TED UNIVERSITY

CMPE 491 Senior Project

OWL Border Security Project Analysis Report

Spring 2026

Team Members:

Ege Yavuz, 14872032366, Computer Engineering

Emre Kaan Arslan, 13021093920, Computer Engineering

Mehmet Yiğit Açdoyuran, 10130437010, Computer Engineering

Supervisor:

Tansel Dökeroğlu

Jury Members:

Mehmet Evren Coşkun

Eren Ulu

1. Introduction

The OWL Border Security System is an AI-powered surveillance and decision-support platform designed to enhance border security by analyzing not only the presence of objects but also the behavioral patterns and intentions behind activities occurring in border regions.

Traditional border monitoring systems primarily focus on detecting objects such as humans or vehicles. However, these systems often fail to interpret the context, sequence of actions, and underlying intent of detected activities. This limitation leads to high false alarm rates and insufficient situational awareness for security personnel.

The OWL system addresses these limitations by integrating computer vision, multi-sensor data, and real-time analytics to monitor border environments intelligently. Instead of treating detections as isolated events, OWL evaluates sequences of movements and interactions to identify meaningful patterns such as reconnaissance, preparation, or illegal crossing attempts.

The system aims to support preventive security strategies by providing interpretable, real-time alerts enriched with behavioral and intent-based classification. By reducing false alarms and increasing contextual understanding, OWL contributes to more effective and proactive border security operations.

2. Current System

Existing Solutions

Current border security systems primarily rely on traditional surveillance technologies such as CCTV cameras, motion sensors, and radar-based detection systems. In recent years, some AI-based solutions have also been introduced, focusing mainly on object detection and tracking.

These systems generally include the following capabilities:

- **Object Detection:**
  Detection of humans, vehicles, and animals using computer vision models (e.g., YOLO, Faster R-CNN)
- **Motion Detection:**
  Identifying movement within restricted areas using basic sensor triggers or video analysis

- **Alarm Systems:**
  Generating alerts when movement or presence is detected in predefined zones
- **Basic Tracking:**
  Following detected objects across frames without deep behavioral understanding

  Data Logging:
  Storing video footage and detected events for later review

Limitations of Current Systems

Despite their widespread use, existing systems suffer from several critical limitations:

- **Lack of Behavioral Understanding:**
  Current systems detect *what is present* but fail to analyze *what is happening* or *why it is happening*. They treat each detection as an isolated event.
- **High False Alarm Rates:**
  Environmental factors such as animals, weather conditions, or irrelevant movements often trigger unnecessary alerts, leading to inefficient resource usage.
- **No Intent Analysis:**
  Systems cannot distinguish between different types of activities (e.g., harmless movement vs. smuggling attempt or reconnaissance behavior).
- **Limited Context Awareness:**
  They do not analyze sequences of actions or interactions between individuals, which is critical in border scenarios.
- **Dependence on Single Data Source:**
  Most systems rely only on video or a single sensor type, reducing reliability and increasing uncertainty.

  Scalability Challenges:
  Expanding these systems across large border areas can be costly and difficult to manage.

Conclusion of Current System Analysis

Existing border security solutions provide basic detection and monitoring capabilities but fall short in delivering intelligent, context-aware, and reliable decision support.

These limitations highlight the need for a more advanced system that can:

- Understand behavioral patterns

- Analyze intent
- Reduce false alarms
- Provide meaningful and actionable insights

The OWL system is proposed to address these gaps.

3. Proposed System

3.1 Overview

The OWL Border Security System is designed as an advanced AI-based surveillance and decision-support platform that enhances traditional border monitoring by incorporating behavioral and intent analysis.

Unlike conventional systems that focus solely on detecting objects, OWL evaluates sequences of actions, interactions between individuals, and environmental context to determine the nature and purpose of activities in border areas.

The system integrates multiple data sources, including video streams and sensor data, to improve detection accuracy and reduce false alarms. By combining these inputs, OWL provides a more reliable and comprehensive understanding of the monitored environment.

