Smart Surveillance System (SSS)

FYP Team

Abdullah Basit	20I-0623
M. Abubakar Siddique	20F-0101

Supervised by

Dr. Usman Ghous

Department of Computer Science

National University of Computer and Emerging Science

Chiniot – Faisalabad Campus, Pakistan

2024

Abstract

The Smart Surveillance System (SSS) revolutionizes campus safety by integrating advanced machine learning, computer vision, and facial recognition technologies for real-time monitoring and behavioral analysis. Targeting behaviors like smoking and fighting, SSS offers a comprehensive solution for universities, encompassing live video feeds, data analytics, immediate alerts, and robust reporting capabilities. It ensures precise individual tracking, anomaly detection, and compliance with campus policies, promoting a safer academic environment. With a web-based dashboard, the system enables efficient surveillance, trend analysis, and incident management. Achieving 63.83% peak mAP during validation, SSS demonstrates reliability in behavior detection and sets a new standard in academic security systems.

Table of Contents

List of Tables

List of Figures

1. Introduction

The Smart Surveillance System (SSS) project aims to revolutionize campus security at universities by deploying an advanced surveillance system equipped with cutting-edge technologies such as facial recognition, behavior analysis, and real-time data analytic. Designed to address significant safety and ethical concerns, the SSS initiative seeks to enhance campus environments by efficiently detecting activities like smoking, and fighting. By integrating machine learning algorithms and computer vision models, the system promises not only to improve upon the limitations of traditional CCTV systems but also to offer a comprehensive solution for precise individual tracking and anomaly detection. This project underscores the critical need for innovative surveillance strategies that adapt to the dynamic and complex nature of human behavior within academic settings, setting a new benchmark for safety and compliance on university campuses.

2. Vision Document

In this section, Project Vision for SSS is discussed.

2.1. Problem Statement

Existing CCTV systems in universities fall short in tracking, identifying, and analyzing individual behaviors like smoking, and fighting in real-time. This technological gap undermines campus safety, security, and ethical standards. Our project aims to develop a Smart Surveillance System (SSS) that integrates facial recognition and behavior detection to address these issues, offering precise monitoring and anomaly detection to ensure a safer and more compliant academic environment.

2.2. Business Opportunity

The Smart Surveillance System (SSS) presents a significant business opportunity in the educational sector by offering universities a state-of-the-art solution for enhancing campus safety and compliance. By accurately tracking, identifying, and analyzing behaviors like smoking, and fighting, the SSS fills a critical market gap for advanced, real-time surveillance technology. This system not only promises to improve campus environments but also opens avenues for future expansions into other high-security settings, broadening its market potential.

2.3. Objectives

Here are the main objectives of the Smart Surveillance System (SSS):

- **Enhanced Surveillance Solution:** Develop an advanced surveillance system tailored for high-security environments like universities, employing individual ID tracking to optimize operational efficiency.
- **Refined Behavior Analysis:** Implement an integrated surveillance solution capable of detecting and addressing specific behavioral violations on campus, including smoking, and fighting, using advanced machine learning and computer vision technologies for real-time identification and analysis.
- **Reliable Monitoring System:** Establish a foolproof monitoring solution that eliminates common human oversights, such as misidentification or lapses in vigilance, ensuring a comprehensive surveillance approach.
- **Safe Campus Environment:** Create a safe and secure campus environment for students and faculty, promoting smoke-free zone, and enforcing university policies against fighting.
- **Immediate Alert Mechanism:** Introduce a rapid alert and notification system to enable swift responses in critical situations, enhancing the capability for timely intervention and resolution of incidents.

2.4. Project Scope

The project scope for the Smart Surveillance System (SSS) encompasses the development and deployment of a comprehensive surveillance system designed to enhance security and compliance within university campuses. Focused on the behaviors of smoking, and fighting, the SSS aims to address the following areas:

2.4.1. Behavior Detection and Analysis

The system will utilize advanced machine learning algorithms and computer vision technologies to accurately detect and analyze instances of smoking, and fighting within the campus. This capability is central to addressing specific behavioral violations that impact campus safety and cleanliness.

2.4.2. Facial Recognition Technology

Incorporating facial recognition to identify individuals engaging in the aforementioned behaviors, the SSS will facilitate real-time tracking and identification, ensuring accountability and enabling appropriate responses.

2.4.3. Real-Time Monitoring and Alert-System

The system will offer real-time surveillance capabilities, with an integrated alert mechanism to notify campus security personnel immediately when violations are detected.

2.4.4. Data Management and Reporting

SSS will include a robust data management framework to log incidents, manage surveillance data, and generate reports. The module generates reports and analytic that can be used for detection of individuals, and insights into the overall happenings related to smoking, and fighting in the facility.

2.4.5. Hardware and Software Integration:

The project scope includes the selection and integration of necessary hardware (e.g., high-resolution cameras) and software (e.g., development tools, databases) to support the surveillance system's functionalities.

