Check for updates

RESEARCH ARTICLE

Machine learning techniques applied in border crossing

[version 1; peer review: 1 approved with reservations, 1 not approved]

Dana Oniga[1], Monica Florea[2], Iacob Crucianu[3], Diana-Ioana Antonescu-Junghie[4], Mark Procter[5], Georgios Kouzas[6], Dimitris Kassimis[7], Martin David[8], Dimitris Perikleous[9], Andreas Lefkatis[10], Leoni Chondromatidou[11], Niklas Palaghias[12], João Ribeiro Pinto[13], Joao Ferreira[14], Stavros Theocharis[15], John Zaras[16]

[1]R&D, Software Imagination and Vision, Bucharest, 013685, Romania
[2]Head of Unit European Projects, Software Imagination and Vision, Bucharest, 013685, Romania
[3]R&D, Software Imagination and Vision, Bucharest, 013685, Romania
[4]R&D, Software Imagination and Vision, Bucharest, 013685, Romania
[5]Science & Technology, Rapiscan, Stoke-on-Trent, ST8 7PL, UK
[6]R&D, Telesto, Athens, 15561, Greece
[7]R&D, Telesto, Athens, 15561, Greece
[8]IBS Digital ID R&D, Thales DIS, Prague, 140 00, Czech Republic
[9]UAV Department, ACCELIGENCE, Nicosia, 1066, Cyprus
[10]UAV Department, ACCELIGENCE, Nicosia, 1066, Cyprus
[11]Machine Learning Engineer, Athens, Greece
[12]CEO, Quadible, London, WC2H 9JQ, UK
[13]Research Engineering, Vision-Box an Amadeus Company, Lisbon, 2790204, Portugal
[14]Research Engineering, Vision-Box an Amadeus Company, Lisbon, 2790204, Portugal
[15]Artificial Intelligence, SquareDev, Kifisia, 145 61, Greece
[16]Artificial Intelligence, SquareDev, Kifisia, 145 61, Greece

v1 **First published:** 03 Mar 2026, **6**:64
https://doi.org/10.12688/openreseurope.21836.1
Latest published: 03 Mar 2026, **6**:64
https://doi.org/10.12688/openreseurope.21836.1

Abstract

Background

Border control authorities face increasing operational pressure due to growing traveller volumes, evolving security risks, and stricter regulatory requirements. Traditional manual procedures alone are no longer sufficient to ensure both security and smooth passenger flow. The ODYSSEUS project was developed to address these challenges by combining artificial intelligence, computer vision, and multi-sensor technologies into a unified, privacy-respecting solution for border management.

Methods

Open Peer Review

Approval Status ? ✗

	1	2
version 1 03 Mar 2026	? view	✗ view

1. **A Karunamurthy**, Sri Manakula Vinayagar Engineering College, Pondicherry, India

2. **Anna Sagana**, Neuroscience Maastricht University, Maastricht, The Netherlands

Any reports and responses or comments on the article can be found at the end of the article.

The project followed a step-by-step methodology starting with an analysis of user needs, operational workflows, and real scenarios provided by border guards. These inputs were used to define use cases and system requirements. Each ODYSSEUS component was then designed according to the principles of the EU Artificial Intelligence Act, with attention to transparency, robustness, and human oversight. The technologies were implemented, tested in controlled environments, and gradually integrated into a modular platform. Finally, the complete system was validated in three pilot locations representing land, sea, and rail border environments.

Results

The ODYSSEUS platform successfully combined several advanced tools, including digital travel credential verification, behavioural authentication, faceless people counting, unmanned aerial vehicle-based vehicle inspection, and artificial intelligence-supported X-ray screening. All components were integrated into a single decision support interface that provided real-time information and alerts. The pilots demonstrated that the system could support officers by improving situational awareness, reducing manual workload, and enabling faster processing, while maintaining strict compliance with data protection requirements.

Conclusions

The project shows that a modular and artificial intelligence-enabled approach can enhance border control operations without compromising privacy or regulatory obligations. The successful demonstrations in three different environments confirm that the ODYSSEUS technologies are mature, functional, and suitable for further deployment and scaling. The work provides a practical foundation for future integration of artificial intelligence systems in European border management.