Key characteristics of the proposed system include:

- **Behavior-Based Analysis:**
  The system analyzes movement patterns and interactions to identify meaningful behaviors such as reconnaissance, preparation, and crossing attempts.
- **Intent Classification:**
  Detected activities are categorized based on inferred intent, enabling security personnel to distinguish between low-risk and high-risk situations.
- **Multi-Sensor Integration:**
  Video data is combined with additional sensor inputs to verify detections and enhance reliability.

- **Real-Time Processing:**
  The system operates with minimal latency, providing immediate alerts and supporting proactive intervention.
- **Geospatial Awareness:**
  Detected events are mapped with precise location data to enable efficient response and monitoring.
- **Decision Support:**
  Alerts are enriched with contextual information, allowing security personnel to make informed and timely decisions.

The OWL system aims to transform border security from a reactive monitoring approach into a proactive and intelligent system capable of predicting and preventing potential threats.

3.2 Functional Requirements

The OWL system shall provide the following functional capabilities:

3.2.1 Detection and Tracking

- The system shall detect humans, vehicles, and objects in real-time from video streams.
- The system shall track detected entities across frames to analyze movement patterns.

3.2.2 Behavioral Pattern Analysis

- The system shall analyze sequences of movements to identify behavioral patterns such as:
  - Reconnaissance
  - Preparation
  - Crossing attempts
- The system shall consider temporal and spatial relationships between actions.

3.2.3 Intent Analysis and Classification

- The system shall classify detected activities into intent-based categories.

- The system shall distinguish between:
    - Harmless activities
    - Suspicious behaviors
    - High-risk events

3.2.4 Multi-Sensor Data Integration

- The system shall integrate data from multiple sources (e.g., cameras, sensors).
- The system shall validate detections using cross-source verification.

3.2.5 Real-Time Geospatial Alerting

- The system shall generate alerts with precise location (GPS) information.
- The system shall display alerts on an interactive map interface.

3.2.6 Secure Evidence Archiving

- The system shall store detected incidents with:
    - Timestamp
    - Visual evidence
    - Behavioral classification
- All stored data shall be encrypted and securely managed.

3.2.7 Role-Based Dashboard Access

- The system shall provide a user interface with role-based access control.
- Users shall only access data relevant to their authorization level.

3.3 Nonfunctional Requirements

The OWL system shall satisfy the following nonfunctional requirements:

3.3.1 Performance

- The system shall process data in real-time with a maximum delay of **2 seconds**.
- The system shall support continuous monitoring without interruption.

3.3.2 Reliability

- The system shall maintain high accuracy in detection and classification.
- The system shall minimize false positives and false negatives.

3.3.3 Scalability

- The system shall support deployment across large border areas.
- The architecture shall allow easy expansion without redesign.

3.3.4 Security and Privacy

- The system shall ensure secure data storage and transmission.
- The system shall implement anonymization where necessary.
- Access to data shall be restricted based on user roles.

3.3.5 Robustness

- The system shall operate reliably under:
    - Low visibility (night, fog)
    - Harsh weather conditions
    - Challenging terrains

3.3.6 Maintainability

- The system shall be modular to allow easy updates and maintenance.
- AI models and system components shall be upgradable over time.

3.4 Pseudo Requirements

The OWL system will follow these implementation-oriented constraints:

- **Programming Language:** Python
- **AI Frameworks:** TensorFlow / PyTorch
- **Operating Systems:** Linux (preferred), Windows
- **Database:** JSON, CSV, SQLite (initial), scalable DB later
- **Hardware:**
    - Multi-core CPU
    - Minimum 8 GB RAM
    - Optional GPU support
- **Architecture:**
    - Modular system design
    - API-based communication between components
- **Data Handling:**
    - Real-time processing of video streams
    - Storage of critical events only
    - Secure and ethical data management

3.5 System Models

3.5.1 Scenarios

Scenario 1: Suspicious Border Reconnaissance

A group of individuals approaches the border area and moves along the borderline without attempting to cross. The system detects repeated movement patterns and prolonged observation behavior.

