



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

AI Surveillance: An Intelligent Video Monitoring and Autonomous Security Operations System

Ms. Sasikala P, Nithinprabu V, Ram Prabhu K, Paramesh P, Ranjith M, Samyuktha P

Department of Computer Science and Engineering, Bachelor of Engineering,
Sri Shakthi Institute of Engineering and Technology Coimbatore-641062

ABSTRACT

Traditional surveillance systems mainly depend on continuous video recording and manual monitoring by security personnel. Monitoring multiple camera feeds simultaneously can lead to operator fatigue, delayed threat identification, missed incidents and time-consuming investigation. Conventional systems also provide limited support for cross-camera tracking, automated alert escalation and verification of recorded evidence.

This paper presents an AI Surveillance and Autonomous Security Operations Center (SOC) Platform, an intelligent multi-camera monitoring system designed to improve security monitoring through artificial intelligence, computer vision and automated incident management. The system is developed using React 18 and Vite for the frontend, Python with FastAPI for backend services, and PostgreSQL with TimescaleDB or SQLite for data storage. It integrates YOLOv8 for object detection, SORT for multi-object tracking, MobileNetV3-based facial feature extraction and person re-identification, and EasyOCR for automatic license plate recognition. Additional analytical modules support detection of suspicious activities, restricted-zone violations, loitering, falls, physical altercations, camera tampering, fire and smoke candidates, and personal protective equipment (PPE) compliance.

The platform provides a centralized Security Operations Center dashboard, live camera monitoring, incident management, multi-camera tracking, audio-event analysis, PTZ camera control, predictive crowd analytics and an AI-based security assistant named NURA. It also supports automated alert escalation and cryptographic mechanisms for protecting the integrity and traceability of video evidence. The system aims to transform conventional passive CCTV monitoring into an intelligent, event-driven security platform that assists operators in identifying, investigating and responding to potential security incidents.

Keywords: Artificial Intelligence, Intelligent Video Surveillance, Computer Vision, YOLOv8, Object Detection, Object Tracking, Facial Recognition, Person Re-Identification, Anomaly Detection, Security Operations Center, Incident Management, Automated License Plate Recognition, Evidence Integrity.

INTRODUCTION

Security monitoring is an essential requirement in public facilities, educational institutions, commercial buildings, industrial environments and other controlled locations. Conventional CCTV systems continuously record video footage but generally depend on human operators to monitor multiple camera feeds and identify suspicious activities. As the number of cameras increases, manual monitoring becomes difficult, time-consuming and vulnerable to human error.

The AI Surveillance and Autonomous Security Operations Center Platform addresses these limitations by combining artificial intelligence, computer vision, real-time video processing and automated incident management. Instead of depending entirely on manual observation, the system analyzes incoming video frames, detects objects and activities, tracks individuals across camera feeds and generates alerts when configured security conditions are identified.

The platform provides a centralized interface through which security operators can monitor cameras, examine detected events, manage incidents, review recorded clips and access analytical information. It also integrates an AI-based assistant to support natural-language interaction with security data.

The system focuses on the following functions:

- Real-time video monitoring and object detection.
- Multi-object tracking and movement analysis.
- Restricted-zone monitoring and virtual tripwire detection.
- Facial watchlist matching and person re-identification.

- Automatic license plate recognition.
- Detection of safety-related events such as falls, altercations, fire, smoke and PPE violations.
- Automated incident creation, notification and escalation.
- Video investigation and evidence-integrity verification.
- AI-assisted security analysis and reporting

Objective:

1. To develop an intelligent surveillance platform that reduces dependence on continuous manual camera monitoring.
2. To detect and track objects and individuals using computer vision techniques.
3. To identify potential security incidents through configurable anomaly and safety-detection mechanisms.
4. To support person re-identification across connected camera feeds.
5. To implement facial watchlist matching and automatic license plate recognition.
6. To provide centralized alert management and automated escalation.
7. To preserve video evidence with cryptographic integrity checks and traceable custody records.
8. To provide a scalable web-based interface for monitoring, investigation and security operations.
9. To integrate AI-assisted querying and reporting through the NURA security assistant.

LITERATURE SURVEY

1. Traditional CCTV Surveillance Systems

Traditional CCTV systems are widely used for monitoring and recording activities in secured environments. These systems capture video through connected cameras and store the footage for later review. However, identifying suspicious activities generally depends on security personnel continuously observing the camera feeds. This approach becomes difficult when monitoring a large number of cameras and may result in delayed incident detection.

2. Video Management Systems (VMS) and Network Video Recorders (NVR)

Modern VMS and NVR platforms provide centralized camera management, video recording, playback and remote access. They improve video storage and retrieval compared with standalone CCTV systems. However, many conventional deployments still depend heavily on manual monitoring and do not provide an integrated analytical workflow for detecting incidents, correlating events across cameras and managing investigations.

3. Deep Learning-Based Object Detection

Deep learning techniques have improved the ability of computer systems to identify objects within images and video frames. The YOLO family of object detection models performs object localization and classification in a unified detection pipeline. This project uses YOLOv8 for detecting objects such as people and vehicles from surveillance frames. The Ultralytics framework provides model prediction, validation, export and tracking workflows.

4. Multiple Object Tracking

Object detection identifies objects in individual frames, while object tracking associates detections across consecutive frames to estimate object movement. The SORT algorithm uses motion estimation and data association to maintain track identities in video sequences. The proposed platform uses SORT-based tracking to calculate object trajectories, movement direction, velocity and dwell time.

5. Facial Feature Extraction and Person Re-Identification

Facial feature extraction and person re-identification techniques are used to compare visual characteristics across images. MobileNetV3 is an efficient neural network architecture designed to provide useful visual representations with attention to computational requirements. In this project, MobileNetV3-based feature extraction supports facial watchlist matching and person re-identification across camera views. Such matches are dependent on image quality, camera conditions and threshold configuration and should be reviewed according to the system's operational policy.

