CSE 564 Project Report Number 3

Team 16

Team Member Names:

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

Table of Contents

Table of Contents

1. Received Requirements

1.1. Realtime Surveillance

1.1.1. Feature

- Continuous real-time surveillance of the industrial area.

1.1.2. Requirement Source

- Industrial Security Team

1.1.3. Inputs and Stimulus

- Data from drones, motion sensors, and perimeter cameras.

1.1.4. Sequence of Operations and Responses

- Drones continuously monitor the industrial area.
- If unauthorized motion is detected, drones send alerts to the central control system.
- The control system triggers an alarm for security personnel to respond.

1.2. Autonomous Operation

1.2.1. Feature

- Drones should operate autonomously without the need of drone operators when needed.

1.2.2. Requirement Source

- System Architecture Team, Technical Team

1.2.3. Inputs and Stimulus

- Video data from the drones, autonomous drone algorithms for encroachment detection

1.2.4. Sequence of Operations and Responses

- Drones operate autonomously, following specified flight patterns and employing algorithms to identify infringement.
- They can make real-time judgments to monitor encroachers.

1.3. Data Processing in Realtime

1.3.1. Feature

- Real-time data processing with reduced latency.

1.3.2. Requirement Source

- Development Team and Data Processing Team

1.3.3. Static Numerical Requirement

- Data must be processed in real-time, with a delay of no more than 500 milliseconds.

1.3.4. Dynamic Numerical Requirement

- The system must process data from up to ten drones at the same time.

1.4. Surveillance Range

1.4.1. Feature

- Extended surveillance range for drones

1.4.2. Requirement Source

- Managers, Factory Owners, and Drone Manufacture

1.4.3. Static Numerical Requirement

- Drones must have a maximum surveillance range of at least 5 kilometers.

1.4.4. Dynamic Numerical Requirement

- The system must operate and provide continuous monitoring with the drones even in inclement weather.

1.5. Data Export Interface

1.5.1. Feature

- Easy data export for external storage and analysis

1.5.2. Requirement Source

- Development Team and Security Administrators

1.5.3. Source of Input or Destination of Output

- Exporting surveillance data to external storage devices or cloud platforms for long-term storage and analysis should be implemented.

1.6. Users Operating Interface

1.6.1. Feature

- User Friendly and interactive Control Interface

1.6.2. Requirement Source

- Drone operators, application users and technicians.

1.6.3. Source of Input or Destination of Output

- Users must be able to control drones and their operations on their devices using a user-friendly interface.

1.7. Data Logging

1.7.1. Feature

- Comprehensive data logging for audit and compliance

1.7.2. Requirement Source

- Compliance Regulations, Data research and Improvement team

1.7.3. Types of data and/or operations performed

- For auditing and compliance purposes, the system must log all intrusion occurrences, including timestamps, position, and drone actions.

1.8. Geographical Data Integration

1.8.1. Feature

- Geographical Data Integration for exact feature mapping

1.8.2. Requirement Source

- Geographic Information System (GIS) Providers

1.8.3. Types of data and/or operations performed

- To improve location-based analysis and accurate monitoring inside the industrial area, the system should integrate geographical data.

2. Derived Requirements

2.1. Real-time Surveillance Streaming

2.1.1. Feature

- Sharing Real-time footage with Central control system

2.1.2. Requirement Source

- Real-time Surveillance, Autonomous operation

2.1.3. Inputs and Stimulus

- Data from drone surveillance cameras

2.1.4. Sequence of Operations and Responses

- Drones should share live footage of the actions of the encroached entity while following it.

2.2. Operation types

2.2.1. Feature

- Operation types in autonomous operation

2.2.2. Requirement Source

- Autonomous operation

2.2.3. Inputs and Stimulus

- Instruction/ requests from Central control system

2.1.5. Sequence of Operations and Responses

- **Scheduled monitoring** - The drones are scheduled to go rounds in regular intervals over the entire industrial zone.
- **Demand monitoring** - The drones can be requested to monitor a particular designated area within the industrial zone for additional protection.

2.3. Load Balancing

2.3.1. Feature

- Load balancing for data processing

2.3.2. Requirement Source

- Data Processing in Realtime

2.3.3. Static Numerical Requirement

- Processing data from all drones simultaneously should not cause delay more than 100ms.

2.3.4. Dynamic Numerical Requirement

- The system should distribute data processing tasks effectively when multiple drones (up to 10) are operating simultaneously, ensuring that performance is not degraded.

2.4. Real-time fused processing

2.4.1. Feature

- Data Fusion and Analysis
- Real-time integration and analysis of data from multiple sources

2.4.2. Requirement Source

- Data processing in real-time

2.4.3. Static Numerical Requirement

- The combined processing of data from all the sensors and synchronization should not cause more than 500ms delay.