Keywords
artificial intelligence, biometrics, border control, explainable artificial intelligence (XAI), identity verification, machine learning, people counting, unmanned aerial vehicles (UAVs)



This article is included in the Horizon Europe gateway.

Corresponding author: Dana Oniga (dana.oniga@simavi.ro)

Author roles: Oniga D: Writing – Original Draft Preparation, Writing – Review & Editing; **Florea M**: Supervision, Writing – Review & Editing; **Crucianu I**: Writing – Original Draft Preparation; **Antonescu-Junghie DI**: Writing – Original Draft Preparation, Writing – Review & Editing; **Procter M**: Writing – Original Draft Preparation; **Kouzas G**: Writing – Original Draft Preparation; **Kassimis D**: Writing – Original Draft Preparation; **David M**: Writing – Original Draft Preparation; **Perikleous D**: Writing – Original Draft Preparation; **Lefkatis A**: Writing – Original Draft Preparation; **Chondromatidou L**: Writing – Original Draft Preparation; **Palaghias N**: Writing – Original Draft Preparation; **Ribeiro Pinto J**: Writing – Original Draft Preparation; **Ferreira J**: Writing – Original Draft Preparation; **Theocharis S**: Writing – Review & Editing; **Zaras J**: Writing – Original Draft Preparation

Competing interests: No competing interests were disclosed.

Grant information: This project has received funding from the [European Union's Horizon 2020 research and innovation programme] under grant agreement No [101073910] (ODYSSEUS EU Project).
The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Copyright: © 2026 Oniga D *et al*. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Oniga D, Florea M, Crucianu I *et al.* **Machine learning techniques applied in border crossing [version 1; peer review: 1 approved with reservations, 1 not approved]** Open Research Europe 2026, **6**:64
https://doi.org/10.12688/openreseurope.21836.1

First published: 03 Mar 2026, **6**:64 https://doi.org/10.12688/openreseurope.21836.1

Introduction

Managing borders today is not just about security, it is about finding the right balance between keeping people safe and making travel smooth and efficient. Nowadays, border authorities must deal with growing passenger numbers, complex threats, and stricter regulations, all while avoiding long lines and frustration for travellers.

The ODYSSEUS project was created to help meet these challenges by bringing advanced technologies like artificial intelligence (AI) and machine learning (ML) into the world of border management. Instead of relying on slow, manual checks, the ODYSSEUS solution uses AI to help border officers make faster, more accurate decisions. It supports better identity verification, risk assessment, and even includes tools for behavioural analysis and biometric matching.

Given the constant changes and challenges in cross-border movements and migration, the European Union (EU) has made border security one of its top priorities.[1] There are significant difficulties at the EU's borders and additionally, irregular migration is expected to be the main problem in 2025. In 2023 the EU borders saw high migration pressures, especially from regions in conflict and that are facing economic difficulties. For example, over 332,000 illegal border crossings were detected, the highest since 2016, with significant movements through the Western Balkans and Eastern and Central Mediterranean routes.[2] Also, cross-border crime is evolving, and criminal networks are adapting to law enforcement by blending contraband in legal flows making detection harder. Geopolitical factors like the war in Ukraine and recent conflicts in the Middle East pose further risks of large migration flows into the EU, so there is a need of strategic and resilient border management solutions that can deliver effective, efficient and precise monitoring has never been more urgent.[2] To address these new risks the European Integrated Border Management (EIBM) framework highlights the need for a unified approach to irregular migration, secondary movements and cross-border crime, to adapt to the growing migration pressures and challenges.[3]

The ODYSSEUS project seeks to address these issues by utilizing machine learning and artificial intelligence technologies to improve border management and security at EU borders.[4]

The usage of machine learning and artificial intelligence in border security can address key challenges like instant threat detection, counting people and automated surveillance, offering accuracy and flexibility. AI-driven solutions like intelligent drones and facial recognition transform traditional security systems by enabling data integration, predictive analysis and faster decision making. This strategic change is in line with EU efforts to build more robust and flexible Integrated Border Management (IBM) systems.[5] Moreover, implementing AI and ML can fill the gaps of traditional systems, especially in processing the increased data volumes related to cross-border activities, therefore security operations at borders can be better and new threat can be prevented.