6. Intelligent Incident Detection and Security Analytics

Recent surveillance systems increasingly combine object detection with event rules, motion analysis, audio processing and automated notifications. Such systems can identify events such as restricted-area entry, loitering, falls, camera tampering and safety-related violations. The proposed platform extends these capabilities through centralized incident management, automated escalation, evidence preservation and AI-assisted investigation.

Research Gap

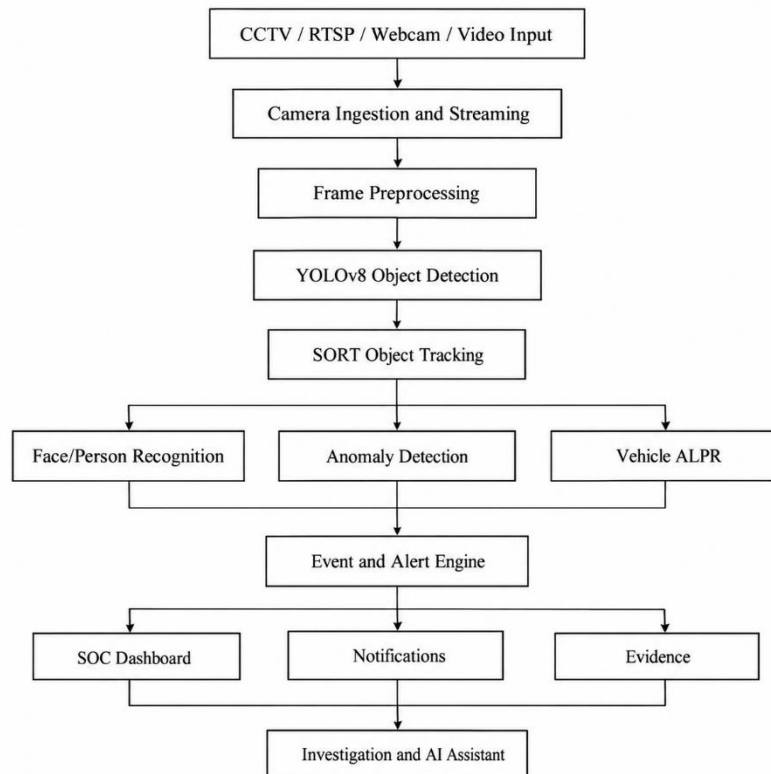
Existing surveillance deployments often treat video recording, AI detection, alerting and investigation as separate functions. The proposed system brings these capabilities together in a common SOC interface. Its intended contribution is an integrated workflow that connects camera monitoring, object detection, tracking, incident handling, evidence verification and operator assistance.

METHODOLOGY

1. System Design

- Frontend: React 18 and Vite for the web-based SOC interface.
- Backend: Python 3.12 with FastAPI for REST APIs and asynchronous services.
- Object Detection: YOLOv8 using PyTorch or ONNX Runtime.
- Object Tracking: SORT-based multi-object tracking.
- Face Feature Extraction: MobileNetV3-based 512-dimensional facial embeddings.
- Person Re-Identification: MobileNetV3-based appearance feature comparison and camera-topology information.
- License Plate Recognition: EasyOCR.
- Image and Video Processing: OpenCV and related computer-vision libraries.
- Database: PostgreSQL with TimescaleDB support and SQLite fallback for local execution.
- Caching and Messaging: Redis.
- Background Processing: Celery workers with a limited thread-pool fallback.
- Video Storage: MinIO-compatible object storage.
- AI Assistant: NURA integrated with a Groq-hosted language model.
- Deployment Support: Docker-based services and Nginx reverse proxy.

2. Architecture Overview



3. Modules

a. Authentication and Role Management Module

- Provides user login and token-based session management.
- Uses JSON Web Tokens for authentication.
- Supports role-based access for administrators, investigators, operators and viewers.
- Controls access to monitoring, configuration, incident and investigation functions.

b. SOC Dashboard Module

- Displays an overall security operations summary.
- Presents camera status, recent alerts and incident information.
- Provides quick navigation to monitoring and investigation modules.
- Displays operational information for security personnel.

c. Live Camera Monitoring Module

- Displays connected camera feeds in a centralized interface.
- Renders object detection boxes and tracking information.
- Displays movement direction, velocity and tracking overlays.
- Supports configurable zones and virtual tripwires.

d. AI Detection and Anomaly Analysis Module

- Detects objects using YOLOv8.
- Identifies configured events such as loitering, zone breaches, falls and altercations.
- Evaluates camera tampering, fire and smoke candidates.
- Checks selected PPE-related visual conditions.
- Generates events for further review and alert handling.

e. Facial Biometrics and Person Re-Identification Module

- Extracts facial feature embeddings for watchlist comparison.
- Supports configured VIP or security watchlists.
- Compares person appearance features across connected cameras.
- Uses camera topology and temporal information to support cross-camera association.

f. Automatic License Plate Recognition Module

- Processes vehicle regions and extracts license plate text using OCR.
- Supports registration and lookup of configured vehicle plates.
- Provides an interface for checking vehicle access status.

g. Acoustic Analysis and PTZ Control Module

- Analyzes audio signals using frequency-domain features.
- Supports configured acoustic event categories.
- Integrates PTZ camera control for target-following workflows where supported by the connected camera.

h. Incident and Alert Management Module

- Creates and maintains alerts based on detected events.
- Supports alert acknowledgement, review and dismissal.
- Integrates webhook notifications and configured escalation workflows.