2.4.4. Dynamic Numerical Requirement

- The system should be capable of fusing data from drones, motion sensors, and perimeter cameras for real-time analysis.
- This analysis should include the identification of intrusions and other anomalies in the industrial area.

2.5. Interactive Control interface

2.5.1. Feature

- Interface to view recordings.

2.5.2. Requirement Source

- User Friendly Control Interface

2.5.3. Source of Input or Destination of Output

- Interface should allow users to view real-time footage captured by drone cameras and the geographic location of drone when encroachment is detected.

2.6. User access control

2.6.1. Feature

- User access authorization and authentication

2.6.2. Requirement Source

- User Control

2.6.3. Source of Input or Destination of Output

- The user-friendly control interface should include role-based access control allowing different users to have varying levels of control and access to the system's features.

2.7. Secure logging

2.7.1. Feature

- Access Management Logging

2.7.2. Requirement Source

- Data Logging

2.7.3. Types of data and/or operations performed

- Surveillance data exported to external storage or cloud platforms should be transmitted securely using encryption and authentication protocols to protect against unauthorized access.

2.8. Geographic data enhancement

2.8.1. Feature

- Updating of geographic data

2.8.2. Requirement Source

- Geographic data integration

2.8.3. Types of data and/or operations performed

- The system should not only integrate geographical data but also continually update and enhance this data to improve feature mapping and location-based analysis.

3. Architecturally Significant Elements

3.1. Overview and Architectural Views

In the context of our drone-based encroachment detection system, a comprehensive architectural view is essential to understand how various components interact to achieve our system's goals. The 4+1 model provides a holistic perspective –

- **Logical View** - The Logical View focuses on the high-level structural elements of our system.
- **Process View** - The Process View delves into the dynamic aspects of our system.
- **Development View** - The Development View provides insights into software development.
- **Physical View** - The Physical View considers the deployment and hardware aspects of the system.

3.2. Logical/Quality Elements and why each is architecturally significant

Several logical and qualitative components contribute to the architectural importance of the system in the Logical View –

- **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.

3.3. Database Elements and why each is architecturally significant

- **Data Storage and Retrieval** - Databases are essential for archiving reference material and historical data, which makes trend analysis and threat tracking easier.
- **Data Consistency** - To guarantee the accuracy of threat detection and reporting, it is essential to maintain consistent, current data throughout the system.
- **Redundancy and Failover** - In the event of a hardware or network failure, database components must have redundancy and failover procedures in place to safeguard system continuity and avoid data loss.
- **Data Privacy and Compliance** - With features like encryption and access controls, the database should support both data privacy and regulatory compliance.

3.4. Reuse Elements and why each is architecturally significant

The creation of a drone-based encroachment detection system must prioritize reusability:

- **Sensor Reusability** - Designing drones with interchangeable sensors allows you to adapt to various situations and applications without having to completely redesign the hardware.
- **Algorithm Reusability** - Reusable computer vision and machine learning algorithms allow for effective adaptation to novel challenges in encroachment detection.
- **Integration Reusability**- By reusing existing integration components, a well-defined integration approach guarantees that the system can be quickly adapted to different environments.
- **Reusable User Interface** - User interface components facilitate the creation of customized dashboards and interfaces for a range of users and stakeholders.

4. Draft Architecture

4.1. Overview and Architectural Views

- In the architectural framework of our drone-based encroachment detection system, each view plays a pivotal role in ensuring a robust and adaptable solution.
- The Logical View describes the key components in charge of user interfaces, camera video processing, intrusion warning creation, and data storage.
- The Process View delineates the dynamic interactions between system components, including drone operations, flight planning, and camera video processing.
- The emphasis of Physical View moves to the hardware components of our system, which includes drones, databases, control networks, and camera setups. It guarantees that the physical architecture of the system is adequately adapted to suit the demands of the specified settings.
- The Deployment View highlights the technological foundations, such as the software programming languages used for intrusion detection in camera video, drone location monitoring, and database administration.
- The system's versatility shows in the Scenarios View, where it handles varied scenarios including user interactions with operators, efficient flight scheduling between charging intervals, and quick alerting systems when encroachments are discovered.
- These architectural perspectives work together to provide a well-rounded system that caters to a wide range of applications while maintaining efficiency, security, and responsiveness.