In this article, we introduce the ODYSSEUS platform and explain how these AI-driven solutions work together to modernize border control. We focus on the core technologies behind the platform, how they are integrated, and the potential benefits they bring for both security and traveller experience.

Methods

The main goal of ODYSSEUS project is to improve security, effectiveness and resilience of border management systems in European Union by using advanced technologies. In a combination of machine learning, artificial intelligence and multi-sensor technologies, the project aims to create a smooth, smart border control and better decision-making processes.

The ODYSSEUS project has five objectives to achieve this goal:

1. **Border Monitoring:** The project will improve real-time surveillance in many border scenarios by utilizing drones, X-ray systems and AI-based analytics.

2. **Identity Verification:** ODYSSEUS will promote non-intrusive identity checks through multi-modal biometric verification, which will improve detection and accelerate the border crossing process for authorized travellers.

3. **Risk Assessment and Predictive Analysis:** The project will use predictive analytics to assess potential dangers so that border agencies can make informed decisions fast on accurate data.

4. **Interoperability and Data Exchange:** To improve border management, ODYSSEUS will focus on interoperability to enable data exchange and to be integrated with current systems across EU Member States.

5. **Sustainable and Ethical AI**: A key objective of ODYSSEUS is to promote sustainable and ethical AI that respects data privacy and EU regulations, so technological progress is done responsibly and transparently.[6]

ODYSSEUS solution combines several AI solutions with a tailored web platform to be used by both border authorities and citizens.

The development of the ODYSSEUS solution followed a step-by-step approach, starting from the needs of border guards and ending with full pilot demonstrations in real environments.

1. **Understanding user needs and defining use cases**

The first phase of the project focused on discussions with border authorities. Together, we analysed how current procedures work, what officers need in their daily activities, and where technology could realistically help. These conversations were translated into specific use cases and operational scenarios that guided the entire technical development.

2. **Designing the solutions according to the AI Act principles**

Once the use cases were clear, the team designed each ODYSSEUS technology: people counting, behavioural authentication, UAV inspection, X-ray analysis, and the main platform, based on the requirements of the upcoming EU AI Act. This meant addressing topics such as transparency, data governance, and human oversight. The goal was to ensure that all components were not only technically strong, but also trustworthy and safe to use.

3. **Implementing the technologies and integrating them into one platform**

Each tool was developed and tested individually and then integrated step by step into the ODYSSEUS platform. A modular architecture allowed the team to connect cameras, sensors, AI models, and the operator interface in a flexible way. For EU-level systems that cannot be accessed directly (such as EES/ETIAS), realistic mock-ups were created so that the workflow could still be demonstrated.

4. **Testing in controlled environments**

Before going to the pilot sites, all components were tested in laboratory settings. This included checking accuracy, response time, performance in different conditions, and the explainability of AI decisions.

5. **Pilot deployment and real-world validation**

The complete ODYSSEUS system was then deployed in three different border environments. Each pilot allowed officers to use the technologies in real scenarios: scanning vehicles with UAVs, analysing X-ray images, verifying digital travel credentials, and monitoring crowds or people flow. These pilots are critical for evaluating the system's technical performance, flexibility, and user experience while keeping privacy, ethics, and being in line with legal compliance. Each pilot was designed to explore how ODYSSEUS's AI-driven technologies can enhance traditional border checks by automating key tasks thus improving border crossings. For example, in rail scenarios, AI models support seamless identity verification using biometrics and behavioural authentication. In maritime and vehicle-focused scenarios, machine learning helps monitor the surroundings using surveillance data and detects anomalies such as unregistered movement or suspicious patterns.

Ethics and consent statements

ODYSSEUS platform and technologies were developed following an ethical-by-design approach, meaning that key values, including privacy, human dignity, fairness, transparency and accountability, were integrated into all the phases of technology development, from design to pilot deployment phases. Such strategy is in line with the GDPR,[7] and AI Act[8] requirements. This approach was supported by a structured ethics governance model within the project that included the setup of an External Independent Ethics Board (EIEB), a Security Advisory Board (SAB), a Project-level Ethics Advisor and Data Protection Officer.