- Maintains event information for subsequent investigation.

i. Video Investigation and Forensic Evidence Module

- Supports uploaded-video analysis and recorded incident review.
- Provides anomaly clip management and investigation timelines.
- Generates evidence packages with cryptographic integrity information.
- Supports evidence verification and custody-record maintenance.

j. NURA AI Security Assistant Module

- Provides a natural-language interface for security-related queries.
- Uses available system telemetry and incident information to support responses.
- Assists with investigation queries and incident-report drafting.
- Its responses should be treated as decision support and checked against source evidence.

k. Predictive Analytics and Spatial Twin Module

- Uses historical or recent tracking information for crowd-density and stagnation forecasting.
- Represents spatial information using calibrated camera-to-ground-plane transformations.
- Displays entity positions and movement information within a facility representation

4. Development Flow

- Requirement gathering and identification of surveillance use cases.
- System architecture and module planning.
- Camera input and streaming integration.
- Backend API and authentication development.
- YOLOv8 object detection integration.
- SORT tracking and anomaly-rule implementation.
- Facial feature extraction, person re-identification and ALPR integration.
- Alert, escalation and evidence-management development.
- React-based SOC dashboard and investigation interface development.
- Integration testing, security testing and performance evaluation.
- Deployment configuration and operational validation.

EXISTING SYSTEM

1. Manual CCTV Monitoring

How it works:

- Security cameras continuously capture video footage.
- Operators observe camera feeds through monitoring screens.
- Suspicious activities are identified through manual observation.
- Operators contact security personnel when an incident is noticed.
- Recorded footage is reviewed manually after an incident.

Drawbacks:

- Continuous monitoring causes operator fatigue.
- Important events may be missed when multiple cameras are monitored.

- Incident identification and response can be delayed.
- Tracking an individual across different camera feeds is difficult.
- Investigation requires time-consuming video playback.

2. Traditional NVR-Based Surveillance Systems

How they work:

- Network cameras transmit video to a Network Video Recorder.
- The recorder stores video based on configured schedules.
- Operators search and replay recordings when required.
- Basic motion detection may generate notifications.

Drawbacks:

- Limited intelligent event interpretation.
- Basic motion alerts may generate false alarms.
- Cross-camera identity tracking is generally not integrated.
- Investigation and evidence verification may require separate tools.
- Human intervention is still required for most response activities.

3. Standalone AI Video Analytics Systems

How they work:

- AI models process camera footage to detect objects or selected events.
- Detection results are displayed through a separate interface.
- Some systems generate notifications when configured conditions are met.

Drawbacks:

- Detection, investigation and evidence management may be separated.
- Limited integration with security response workflows.
- Model performance may vary across camera angles and lighting conditions.
- Cross-camera movement analysis may be unavailable or limited.
- Operators may need to use multiple applications.

4. Separate Biometric and Vehicle Recognition Systems

How they work:

- Dedicated systems compare faces against registered identity databases.
- OCR-based systems extract vehicle registration numbers.
- Access-related results are displayed through separate applications.

Drawbacks:

- Information may not be correlated with other surveillance events.
- Separate databases increase integration complexity.
- Recognition quality depends on image resolution, angle and environmental conditions.
- A recognition result may require manual confirmation.

5. Conventional Security Alert Systems

How they work:

- Sensors or surveillance applications generate an alert.

- Operators receive notifications through a monitoring interface.
- Security personnel manually acknowledge and handle the incident.

Drawbacks:

- Alerts may remain unattended.
- Escalation may depend on manual follow-up.
- Incident records and evidence can be maintained separately.
- It may be difficult to reconstruct a complete incident timeline.

PROPOSED SYSTEM**1. Real-Time Camera Monitoring**

- Receives video from supported camera sources such as RTSP streams, webcams and other configured inputs.
- Displays multiple camera feeds through a centralized monitoring interface.
- Processes video frames through computer-vision pipelines.
- Displays detection and tracking overlays.

2. AI-Based Object Detection

- Uses YOLOv8 to identify supported object categories.
- Generates bounding boxes and confidence information.
- Supplies detection results to tracking and event-analysis modules.
- Supports inference through PyTorch CUDA or ONNX Runtime configurations.

3. Object Tracking and Movement Analysis

- Uses SORT-based tracking to associate detections across video frames.
- Maintains track identifiers within the tracking workflow.
- Calculates movement information such as velocity, direction and dwell time.
- Supports movement heatmaps and zone monitoring.

4. Anomaly and Safety Event Detection

- Detects configured restricted-zone and virtual-tripwire violations.
- Evaluates loitering and selected suspicious movement conditions.
- Identifies candidate fall and altercation events.
- Detects camera obstruction or tampering conditions.
- Analyzes optical fire and smoke candidates.
- Supports selected PPE compliance checks, including helmet and high-visibility vest conditions.

5. Facial Watchlist and Person Re-Identification

- Extracts facial features for comparison against configured watchlists.
- Supports person appearance matching across connected camera views.
- Uses camera adjacency and temporal information to improve cross-camera association.
- Provides tracking and identity information for operator review.

6. Automatic License Plate Recognition

- Processes vehicle images and extracts license plate text using EasyOCR.
- Supports registered plate information and access-status checking.

- Provides vehicle information for investigation and monitoring workflows.

7. Audio Analysis and PTZ Camera Control

- Analyzes configured audio signals for selected acoustic event categories.
- Supports the integration of acoustic events with surveillance workflows.
- Provides PTZ camera control and tracking capabilities for compatible cameras.

8. Automated Alerts and Incident Escalation

- Creates alerts from configured detection and analysis events.
- Displays incident severity and event information.
- Supports acknowledgement and incident-management actions.
- Uses configured webhooks and escalation mechanisms to notify responsible personnel.

9. Forensic Evidence Management

- Generates incident-related video clips and evidence packages.
- Uses SHA-256 hashing and HMAC-based seals for integrity verification.
- Maintains evidence custody information.
- Supports verification workflows to identify changes to stored evidence.

10. AI Security Assistant and Predictive Analytics

- Integrates NURA / J.A.R.V.I.S. for natural-language security queries.
- Supports incident-report drafting and security-data exploration.
- Provides crowd-density and stagnation forecasting features.
- Displays spatial movement information through the facility representation.

