	Admin Panel	Allows assignment of roles & permissions	*Yes*	Managed by system administrators

5. IMPLEMENTATIoN DETAILS

5.1 Development Setup

1. **Programming Language:**

- **Python**
  - Used as primary language for backend development, integration of AI and system logics.

2. **AI Libraries / Frameworks:**

- **TensorFlow, Keras, Pytorch**
  - Used for building and training deep learning models (eg. For behaviour analysis).
- **OpenCV, Pillow, Yolo**
  - Used for image and video processing.
  - Object detection & loitering detection.
- **SciPy, Scikit-image**
  - Used for NLP tasks in ChatBot module and pattern recognition.
- **Matplotlib, Seaborn**
  - Used for visualization and analysis.

3. **Database:**

- **Supabase with PostgreSQL**
  - For structured data storage like user logs, reports and chat integractions.

4. **Version Control:**

GitHub

5. **Operating Systems:**

Microsoft Windows, Android

5.2 Deployment setup

- Integration with Existing Surveillance Systems.
- A web dashboard for law enforcement officers.
- A mobile accessible chatbot app or interface for victims.

Problems Faced & How They Were Overcome:

- **System Downtime** (as mentioned in alternative flows):
  - Handled by sending alerts and switching to backup surveillance mode.

- **Chatbot Errors**:
  - Redirected to human operators if AI failed to interpret input.
- **False Positives in Detection**:
  - Officer marks alerts as resolved.

5.3 Algorithms

Suspicious Activity Detection Algorithm:

- Uses pattern and behavioral analytics on live camera feeds.
- Triggers alerts with time stamps, camera IDs and threat classification. (YOLOv8, Tensorflow/Keras, Buffalo)

Chatbot Crime Reporting Flow:

- NLP models for understanding and processing user inputs.
- Maps input to crime types, location, urgency and generates structured reports.

Red Alert Recognition (License Plates, etc.):

- Use object recognition and database matching to detect flagged elements. (FastANPR)

5.4 Constraints

5.4.1 Assumptions

- AI models are assumed to sufficiently accurate to minimize false positive/negatives.
- Stable and highspeed internet will be available for real-time video feed processing.
- Victims will provide accurate and honest information to chatbot.
- Officers will be registered and available to respond to alerts.

5.4.2 System constraints

- System must work in real-time with anomaly detection under 5 seconds.
- Chatbot must response in less than 3 seconds per query.
- Must be compatible with existing infrastructures.
- Must maintain data privacy and security as per legal standards.

5.4.3 Restrictions

- No real-time integration with external accounting or financial system.
- Only registered users can access sensitive data or features.
- Only predefined crime types and suspects can be selected from dropdowns.

5.4.4 Limitations

- Cannot operate without active surveillance cameras.
- Cannot operate without stable internet.
- Chatbot may misunderstand victim inputs.
- System cannot autonomously enforce or take legal action.

- Only works with CCTV footage format (.AVI, .MOV, .TS).

6. TESTING (IN PROGRESS)

6.1 Extended Test Cases

Test Case ID: TC_01	**Test Design by:** Arshad Mehmood
Test Module Name:	**Test Design Date:** 17/5/2025
Test Priority:	**Test Executed by:** Arshad Mehmood
Test Title/Name:	**Test Executed Date:** 12/6/2025
Description:	

Pre-condition:						
Dependencies						
Step	**Test Step**	**Test Data**	**Expected Result**	**Actual Result**	**Status (Pass/Fail)**	**Notes**
1	Turn on the system			.		
2						
3						
4						
Post Condition:						

Test Case ID: TC_01			**Test Design by:** Arshad Mehmood			
Test Module Name:			**Test Design Date:** 19/5/2025			
Test Priority:			**Test Executed by:** Arshad Mehmood			
Test Title/Name:			**Test Executed Date:** 13/6/2025			
Description:						
Pre-condition:						
Dependencies						
Step	**Test Step**	**Test Data**	**Expected Result**	**Actual Result**	**Status (Pass/Fail)**	**Notes**
1	Turn on the system			.	PASS	
2						
3						
4						
Post Condition:						

6.2 Decision Table

6.2.1 Code snippet

6.2.2 Decision coverage table

Decision Condition	True Action	False Action
Is suspicious activity detected?	Generate alert and notify officers	Continue monitoring
Is the user authenticated?	Allow access to system	Show error or deny access
Is it a high-priority emergency report?	Send urgent notification to law enforcement	Process as normal priority
Is the chatbot able to understand victim input?	Proceed with crime report flow	Redirect to human operator
Is network connectivity available?	Send real-time alerts	Store locally and retry later
Is the law enforcement officer available to respond?	Assign task and show report	Store alert and retry later

Table 10: Decision Coverage

6.3 Traceability Matrix

6.3.1 RID vs UCID (requirements vs use cases)

Requirement ID	Use Case ID	Description
R1	UC-1	Detect and alert suspicious activity via AI
R2	UC-2	Send alerts to law enforcement in real-time
R3	UC-3, UC-8	Chatbot for crime reporting and emotional support
R4	UC-6, UC-9	Evidence storage and integration with external databases
R5	UC-4, UC-6, UC-11	Secure login, case logs, and system maintenance