The behavioral analysis module classifies this as **reconnaissance activity** and generates a medium-risk alert for monitoring.

Scenario 2: Preparation for Illegal Crossing

Multiple individuals gather in a hidden area near the border, remain stationary for a period, and then start moving together toward a crossing point.

The system detects coordination and grouping behavior.

The activity is classified as **preparation**, and a high-risk alert is triggered.

Scenario 3: Illegal Border Crossing Attempt

A group rapidly moves toward the border line and attempts to cross within a short time frame.

The system detects sudden acceleration and directional movement.

The event is classified as a **crossing attempt**, and an immediate high-priority alert is generated with location data.

Scenario 4: False Alarm – Animal Movement

An animal moves within the monitored area.

The system detects motion but correctly classifies the object as **non-human**, preventing unnecessary alerts.

Scenario 5: Multi-Sensor Verification

A camera detects movement, but sensor data does not confirm it.

The system cross-checks inputs and suppresses the alert, reducing false positives.

3.5.2 Use Case Model

Use Case 1: Monitor Border Activity

Actors: System, Security Officer

Description:

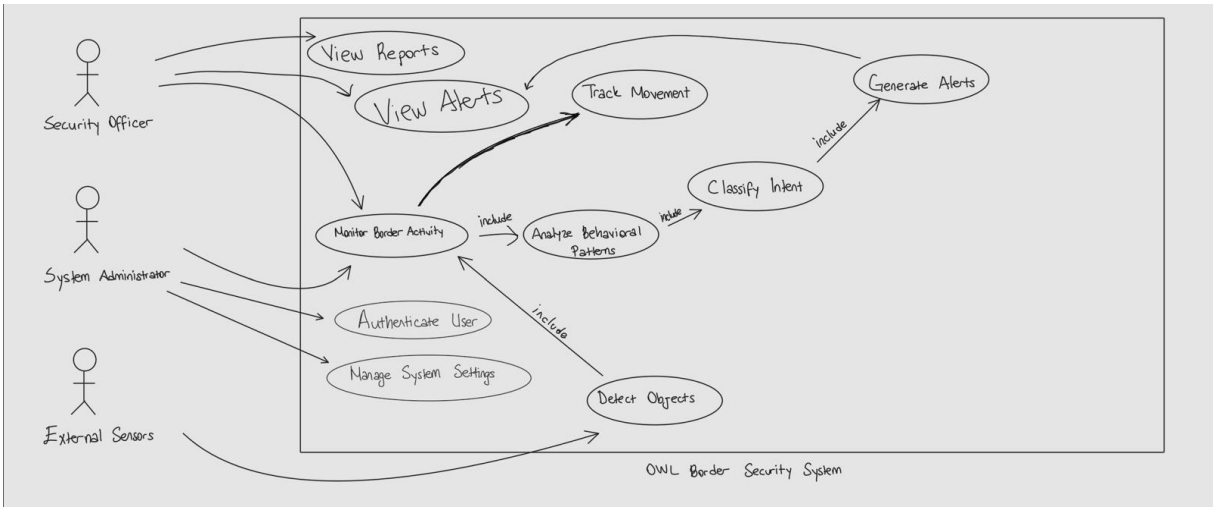
The system continuously monitors video streams and sensor data to detect and analyze activities in border regions.

Main:

1. System receives real-time video input
2. Detects objects (humans, vehicles, etc.)
3. Tracks movements across frames
4. Performs behavioral analysis
5. Classifies activity based on intent

Alternate Flow:

- If no significant activity is detected → system continues monitoring
- If suspicious activity is detected → alert is triggered



Use Case 2: Classify Intent

Actors: System

Description:

The system evaluates detected behaviors and assigns an intent category.

Main Flow:

1. Movement patterns are analyzed
2. Interaction between individuals is evaluated
3. Contextual data is processed
4. Activity is classified (recon / preparation / crossing)

Use Case 3: Generate Alert

Actors: System, Security Officer

Description:

The system generates alerts for suspicious or high-risk activities.