Advantages of the Proposed System

- Reduces dependence on continuous manual observation.
- Helps operators identify potential security incidents faster.
- Combines detection, tracking, alerting and investigation in a single platform.
- Supports cross-camera movement analysis.
- Improves incident traceability through centralized records.
- Provides configurable alert escalation.
- Adds cryptographic integrity checks to evidence workflows.
- Helps operators examine security information through an AI assistant.
- Supports modular integration of additional cameras and analytics.
- Provides a foundation for future multi-site security operations.

SYSTEM REQUIREMENTS

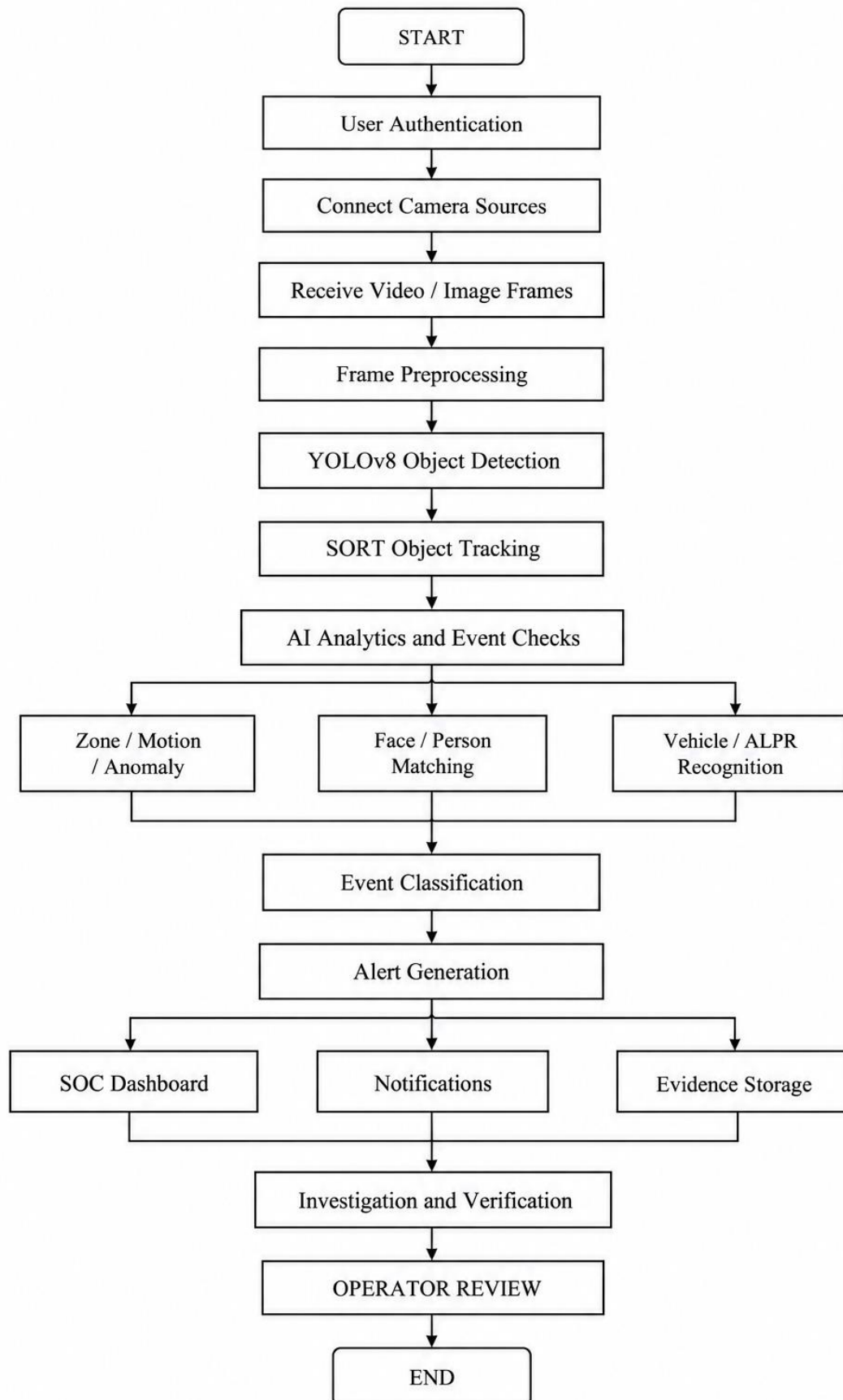
1. Hardware Requirements

Component	Minimum indicative specification	Recommended indicative specification
Processor	4-core 64-bit CPU	8-core or higher CPU
RAM	16 GB	32 GB or higher
Storage	512 GB SSD	1 TB NVMe SSD or higher

Component	Minimum indicative specification	Recommended indicative specification
AI acceleration	CPU or compatible inference runtime	NVIDIA CUDA-capable GPU; VRAM sized for model and stream load
Network	Gigabit Ethernet	Higher-capacity network based on concurrent streams
Display	1366 × 768	1920 × 1080 or higher
Camera input	One supported video source	Multiple compatible IP cameras

2. Software Requirements

Category	Technology used
Operating System	Windows / Linux (deployment dependent)
Frontend	React 18, Vite, JavaScript, HTML5, CSS3
Backend	Python 3.12, FastAPI
Application Server	Uvicorn
Object Detection	YOLOv8, Ultralytics
Deep Learning	PyTorch, Torchvision
Inference Runtime	ONNX Runtime (where configured)
Computer Vision	OpenCV
Object Tracking	SORT
Facial Feature Extraction	MobileNetV3
License Plate Recognition	EasyOCR
Database	PostgreSQL with TimescaleDB / SQLite fallback
Cache and Messaging	Redis
Background Tasks	Celery
Video/Object Storage	MinIO-compatible storage
AI Assistant	Groq-hosted language model integration
Reverse Proxy	Nginx
Development Tool	Visual Studio Code
Browser	Chrome / Edge / Firefox