By targeting the specific behaviors of smoking, and fighting, the SSS project aims to significantly improve campus safety, promote a healthier and cleaner environment, and ensure a more secure academic setting for all members of the university community.

2.5. Constraints

SSS faces 3 major constraints to its development:

2.5.1. High-Quality Camera Requirement

The system necessitates the use of high-resolution cameras (minimum 720p) to ensure clear imagery for accurate facial recognition and behavior detection. The effectiveness of detecting smoking, and fighting behaviors is contingent upon the quality of video feeds.

2.5.2. Technical Limitations

The system's performance is subject to the limitations of current machine learning and computer vision technologies, which may affect its ability to distinguish between similar behaviors or operate in low-light conditions.

2.6. Stakeholder and User Description

Stakeholders and user descriptions are discussed below.

2.6.1. Market Demographics

The SSS targets a focused group of stakeholders and users within the educational sector, specifically:

- **Universities:** Academic institutions seeking to enhance campus safety and security through advanced surveillance.
- **Campus Security Personnel:** Individuals responsible for maintaining safety and addressing violations on campus.
- **Students:** The primary inhabitants of university campuses, whose behaviors the system monitors.
- **Regulatory Bodies:** Entities that oversee privacy, data protection, and ethical standards in educational environments.

2.6.2. Stakeholder Summary

Key stakeholders in the SSS ecosystem include:

- **Universities:** Entities looking to adopt cutting-edge technology for improving campus security and behavioral monitoring.
- **Campus Security Teams:** Front line users of the SSS, utilizing the system for real-time surveillance and incident response.
- **Students:** Directly impacted by the system’s deployment, contributing to a safer campus environment.
- **Regulatory Authorities:** Organizations ensuring the system's compliance with legal and ethical standards.

2.6.3. User Environment

The SSS is deployed within the university campus environment, integrating seamlessly with existing IT and security infrastructure. The system is accessible to authorized personnel, including security teams and administrative staff, ensuring ease of use and accessibility from various devices connected to the campus network.

2.6.4. Stakeholder Profiles

Let's take a closer look at a few stakeholder profiles that exemplify the diversity of Smart Surveillance System users:

- **University:** A large public university looking to modernize its campus surveillance system to address safety concerns and behavioral issues effectively.
- **Campus Security Personnel:** A security manager leveraging the SSS to monitor campus activities, quickly identify incidents of smoking, and fighting, and respond promptly.
- **Student:** A university student who experiences a safer campus environment as a result of the effective monitoring and deterrence of inappropriate behaviors.

In this diverse ecosystem, the SSS is designed to meet the unique needs of each stakeholder, enhancing campus safety, ensuring regulatory compliance, and fostering a secure learning environment.

3. System Requirement Specification

In this section, features and requirements of SSS are discussed.

3.1. System Features

The Smart Surveillance System (SSS) project aims to enhance campus security through the development of a sophisticated web application capable of real-time surveillance, behavior analysis, and incident management. Leveraging advanced technologies such as machine learning, facial recognition, and data analytics, the SSS will monitor specific behaviors like smoking, and fighting within university campuses, providing a proactive approach to safety and compliance. The project encompasses the following features:

3.1.1. Dashboard Overview

A centralized web-based dashboard will serve as the nerve center of the SSS, offering administrators and security personnel a real-time overview of surveillance operations. This dashboard will display critical data, including live alerts, system status, and operational metrics, allowing users to quickly assess the security posture of the campus. The intuitive interface will enable easy navigation and instant access to all system functionalities.

3.1.2. Live Video Feeds

The system will provide access to live video feeds from strategically placed cameras across the campus. Users will have the flexibility to switch views, zoom in/out, and track individuals using displayed IDs in real-time. This feature is crucial for detailed monitoring and immediate identification of individuals involved in specific behaviors or incidents, enhancing the responsiveness of campus security measures.

3.1.3. Activity Logs and Analytic

SSS will offer visual representations of data analytics and activity logs through an interactive interface. It will include graphs, charts, and tables that provide easy interpretation and analysis of occurrences of specified behaviors on campus. This feature aims to assist in identifying trends, peak times for violations, and areas that may require additional surveillance or intervention, enabling data-driven decision-making.

3.1.4. Alerts and Notifications Panel

A dedicated alerts and notifications panel on the web-based application will ensure that all users are promptly informed about real-time alerts and notifications that require immediate attention. This could include detections of unauthorized activities or behaviors that violate campus policies. The system will prioritize alerts based on severity, ensuring that critical issues are addressed swiftly.

3.1.5. Search and Filter Operation

The system will incorporate a comprehensive search functionality, allowing users to query data based on various criteria such as roll number, violation type, location, or time. Robust sorting and filtering options will enable precise and efficient data retrieval, making it easier for security personnel to pinpoint specific incidents or patterns. This feature is vital for managing and analyzing the vast amounts of data generated by the surveillance system, facilitating a proactive approach to campus security.

