CSE 564 Project Report Number 6

Team 16

Team Member Names:

1. Aditya Pant
2. Ameya Shahu
3. Lalit Arvind Balaji
4. Pravalika Mukkiri

Table of Contents

1. The Problem

1.1. Description

1.1.1. Management System

Ensuring a secure working environment in large industrial facilities is paramount due to potential threats such as encroachment by foreign entities, which could jeopardize the safety of workers or lead to property theft. Securing expansive areas, whether in government or private sectors, poses a challenge that demands significant manpower. Efficiently monitoring these vast spaces with limited human resources becomes a critical need. However, the associated costs of employing a substantial workforce for security measures can be a significant financial burden. To address this challenge, a strategic approach is required to optimize security protocols, balance manpower efficiency, and mitigate the economic impact associated with the extensive workforce needed for safeguarding large industrial spaces.

1.1.2. Security team

The security system faces multifaceted challenges, necessitating a comprehensive approach. Regular encroachment patrols are essential to secure the perimeter, but the need for consistent monitoring poses logistical difficulties. Swift and seamless information transmission during encroachment incidents is critical; however, ensuring the entire team receives real-time updates, including the intruder's GPS coordinates, adds complexity. Real-time monitoring capabilities are crucial for tracking intruders, demanding constant vigilance to acquire timely information about their location and actions. Access to advanced surveillance tools, particularly drone cameras providing live imaging, is pivotal for informed decision-making, yet introduces the challenge of managing and interpreting real-time data effectively. These issues underscore the intricate nature of maintaining a secure environment, calling for a holistic strategy that balances regular patrols, efficient communication, real-time monitoring, and the integration of advanced surveillance technologies.

1.1.3. Technology providers

Ensuring effective real-time information sharing is a primary concern, requiring drones to seamlessly transmit live footage and sensor images to the system. The challenge is compounded by the necessity for a robust drone fail-safe system, essential for addressing potential malfunctions arising from adverse conditions to prevent harm to individuals and property. Another critical aspect is the storage of real-time data and footage in a cloud database for a specified period, introducing considerations of data volume and accessibility. Concurrently, maintaining the security of stored data is paramount, demanding stringent measures to safeguard information extracted from drones and prevent unauthorized access.

1.2. Previous and current attempts at a solution

Traditional surveillance systems, exemplified by CCTV cameras and human patrols, exhibit significant drawbacks that hinder their overall effectiveness. CCTV cameras, while widely used, face limitations in scalability, struggling to cover vast areas or properties comprehensively. Additionally, they encounter challenges in monitoring specific terrains or locations, leading to potential blind spots in surveillance coverage. Human patrols, on the other hand, prove resource-intensive with high associated costs, making

continuous presence financially burdensome. The inherent risk of human error introduces the possibility of missing encroachments due to fatigue or oversight, further compounded by the inability to sustain continuous coverage over extensive areas.

Fixed-position drone surveillance, while offering unique advantages, is beset by notable drawbacks. The primary limitation lies in its inherent limited mobility, as drones are stationed at fixed locations, constraining the scope of coverage. Moreover, the effectiveness of monitoring heavily depends on operator skills, introducing a potential bottleneck in operational efficiency. The restricted integration capability poses another challenge, creating difficulties in seamlessly incorporating fixed-position drone surveillance into existing security infrastructure. Additionally, legal and regulatory hurdles present significant barriers to deployment, adding complexity and compliance concerns.

These combined limitations underscore the need for more advanced and scalable surveillance solutions to address the shortcomings inherent in traditional approaches.

2. A Vision for a Solution

2.1. Overview

In envisioning a Drone-based Encroachment Detection System, our focus goes beyond the technical intricacies. We picture a comprehensive system where effective communication and teamwork are at the forefront. This means creating a collaborative environment where security personnel, management, and drone operators seamlessly work together towards a common goal.

With a focus on responsible business and economy, the system aims to strike a balance between security needs and sustainable practices. The system optimizes the need for human interaction and automates the laborious work to the drones and leaves technical work to people.

Social responsibility is embedded, in the sense that it opens up jobs in niche segments such as drone operations, drone technicians that are not common job opportunities in the industry.

Environmental impact assessments lead to the decision to use solar energy to power the drone which leads to reduced emissions and minimize adverse effects.

In design, user-centric principles drive interfaces, ensuring accessibility and usability. The system also promotes teamwork and communication through Real-time data streaming and notifications.

Critical thinking underpins the system's adaptability, allowing it to evolve with changing security landscapes and weather conditions.

This visionary drone-based system seeks to redefine encroachment detection by intertwining technological innovation with a profound commitment to communication, sustainability, social responsibility, and ethical considerations, ultimately contributing to a safer, more secure, and environmentally conscious future.

2.2. Solution Concept

2.1.1. Scene 1: Introduction

- A user opens the drone-based encroachment detection system application on his tablet.
- User is greeted with a user-friendly interface

2.1.2. Scene 2: System Status Check

- User notices a notification indicating a potential encroachment.
- User taps the notification, and the system displays real-time footage from a drone patrolling the area along with the location, type and severity of encroachment.

2.1.3. Scene 3: Communication

- User uses the communication feature to provide instructions to the security team about the situation.
- The system notifies the team, and they acknowledge the alert.

2.1.4. Scene 4: Resolution

- The security team, with the help of the drone system, successfully addresses the encroachment.
- User receives a system notification confirming the resolution of the incident.
- Scene 5: Post-Incident Logging
- The system automatically generates a post-incident log with all details to the database.
- User reviews the report, providing insights for future improvements in the system.

This storyboard illustrates a seamless interaction between the user and the drone-based encroachment detection system, showcasing features like real-time monitoring, communication, collaboration, and advanced surveillance tools in addressing security incidents.

3. Requirements

3.1. Introduction

Imagine a state-of-the-art system for drone-based encroachment detection. Autonomous drones equipped with advanced sensors ensure real-time monitoring, rapidly reporting unauthorized movements. AI algorithms process data swiftly with minimal delays. Drones operate on programmable routes, supporting scheduled and demand-based surveillance. Real-time data sharing, remote operation, and user-friendly interfaces enhance adaptability. Load balancing optimizes performance, and robust access controls and encryption secure sensitive data. This comprehensive solution ensures precise and efficient encroachment detection in various environments.

3.2. Operational Requirements

3.2.1. Autonomous Drones

The system must employ autonomous drones with advanced sensor capabilities for real-time monitoring. The integration of these advanced sensors not only elevates the efficiency of the monitoring process but also enhances the responsiveness of the entire surveillance system. By entrusting the drones with autonomous operations, the system can promptly and intelligently adapt to dynamic environmental conditions, ensuring a more robust and effective approach to surveillance tasks.

Source: Handbook of Unmanned Aerial Vehicles. Springer[1]

3.2.2. Real-Time Surveillance

The system is required to react promptly and decisively to any unauthorized movements within its surveillance domain. Drones, serving as vigilant sentinels, play a pivotal role in this responsiveness. Their primary function is to swiftly detect and report any irregular or unauthorized activities to the central control system. The immediacy of this reporting mechanism is crucial, as it sets the stage for an agile and proactive response from security personnel. Once an alarm is triggered, security teams must mobilize swiftly, ensuring a timely and decisive intervention in potential security threats.

Source: Handbook of Unmanned Aerial Vehicles. Springer[2]

3.2.3. Data Processing in Real-Time

To achieve efficient surveillance, the implementation of AI-powered detection algorithms stands as a cornerstone, enabling the system to meticulously analyze incoming data and identify potential encroachments in real-time. The crucial element here lies in the demand for swift processing, with an upper limit of 500 milliseconds for decision-making. This stringent time frame ensures that the system can promptly respond to emerging threats, enhancing its overall effectiveness. The ability to process data from up to 10 drones simultaneously is also crucial to secure the entire area.

Source: Pattern Recognition and Machine Learning. Springer[3]

3.2.4. Programmable Routes

It's necessary for drones to support programmable routes. The system is designed to enable the configuration of specific flight paths for drones, ensuring comprehensive coverage of designated areas within the industrial zone. Scheduled monitoring is a crucial component of this feature, directing drones to systematically traverse the entire industrial area at predefined regular intervals. This scheduled approach enhances the system's ability to consistently monitor the entire environment, providing a baseline level of surveillance. Additionally, the requirement emphasizes demand monitoring, allowing for the flexibility to instruct drones to focus on specific sections within the industrial zone when an extra layer of security is deemed necessary. This combination of scheduled and demand-based monitoring ensures a well-rounded and adaptable surveillance strategy, aligning with the dynamic nature of security needs in industrial settings.

Source: Onboard IMU and Monocular Vision-based Control for Aggressive Quadrotor Flight. In Robotics: Science and Systems (RSS).[4]

3.2.5. Real-time Data Sharing

The system must facilitate real-time data sharing with law enforcement agencies and relevant authorities. Drones tracking encroached entities are expected to communicate real-time footage of movements, enabling swift and collaborative responses to security incidents. This proactive sharing of live video feeds enables swift, informed, and collaborative responses to security incidents.
Source: Dictionary of Computer Science, Engineering, and Technology[5]

3.2.6. Autonomous Drones

The system must employ autonomous drones with advanced sensor capabilities for real-time monitoring. The integration of these advanced sensors not only elevates the efficiency of the monitoring process but also enhances the responsiveness of the entire surveillance system. By entrusting the drones with autonomous operations, the system can promptly and intelligently adapt to dynamic environmental conditions, ensuring a more robust and effective approach to surveillance tasks.
Source: Handbook of Unmanned Aerial Vehicles. Springer[1]

3.2.7. Real-Time Surveillance

The system is required to react promptly and decisively to any unauthorized movements within its surveillance domain. Drones, serving as vigilant sentinels, play a pivotal role in this responsiveness. Their primary function is to swiftly detect and report any irregular or unauthorized activities to the central control system. The immediacy of this reporting mechanism is crucial, as it sets the stage for an agile and proactive response from security personnel. Once an alarm is triggered, security teams must mobilize swiftly, ensuring a timely and decisive intervention in potential security threats.
Source: Handbook of Unmanned Aerial Vehicles. Springer[2]

3.2.8. Programmable Routes

It's necessary for drones to support programmable routes. The system is designed to enable the configuration of specific flight paths for drones, ensuring comprehensive coverage of designated areas within the industrial zone. Scheduled monitoring is a crucial component of this feature, directing drones to systematically traverse the entire industrial area at predefined regular intervals. This scheduled approach enhances the system's ability to consistently monitor the entire environment, providing a baseline level of surveillance. Additionally, the requirement emphasizes demand monitoring, allowing for the flexibility to instruct drones to focus on specific sections within the industrial zone when an extra layer

of security is deemed necessary. This combination of scheduled and demand-based monitoring ensures a well-rounded and adaptable surveillance strategy, aligning with the dynamic nature of security needs in industrial settings.

Source: Onboard IMU and Monocular Vision-based Control for Aggressive Quadrotor Flight. In Robotics: Science and Systems (RSS).[4]

3.3. Quality Requirements

- **Scalability** - Scalability is essential for adjusting to changing environmental conditions, allowing for smooth growth for monitoring small and large regions without sacrificing performance.
- **Modularity** - By grouping logical pieces into reusable modules, modularity increases flexibility and facilitates maintenance, upgrades, and the integration of new features or sensor types.
- **Security** - Security is critical for protecting sensitive data and system integrity, as well as preventing unwanted access to drone hardware and transmitted data via built-in logical security.
- **Efficiency** - Efficiency is critical for real-time threat detection, which necessitates improved logical architecture of algorithms and data flows to enable fast notifications.