4.2. Logical / Quality Elements

- **Alert System** - The alert system's roles include notifying authorities and property owners about detected encroachments for timely responses.
- Simultaneously facilitating emergency management, environmental preservation, and perimeter security for various locations, such as factories, farmlands, and forested areas.
- **Drones** - Drones offer efficient boundary surveys, routine patrols, high-resolution data collection, and swift response for encroachment detection, enhancing system accuracy and timely action.
- **Drone Operation** - A drone management system supervises fleets, streamlines mission planning, and enforces regulatory adherence.
- It provides real-time monitoring, schedules maintenance, and optimizes operational costs, enhancing drone efficiency in diverse sectors.
- **Video Processing System** - Camera systems in encroachment detection monitor boundaries, detect intrusions, and offer continuous surveillance, enabling quick responses to encroachments.
- They also aid in dispute resolution, community awareness, and historical record-keeping for trend analysis and ongoing monitoring.

4.3. Database Elements

- **Centralized Information Management Database** - The centralized RDBMS serves as the core data repository for storing critical information in our drone-based encroachment detection system.
- **Surveillance Record Storage** - Camera video and accompanying data are archived efficiently in our drone-based encroachment detection system for analysis and retrieval.

4.4. Reuse Elements

- State of the Art open-source drone simulator which can efficiently work in limited computing.

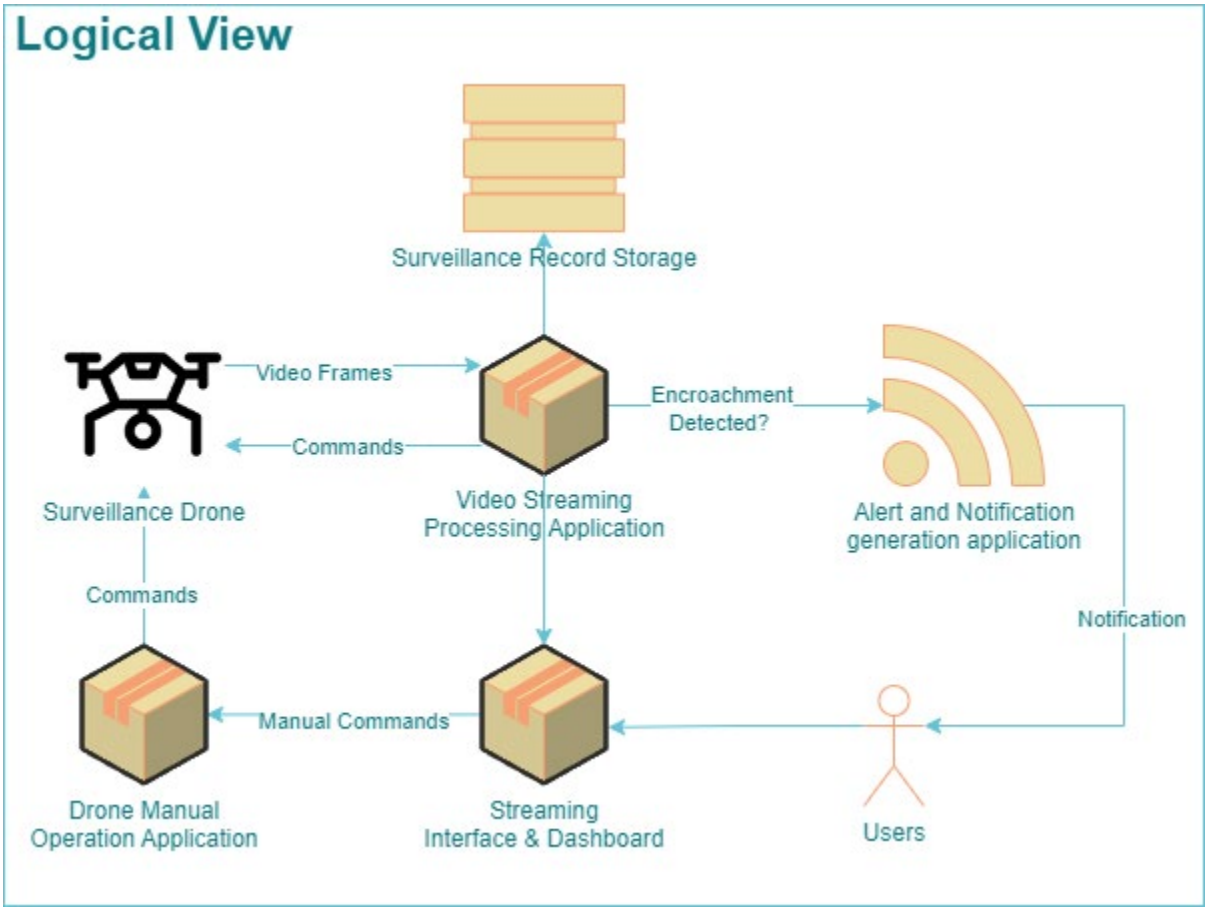
- Open-source drone footage for data model training for encroachment detection engine.
- Stable and community developed data cleaning and machine learning libraries.
- State of the art pretrained deep learning data model which are trained on millions of images.
- Open-source programming language, python for model training and video stream processing.
- Cloud based RDBMS database and storage service such as AWS S3.