Main Flow:

1. System detects high-risk behavior
2. Alert is created with:
    - Type of activity
    - Risk level
    - Location
3. Alert is sent to user interface

Alternate Flow:

- If activity is low-risk → logged without alert
- If repeated behavior → escalation occurs

Use Case 4: View Alerts and Reports

Actors: Security Officer

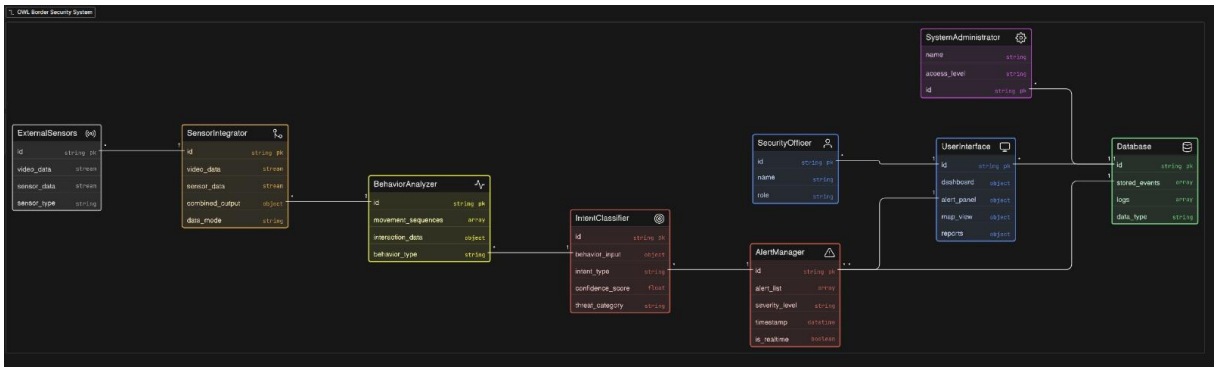
Description:

Authorized users access the system dashboard to monitor alerts and analyze historical data.

Main Flow:

1. User logs into system
2. Views real-time alerts
3. Accesses historical logs
4. Analyzes trends and incidents

3.5.3 Object and Class Model



Class: BehaviorAnalyzer

Attributes:

- movement_sequences
- interaction_data
- behavior_type

Methods:

- analyze_movement()
- detect_patterns()
- classify_behavior()

Class: IntentClassifier

Attributes:

- behavior_input
- intent_type
- confidence_score

Methods:

- evaluate_intent()
- assign_category()

Class: SensorIntegrator

Attributes:

- video_data
- sensor_data
- combined_output

Methods:

- merge_data()
- validate_detection()