3.2. Functional Requirements

Functional requirements of the project are mentioned below:

3.2.1. Facial Recognition

- The system must accurately identify individuals in real-time using facial recognition technology, enhancing security and individual tracking across campus.
- Facial recognition should work across various lighting conditions and angles, ensuring robust and reliable identification.

3.2.2. Smoking Behavior Detection

- The system must automatically detect instances of smoking within the university premises using image recognition algorithms to enforce facility policies and health regulations.
- Real-time alerts should be sent to the dashboard for immediate action.

3.2.3. Fighting Behavior Detection

- The system must identify physical altercations or fights to maintain safety and security within the facility.
- It should analyze video feeds for aggressive behaviors or movements indicative of a fight, alerting security personnel to intervene swiftly.

3.2.4. Time and Location Logging

- The system must provide real-time tracking of individuals’ movements across campus through live camera feeds, including recording the exact location (camera name) and timestamp for each observed activity.
- This feature should facilitate easy retrieval of video footage associated with specific incidents, enhancing the investigation and response process.

3.2.5. Data, Reporting, and Alert System

- A comprehensive database must record individuals' locations and timestamps upon the occurrence of specific incidents i.e. smoking, and fighting.
- The system should generate real-time alerts in the web application for immediate attention by security personnel and provide detailed reports for analysis and decision-making.

3.3. Non-Functional Requirements

Non-Functional requirements of the project are mentioned below:

3.3.1. Performance and Efficiency

The Smart Surveillance System must process and analyze video data in real-time, ensuring that behavior detection algorithms operate with a maximum latency of 2 seconds under standard conditions. This requirement is critical for enabling immediate incident detection and response

3.3.2. Reliability and Availability

The Smart Surveillance System is required to achieve 99% uptime excluding power failures and other technical issues not related to this system, thereby, ensuring consistent surveillance and monitoring capabilities. Upon facing a technical issue, the system must also prompt the user to contact developers in an attempt to minimize downtime.

3.3.3. Compatibility

The surveillance software shall be compatible with Windows operating system, and must be accessible through major web browsers such as Chrome, Firefox, and Edge. This ensures that the system is usable on a wide range of devices, enhancing accessibility for all users.

4. Use Case Diagram

This section contains the Use Case Diagram for the project.

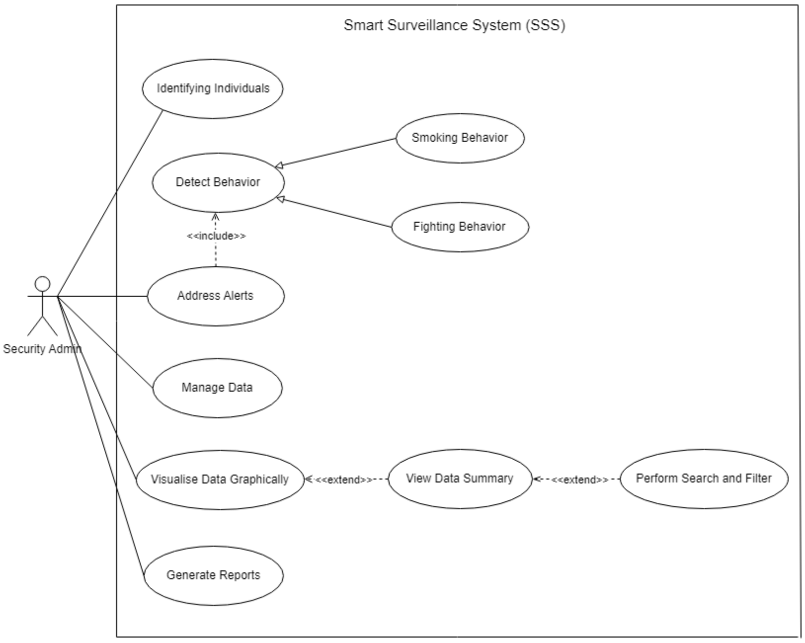


Figure 1. Use Case Diagram

5. Expanded Use Case

This section explains on the Expanded Use Cases for the project.

5.1. Address Alerts

Address Alerts Use Case is discussed below:

Table 1. Use Case – Address Alerts

Field	**Details**
Use Case Name	Address Alerts
Actor	Security Admin
Description	Describes how system alerts are managed by the Security Admin
Precondition	The system has detected a behavior (smoking, or fighting) that triggers an alert.
Basic Flow	1. An alert is generated by the system. 2. The alert is displayed on the dashboard. 3. Security Admin reviews the alert. 4. Appropriate action is taken to address the alert by the admin. 5. The alert is marked as addressed in the system.
Alternative Flows	If the alert is false, it is dismissed after review.
Post condition	The situation causing the alert is resolved, and the alert status is updated in the system.