4. Architecture

4.1. Architectural Overview

We are using Kruchten's 4+1 to provide a formal understanding of the system. The Logical View delineates the critical components in charge of user interfaces, camera video processing, intrusion alert generation, and data storage. The Process View depicts the dynamic interactions between system components, including drone operations, flight planning, and video processing. The Physical View focuses on the system's hardware, such as drones, databases, and control, to ensure compliance with environmental requirements. The Deployment View focuses on the technological underpinnings, such as the software programming languages used for camera video detection and database management. The Scenarios View demonstrates the system's adaptability by efficiently managing various situations such as user interactions with operators, optimizing flight schedules between charging intervals, and enabling rapid alert systems for incursion detection. These architectural perspectives collaborate to create a comprehensive system capable of supporting a wide range of applications while maintaining efficiency, security, and responsiveness.

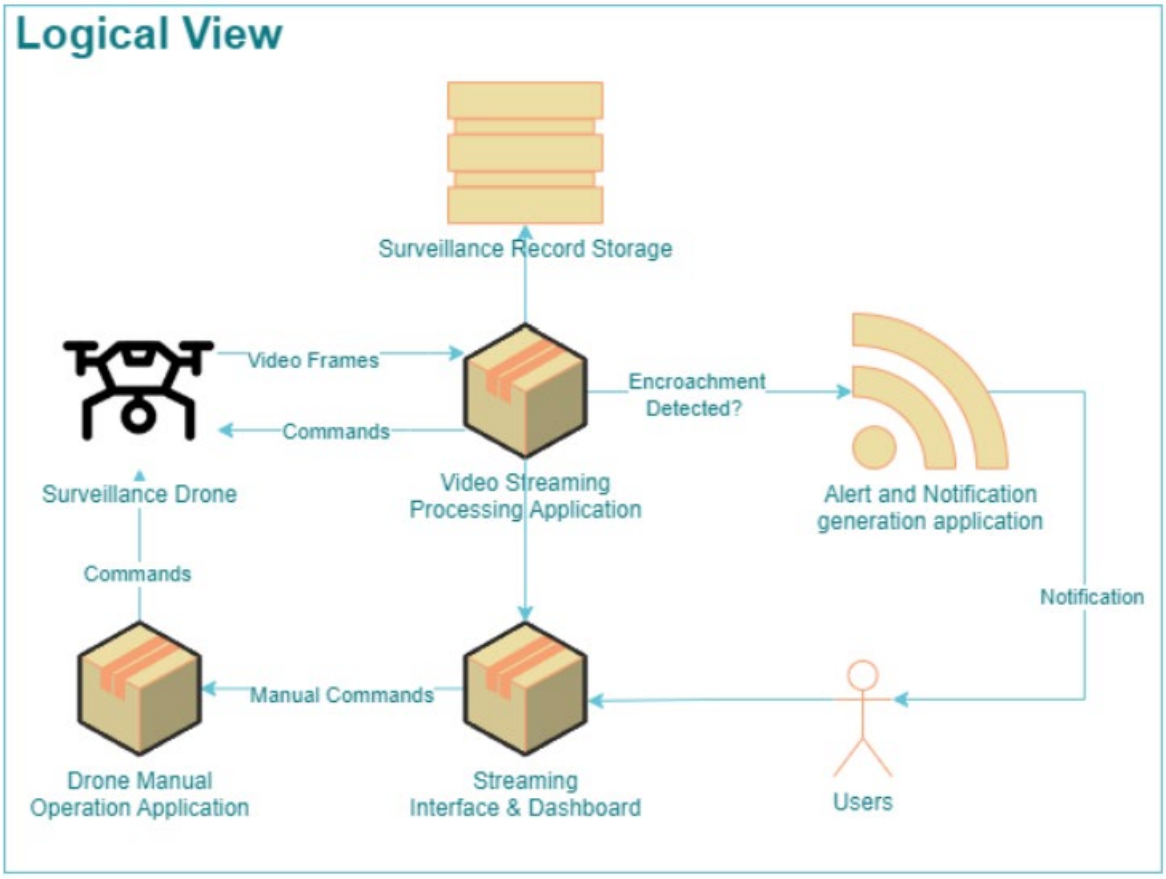
4.2. Architectural Views

4.2.1. Logical View

- Introduction: Logical View

In adopting a logical approach, emphasis is placed on the fundamental elements of the system, including software components, user interfaces, and alert systems. These elements collectively form the bedrock of the system, ensuring its robustness and efficiency. The strategic prioritization of these components facilitates dual functionality, enabling the seamless integration of live streaming and archival capabilities for surveillance footage. This dynamic capability empowers the system to support real-time monitoring, providing immediate insights into ongoing activities, while also facilitating retrospective analysis of historical encroachment incidents. Such a comprehensive approach not only enhances the system's responsiveness but also equips it with the tools necessary for a thorough examination of past events, contributing to a more informed and effective security strategy.

- UML Representation

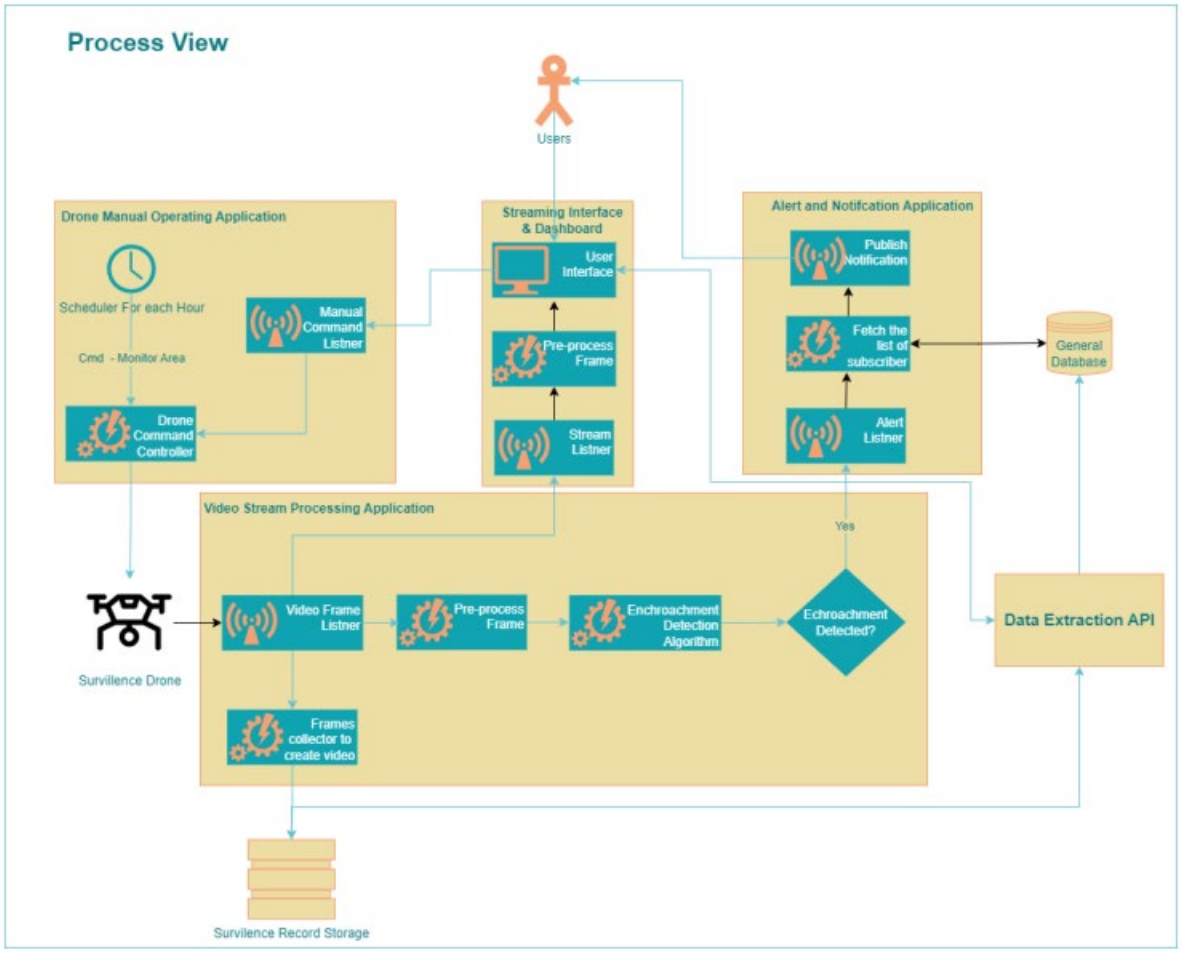


4.2.2. Process View

- Introduction

The main parts of the system are the Drone Operating Application, which oversees real-time control, planned patrols, and intrusion warnings; the Live Streaming Interface, which controls camera access, guarantees data security, and gathers real-time drone data; and the Alert Application, which promptly sends out alerts, records intrusion details for later analysis, and examines camera data to find intrusions. Together, these interconnected parts create a complete system for efficient drone-based surveillance and intrusion detection.

- UML Representation



- Key Details

- The Dashboard and Streaming Interface form the nucleus of the system, offering a comprehensive set of features for efficient monitoring and user interaction. The Real-Time Video Display continuously streams live video feeds, ensuring a constant pulse on the monitored area. User-Driven Navigation empowers users to customize their experience, tailoring the interface to their specific needs. In the realm of drone operations, the application provides an Alert Response mechanism for swift reaction to intrusion alerts and incorporates safety safeguards to guarantee secure drone operations.

-

- The Drone Surveillance module introduces GPS tracking, furnishing precise location information for enhanced operational control. Simultaneously, real-time data transmission facilitates prompt analysis. The Application for Notification presents the Alert Dashboard, a real-time hub for situational analysis, displaying detailed information about intrusion alerts.

-

In the Surveillance Data domain, the system boasts a Camera Footage Archive for storing high-resolution camera data and maintaining Historical Encroachment Records. This dual functionality enables the system

not only to capture and store real-time data efficiently but also to track and analyze historical intrusion incidents. This holistic approach ensures a comprehensive security strategy, combining immediate response capabilities with a thorough examination of past events for informed decision-making.

4.2.3. Development View

- Introduction

The developmental aspect of the encroachment detection system involves three key elements, each playing a crucial role in the system's functionality.

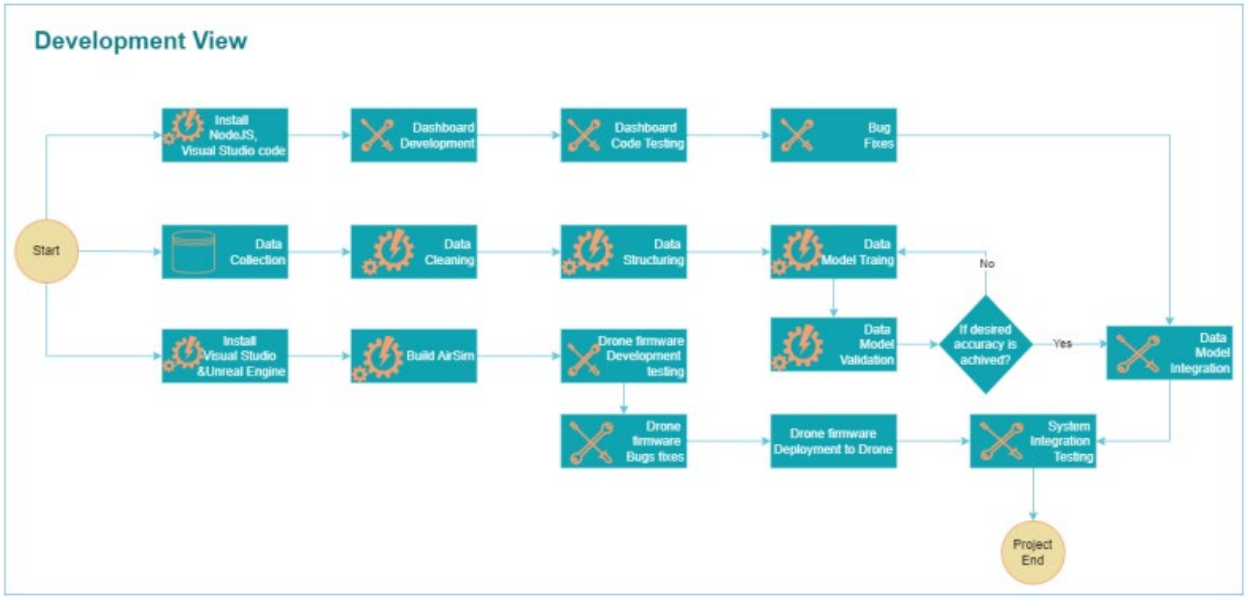
Firstly, there is the creation of a machine learning model designed specifically for identifying invasions. This involves leveraging advanced techniques within the field of machine learning to develop a robust and accurate model capable of recognizing potential encroachments or security threats. The model is trained to analyze data from the drone's video footage, providing a sophisticated layer of intelligence to the system.