Class: AlertManager

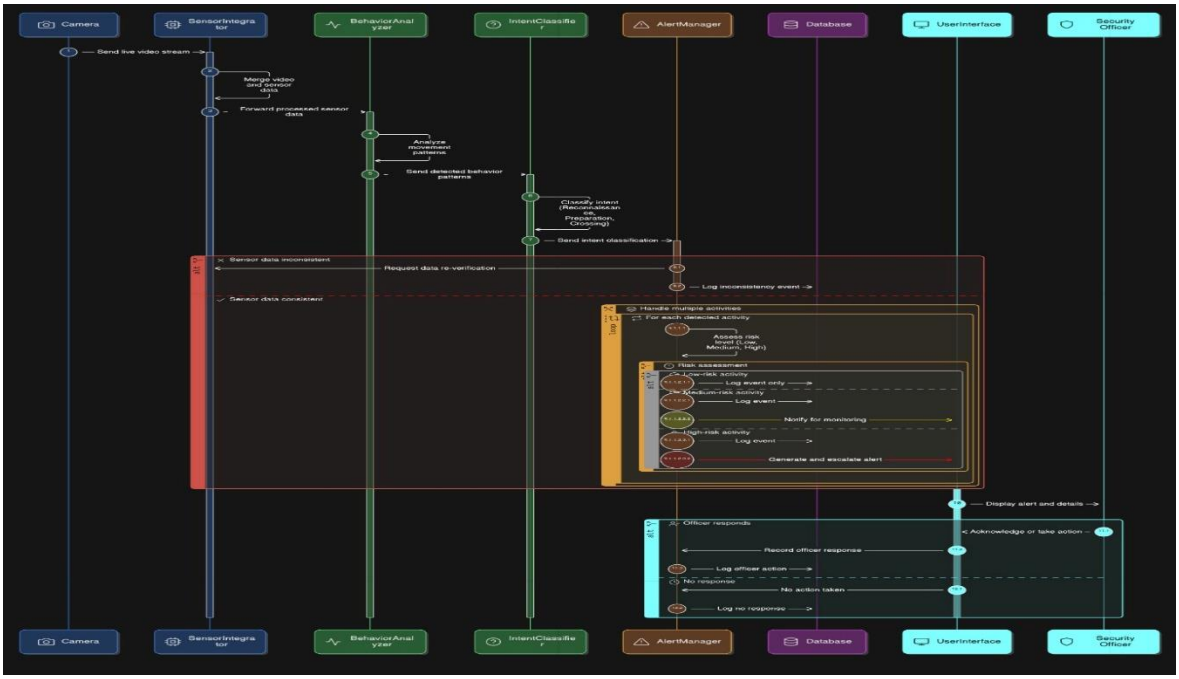
Attributes:

- alert_list
- severity_level
- timestamp

Methods:

- generate_alert()
- send_alert()
- log_alert()

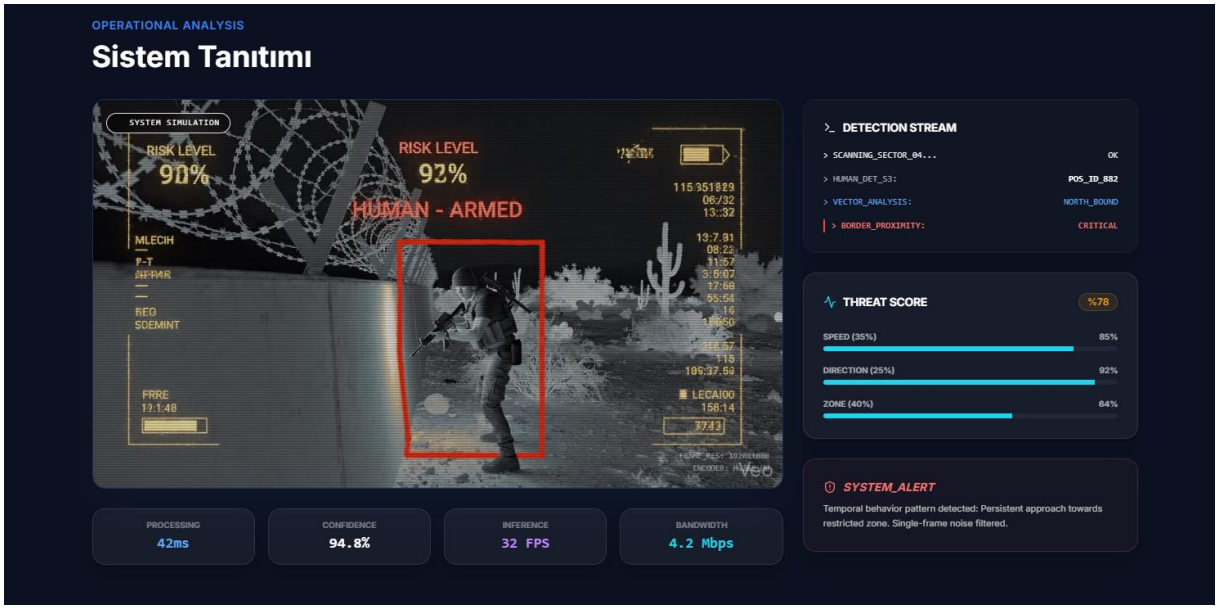
3.5.4 Dynamic Models



System Flow Description

1. **Input Stage**
    - Cameras and sensors provide real-time data
2. **Detection Stage**
    - Objects are detected and tracked
3. **Analysis Stage**
    - Behavioral patterns are analyzed
    - Intent classification is performed
4. **Decision Stage**
    - Risk level is determined
5. **Alert Stage**
    - Alerts are generated and sent
6. **Logging Stage**
    - Events are recorded for future analysis