PROCESSING :

MODE OF DESCRIPTION

1. Facility Spatial Twin and Sensor Radar

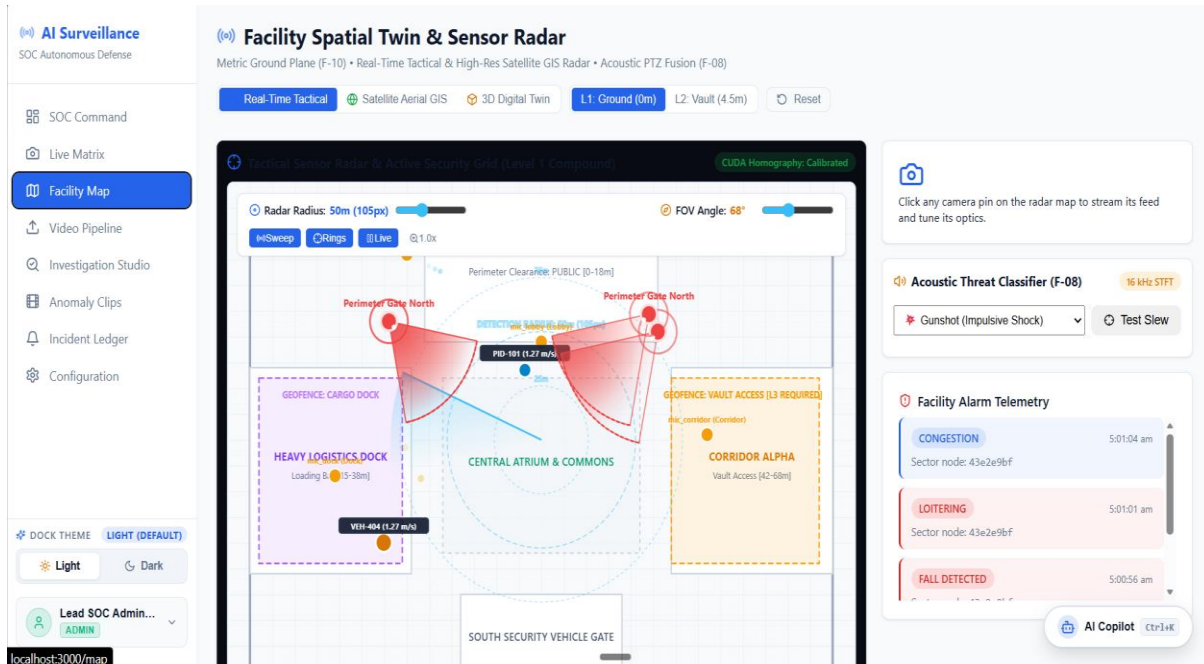


Fig. 1. Facility Spatial Twin and Real-Time Sensor Radar Interface.