The second element focuses on establishing and modeling drone flight characteristics. This entails defining the flight patterns, behaviors, and operational characteristics of the drones within the system. By modeling these aspects, the system can optimize drone movements, ensuring efficient surveillance and timely response to detected invasions. This element is essential for the overall effectiveness and reliability of the encroachment detection system.

The third and equally significant element involves creating a dashboard and configuring drone communication channels. The dashboard serves as a user interface, allowing operators to interact with the system, visualize data, and make informed decisions. Simultaneously, establishing communication channels ensures seamless and real-time data exchange between the drones and the central system. This communication infrastructure is vital for transmitting commands to the drones and receiving critical data, contributing to the system's overall responsiveness and functionality.

In summary, the developmental aspect encompasses the creation of a machine learning model for invasion identification, the establishment and modeling of drone flight characteristics, and the development of a dashboard with configured communication channels. Together, these elements form a cohesive and sophisticated system designed to detect and respond to encroachments effectively.

- UML Representation



- Key Details

The creation of the dashboard for the encroachment detection system involves a multifaceted approach with distinct components and technologies. Firstly, a NodeJS web application serves as the foundation for the dashboard interface, providing users with a seamless platform to interact with the drones and oversee the system's functionalities. This NodeJS web app acts as the frontend, allowing for intuitive communication and control.

To establish effective communication between the drones and the application server, robust communication channels are implemented. These channels serve as conduits for the exchange of commands and data, facilitating real-time interaction. Users can send commands to drones and receive crucial data from them through these communication channels, ensuring a responsive and dynamic user experience.

The model training aspect involves leveraging the YOLO8 (You Only Look Once) model, a state-of-the-art object detection algorithm. This model is trained using Python, a versatile and widely adopted language in the realm of machine learning. The trained YOLO8 model is specifically designed to recognize and detect objects within drone video footage, a pivotal capability for encroachment detection.

An integral part of the process is the extraction of object positions from the video feed. This technique, incorporated within the YOLO8 model, precisely locates objects within the video, providing spatial awareness and crucial positional information. This step is fundamental to identifying potential encroachments or objects of interest in the monitored area.

Additionally, simulation tools are employed to emulate various components of the system and conduct comprehensive tests in a controlled environment. Simulation enables thorough testing without the need for physical drones, ensuring that different parts of the system function harmoniously and as intended. This comprehensive approach to dashboard creation, communication channels, model training, object position extraction, and simulation collectively contributes to the development of a robust and effective encroachment detection system.

5. Detailed Design

5.1. System Context and Interactions

5.1.1. Drone Operations

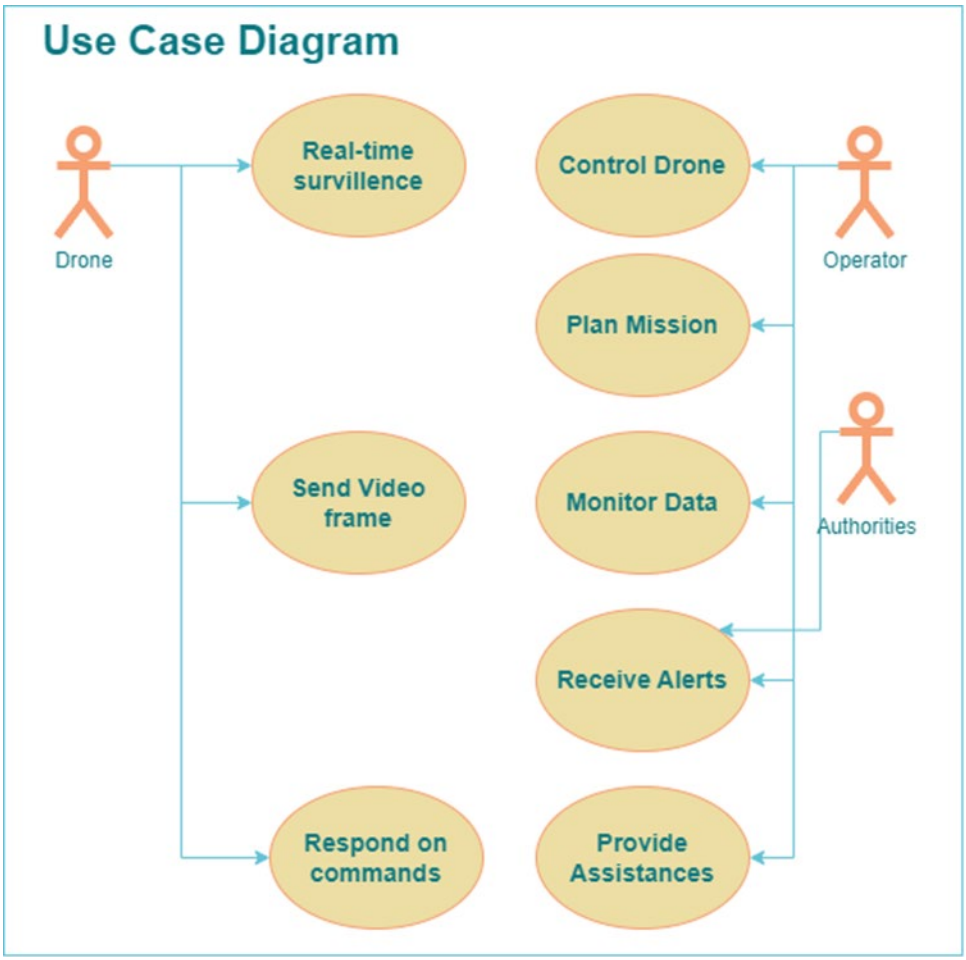
- Overview

A drone is a versatile aerial vehicle, remotely controlled or autonomous, equipped with specialized sensors designed for visual and environmental data collection, primarily employed for surveillance purposes. The drone operating application serves as the key software interface for operators, facilitating the management and monitoring of drone operations. This application empowers operators to manipulate the drone's movements, adjust sensor settings, and access real-time data, enabling swift responses to detected encroachments.

- Technical Details

Developed within the framework of Kruchten's 4+1 design pattern, this component serves as a critical element in our encroachment detection system. The drone and the drone operating application are the core technological components of the encroachment detection system. They are significant and prioritized for several reasons. First, they make it possible for real-time data collection and surveillance by integrating contemporary sensors, such as environmental sensors and high-resolution cameras. This ability is very helpful in identifying and assessing possible intrusions, security breaches, or safety concerns, especially in difficult-to-reach or unreachable locations. Moreover, their integration with alert systems guarantees timely responses to emerging issues by ensuring timely notifications and alarms when anomalous behavior or intrusions are detected. Furthermore, drones' scalability and coverage allow them to cover large areas quickly and efficiently, providing a comprehensive view that is superior to that of manned patrols or fixed surveillance systems. This scalability is essential for keeping an eye on large perimeters, vital infrastructure, and areas affected by disasters. Finally, the operating application's and the drone's adaptability and flexibility enable customization to particular use cases, meeting a variety of operational demands, security specifications, and environmental conditions, making them extremely versatile in a broad range of applications.

- Use Case Diagram and Use Cases



Use Case: Real Time Surveillance

Use Case ID:	001		
Use Case Name:	Real-Time Surveillance		
Traceability:			
Created By:	Ameya Shahu	Last Updated By:	10/19/2023
Date Created:	10/19/2023	Date Last Updated:	10/19/2023

Actor:	Drone
Description:	This use case describes the process by which the drone conducts real-time surveillance over a designated area to detect any encroachments.
Preconditions:	• The drone is fully charged and operational. • The drone's cameras and sensors are functional. • The flight path has been predefined and uploaded to the drone's system.
Postconditions:	• The drone has completed the surveillance mission. • The surveillance data has been recorded and is available for review.
Primary Pathway:	• The operator initiates the surveillance mission. • The drone follows the predefined flight path, capturing real-time video and sensory data.

	• The drone processes and streams data to the operator's dashboard. • The operator monitors the data feed for any encroachments. • The drone completes the surveillance loop and returns to the starting position.
Alternate Pathways:	• If an encroachment is detected, the drone sends an alert to the operator and continues to monitor the area. • If the drone encounters a flight or mechanical issue, it returns to base immediately.
Exception Pathways:	• In case of a low battery or signal loss, the drone initiates an emergency landing protocol.

Use Case: Control Drone

Use Case ID:	002		
Use Case Name:	Control Drone		
Traceability:			
Created By:	Ameya Shahu	Last Updated By:	10/19/2023
Date Created:	10/19/2023	Date Last Updated:	10/19/2023

Actor:	Drone Operator
Description:	This use case details the operator's interaction with the drone to initiate, control, and manage its operations during a mission.
Preconditions:	• The drone is operational and in communication range. • The operator is trained and authorized to control the drone.
Postconditions:	• The drone has been successfully controlled and managed by the operator.
Primary Pathway:	• The operator sends a command to initiate the drone's operations. • The drone receives the command and executes the start-up sequence. • The operator continues to send control commands during the drone's flight.
Alternate Pathways:	• The operator sends a command to land the drone in case of an emergency.
Exception Pathways:	• Communication failure between the operator and the drone.