3.5.5 User Interface (Description Only)



- Dashboard showing:
    - Real-time alerts
    - Activity map
    - Risk levels
- Interactive map displaying:
    - Event locations
    - Movement paths
- Alert panel including:
    - Event type
    - Timestamp
    - Risk classification
- User roles:
    - Security officer
    - System administrator

4. Glossary

Behavioral Analysis

Analysis of movement patterns and interactions between individuals to identify meaningful activities.

Intent Analysis

The process of determining the purpose behind detected behaviors (e.g., reconnaissance, preparation, crossing).

Multi-Sensor Integration

Combining data from multiple sources (e.g., cameras, sensors) to improve detection accuracy and reliability.

False Positive

An incorrect alert generated for a non-threatening activity.

False Negative

Failure to detect a real threat or suspicious activity.

Real-Time Processing

The ability of the system to analyze data and produce results with minimal delay.

Geospatial Alerting

Generating alerts with precise location information (e.g., GPS coordinates).

Anonymization

The process of protecting personal identity by obscuring sensitive data (e.g., face blurring).

AI (Artificial Intelligence)

Technologies that enable systems to perform tasks such as detection, classification, and decision-making.

Computer Vision

A field of AI that enables systems to interpret and analyze visual data from images or video.

Alert

A notification generated by the system to indicate a detected event or potential threat.

Logging

Recording system events, detections, and alerts for future analysis.

Scalability

The ability of the system to expand and handle increased workload without performance loss.

5. References

1. **ACM Code of Ethics and Professional Conduct**
   Association for Computing Machinery (ACM), 2018.
   Available: https://www.acm.org/code-of-ethics

2. **IEEE Code of Ethics**
   Institute of Electrical and Electronics Engineers (IEEE).
   Available: https://www.ieee.org/about/corporate/governance/p7-8.html

3. **Software Engineering Code of Ethics and Professional Practice**
   IEEE Computer Society & ACM Joint Task Force.
   Available: https://www.computer.org/education/code-of-ethics

4. **Computer and Information Ethics**
   Stanford Encyclopedia of Philosophy.
   Available: https://plato.stanford.edu/entries/ethics-computer/

5. **Redmon, J. et al. – YOLO: Real-Time Object Detection**
   Available: https://pjreddie.com/darknet/yolo/

6. **Ren, S. et al. – Faster R-CNN: Towards Real-Time Object Detection**
   IEEE Transactions on Pattern Analysis and Machine Intelligence, 2015.
   Available: https://arxiv.org/abs/1506.01497

7. **Sun, Y., Sun, Z., Chen, W. – The Evolution of Object Detection Methods**
   Engineering Applications of Artificial Intelligence, 2024.
   Available: https://doi.org/10.1016/j.engappai.2024.107862

8. **Rahaman, M. F. – Current Trends in Object Detection Algorithms**
   Available: https://arxiv.org/abs/2308.00000

9. **Behavioral Analysis in Video Surveillance Systems**
   IEEE Xplore Digital Library.
   Available: https://ieeexplore.ieee.org/

10. **Border Security Technologies and Surveillance Systems Report**
    RAND Corporation / Security Studies.
    Available: https://www.rand.org/topics/border-security.html

11. **Roboflow Universe – Object Detection Datasets**
    Available: https://universe.roboflow.com/

12. **Kaggle – Computer Vision Datasets**
    Available: https://www.kaggle.com/datasets

13. **OpenCV Library Documentation (Computer Vision Framework)**
    Available: https://docs.opencv.org/