4.5. Logical View

4.5.1. Introduction and rationale for the view

Our surveillance system integrates drones, cameras, and deep learning for encroachment detection. The logical view highlights software components, user interfaces, and alerting systems that structure its operation. It also enables live streaming and archives surveillance footage, fostering real-time monitoring and historical analysis of encroachment.

4.5.2. Model / Graphical Representation



4.5.3. Key Details

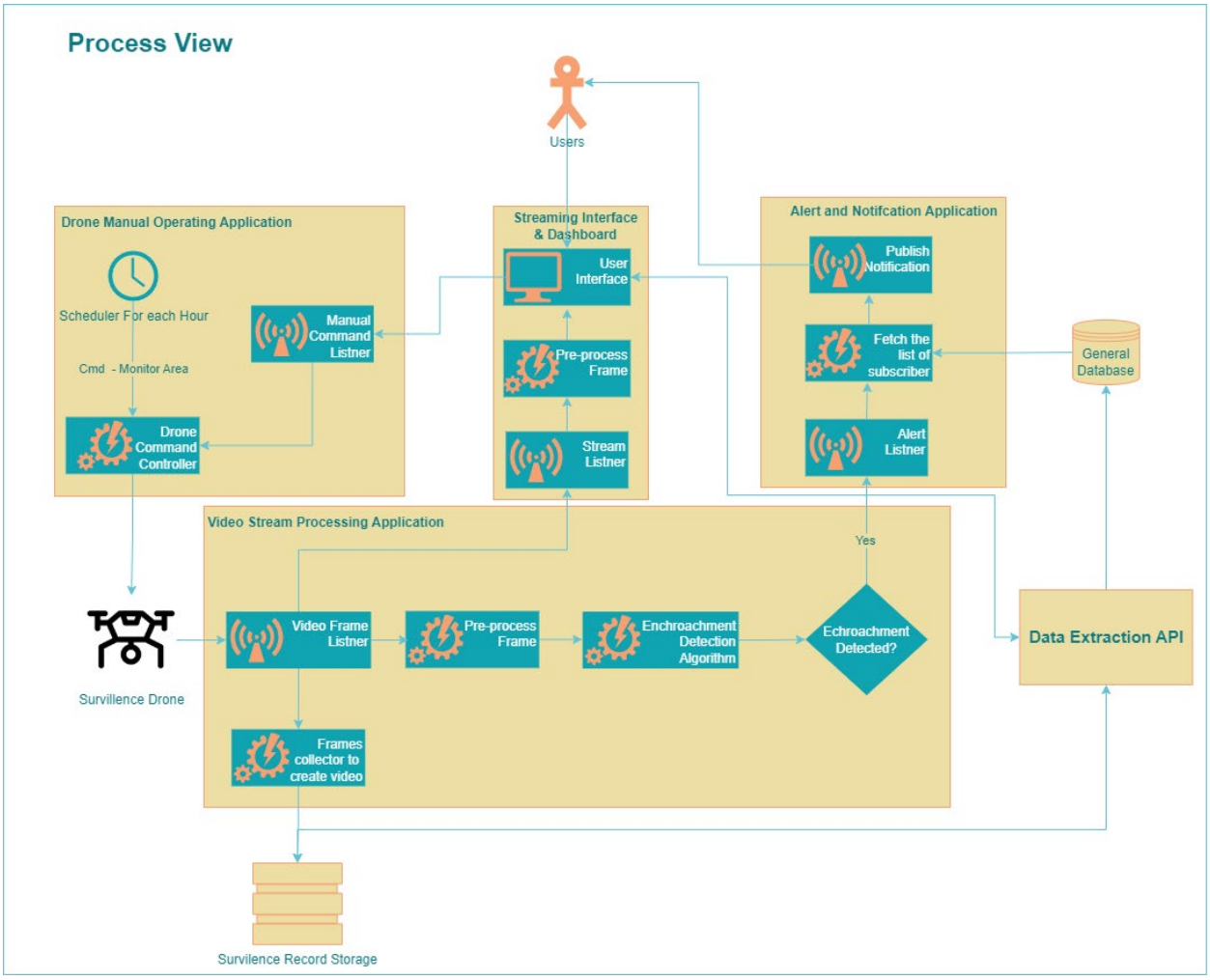
- **Streaming Interface and Dashboard** - The interface offers live video streams from drones' cameras for real-time area monitoring, accompanied by user-customizable camera views, geographic positioning, and navigation.
- Additionally, it supports video review and in-depth analysis for post-event investigative work.
- **Drone Operation Application** - The system enables prompt responses to intrusion alerts through user-directed drone actions and incorporates safety measures like geofencing.
- It offers robust access control, seamless machine learning integration for intrusion detection, and a live telemetry dashboard for real-time drone performance data.
- **Surveillance Drone** - The system leverages GPS tracking for precise drone navigation and location data.
- It ensures real-time data transmission, automatic alert responses, and remote manual drone control with live camera feed for dynamic surveillance adjustments.
- **Alert Application** - The application offers an alert dashboard providing real-time grouped notifications for quick situational analysis, with detailed alert information accessible, including intrusion type, timestamp, coordinates, and media.
- It supports various notification channels, tracks alert history for trend analysis, and integrates a map overlay for enhanced situational awareness and precise event location display.
- **Surveillance Records Storage** - The database manages user profiles, ensuring authorized access with contact details and access permissions.
- It maintains a substantial archive of timestamped, geotagged camera footage, historical encroachment records, and robust data resilience through backups and redundancy, enhancing system reliability and historical analysis capabilities.