2. Video Intelligence and Forensic Analysis

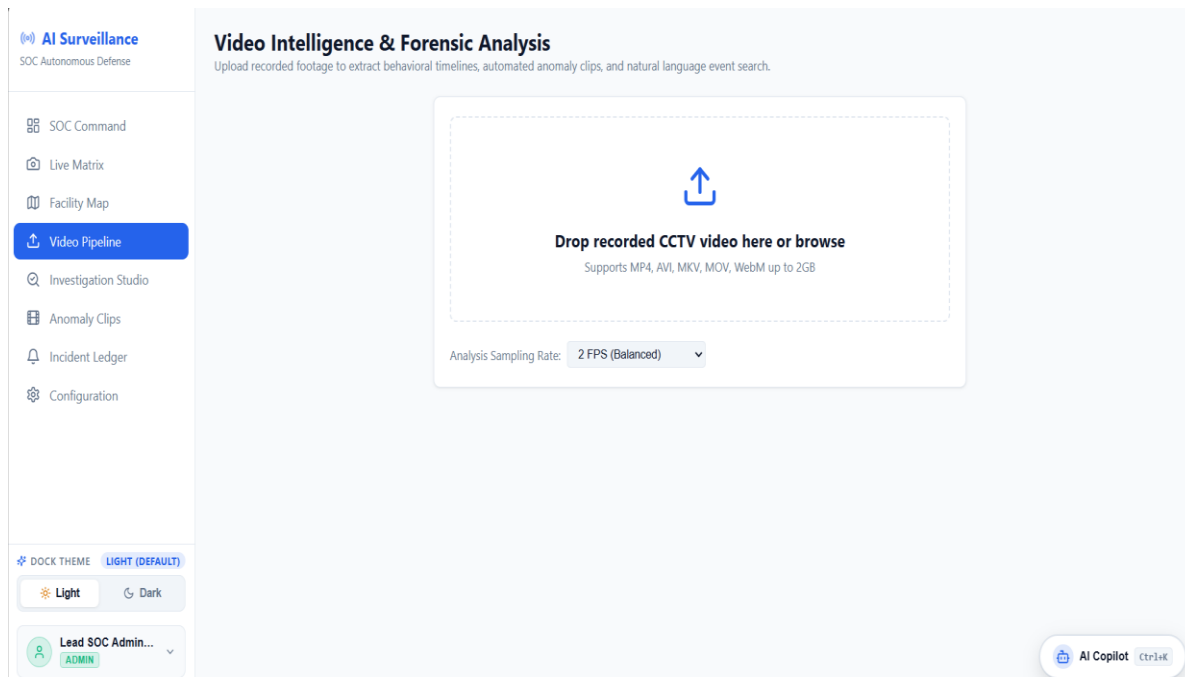


Fig. 2. Video Upload and AI-Based Forensic Analysis Interface

3. Forensic Investigation Studio

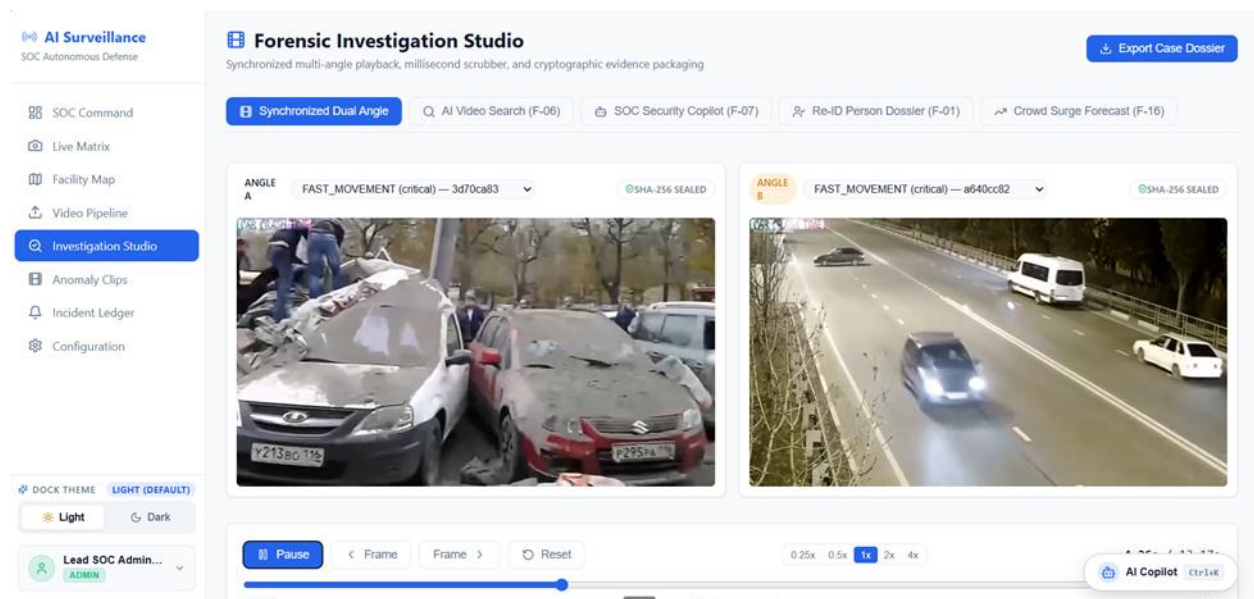


Fig. 3. Synchronized Multi-Angle Video Investigation Interface.

4. Anomaly Clips Management

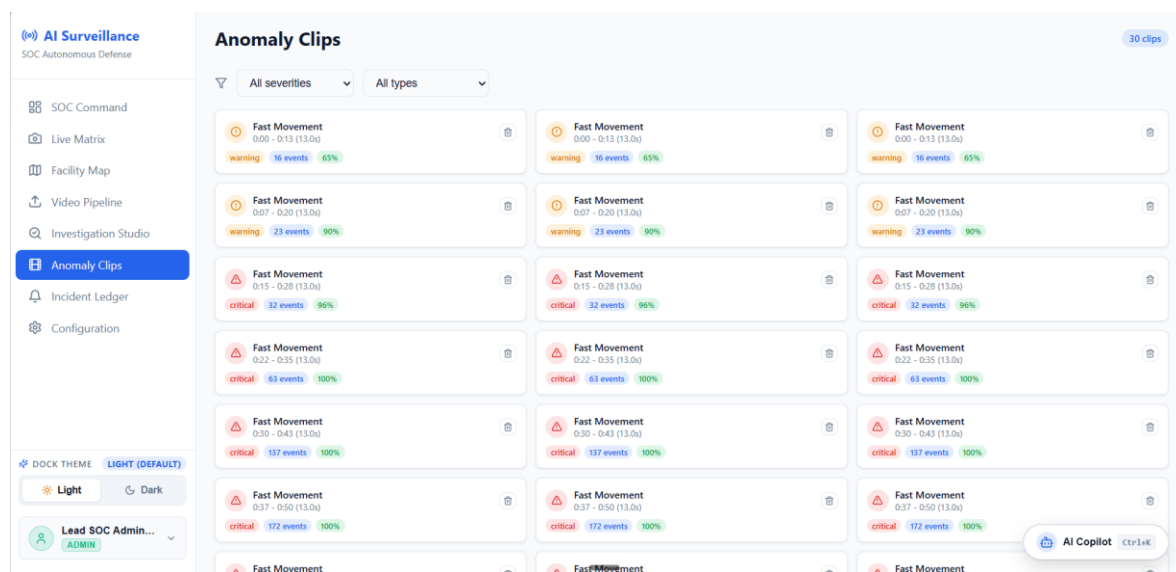


Fig. 4. AI-Detected Anomaly Clips and Evidence Management Interface.