Ethics opinions for the research with humans and with artificial intelligence for the ODYSSEUS project were issued by Project partners' as individual declarations (as organisations that do not have an ethics committee) and also by the EIEB board.

A set of documents based on GDPR and AI Act requirements have been developed to cover the data protection and ethics for the organization and successful completion of the planned trials. Considering the different roles that volunteers participants play in the pilots, informed consents for each of the specific roles and specific pilot has been prepared. For assessing ethical aspects and the respect of ODYSSEUS data protection and ethical principles an assessment questionnaire was prepared, to be distributed to the volunteers-participants and collected after the termination of the pilots. The participants to the pilots signed the writen consent before each pilot iteration. The ethics responsible monitored compliance with ethical and data protection standards during the events and performed the evaluation through questionnaires/debriefing sessions focusing on integrity, privacy, and impact post-event.

Respondents to the ethics assessments considered that pilot activities were non-intrusive, courteous, and they were carried out in a manner that did not threaten comfort and well-being. Their perception of privacy and confidentiality was deemed as heavily secured, as well as strong confidence in data handling in accordance with GDPR requirements was expressed.

No children and minors under 18 years of age took part in the pilots.

Overall, the pilots demonstrate how AI and ML can transform border control into a more efficient, responsive, and user-friendly experience for both travellers and authorities without compromising security or fundamental rights.

Building on this methodology, the ODYSSEUS project brought together all these elements into a coherent technological solution. The insights collected from users, the design choices aligned with EU regulations, and the iterative development cycles all contributed to shaping a platform that can support real border operations. In the following section, we present the ODYSSEUS solution in detail - its main components, how they work together, and the role each technology plays within the overall system.

Results - ODYSSEUS solution

This study presents the ODYSSEUS solution, an AI-based system for improving the efficiency and security of border management processes. The system integrates several key technologies, including digital and virtual passports, AI-powered behavioural verification, UAV-assisted vehicle scanning, and privacy-preserving faceless traveller counting with the ODYSSEUS Platform, allowing the system to be used by both travellers and Border Guards. These technologies work together to optimize identity verification at border crossings, allowing travellers to pass without stopping while maintaining strict security standards. It is tested across various border types, as land and sea, offering a comprehensive approach to managing border crossings and risk assessments.

The main functions of the system can be grouped in:

1. Traveller Enrolment and Pre-Registration

    i. **Digital Travel Credentials (DTC) Creation:** AI validates traveller identity through facial recognition and liveness detection. ML models ensure secure matching between passport data and real-time selfies.

    ii. **Pre-registration:** ML algorithms analyse travel data and compare it against historical ones and external risk indicators to perform preliminary risk assessment.

2. Identity Verification

    i. **Facial Recognition:** Advanced AI models match live facial data against stored Digital Travel Credentials (DTC) or passports, reducing manual verification errors.

    ii. **Liveness Detection:** AI ensures the authenticity of biometric input by distinguishing real users from spoof attempts.

    iii. **1:N Face Matching:** AI-powered biometric systems compare traveller faces against large datasets in seconds, enabling swift identity verification even for high-traffic scenarios.

3. Vehicle And Train Scanning

    i. **X-Ray Inspection:** AI analyses high-resolution X-ray images to detect anomalies, threats, or contraband. ML models identify unusual patterns, reducing reliance on human adjudication.

    ii. **UAV-Assisted Vehicle Scanning:** AI-driven UAV systems count passengers, detect modifications, and perform license plate recognition. ML algorithms process these inputs to flag potential risks in real-time.

4. Risk Assessment

    i. **Threat Detection:** AI tools process a combination of biometric data, X-ray scans, and behavioural analysis to identify risks or anomalies.

    ii. **Behaviour Analysis:** ML models track movement patterns, dwell times, and crowd behaviours, providing real-time insights into suspicious activity.

    iii. **Decision Support System (DSS):** AI aggregates data from multiple sources, generates actionable insights, and flags high-risk individuals or vehicles for further investigation.

5. Data Security and Sharing

    i. **Secure Data Storage:** AI monitors data access patterns to identify and prevent unauthorized activity. Encryption and anonymization algorithms ensure compliance with privacy standards.

    ii. **Digital Wallet:** AI automates secure sharing of travel and health documents, ensuring minimal human intervention and seamless integration with border control systems**.**

6. Administrative Capabilities

    i. **User Management:** ML models analyse usage patterns to detect unusual activities among authorized users.

    ii. **System Monitoring and Reporting:** AI generates insights from operational and statistical data, helping administrators optimize processes and enhance security.