4.6. Process View

4.6.1. Introduction and rationale for the view

The Drone Operating Application for real-time control, scheduled patrols, and intrusion alerts are the three main parts of the system. The Live Streaming Interface controls camera access, guarantees data security, and collects drone data in real-time. The Alert Application logs intrusion details for analysis, quickly initiates alerts, analyzes camera data, and detects intrusions.

4.6.2. Model / Graphical Representation



4.6.3. Key Details

- **Drone Data Monitoring** - To keep operators informed and in control, the app collects real-time data from drones, such as GPS information, height, speed, and more.
- By providing waypoints and flight information in advance, users can make routine patrols easier with pre-planned drone routes.
- **Video Stream Processing** - The system receives live video feeds from drones, processing them in real-time to detect encroachments through deep learning algorithms.
- It will generate alert if encroachment is detected to ensure timely responses to potential threats.
- **Alert Management** - The system efficiently manages alerts by grouping them based on severity and location, allowing for rapid situational analysis.
- Alerts are promptly delivered through various channels such as email, SMS, and push notifications, ensuring responsible personnel are notified for swift responses.
- **User Instruction Processing and Live Streaming** - The Live Streaming Interface ensures controlled access to live camera feeds based on user roles, while collecting real-time video and data from nearby drones.

- It prioritizes data privacy through encryption and robust security measures to prevent unauthorized access or manipulation of camera feeds.
- **Drone Scheduling and Operation** - The Drone Operating Application not only controls drone operations but also schedules routine monitoring patrols, ensuring hourly surveillance for enhanced security and threat detection.