5.2. View Data Summary

View Data Summary Use Case is discussed below:

Table 2. Use Case – View Data Summary

Field	**Details**
Use Case Name	View Data Summary
Actor	Security Admin
Description	Users can view summaries of the data collected and analyzed by the system, including incident statistics and behavior trends.
Precondition	Data is collected and processed by the system.
Basic Flow	1. Admin accesses the dashboard. 2. Admin selects the option to view data summaries. 3. The system displays various summaries, including incident rates, incident frequent times, locations (camera names) with more incidents and other relevant statistics. 4. Admin reviews the summaries for insights.
Alternative Flows	N/A
Post condition	Admin gains insights into the system's findings and the campus's security status.

5.3. Generate Reports

Generate Report Use Case is discussed below:

Table 3. Use Case – Generate Reports

Field	**Details**
Use Case Name	Generate Reports
Actor	Security Admin
Description	Allows the Security Admin to generate detailed reports based on the data collected, including incidents related to smoking, fighting detected by the system. The reports can be used for analysis, compliance, and decision-making.
Precondition	The system has collected and processed sufficient data on incidents, including timestamps, locations, and behavior types.
Basic Flow	1. Admin accesses the dashboard. 2. Admin selects the option to generate a report. 3. The system prompts for report criteria (date range, incident type, location, etc.). 4. Admin specifies the desired parameters. 5. The system generates a detailed report based on the selected criteria. 6. The report is presented to the admin in a viewable and downloadable format.
Alternative Flows	N/A
Post condition	A report is generated, providing a comprehensive summary of incidents and behaviors for further review and analysis.

6. Data Flow Diagram

This section contains the Data Flow Diagrams for the project.

6.1. Data Flow Diagram Level 0

Level 0 Data flow Diagram is shared below:

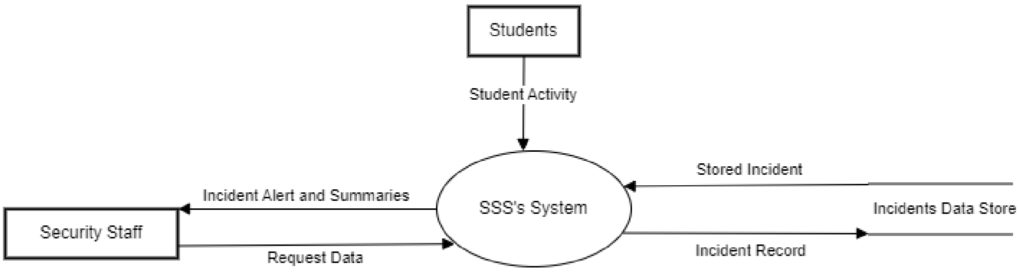


Figure 2. Data Flow Diagram Level 0

6.2. Data Flow Diagram Level 1

Level 1 Data flow Diagram is shared below:

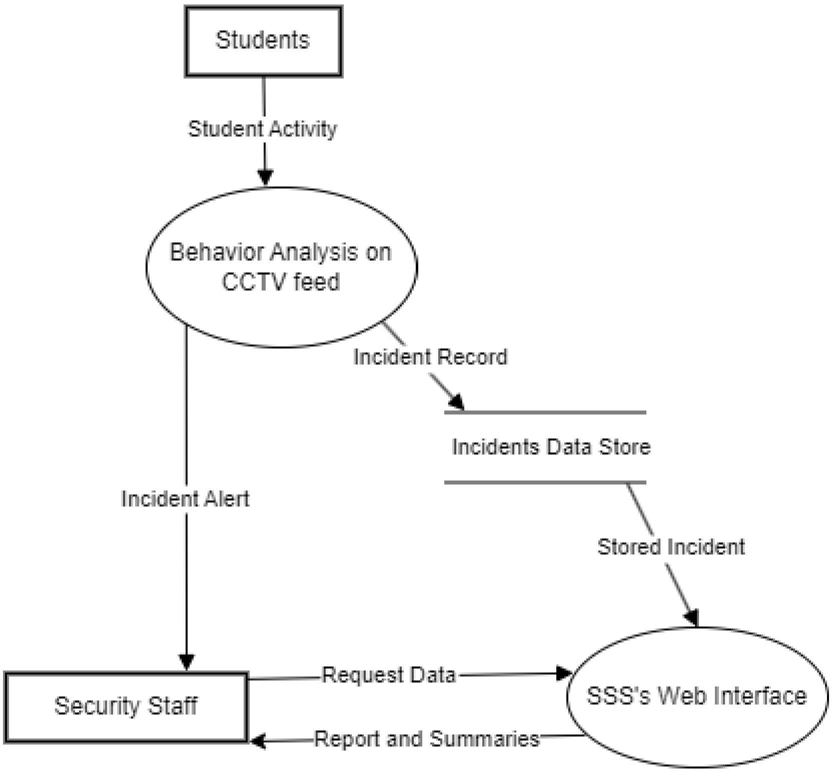


Figure 3. Data Flow Diagram Level 1

6.3. Data Flow Diagram Level 2

Level 2 Data flow Diagram is shared below:

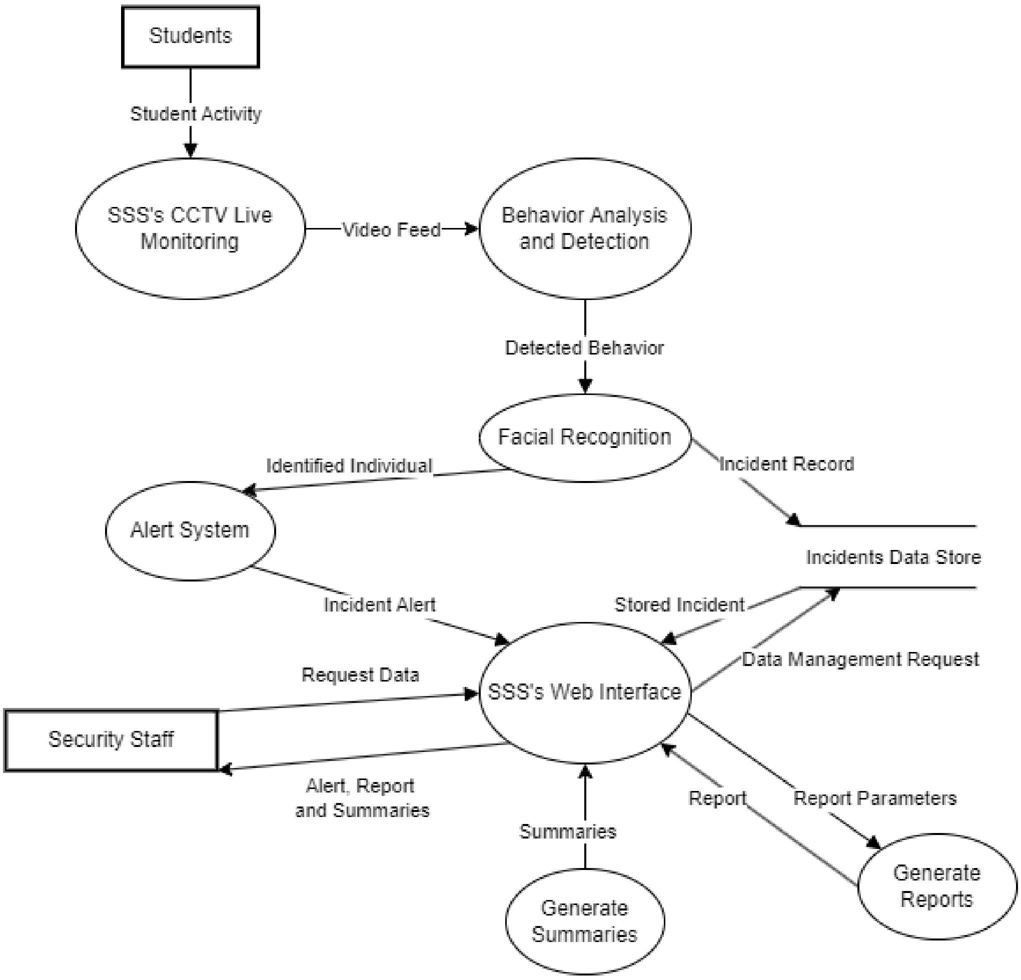


Figure 4. Data Flow Diagram Level 2

7. Activity Diagram

This section contains the Activity Diagram for the project.