The main AI and ML technologies and the ODYSSEUS platform are explained in the following sections.

Traveller Enrolment And DTC Issuance

The ODYSSEUS platform implements several identity verifications for travellers. Verification of electronic passport (eMRTD - electronic Machine-Readable Travel Document) is included for any traveller, but to use full functionality of the platform the users are encouraged to obtain ODYSSEUS Mobile Wallet App and register to the platform. After registration, the users obtain a digital copy of their passport: an ICAO (International Civil Aviation Organization) Digital Travel Credential that will be used as their travel document and as an authentication token to ODYSSEUS platform self-care portal.

Digital Travel Credential is specified by ICAO organization and is a new type of digital credential that in future will at least partially replace current electronic passports.[9] The Credential is a cryptographic token and contains similar data as the electronic passport. The Credential may be issued as two components: Virtual Component (DTC-VC) is purely copy of the original passport data. It is a data file that contains original data groups and a digital signature of the original passport (SOD - Document Security Object). The Virtual Component is a simple file that may be transferred by any digital means and does not have any additional security apart from the original authenticity and integrity protections provided by the digital signature. Physical Component (DTC-PC) is a cryptographic token that contains the original data, but the ICAO specification also defines it must have own key pair protected by a security mechanism. Additionally, the specification defines NFC - Near-field communication mechanism that is like the original ICAO eMRTD (electronic Machine-Readable Travel Document) specification. ICAO defines the token in a generic way, but the most natural way to implement it is a mobile App in a handset with a secure element and NFC capabilities.

During registration to the platform the users need to provide their eMRTD, their selfie is matched with the picture from the eMRTD and verified for liveness. Then the DTC is issued with the obtained data and shared with the platform. The users are then required to schedule their travel in advance. They provide the expected dates, place and registration plate of a car they are going to use.

The identity verification flow at the border is as follows:

- The user's face is scanned by either BCA (Border and Coastguard Agency) terminal or stationary camera and the ODYSSEUS platform attempts to match it to faces of pre-registered users. If the match is found, then the platform assumes previously shared DTC-VC as the travel document.

- If the match is not successful, then the border control officer requests the user to present his ODYSSEUS Wallet App and reads DTC-PC. This also happens in case the face match is passed with inconclusive result.

- If the DTC-PC is not successful for some reason or if the traveller is assumed substantial risk by the BCA officer or the platform DSS then the BCA will fall back to verification of eMRTD and will follow state of the art identity verification flow.

AI-Powered Continuous Behavioural Authentication

AI-powered continuous behavioural authentication system is used to enhance access control for Digital and Virtual Passports within a mobile wallet application used at border identity verification points. The system collects and processes sensor data such as GPS (Global Positioning System) location, accelerometer, gyroscope, magnetic field, Bluetooth, Wi-Fi traces, and screen touch events to extract behavioural patterns that verify users with measurable confidence levels. The system uses multiple models, each tailored to specific behavioural characteristics, to predict user legitimacy. These predictions are then combined through a fusion model, generating a unified risk score that determines whether the individual accessing the mobile wallet is the legitimate owner. Integration is achieved via an SDK (Software Development Kit) embedded in the mobile app, which securely transmits collected data to a backend for processing and inference. The risk score is accessible at both the app level and the ODYSSEUS platform, supporting its Decision Support System (DSS). To aid border authorities in interpreting these scores, the system incorporates explainable AI techniques. Lastly, the system follows privacy-by-design principles, allowing users to control their data, to grant or withdraw consent, stop processing, or delete it anytime.

One of security threats we identified during analysis of the state of the art of border control processes is an impersonation attack, an attack when illegitimate attacker uses passport issued for someone who is similar to him, either when the passport was stolen or even the legitimate user shares the passport willingly. We can expect this type of attack may be even more frequent when DTC issued from eMRTD is used. The situation when the DTC is issued and the eMRTD is not needed anymore may be exploited by criminal organizations that would build libraries of stolen or even legitimate passports that would allow search for best lookalike match for illegitimate travellers.