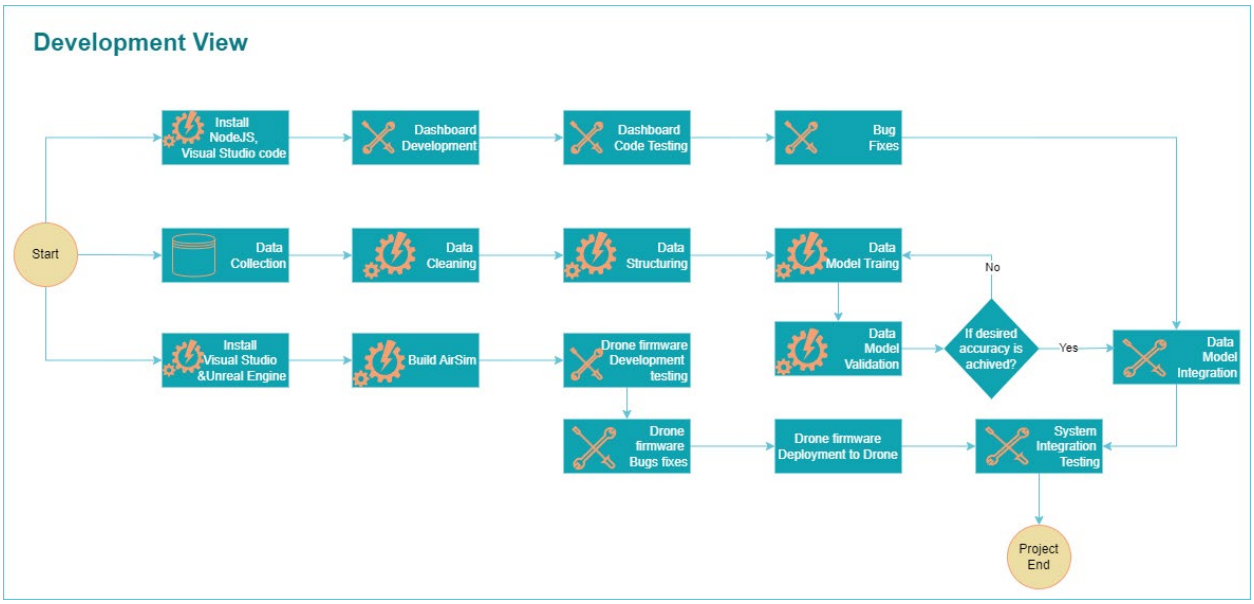
4.7. Development View

4.7.1. Introduction and rationale for the view

The Development View in the drone-based intrusion detection system's design gives insight into the software development perspective. It entails the selection of programming languages, the incorporation of machine learning models, and the development of a unified software infrastructure that enables real-time data processing, alert production, and responsive surveillance operations. This viewpoint assures that software components are efficiently planned, built, and maintained to serve the system's mission-critical functions. The development view can be segmented into 3 parts –

- Training Deep Learning model to identify encroachment.
- Simulation and configuration of drone flight patterns
- Dashboard creation and setting up communication channels to drones.

4.7.2. Model / Graphical Representation



4.7.3. Key Details

- **User Dashboard Development** - NodeJS is employed for web-app interface development, enabling user instructions and drone operation configuration.

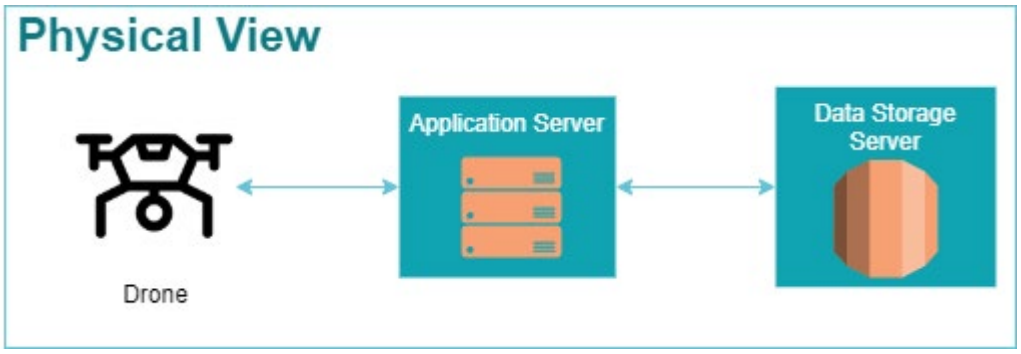
- Communication channels with the application server connect to all drones for data exchange, while the application server serves as a central hub for user commands and database connectivity, allowing access to real-time drone data and historical records.
- **Encroachment Detection Model Training** - Python is the language of choice for training the YOLO8 model, enabling object detection in drone footage, and extracting object positions.
- An algorithm is designed to calculate object distance and provide drone motion directives, enhancing the system's ability to track and follow detected objects effectively leveraging CV2.
- **Drone Simulation Setup and Firmware Development** - The Microsoft AirSim Drone Simulation Setup facilitates realistic testing and development of drone operations in various environments, ensuring system readiness.
- Drone firmware development is essential to customize drone behavior, optimizing performance and responsiveness for real-world encroachment detection scenarios.

4.8. Physical View

4.8.1. Introduction and rationale for the view

The Physical View of the drone-based encroachment detection system encompasses the hardware and infrastructure aspects. It involves the deployment of drones with specific capabilities and sensors, along with the selection of cameras for high-quality footage capture. The control network plays a crucial role in facilitating communication and data transmission. This view ensures that the hardware components are robust and resilient to withstand varying environmental conditions. It also includes considerations such as power supply and charging stations to maintain uninterrupted surveillance and swift threat response capabilities.

4.8.2. Model / Graphical Representation



4.8.3. Key Details

- **Drone** - The drone conducts encroachment monitoring by flying in designated areas, with options for scheduled monitoring at intervals or demand-driven focused surveillance.
- It adapts to adverse weather conditions to ensure operational effectiveness and security objectives.
- **Bare Metal Application Server** - The Application server receives user dashboard requests, communicates instructions to drones, and collects live drone data.