Table 11: RID vs UCID

6.3.2 Test Cases (RID vs TID)

Requirement ID	Test Case ID	Test Case Description
R1.1	T1	Test if the system detects a person loitering
R1.2	T2	Test if alert is generated within 3 seconds
R1.3	T3	Test chatbot response time < 3 seconds
R1.4	T4	Test if evidence is processed in < 10 seconds

Requirement ID	Test Case ID	Test Case Description
R1.5	T5	Check secure data storage and privacy compliance

Table 12: RID vs TID

6.3.3 Coverage (UCID vs TID)

Use Case ID	TID Test Case ID	Test Case Description
UC-1	T1, T2	Detect & alert suspicious activity
UC-2	T2	Automated real-time alert
UC-3	T3	Victim reports crime via chatbot
UC-4	T5	User authentication flow
UC-6	T4, T5	Store and retrieve crime reports and evidence
UC-8	T3	AI Chatbot assisting victims

Table 13: UCID vs TID

7. RESULTS/OUTPUT/STATISTICS

7.1 100% completion

7.2 92% accuracy

7.3 92% correctness

8. CONCLUSION

The Crime Detection & Prevention System (CDPS) use AI-driven technologies to successfully addresses some key challenges in traditional surveillance and crime reporting. The system is capable of detecting suspicious behavior in real-time and notifying law enforcement within seconds, reducing human workforce, response time and error rates by the integration of machine learning, computer vision and natural language processing.

For supporting victims to report crimes, especially for those who feel uncomfortable with face-to-face interactions, an AI- powered chatbot offers a secure and private channel. This system not only help to detect and prevent crimes but also support victims to report and assists law enforcement in acting swiftly and efficiently.

This project validates how smart surveillance and automated alert system can contribute to building safer communities with lower manpower dependency and improved situational awareness.

9. FUTURE WORK

Future work for the CDPS system could involve several aspects:

- **Use Cloud Services** – for better storage, speed and access from anywhere.
- **Mobile App for Police** – Officers can get alerts and updates on their phones.
- **Add More Languages** – So more people can use the chatbot easily.
- **Voice Chatbot** – So victims speak instead of typing, with emotion detection.
- **Work without Internet** – Use edge devices for areas with poor network.
- **Crime Prediction** – Show areas where crimes might happen next.
- **Allow Public Tips** – Let people report suspicious activity anonymously.
- **Connect with Police Databases** – To improve face and license plate recognition.

10. BIBLIOGRAPHY

1. AI-Based Automatic Crime Detection System, “AI-Based Automatic Crime Detection System,” International Journal of Advanced Research in Management and Social Sciences, Aug. 2023. [Online]. Available: https://garph.co.uk/IJARMSS/Aug2023/1.pdf.

2. The Associated Press, “Police Officers Are Starting to Use AI Chatbots to Write Crime Reports,” AP News, 2024. [Online]. Available: https://www.ap.org/news-highlights/spotlights/2024/police-officers-are-starting-to-use-ai-chatbots-to-write-crime-reports-will-they-hold-up-in-court/.

3. Innefu Labs, “How Artificial Intelligence in Policing Helps Crime Detection,” Innefu Blog, 2024. [Online]. Available: https://www.innefu.com/blog/how-artificial-intelligence-in-policing-helps-crime-detection.

4. International Journal of Scientific Research and Applications, “AI-Powered Financial Crime Prevention,” IJSRA, 2024. [Online]. Available: https://ijsra.net/sites/default/files/IJSRA-2024-2143.pdf.

10.1 Research papers

1. **Apene, O.Z., Blamah, N.V., & Aimufua, G.I.O.** (2024). *Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions.* European Journal of Applied Science, Engineering and Technology, 2(2), 285-297.
2. **Shah, N., Bhagat, N., & Shah, M.** (2021). *Crime Forecasting: A Machine Learning and Computer Vision Approach to Crime Prediction and Prevention.* Visual Computing for Industry, Biomedicine, and Art, 4(9).
3. **Jenga, K., Catal, C., & Kar, G.** (2023). *Machine Learning in Crime Prediction.* Journal of Ambient Intelligence and Humanized Computing, 14, 2887–2913.
4. **Palanivinayagam, A., Gopal, S.S., Bhattacharya, S., Anumbe, N., Ibeke, E., & Biamba, C.** (2021). *An Optimized Machine Learning and Big Data Approach to Crime Detection.* Wireless Communications and Mobile Computing, 2021, Article ID 5291528.

11. APPENDIX

11.1 Glossary of terms

CDPS	Crime Detection & Prevention System
UMT	University of Management and Technology
GUI	Graphic User Interface
ML	Machine learning
CV	Computer Vision
CNN	Convolutional Neural Networks
DNN	Deep Neural Network
FYP	Final Year Project
POF	Proof of Work
HOG	Histogram of Oriented Gradient
SLCV	Surveillance & logging Using Computer Vision
NLP	Natural Language Processing