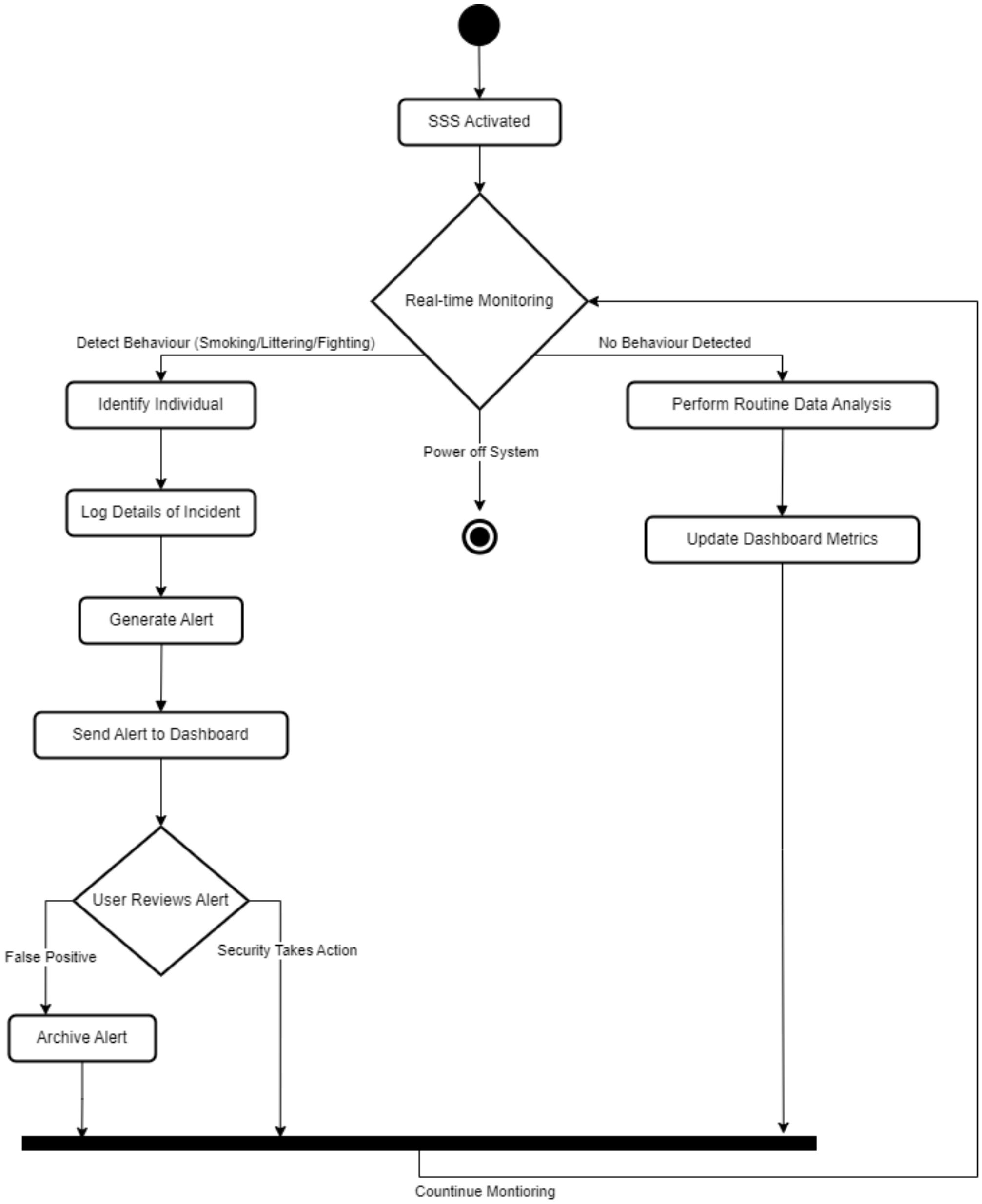


Figure 5. Activity Diagram

8. Entity Relationship Diagram

This section contains the Entity Relationship Diagram for the project.

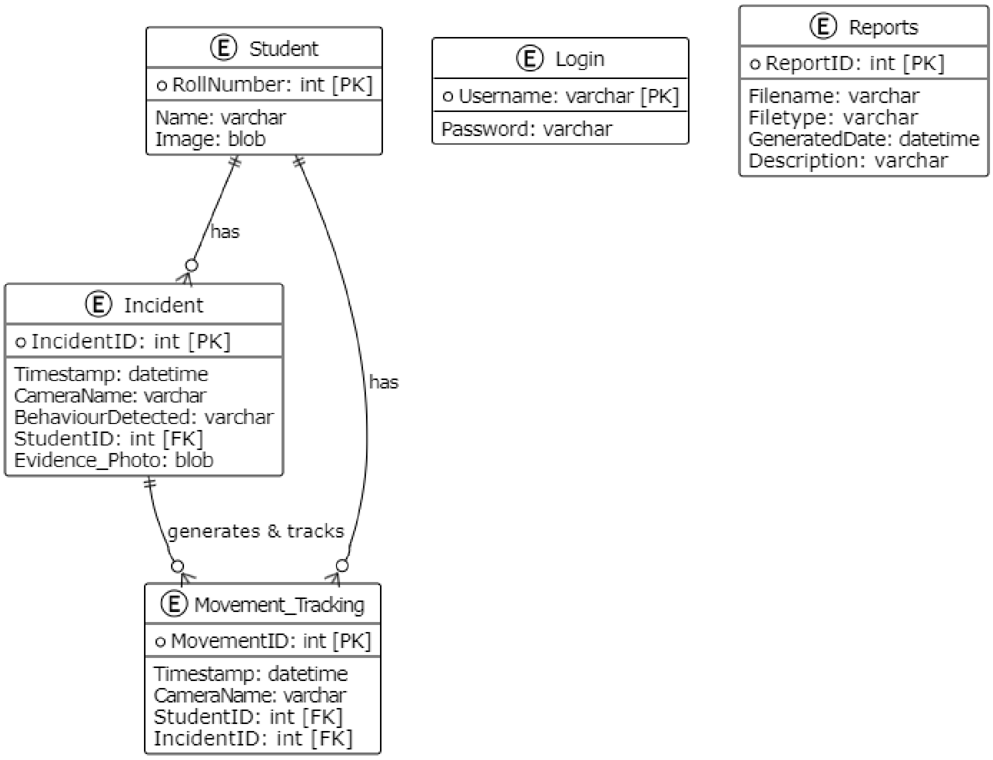
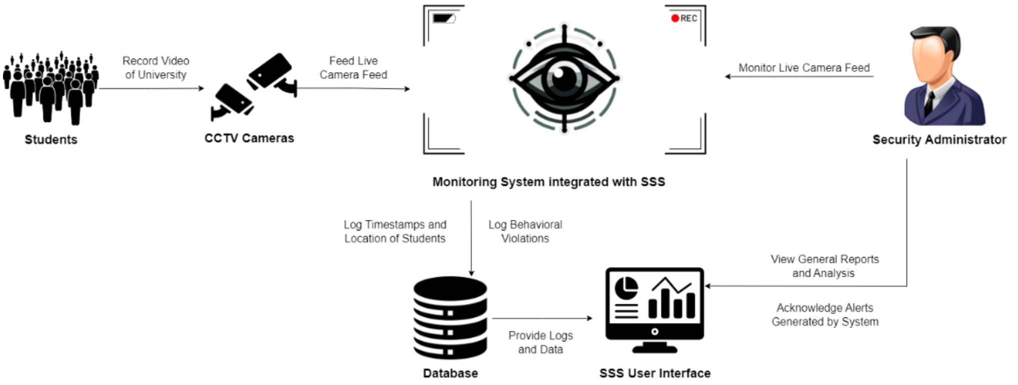