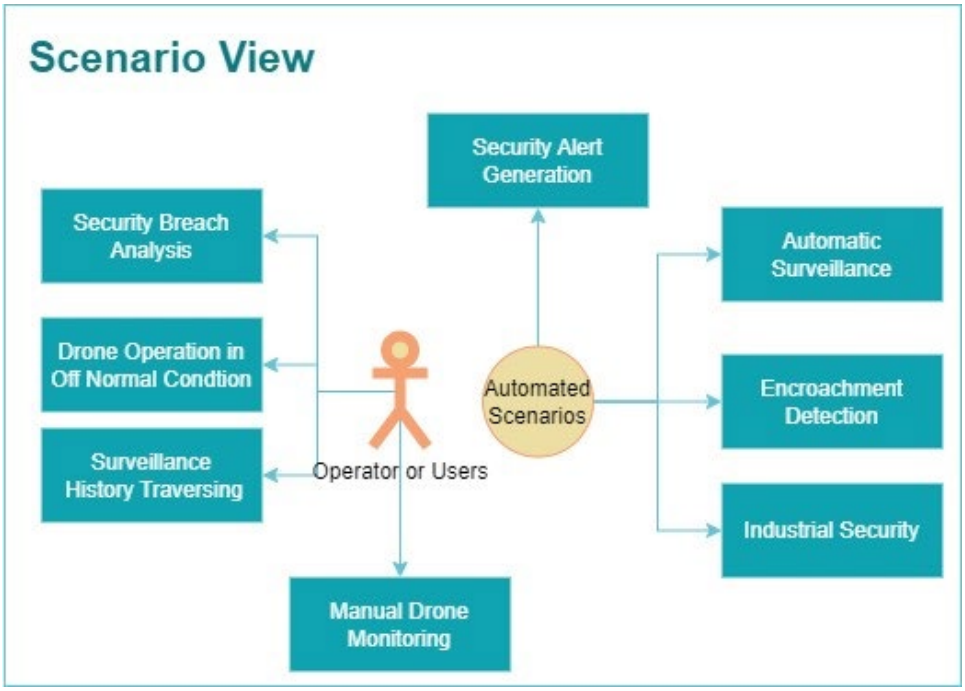
- It streams real-time information to the user dashboard, encrypts and transfers data to the Data Storage server, and accesses past data from the Data Storage server, decrypting and delivering it to the user dashboard upon request.
- **Database and Data Storage Server** - The Data Storage Server receives encrypted drone data from the Application server, stores, and indexes it for efficient access.
- It retrieves stored data upon request, automatically managing data retention by removing older records after a configured time, enhancing storage efficiency.

4.9. Scenario View

4.9.1. Introduction and rationale for the view

The Situation A look inside the drone-based incursion detection system reveals information about its flexibility in real-world circumstances. It includes user interactions with operators, scheduled monitoring, and real-time warning in the event of an incursion. The perspective displays the system's efficiency in a variety of settings, ranging from industrial sites to rural landscapes. It demonstrates the system's adaptability and response to changing operating needs, allowing it to be used in a variety of applications.

4.9.2. Model / Graphical Representation



4.9.3. Key Details

- **Automated Scenarios** - The system automatically detects encroachments in camera footage, generating alerts for designated personnel.
- Continuous surveillance is carried out autonomously, monitoring for encroachments in real-time without manual intervention.

- Advanced data models ensure highly accurate and precise detection of encroachments, enhancing security for industrial applications with state-of-the-art measures.
- **User Driven Manual Scenarios** - Users can seamlessly review camera footage in real-time or retrospectively, offering detailed examination through zoom and navigation controls.
- Drones exhibit reliable performance even in challenging weather conditions, including rain, extreme heat, and low battery situations.
- Access to one month of stored footage empowers users for retrospective review and in-depth analysis of surveillance history.

5. Initial Risk Analysis

5.1. Overview

Our project faces several key risks that require meticulous attention. Drone performance degradation due to adverse weather conditions is the top priority, with a prototype being developed and tested to ensure reliability. The challenge of correctly identifying known entities in an industrial environment without generating false alarms is significant and addressed by dynamically adjusting detection thresholds. The risk of exceeding storage capacity is managed through data caching and a retention policy. Finally, cybersecurity is of utmost concern, with robust measures like encryption and secure protocols in place to safeguard against cyberattacks and data breaches, ensuring system integrity and data protection. Each risk is being diligently addressed by dedicated team members to ensure the system's effectiveness and reliability in diverse operational scenarios.

5.2. Drone Performance Degradation and Connectivity Issues

- The highest priority risk is the performance degradation of the drone during adverse weather conditions such as hurricane, snow, thunderstorms etc.
- The drone may even fly away to somewhere in extreme situations. In these situations, encroachment detection is questionable because the drone cannot operate properly in those situations.
- The risk is significant because it has a direct impact on the system's essential functionality. It is the top priority since it is the most urgent threat to the project's success.
- **Pravalika Mukkiri** is closely analyzing the risk and collecting datapoints to mitigate the risk.
- To mitigate this risk, a specific prototype will be built and carefully tested to reduce the danger of severe weather affecting drone performance.
- This prototype will go through controlled adverse weather scenarios, gathering data on flight stability, sensor accuracy, and communication reliability.
- Data analysis will reveal areas for improvement, allowing tweaks to be made to improve the drone's performance in difficult settings.
- The prototype will be tested and validated iteratively to ensure that it fulfills set performance standards.
- Lessons acquired and enhancements achieved will be incorporated into production drones, lowering the danger of degraded surveillance in the operational system during severe weather conditions.