5. Security Incident Management and Audit Ledger

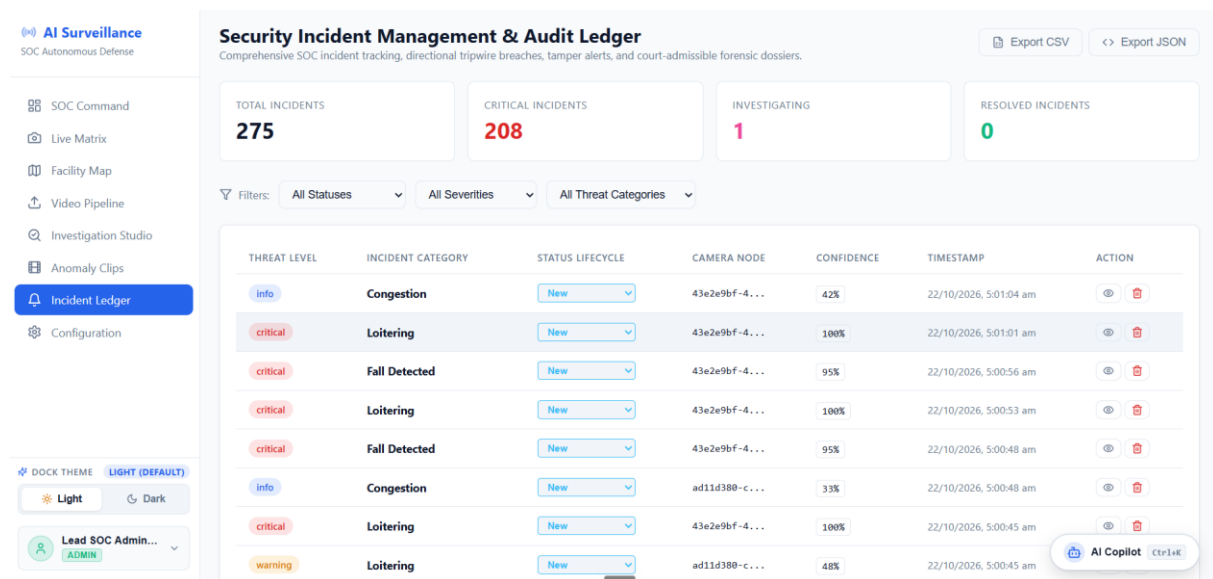


Fig. 5. Security Incident Tracking and Audit Management Interface.

6. System Intelligence and Security Controls

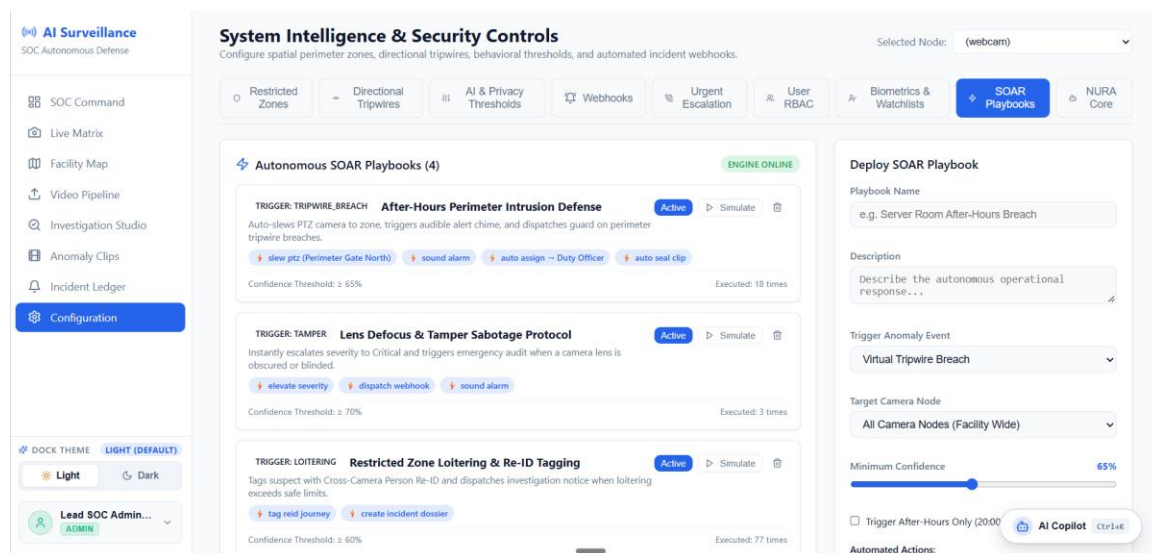


Fig. 6. System Configuration and Autonomous SOAR Playbook Management Interface.

7. SOC Command Center Dashboard

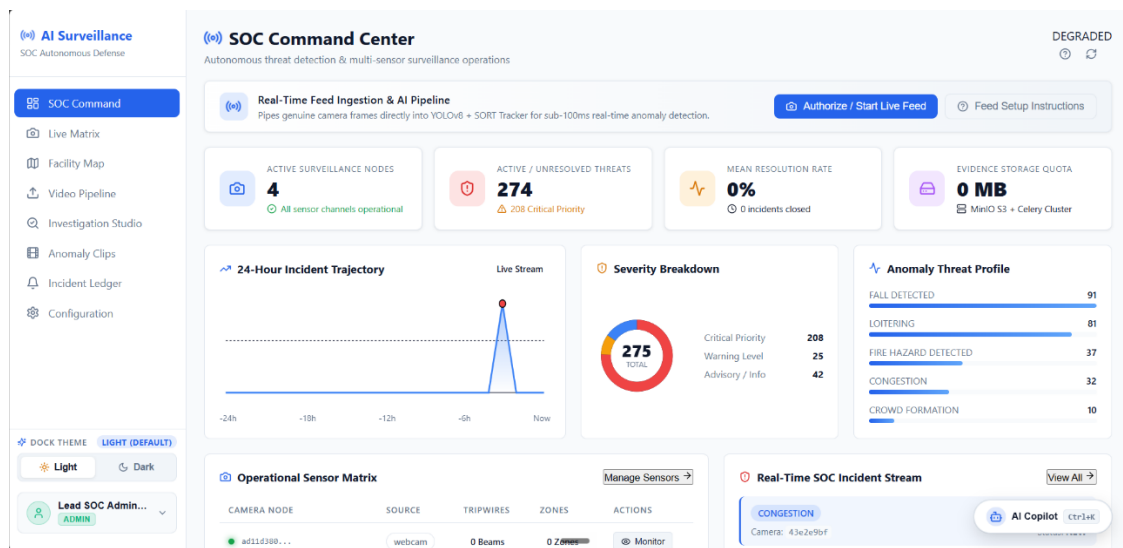


Fig. 7. Centralized Security Operations Command Dashboard.