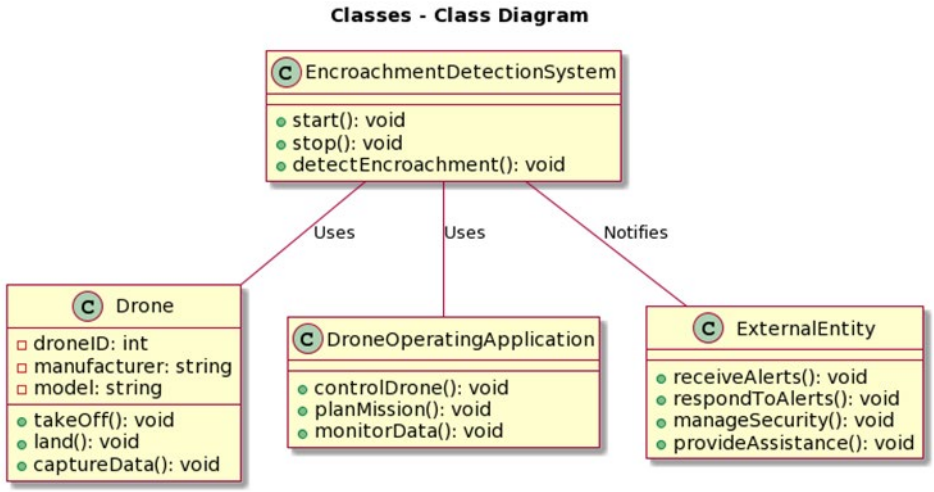
Use Case: Plan Mission

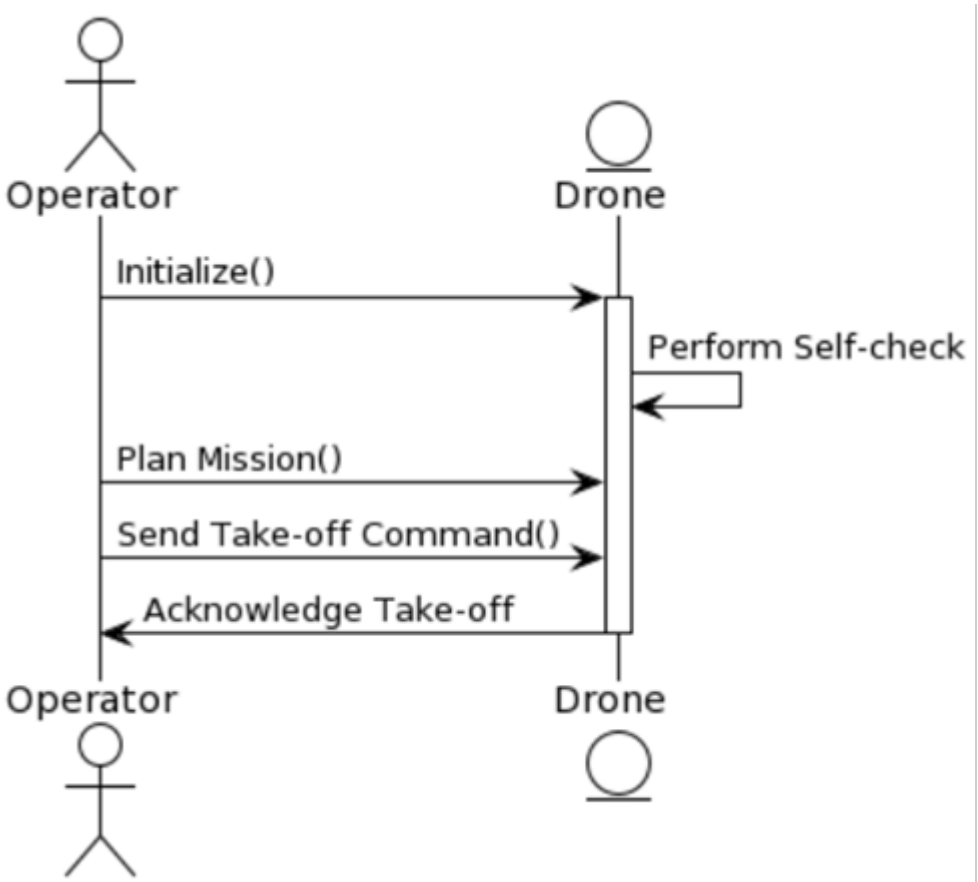
Use Case ID:	003		
Use Case Name:	Plan Mission		
Traceability:			
Created By:	Ameya Shahu	Last Updated By:	10/19/2023
Date Created:	10/19/2023	Date Last Updated:	10/19/2023

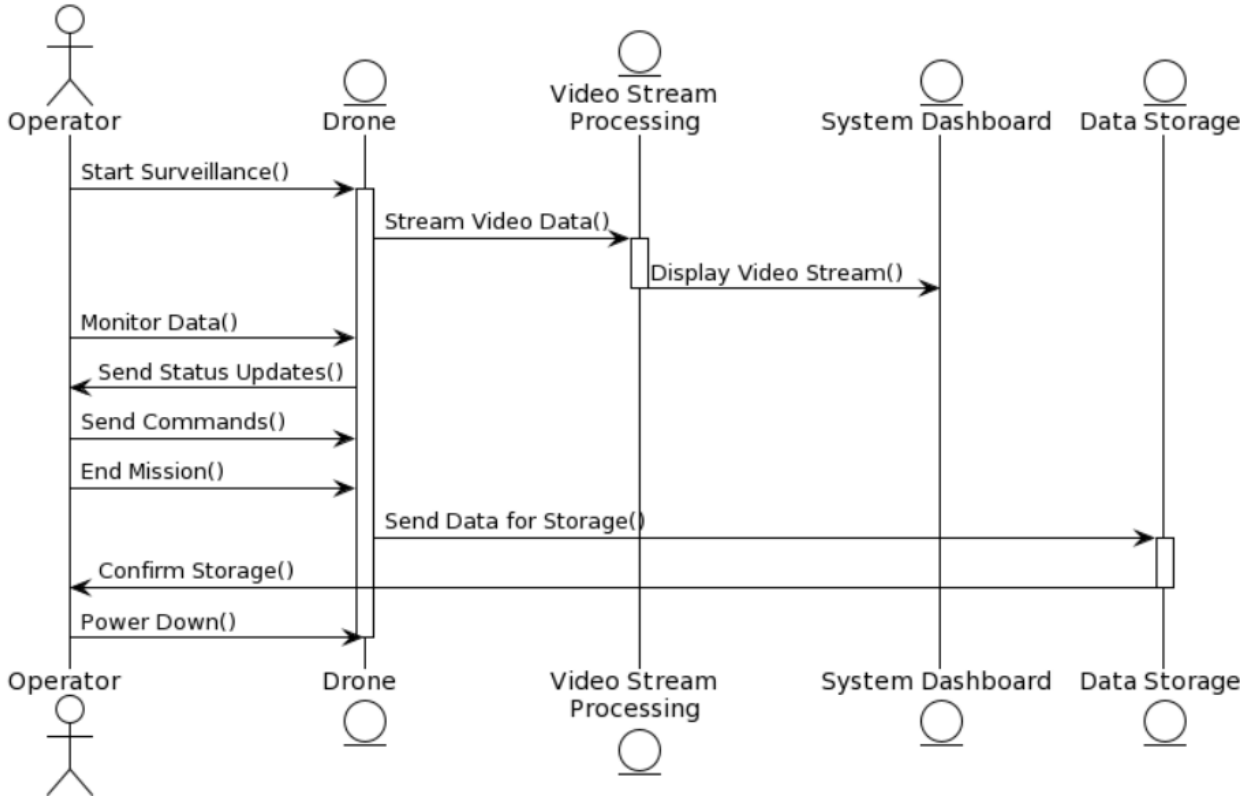
Actor:	Operator
Description:	This use case describes the operator's process to plan and upload a mission for the drone to execute, including route, altitude, and behavior.

Preconditions:	• The operator has access to the mission planning tools. • The drone is available and ready to receive mission parameters.
Postconditions:	• The drone has a complete and executable mission plan.
Primary Pathway:	• The operator accesses the mission planning tool. • The operator inputs the necessary parameters for the mission. • The mission is uploaded to the drone. • The drone acknowledges receipt of the mission plan.
Alternate Pathways:	• The operator adjusts the mission plan in response to real-time events or data.
Exception Pathways:	• Mission planning tool fails to upload the plan to the drone.

- Class Diagram and Sequence Diagrams




Operator
Drone
Initialize()
Perform Self-check
Plan Mission()
Send Take-off Command()
Acknowledge Take-off
Operator
Drone



5.1.2. Video Processing Module

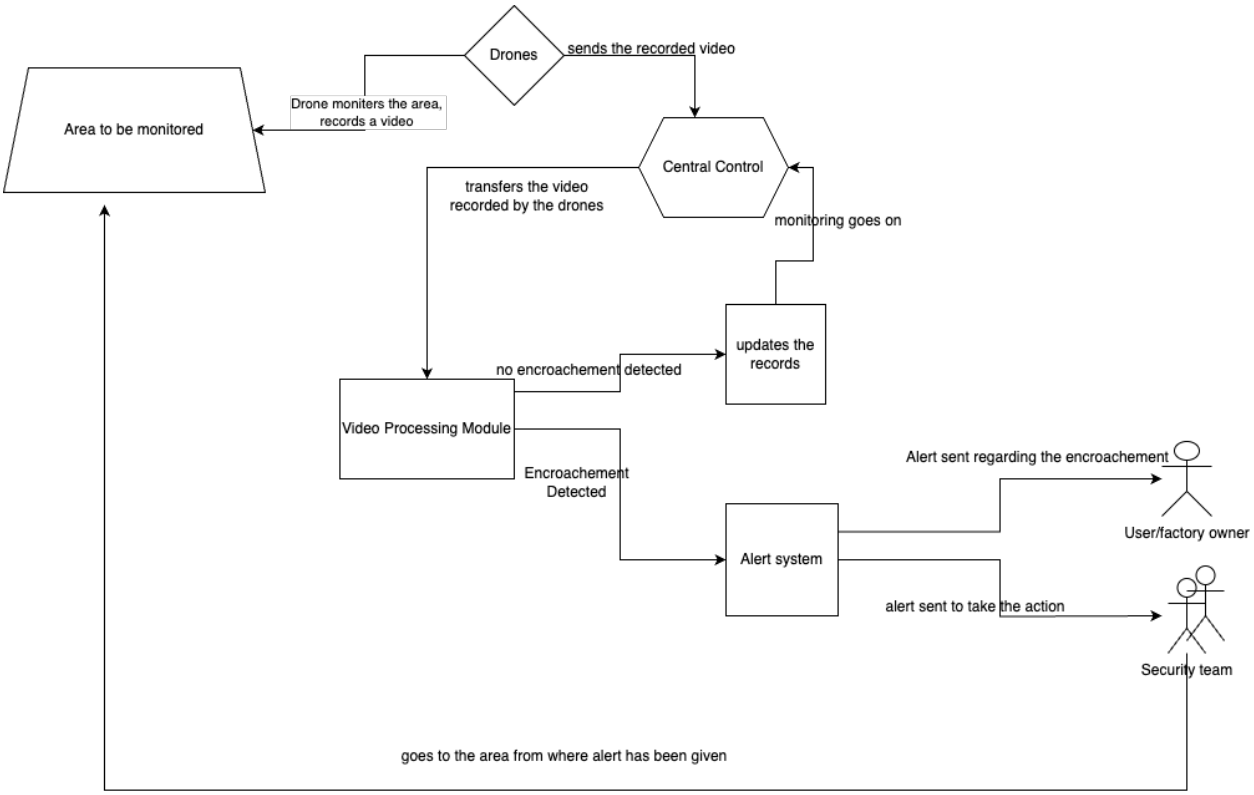
- Overview

The video processing component is crucial within our system, providing real-time analysis of drone footage to identify encroachments in industrial areas. The Video Processing Module plays a pivotal role in our system, facilitating the real-time processing of drone data specifically for detecting incursions in industrial regions. Leveraging image processing and computer vision techniques, it ensures accurate identification of potential security concerns, contributing significantly to the overall functionality and effectiveness of the system.

- Technical Details

The "Video Processing Module" stands as a crucial design feature, spearheading real-time video data analysis and playing a pivotal role in achieving the primary objective of identifying encroachments within the industrial area. Employing image processing and computer vision techniques, this module is dedicated to detecting any illicit activities, ensuring swift and accurate identification of genuine security threats. Its rapid and precise operation is of utmost importance, functioning as the core of our intrusion-detection system, guaranteeing that security threats are promptly discovered and notified for immediate response.

- Use Case Diagram and Use Cases



Use Case: Video Surveillance Processing

Use Case ID:	001		
Use Case Name:	Video Surveillance Processing		
Traceability:			
Created By:	Pravalika Mukkiri	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

Actor:	• Drone, Security Team, User/Factory Owner •
Description:	• This use case represents the normal operation of the system during video surveillance. It involves capturing video data, processing it for encroachments, triggering alarms if threats are detected, and notifying relevant parties.
Preconditions:	• Drones actively surveilling, video data available.
Postconditions:	• Encroachment detection results generated, alerts sent, processed data archived.
Primary Pathway:	• Drone captures video → Sent to central control system → Processed for encroachments → Alarm triggered if detected → Alerts delivered → Encroachment data archived.
Alternate Pathways:	• In case of poor video quality or incomplete data, the system may request retransmission of video data from the drone.
Exception Pathways:	• If the central control system is unavailable, the system may store the video data locally and retry transmission once connectivity is restored.