5.3. Encroachment Detection model identifying known entity

- In the presence of multiple ongoing activities in the industry, especially when conducted by recognized industry professionals, the system should not misidentify them as encroachments, as this could result in false alarms.
- The risk is highly significant because such false alarms would erode trust in the system's performance, potentially leading to confusion between legitimate alerts and false ones, thereby hindering the security team's decision-making process.

- **Lalit Arvind Balaji** is actively addressing this risk by implementing dynamic encroachment detection threshold adjustments based on environmental conditions and the industrial area's activity level, ultimately reducing the occurrence of false alarms during peak operational periods.

5.4. Exceed Storage capacity

- Data is collected from various sensors and drones, including video cameras and motion sensors.
- This data is stored in a scalable storage/database.
- The risk is a priority due to limited and expensive storage, making efficient data management crucial for incident reference.
- Storage of captured data is essential for the system's functionality, emphasizing the need for storage management to adapt to data volume.
- **Aditya Pant** is responsible for addressing this risk.
- A prototype solution involves caching data for a short interval after recording.
- After the caching period, data is moved to storage.
- A fixed retention period of three months is established, with data erasure unless needed for specific purposes.

5.5. Security of the System and Unauthorized Access

- Unauthorized access jeopardizes the integrity and security of the system.
- This illegal access might damage vital data, jeopardizing the system's credibility and functioning.
- **Ameya Shahu** is exploring different security standards as well as best practices to address security risk.
- To address this risk, rigorous authentication and access control techniques are used to prevent unauthorized workers from accessing sensitive information.
- Continuous monitoring and audit trials are set up to detect and respond to any illegal access attempts as soon as possible.
- Data encryption provides further protection against data disclosure, even in the case of unwanted access.
- Security audits and penetration testing are performed on a regular basis to detect weaknesses and increase the system's defenses against cyber-attacks.

6. Conclusion

6.1. Expanded Derived Requirements

6.1.1. Core System Requirements

- Derived requirements expand on the core system requirements, including real-time surveillance streaming, operation types, load balancing, real-time fused processing, control interface, user access control, secure logging, and geographic data enhancement.
- Database elements, such as data storage and retrieval, data consistency, redundancy and failover, and data privacy and compliance are discussed and explained.

6.2. Draft Architecture and Associated Initial Risk

6.2.1. 4+1 Architecture Model

- Database elements, such as data storage and retrieval, data consistency, redundancy and failover, and data privacy and compliance are discussed.
- The logical view of the system highlights key components like the streaming interface, drone operation application, and alert application.
- The process view outlines how the system's components interact dynamically. It includes drone data monitoring, pre-planned paths, intrusion alerts, controlled access to live camera feeds, camera data management, and alert generation.
- The development view provides insights into the development process, including model training, simulation, dashboard creation, and communication channels setup.
- The scenario view explores automated scenarios and user scenarios, demonstrating the system's capabilities in detecting encroachments, generating alerts, and providing users with historical surveillance data.

6.2.2. Architectural Initial Risk

- The initial risk analysis identifies and prioritizes key risks, including drone performance degradation, false alarms, storage capacity issues, and security threats.

6.3. Future Enhancements

6.3.1. Scalability in terms of Future Security Standards

- As the industrial base may expand or it requires new surveillance methods or modes, the system should be scalable for all the future updates.
- The system should be able to adapt to improved security guidelines by the authorities.

6.3.2. Advanced Sensor Integration

- Investigating the use of sophisticated sensors and technologies, such as thermal imaging, LiDAR, or AI-based anomaly detection, to improve surveillance capabilities.
- This advanced sensor integration will help in better data collection and improve data analysis process.

7. Appendix A: Credit Sheet

Team Member Name	Contributions
Aditya Pant	Architecturally Significant Elements, Draft Architecture and Conclusion
Ameya Shahu	Architecturally Significant Elements, Draft Architecture - Views and graphical Representation Conclusion Document Formatting and presentation
Lalit Arvind Balaji	Derived Requirements Draft architecture – physical view, development view Initial Risk analysis – priority risk 2,3,4 Conclusion
Pravalika Mukkiri	Received Requirements Risk Analysis, Priority Risk 1 Conclusion, Items for Future consideration Part