8. Live Surveillance Matrix

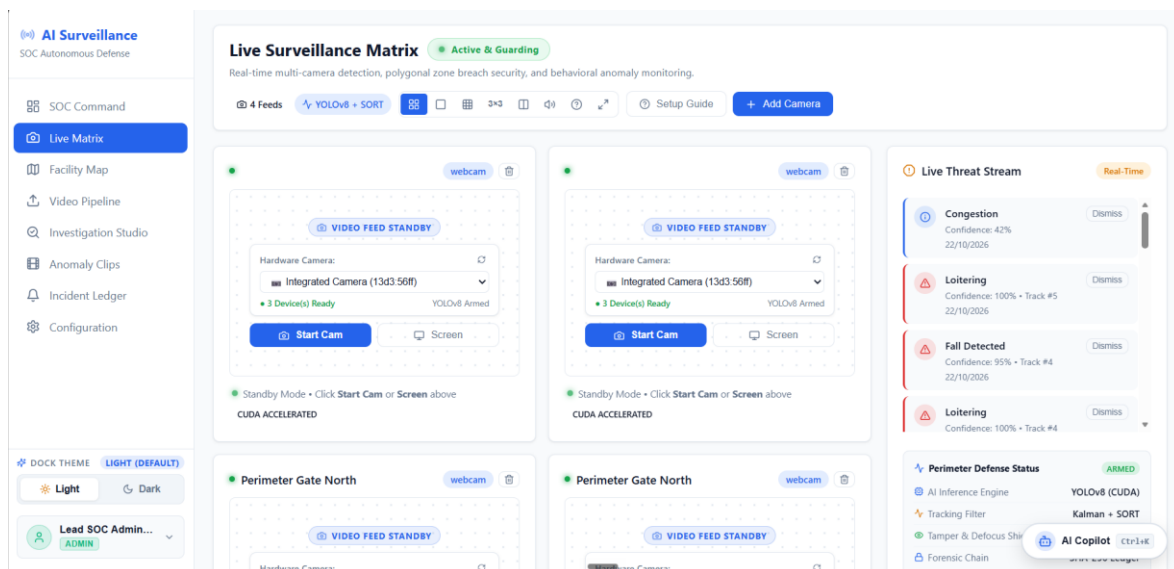


Fig 8. Real-Time Multi-Camera Surveillance and Threat Monitoring Interface.

CONCLUSION

The **AI Surveillance and Autonomous Security Operations Center (SOC) Platform** provides an intelligent and centralized solution for monitoring, analyzing and managing security activities across connected surveillance cameras. Developed using React.js, Python (FastAPI), and modern AI and computer vision technologies, the system transforms conventional CCTV monitoring into an event-driven surveillance platform. It integrates YOLOv8-based object detection, SORT object tracking, facial feature extraction, person re-identification, automatic license plate recognition and anomaly detection to identify potential security events from video feeds.

The platform provides several integrated functionalities, including real-time multi-camera monitoring, facility spatial mapping, video intelligence and forensic analysis, anomaly clip management, incident tracking and automated security workflows. Additional capabilities such as acoustic event analysis, PTZ camera control, predictive crowd analytics and the NURA AI Security Assistant enhance the system's ability to support security operators during monitoring and investigation. Cryptographic hashing and evidence-management mechanisms also help maintain the integrity and traceability of stored surveillance evidence.

By combining AI-based detection, centralized incident management and automated notification workflows, the system helps reduce dependence on continuous manual surveillance and supports faster identification and investigation of potential security incidents. Its modular architecture provides a foundation for extending surveillance capabilities across different security environments.

Overall, the AI Surveillance platform aims to improve security monitoring, operational efficiency and incident traceability through intelligent video analytics and centralized security operations. Further improvements in real-world model validation, semantic video search, video-streaming infrastructure, scalability and security testing will strengthen its reliability and suitability for large-scale deployment. The system is designed to assist security personnel in decision-making, with important security events and AI-generated results remaining subject to human verification.

REFERENCES

- 1) Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016). *Simple Online and Realtime Tracking*. 2016 IEEE International Conference on Image Processing (ICIP), pp. 3464–3468. <https://doi.org/10.1109/ICIP.2016.7533003>
→ For real-time multi-object tracking, object association and movement tracking across consecutive video frames.
- 2) Howard, A., Sandler, M., Chu, G., Chen, L. C., Chen, B., Tan, M., et al. (2019). *Searching for MobileNetV3*. Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), pp. 1314–1324. <https://doi.org/10.1109/ICCV.2019.00140>
→ For efficient deep-learning architecture and visual feature extraction used as a foundation for the project's MobileNetV3-based biometric and person re-identification components.
- 3) Ultralytics. *YOLOv8 Documentation*. Available at: <https://docs.ultralytics.com/models/yolov8/>
→ For YOLOv8 object detection, model inference and computer vision implementation.
- 4) OpenCV. *OpenCV Documentation*. Available at: <https://docs.opencv.org/>
→ For image processing, video frame handling, motion analysis, camera calibration and computer vision operations.
- 5) React Team. *React Documentation*. Available at: <https://react.dev/>
→ For developing the component-based frontend interface, dashboards and interactive surveillance monitoring pages.
- 6) Sebastián Ramírez. *FastAPI Documentation*. Available at: <https://fastapi.tiangolo.com/>
→ For Python-based backend development, REST API implementation, request validation and asynchronous communication.
- 7) PyTorch Contributors. *PyTorch Documentation*. Available at: <https://docs.pytorch.org/docs/stable/>
→ For deep-learning model execution, tensor processing, GPU acceleration and neural network implementation.
- 8) JaidedAI. *EasyOCR: Optical Character Recognition Documentation*. Available at: <https://github.com/JaidedAI/EasyOCR>
→ For extracting text from vehicle license plate images through optical character recognition.
- 9) PostgreSQL Global Development Group. *PostgreSQL Documentation*. Available at: <https://www.postgresql.org/docs/>
→ For relational data storage, database management and structured storage of surveillance events and incident records.
- 10) Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. National Institute of Standards and Technology (NIST). <https://doi.org/10.6028/NIST.AI.100-1>
→ For trustworthy AI development, risk assessment, responsible AI deployment and evaluation of AI system reliability.