Use Case: Scheduled Maintenance

Use Case ID:	002

Use Case Name:	Scheduled Maintenance		
Traceability:			
Created By:	Pravalika Mukkiri	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

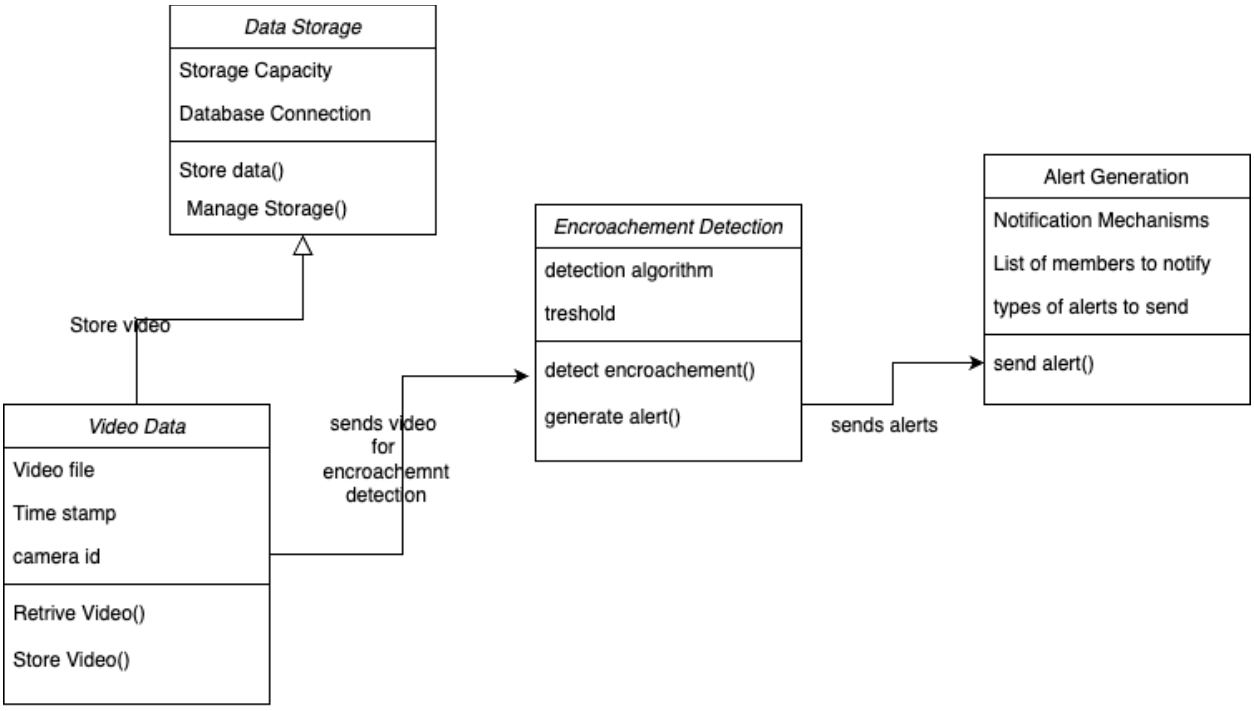
Actor:	Maintenance Team
Description:	This use case represents the scheduled maintenance of the system to ensure its continued functionality.
Preconditions:	• Scheduled maintenance time reached.
Postconditions:	• Maintenance tasks completed, system operational.
Primary Pathway:	• Maintenance team notified → System enters maintenance mode → Scheduled tasks performed → System exits maintenance mode
Alternate Pathways:	• If a critical issue is identified during maintenance, the system may remain in maintenance mode until the issue is resolved.
Exception Pathways:	• If the maintenance team encounters difficulties, the system may roll back to the previous operational state to avoid disruptions.

Use Case: Emergency Shutdown

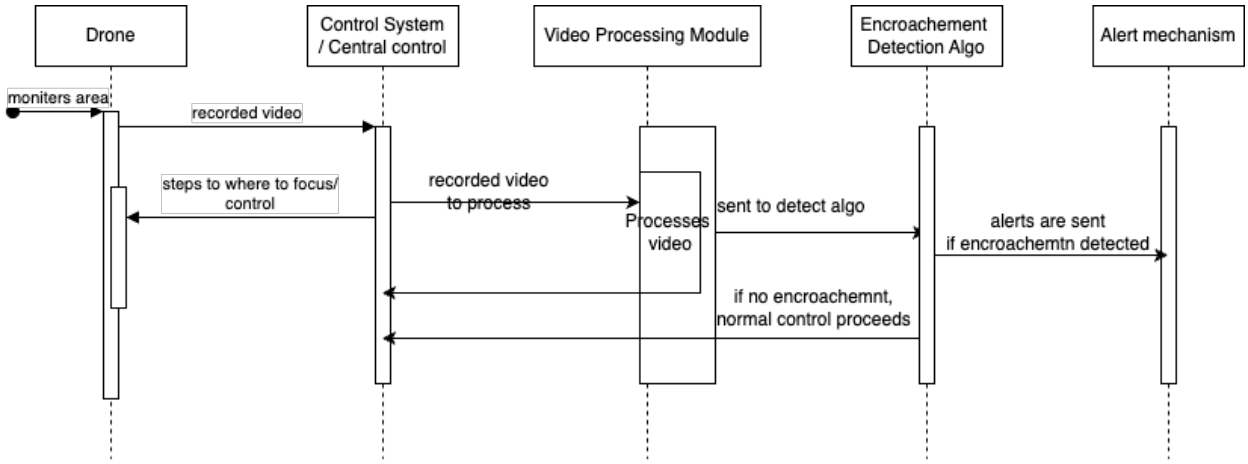
Use Case ID:	003		
Use Case Name:	Emergency Shutdown		
Traceability:			
Created By:	Pravalika Mukkiri	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

Actor:	Emergency Operator
Description:	This use case represents the emergency shutdown of the system in response to a critical situation. It involves an emergency operator triggering the shutdown, ceasing normal operations, and activating emergency protocols.
Preconditions:	• Emergency detected.
Postconditions:	• System safely shut down; emergency protocols initiated.
Primary Pathway:	• Emergency operator triggers shutdown → Central control system ceases normal operation → Emergency protocols activated → System safely shuts down.
Alternate Pathways:	• If the emergency is resolved before the shutdown is complete, the system may abort it.
Exception Pathways:	• If the shutdown process encounters errors, the system may initiate a safe mode to prevent further complications.

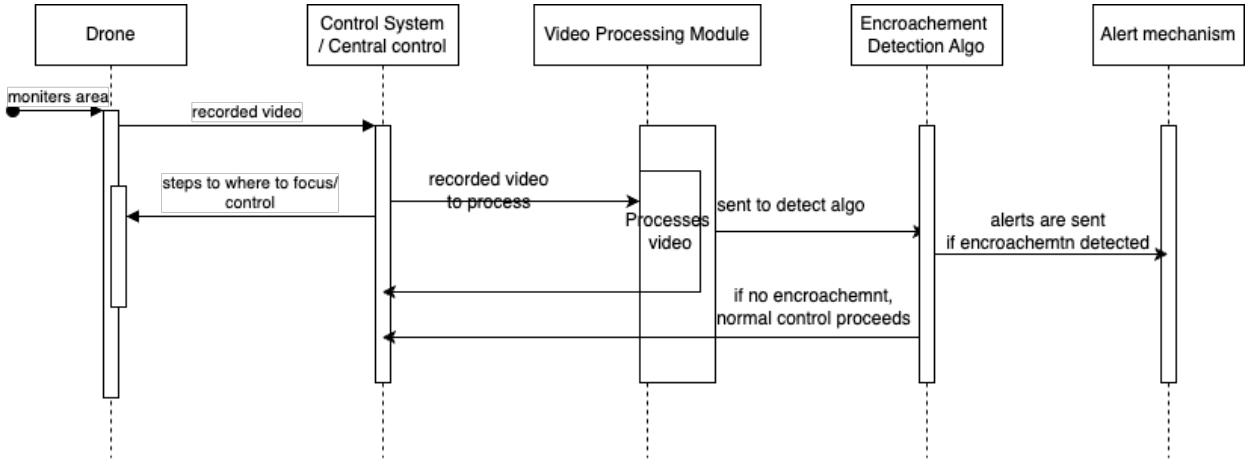
- Class Diagram and Sequence Diagrams



The "Video Data" class manages raw video data from drones, encompassing attributes like Timestamp, Video File, and Camera ID. The methods "RetrieveVideo()" and "StoreVideo()" facilitate video data retrieval and storage, with the latter strongly associated with the "Data Storage" class. The "Encroachment Detection" class oversees encroachment identification, utilizing attributes such as Detection Algorithm and Threshold. The "DetectEncroachment()" method applies algorithms to video data, while "GenerateAlert()" creates alerts upon encroachment detection. This class is linked to the "Video Data" class for data reception and the "Alert Generation" class for alert creation. The "Data Storage" class is responsible for storing processed data, featuring attributes like Database Connection and Storage Capacity. The "StoreData()" method manages processed data storage, while "ManageStorage()" ensures effective capacity and retention management. This class is linked to the "Video Data" class via the "StoreData()" function. The "Alert Generation" class concentrates on alert creation, incorporating attributes related to Notification Mechanisms. The "SendAlert()" method delivers alerts when encroachments are detected, and for distribution, this class can be linked to external notification systems. Together, these classes collaborate to facilitate efficient video processing, encroachment detection, and ensure the integrity of the system. A visual representation of these relationships and each class's roles should be shown in the class diagram for this system.



This sequence diagram delineates the dynamic interactions within the Video Processing Module during a standard threat detection scenario. It commences with the drone capturing video data, which is then transmitted to the central control system for processing. The video data undergoes scrutiny in the Video Data class, where it is examined for signs of invasion. Upon the detection of an encroachment, the Alert Generation class is activated, triggering notifications to either the central control system or security personnel. Concurrently, the Data Storage class ensures the retention of processed data, securing its accessibility for future reference. This depiction illustrates the coordinated and sequential actions that take place within the Video Processing Module during the process of threat detection.



This flow diagram illustrates the interactions involved in the retrieval and storage of video data within the Video Processing Module. The process begins with the Video Data class retrieving raw video data, incorporating properties like Timestamp, Video File, and Camera ID. The subsequent step involves the storage of the video data through the "StoreVideo" method, which interfaces with the Data Storage class. The Data Storage class, in turn, employs methods such as "StoreData" and "ManageStorage" to ensure effective storage capacity and data retention management. This sequential representation highlights the seamless collaboration of classes in handling video data from its retrieval stage to storage within the Video Processing Module.