Figure 6. Entity Relationship Diagram

9. High Level Diagram

This section contains the High-Level Diagram for the project.



Students
Record Video of University
CCTV Cameras
Feed Live Camera Feed
REC
Monitoring System integrated with SSS
Monitor Live Camera Feed
Security Administrator
Log Timestamps and Location of Students
Log Behavioral Violations
View General Reports and Analysis
Acknowledge Alerts Generated by System
Database
Provide Logs and Data
SSS User Interface

Figure 7. High Level Diagram

10. Facial Recognition and Spatio-Temporal Action Detection Model Evaluation

This section provides an overview of the model training process and evaluates the performance of the trained model.

For behavior detection, The **ResNet3D SlowFast backbone** implements a dual-pathway architecture designed to process video data at different temporal resolutions. The slow pathway operates at 1/8th the frame rate of the fast pathway and uses deeper channels (256) to capture detailed spatial features. Meanwhile, the fast pathway, with its higher temporal resolution and shallower channels (32), excels in capturing motion dynamics. Together, these pathways achieve superior performance by effectively combining spatial and temporal information.

For person identification, the **face recognition pipeline** uses dlib's CNN-based face detector and recognition models. It generates 128-dimensional feature vectors for comparison and stores known encodings in a pickle file for rapid matching. A similarity threshold of 0.6 ensures a balance between false positives and false negatives.

10.1. Machine Learning Pipeline Architecture

In this subsection, we outline the training setup, including the model architecture and key milestones achieved during training.

10.1.1. Dataset Details

Dataset comprised of custom recorded CCTV videos.

- **Dataset size:** 108 videos (54 smoking, 54 fighting)
- **Training Split:** 90 videos
- **Validation Split:** 18 videos

Both training and validation split were equally divided.

10.1.2. Model Architecture

- **Model:** FastRCNN with a ResNet3dSlowFast backbone, adapted for AVA-style action detection.
- **Base Checkpoint**: Pretrained SlowFast model on Kinetics-400.
- **Frozen Stages:** 2
- **Epochs:** 40
- **Optimizer:** AdamW
- **LR Schedule**: Linear warm-up for 5 epochs, followed by CosineAnnealingLR until epoch 40.
- **Batch Size**: 8 for training, 1 for validation.

10.1.3. Data Preprocessing

Video frames undergo multiple preprocessing steps:

1. Resize to maintain the aspect ratio with a short side of 256 pixels.
2. Apply random rescaling between 256-320 pixels for scale invariance.
3. Crop randomly to 256x256 pixel inputs.
4. Perform color augmentation:
   - Brightness, contrast, and saturation (±20% each)
   - Hue adjustment (±10%)
5. Normalize pixel values using:
   - Mean: [123.675, 116.28, 103.53]
   - Standard deviation: [58.395, 57.12, 57.375]

10.1.4. Key Milestones

- **Checkpoints Saved:** Every epochs.
- **Best Validation Accuracy:** 63.83% at epoch 7 (overall action detection mAP).

10.2. Training Metrics

This subsection presents the training metrics obtained during the training process.

10.2.1. Training Loss

- **Initial**: 1.5158
- **Final**: 0.0487

10.2.2. Validation Accuracy

- **Epoch 1**: 47.46%
- **Epoch 7 (Peak)**: 63.83%
- **Epoch 40**: 52.12%.

  While the model achieved its highest overall mAP at epoch 7, later epochs did not surpass this peak. The mAP gradually fluctuated and then settled around the 0.52–0.58 range near the end of training.