5.1.3. Alert Manager

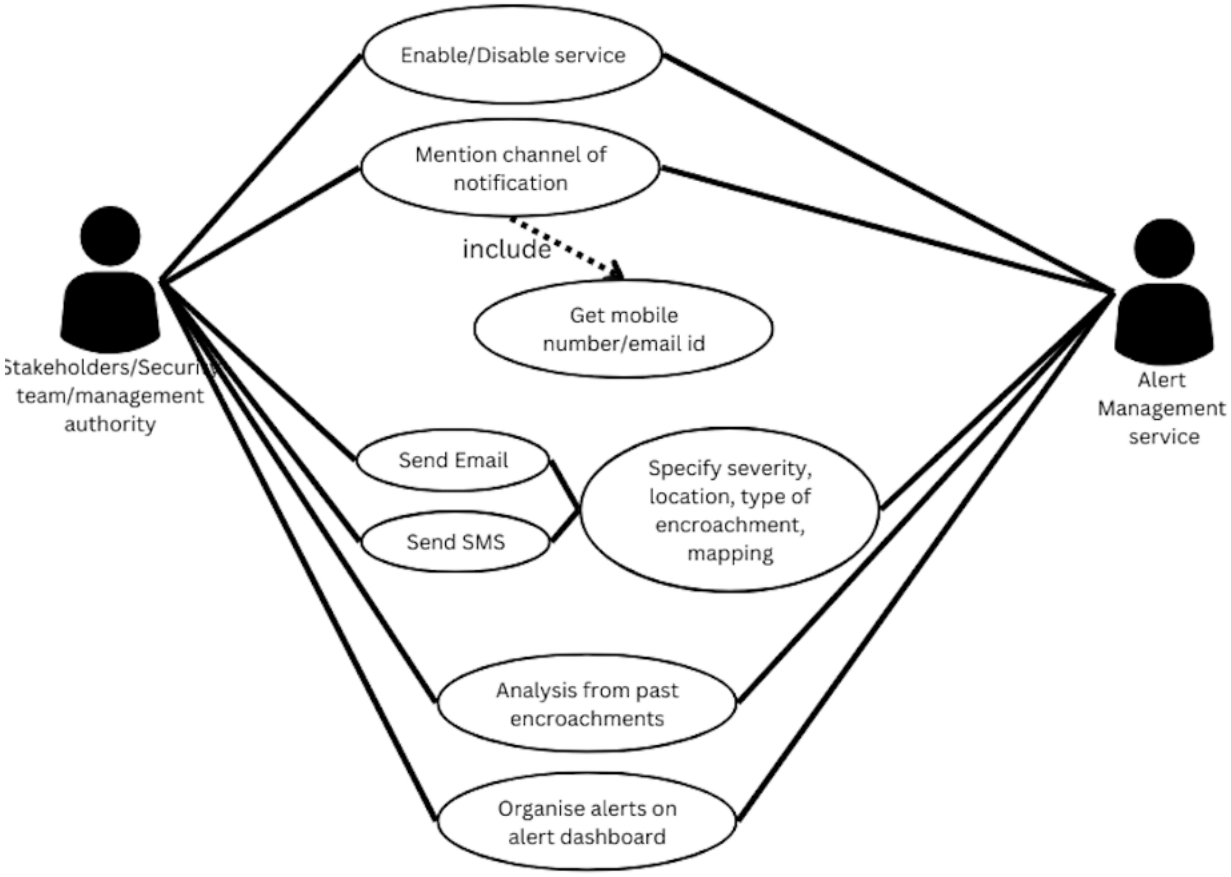
- Overview

The Alert Details Retriever function acquires the encroachment location from the drone, along with videos that aid in determining the severity and type of the encroachment. Subsequently, the location details are transmitted to the Mapping Integration component, where they are overlaid on a map to assist the security team in navigating to the specific location. The Notification Manager receives the mapping information along with other alert details and notifies the registered authorities through their preferred communication channels, providing comprehensive details. Simultaneously, the Alert Dashboard receives the alert, prioritizes them based on severity, and displays them for immediate attention and analysis. This cohesive process ensures efficient handling of alerts, from retrieval and mapping to notification and display, facilitating swift and informed responses to encroachments.

- Technical Details

The Alert Aggregation and Categorization API plays a pivotal role in the encroachment detection system by consolidating alerts from drones and categorizing them based on severity, location, and type of encroachment. It oversees the distribution of alerts to relevant stakeholders or response teams through diverse communication channels like email, SMS, and push notifications. The API also enables trend analysis and report generation, offering valuable insights into patterns related to encroachments. Additionally, it powers a real-time alert dashboard for quick situational analysis and integrates with mapping services, overlaying alerts on a map for precise location details. The significance of this API lies in its contribution to rapid response times, enhancing situational awareness, enabling data analysis for trend identification, and facilitating integration and coordination among different stakeholders or response teams. Efficient alert management is crucial for swift responses to unauthorized encroachments, and the API ensures the prompt handling and appropriate distribution of alerts, reducing response times to potential threats or intrusions. The organized display of alerts in real-time enhances situational awareness, providing response teams with detailed information about the exact locations and types of encroachments, thereby supporting effective decision-making. Furthermore, the historical data stored in the database allows for insightful trend analysis, aiding in the identification of patterns and the improvement of security measures. The API's role in facilitating coordination ensures that pertinent information reaches the right individuals through various communication channels, fostering effective collaboration among different stakeholders or response teams.

- Use Case Diagram and Use Cases



Use Case: Alert Configuration and Setup

Use Case ID:	401		
Use Case Name:	Alert Configuration and Setup		
Traceability:			
Created By:	Lalit Arvind Balaji	Last Updated By:	Lalit Arvind Balaji
Date Created:	11/19/23	Date Last Updated:	11/19/23

Actor:	Admin User
Description:	Setting up profile in notification interface to obtain notifications in case any encroachment occurs
Preconditions:	User is authorized personnel in industry
Postconditions:	Interface obtains user's preference and notification channel details
Primary Pathway:	• User enables notifications • User chooses preferred notification channel: SMS/E-Mail • User provides details for chosen notification channel: Mobile no./E-Mail ID
Alternate Pathways:	• User disables notifications
Exception Pathways:	• Provided E-Mail ID/Phone no does not exist

Use Case: Alert Notification

Use Case ID:	402		
Use Case Name:	Alert Notification		
Traceability:			
Created By:	Lalit Arvind Balaji	Last Updated By:	Lalit Arvind Balaji
Date Created:	11/19/23	Date Last Updated:	11/19/23

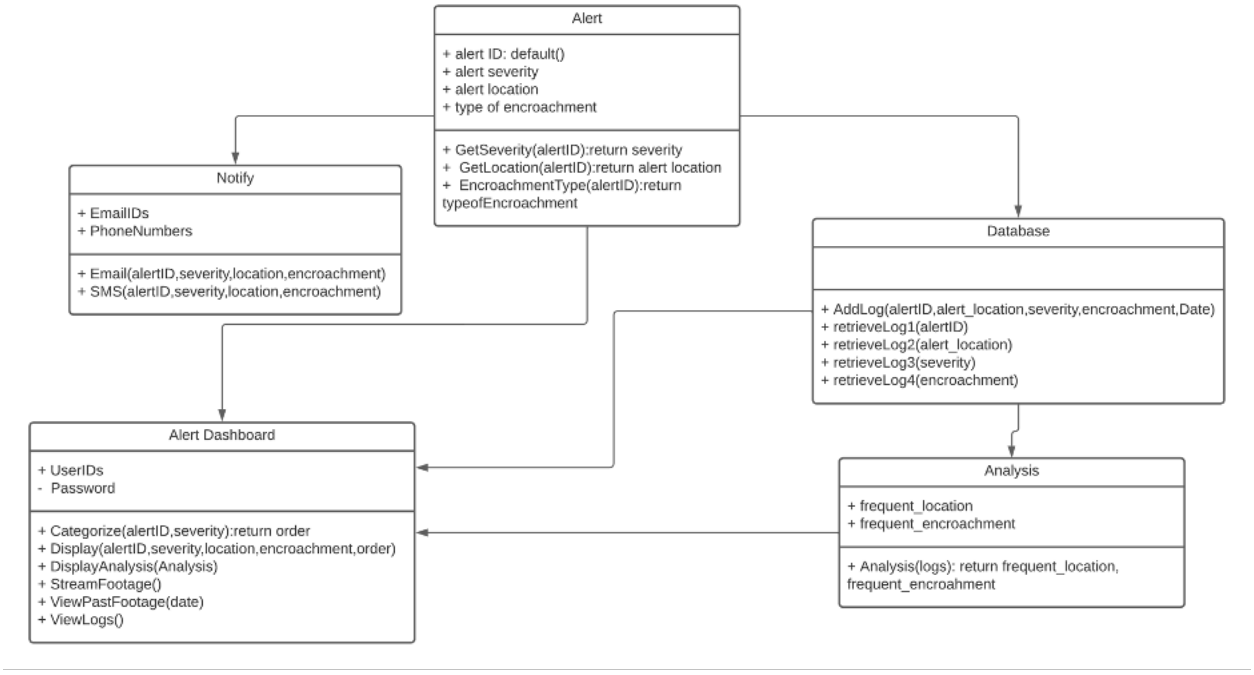
Actor:	Alert Subscribed Users
Description:	Alerts are sent to Security team members, and management authorities who have enabled notification channels and provided details through their chosen notification channel.
Preconditions:	• Authority has enabled notification • Authority has provided correct details during sign up • Encroachment has been detected by drones
Postconditions:	• Alert notification has been sent to authority through their preferred notification channel
Primary Pathway:	• Encroachment has been detected by drones and alerted from Video Processing API • Details about the encroachment are obtained: Severity, Location and type of encroachment from the Drone Firmware API • Alerts with all details are sent through SMS/Email to all registered users
Alternate Pathways:	• No notification is sent when no encroachment is detected
Exception Pathways:	Alert was not sent to registered users due to network issue

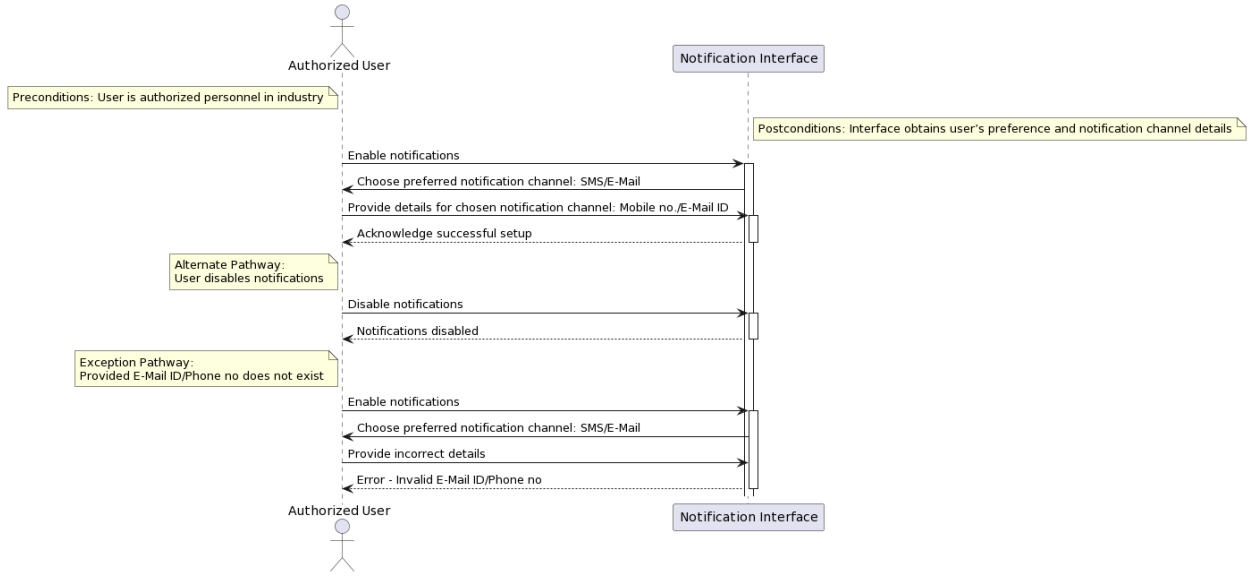
Use Case: Alert Analysis

Use Case ID:	403		
Use Case Name:	Analysis		
Traceability:			
Created By:	Lalit Arvind Balaji	Last Updated By:	Lalit Arvind Balaji
Date Created:	11/19/23	Date Last Updated:	11/19/23

Actor:	Authorized Admin User
Description:	Retrieves logs from database and makes analysis on vulnerabilities on current security system, the location where security needs to be tightened etc.
Preconditions:	• The database contains previous records of encroachment
Postconditions:	• An analysis on past encroachment records
Primary Pathway:	• Retrieves logs from the database • Algorithm extracts prominent common factors in encroachment logs • Analysis is consolidated and sent to user dashboard for the management to take appropriate decisions
Alternate Pathways:	• None
Exception Pathways:	• No previous records leads to no analysis made

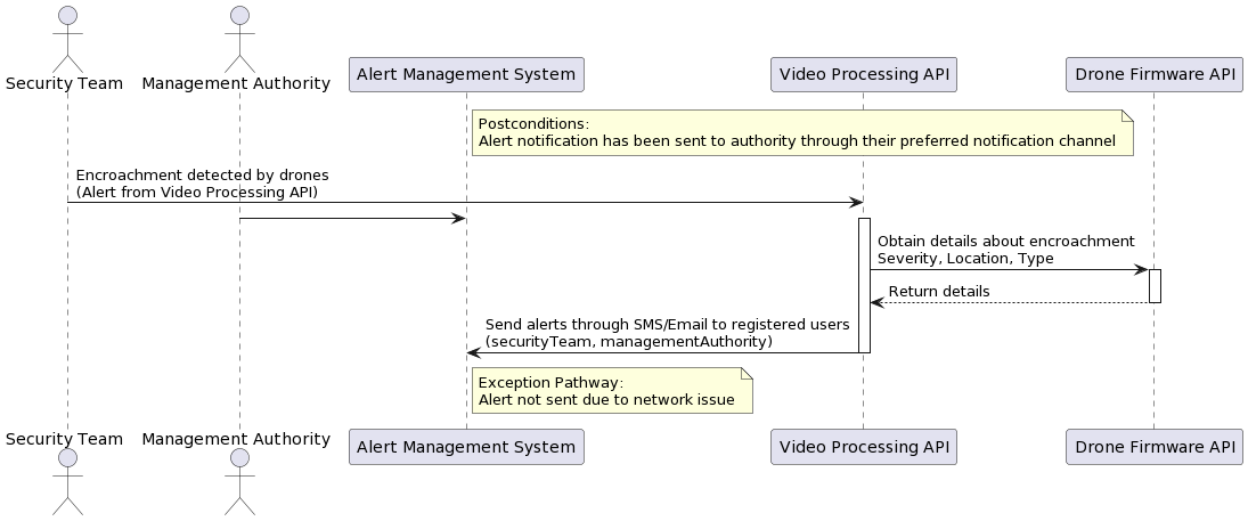
- Class Diagram and Sequence Diagrams





The diagram illustrates the interaction between an authorized user and a notification interface. The user has the option to enable or disable notifications. When choosing to enable notifications, the user must select a notification channel and furnish the required details. Conversely, if the user opts to disable notifications, the system will deactivate the notification feature. In cases where the user provides

incorrect details, the notification interface responds by displaying an error message to inform the user of the issue.



The diagram illustrates the workflow involving the security team management authority, the video processing app, and the drone firmware app for detecting and responding to encroachments. Upon detecting an encroachment, the video processing app initiates an alert sent directly to the security team management authority. Subsequently, the security team management authority retrieves detailed information about the encroachment and proceeds to send an alert to registered users, ensuring a swift and comprehensive response to potential security threats.

5.1.4. Dashboard

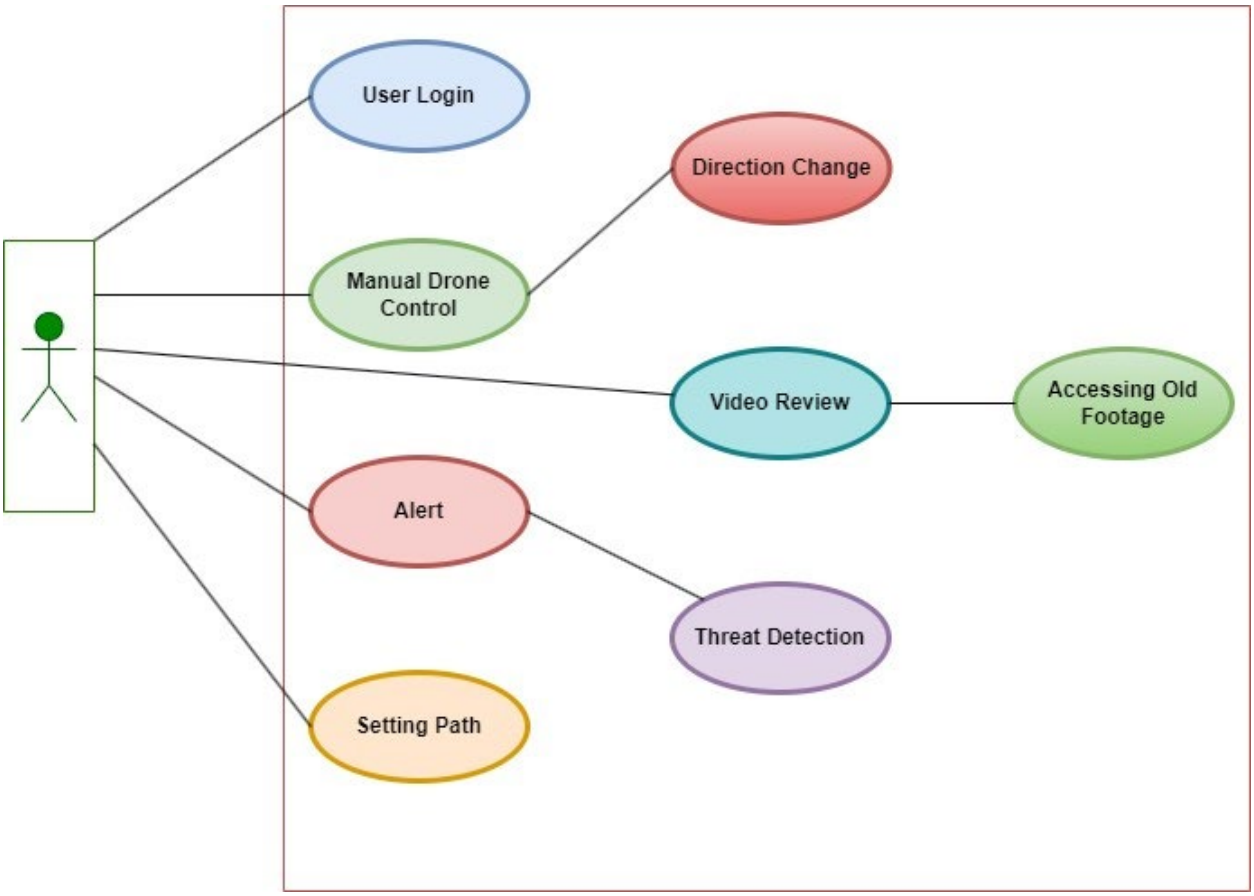
- Overview

The user requires an application to both send commands and receive information regarding the system's core functionality. The Dashboard facilitates user control over the drone, allows for footage viewing, and provides updates on any detected intrusions.

- Technical Details

The Live Stream Dashboard sub-component enriches user experience by offering diverse live camera footage options from the drone. When manual control or access to drone information is needed, the Drone Manual Control component provides users with the necessary controls, allowing them to draw predefined drone paths. In the case of intrusions, the Alert Display API promptly notifies the user. Additionally, the application stores drone footage for retrospective viewing through the dashboard, ensuring a comprehensive and accessible record of earlier activities. This integrated functionality enhances user engagement and situational awareness within the system.

- Use Case Diagram and Use Cases



Use Case: User Login

Use Case ID:	001		
Use Case Name:	User Login		
Traceability:			
Created By:	Aditya Pant	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

Actor:	Operator
Description:	This use case entails users logging in and logging out
Preconditions:	• The operator has the username and password
Postconditions:	• The user ID and password match and login is successful.
Primary Pathway:	• The operator goes to the dashboard where they put their ID and password to login.
Alternate Pathways:	• None
Exception Pathways:	• The user ID and password mismatch.

Use Case: Manual Drone Control

Use Case ID:	002
Use Case Name:	Manual Drone Control
Traceability:	

Created By:	Aditya Pant	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

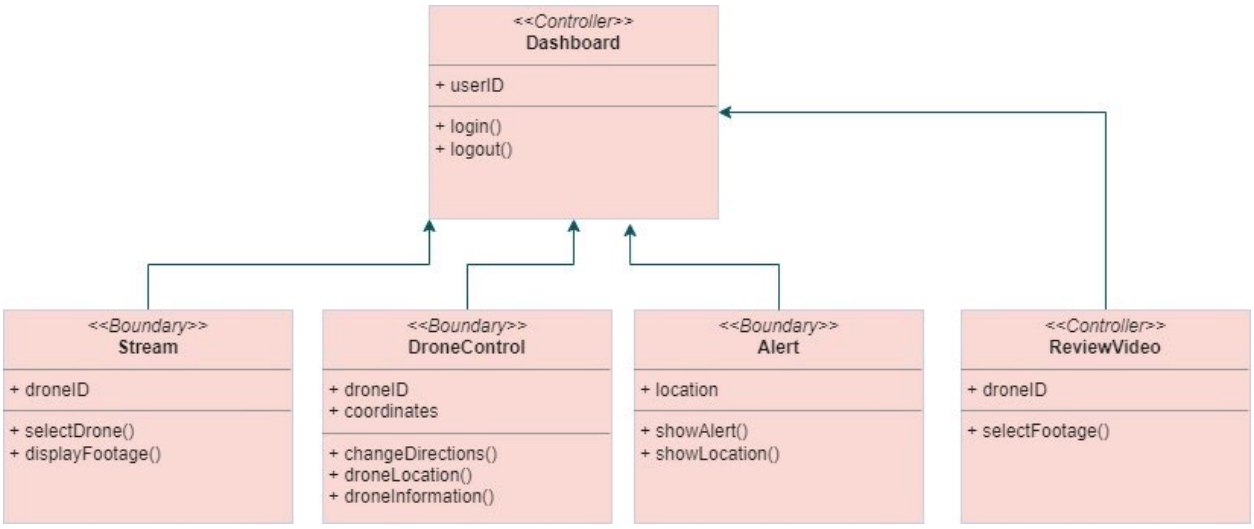
Actor:	Operator
Description:	This use case describes the operator's process of controlling the drone.
Preconditions:	• Logged into the system as the operator. • Knowledge about controlling drones1.
Postconditions:	• Drone is maneuvered in the right path.
Primary Pathway:	• The operator logs into the dashboard using user ID and password. • The operator uses the Manual Drone Controller to maneuver the drone.
Alternate Pathways:	• Use the physical drone controller instead of the software one.
Exception Pathways:	• The controller loses contact with the drone.