10.2.3. Per-Class AP at Best Epoch

- **Smoking AP:** 57.08%
- **Fighting AP:** 70.58%

10.3. Results Interpretation

The training results suggest that the model reached its performance peak relatively early (around epoch 7) and did not improve significantly afterwards, despite adjustments in the learning rate. The early peak indicates that the model quickly learned to identify the given actions but had difficulty making further gains. Additionally, class-specific analysis showed better detection for the Fighting action than for Smoking, implying that certain classes are inherently easier for the model to distinguish.

10.3.1. Convergence

The model achieved a stable level of performance early, converging by epoch 7. After this point, no substantial improvements were observed, indicating that the model had likely reached a plateau under the current training conditions.

10.3.2. Learning Rate Impact

Although reducing the learning rate helped stabilize training, it did not lead to continued improvements in the validation metrics. This suggests that the model had already extracted most of the discriminative features it could with the provided data and configuration.

10.4. Reasons for Performance Differences

A key reason for the discrepancy in detection performance between Fighting and Smoking is the nature of the actions themselves. Fighting actions involve more pronounced and rapid movements that are easier to identify in a spatio-temporal context. In contrast, Smoking is characterized by subtler, often minimal arm movements. These more nuanced actions are harder to distinguish from background or other non-action elements, resulting in lower detection accuracy.

11. Web Application Architecture

The frontend is built using React and follows a modular component hierarchy. It features five main sections: Dashboard, Incident Management, User Administration, Analytics, and System Configuration. Components adhere to atomic design principles, ensuring reusability. Styling is handled with Tailwind CSS, customized to meet institutional branding requirements.

11.1. State Management

State is managed using Redux Toolkit with slices for:

- User authentication
- Real-time monitoring data
- Incident records
- System configuration
- Analytics

This setup enables selective re-rendering through state normalization.

11.2. WebSocket Integration

Real-time communication is powered by Socket.IO with custom event handlers for:

- New incident detection
- Alert acknowledgment
- System status updates
- User activity synchronization

11.3. Real-time Video Processing Pipeline

The system processes video feeds through a multi-stage pipeline that ensures real-time performance:

1. Extracts frames at 30 FPS and feeds them into a circular buffer with a 32-frame window for temporal analysis.
2. Preprocesses each frame through resizing and normalization.
3. Implements temporal smoothing to aggregate detection results and reduce false positives.
4. Triggers alerts when confidence thresholds are met:
    - Smoking: 0.97.
    - Fighting: 0.92.

Alerts include incident details, captured images, and metadata.

11.4. Security Framework

The system's security framework is robust and multi-layered.

Authentication employs Bcrypt with a work factor of 10 for password hashing. Measures include configurable password complexity requirements, rate limiting, secure password reset mechanisms, and support for multi-factor authentication. Session management uses a hierarchical JWT token structure with:

- Access tokens (15-minute expiration)
- Refresh tokens (24-hour expiration)
- Remember-me tokens (30-day expiration)
- Token rotation and a blacklist of revoked tokens

Role-based access control (RBAC) defines three primary roles:

1. System Administrator: Full access.
2. Security Officer: Read-only access.

Data is encrypted at multiple levels:

- **Data at Rest:** AES-256 encryption for sensitive fields in the database.
- **Video Feeds:** Real-time encryption via secure WebRTC protocols.
- **File Storage:** Encrypted file system safeguards images.

This comprehensive security approach ensures data integrity and protection across all components.

12. System Impact and Outlook

The Smart Surveillance System aims for a transformative leap forward in enhancing campus safety and regulatory compliance. Integrating advanced technologies to provide comprehensive, real-time surveillance, SSS is aimed at redefining security norms within educational settings. Anticipated outcomes include a marked reduction in campus incidents and the establishment of a vigilant, responsive security infrastructure. As we move forward, the evaluable milestones will include the system's adaptability, effectiveness in behavior detection, and contribution to a proactive security culture on campus.

13. References

[1] A. Lee, "What is China’s social credit system and why is it controversial?" South China Morning Post, 09 Aug. 2020. [Online]. Available: https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.

[2] H. Kuehne, H. Jhuang, E. Garrote, T. Poggio, and T. Serre, "HMDB: A Large Video Database for Human Motion Recognition," in ICCV, 2011. [Online]. Available: https://serre-lab.clps.brown.edu/resource/hmdb-a-large-human-motion-database/.

[3] K. Dhanalakshmi Srivani, "YOLO Algorithm for Custom Object Detection," Analytics Vidhya, 30 Oct. 2023. [Online]. Available: https://www.analyticsvidhya.com/blog/2022/06/yolo-algorithm-for-custom-object-detection.

[4] Correspondent, "Bikers sans helmet to receive e-challan," The Express Tribune, 26 Jan. 2024. [Online]. Available: https://tribune.com.pk/story/2454420/bikers-sans-helmet-to-receive-e-challan.

[5] S. Akti, "New generated dataset for fight detection in surveillance cameras," GitHub repository, 2023. [Online]. Available: https://github.com/seymanurakti/fight-detection-surv-dataset.