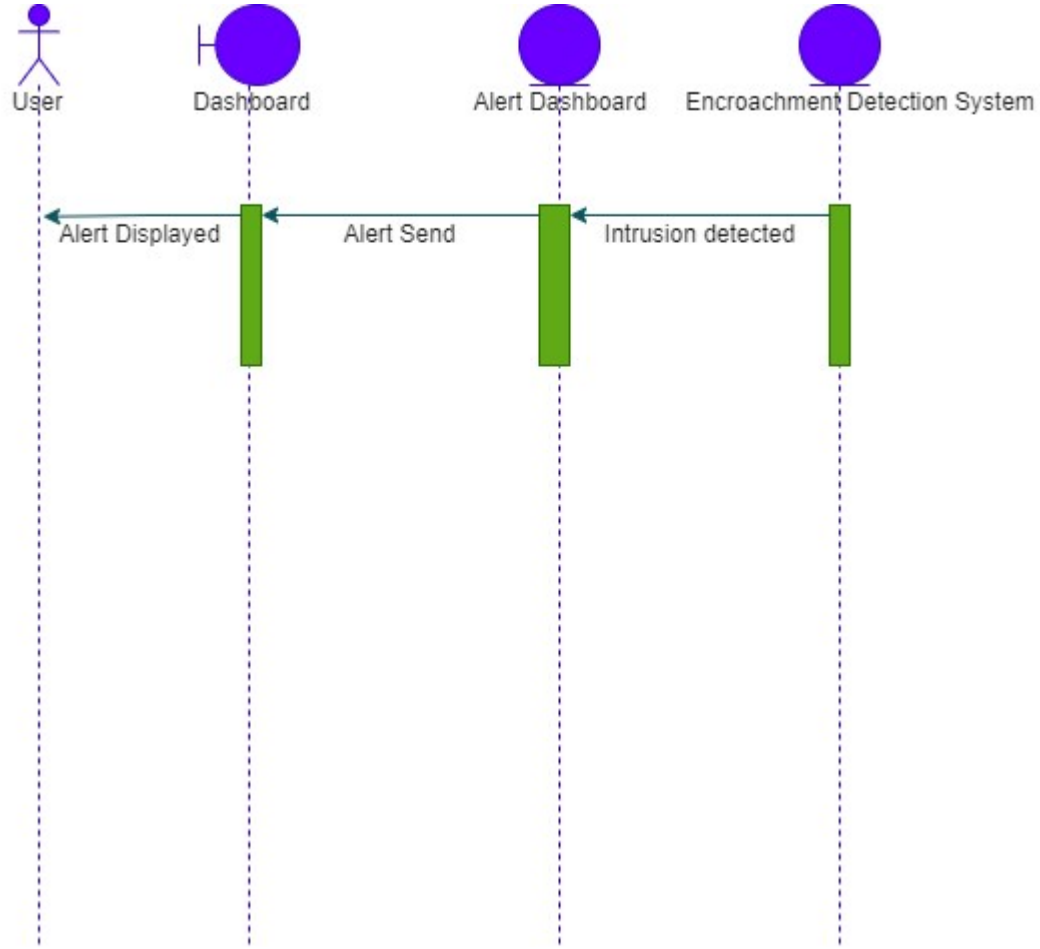
Use Case: Alert

Use Case ID:	003		
Use Case Name:	Alert		
Traceability:			
Created By:	Aditya Pant	Last Updated By:	11/19/2023
Date Created:	11/19/2023	Date Last Updated:	11/19/2023

Actor:	Operator
Description:	This use case describes the operator's process of receiving alerts.
Preconditions:	• Logged into the system as the operator.
Postconditions:	• Requirement actions taken against the intrusion.
Primary Pathway:	• The operator logs into the dashboard using user ID and password. • The operator watches out for an alert in the dashboard.
Alternate Pathways:	• The intrusion is not detected, and the alert is not issued.
Exception Pathways:	• The alert malfunctions and does not reach all required users.

- Class Diagram and Sequence Diagrams





Drone surveillance operates continuously, with the drone constantly monitoring the designated area. Upon detecting an intrusion, the alert dashboard is promptly notified.

6. Implementability

6.1. Overview

The Drone-Based Encroachment Detection System introduces a cutting-edge approach to security, combining drone technology, AI algorithms, and real-time surveillance. This overview encompasses an analysis of the system's implementability through both theoretical examination and practical prototype demonstration.

6.2. Structure and Naming

6.2.1. Aerial Surveillance Drones

- Description: Equipped with advanced cameras and sensors for data collection.
- Naming: Identified as "Eye in the Sky" drones, emphasizing their role in comprehensive surveillance.

6.2.2. Ground Control Station

- Description: Centralized control hub managing drone fleets, mission planning, and regulatory compliance.
- Naming: Referred to as "Command Central," highlighting its pivotal role in orchestrating drone operations.

6.2.3. Encroachment Detection Algorithm

- Description: Employs computer vision and machine learning for real-time threat identification.
- Naming: Known as the "Guardian Algorithm," emphasizing its protective function.

6.2.4. User Interface

- Description: Comprises a real-time dashboard and an alert application for user interactions.
- Naming: Named "Watchtower Interface" for the dashboard and "Alert Sentinel" for the alert application.

6.2.5. Data Management

- Description: Utilizes a centralized RDBMS for critical data storage and a surveillance record storage for archiving.
- Naming: Referred to as the "Data Citadel" for the RDBMS and "Archive Fortress" for surveillance record storage.

6.3. Use Case Implementability Analysis and Rationale

6.3.1. Use Case 1: Real-Time Surveillance

- Rationale: Efficient Monitoring: The "Watchtower Interface" provides a centralized view for efficient monitoring of live video feeds.
- Operational Continuity: The continuous operation of "Eye in the Sky" drones ensures comprehensive surveillance, minimizing blind spots.
- User Accessibility: The intuitive design of the interface allows users to customize views, enhancing user experience.
- Path Accuracy: Predefined drone paths are designed for optimal coverage, ensuring no areas are left unmonitored.

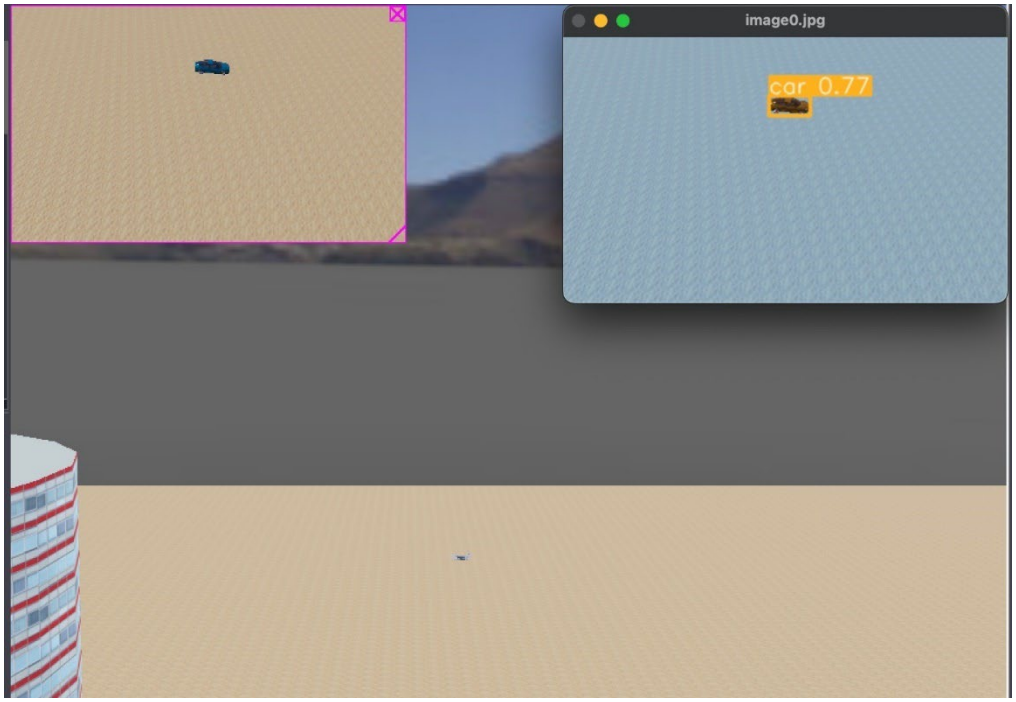
6.3.2. Use Case 2: Intrusion Alert Response

- Rationale: Timely Responses: The "Alert Sentinel" application facilitates swift responses to detected intrusions, minimizing response time.
- User Empowerment: Users are empowered with detailed information, including intrusion location and nature, for informed decision-making.
- Alert Generation: The algorithmic logic behind intrusion detection ensures accuracy, reducing false positives and negatives.
- Communication Channels: The application establishes secure communication channels, ensuring reliable alert delivery to relevant stakeholders.

6.4. Implementability Details

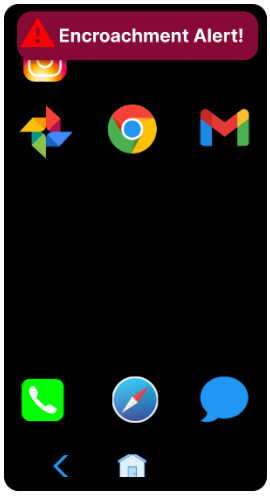
6.4.1. Real time monitoring

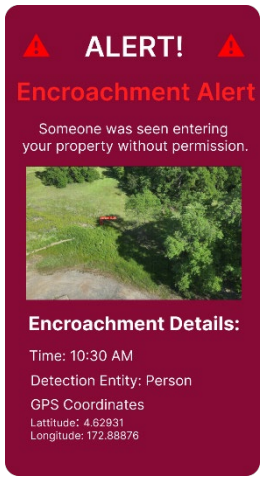
- Operation:
  .1. Realtime surveillance dashboard
  .2. The drones continuously monitor the industrial area.
- Screenshot:



6.4.2. Intrusion Alert

- Operation:
  .1. Users receive alerts if the system detects any encroachment.
  .2. The alerts will be sent to the user's registered mobile phone.
  .3. It will send the time and encroachment details along with the GPS Coordinates.
- Screenshot:





7. Presentations

7.1. Overview Screencast

- The overview screencast is a high-level presentation of overall system idea and overview.
- It is aimed for the non-technical stakeholder.
- URL - https://youtu.be/ArMCFcpaHNA

7.2. Detailed Presentation of Flow and Implementability

7.2.1. Drone Operations

- Ameya Shahu is responsible for this function
- The drone operation components responsible for the controlling drone
- Screencast - https://youtu.be/X4ZLF7K6O68

7.2.2. Video Processing

- Lalit Arvind Balaji is responsible for this function
- The video processing component of our system is essential for real-time analysis of drone footage to detect encroachments in the industrial area.
- Click here to view Screencast

7.2.3. Alert Generation

- Pravalika Mukkiri is responsible for this function.
- Alert Generation is an important function of the system. It handles sending real time notifications to the registered users when an encroachment is detected.
- Screencast https://drive.google.com/file/d/1noAIN3IEbzml6UCS_1URWI0nx8425Tli/view?usp=drive_link

7.2.4. Dashboard

- Aditya Pant is responsible for this function.
- Dashboard is the main UI component that helps the user make full use of the range of features offered by our system.
- Screencast link:

https://drive.google.com/drive/folders/1Wa09NK9xNkpil0Om-2oeOkYfKtEuEXHl?usp=sharing

8. Conclusion

8.1. Overview

Our Drone-Based Encroachment Detection System has ushered in a new era of security, seamlessly integrating drone technology, AI algorithms, and data management. This innovative solution offers real-time surveillance, alerting, and historical data analysis, setting unprecedented standards in industrial security. By fostering adaptability and resilience, our project not only addresses immediate security concerns but also lays the groundwork for the future evolution of surveillance practices.

8.2. Lessons Learned

- System Resilience Matters: Unexpected challenges highlighted the importance of designing a resilient system capable of withstanding diverse environmental conditions and potential failures.
- User Feedback Drives Improvement: Real-world feedback from operators shed light on the importance of incorporating user suggestions for a more intuitive and efficient system.
- Cybersecurity Vigilance: Instances of potential cyber threats underscored the critical need for robust cybersecurity measures to protect the integrity of the system.
- Scalability is Crucial: As the project expanded, the significance of scalability became evident, emphasizing the need for a system that can seamlessly grow with evolving requirements.

8.3. Recommendations for Improvement

- Enhanced Cybersecurity Protocols: Continuously update and reinforce cybersecurity protocols to stay ahead of emerging threats and ensure the system's integrity.
- Scalability Enhancements: Invest in technologies and infrastructure that facilitate easy scalability, accommodating an increasing number of drones and surveillance areas.
- User-Centric Updates: Regularly update the user interface based on user feedback, making it more intuitive and user-friendly for efficient operation.
- Collaborative Partnerships: Forge partnerships with other technology innovators and security solution providers to foster collaboration and integrate complementary features.
- Environmental Adaptation: Further refine the system's adaptability to diverse environmental conditions, ensuring optimal performance in various industrial settings.
- Continuous Training Programs: Establish ongoing training programs for operators to keep them abreast of the latest features and ensure proficient use of the system.

9. Appendix A: Credit Sheet

Team Member Name	Contributions
Aditya Pant	Detailed Design, Architecture and Conclusion
Ameya Shahu	Architecture, detail design, Presentation, Conclusion
Lalit Arvind Balaji	Problem Vision for a solution Requirements
Pravalika Mukkiri	Implementability Presentations Conclusion