In the ODYSSEUS project we plan to mitigate the risk by deploying additional biometric verification that would be linked to the original eMRTD but used by the ODYSSEUS Mobile Wallet App that holds the DTC: Continuous Behavioural Authentication.

We consider that the first time the eMRTD instance is used for the first time user's interactions will be recorded and next time the same eMRTD instance is used the platform will verify the interactions are similar. In case they differ, the ODYSSEUS platform will not prevent the user from traveling but will mark him as substantial risk and advise the BCA officer to high caution.

Continuous Behavioural Authentication uses Machine Learning techniques to ensure the mobile wallet app is secure and accessible only to its legitimate owner. It combines facial recognition and behavioural patterns to continuously verify the user while they interact with the app.

Behavioural biometrics continuously monitor the user's actions while they interact with the app. The system collects data from GPS for location, motion sensors like accelerometers and gyroscopes, and touch interactions on the screen. It learns unique patterns, such as how the user types, swipes, or navigates through the app. Typing behaviour is analysed based on keypress timing, while touch interactions measure scrolling and swiping patterns. Movement patterns, including frequently visited locations and typical motion while using the app, are also tracked.

The system uses machine learning models to ensure continuous verification:

- Movement Patterns: Random Forest analyses GPS data to identify routines, such as frequently visited locations and travel speeds.
- Device Usage Patterns: XGBoost evaluates touch interactions (swiping, scrolling) using features like scrolling straightness and touch frequency. Typing dynamics are analysed with sequence-to-embedding models that assess keypress timing. Transformers and one-time learning enable effective training with minimal data (e.g., 5 swipes or 140 characters).
- Relevant Actions: SVM (Support Vector Machines) models analyse app navigation, including screen transitions and interaction patterns.
- Fusion Model: A Random Forest-based fusion model combines outputs from all modalities into a unified risk score.

Vehicles Screening

Non-Obtrusive and Safe X-Ray Technologies for Vehicle Scanning

X-ray screening technology for occupied vehicles provides a means for creating non-intrusive penetrative inspection capabilities for cars and passenger vehicles with little to no impact to the flow of traffic through a check point. High-speed imaging, upwards of 10 KPH, shifts the bottleneck in the inspection process from data capture to image analysis and adjudication. With significant numbers of border crossing points into the European Union, and limited numbers of border security personnel to support screening requirements, particularly at peak travel times, other methods are required to aid in the image adjudication process.

The use of machine learning approaches to support the inspection of X-ray data for vehicles is becoming increasingly more prevalent[10,11] as more border security and Customs agencies realize the potential that automated inspection capabilities can have in managing concealed threat identification in high-throughput environments. The approach taken borrows extensively from that developed within the medical industry in support of diagnostic X-ray analysis. AI tools, particularly Convolutional Neural Network (CNN) techniques, can help to identify subtle and complex patterns in image data with high reliability.

In support of the ODYSSEUS ambition, algorithms will be deployed on a multimodal X-ray inspection product to assist in both the detection of illicit materials as well as identification of the number of occupants within the vehicle. The inspection platform comprises two inspection modalities. Firstly, transmission X-ray inspection, where X-rays are detected as they pass through vehicles. Such attenuation images probe the metallic nature of objects within the vehicle. Secondly, backscatter X-ray inspection, utilizing the X-rays scattered backwards to identify predominantly organic materials that reside in front, or on top of, otherwise heavily attenuating metallic objects. Backscatter imaging can penetrate the outer shell of a vehicle and readily show materials secreted within the vehicle frame as well as occupants inside the carriage.

Occupancy detection

The occupancy detection algorithm is based on the popular object detection model YOLOX.[12] Benefitting from a single-pass of the network, the computational requirements are reduced such that results can be returned in near real time, supporting the high-throughput Concept of Operations (CONOPs) of the X-ray inspection platform. At the same time, the use of Feature Pyramid Networks supports the detection of a range of feature resolutions from varying object sizes – in this case the variety of people sizes and positions within vehicles.

The YOLOX model was trained on 180 stream-of-commerce images, using solely the top-down backscatter image data. YOLOX-L architecture with pre-trained weights was used with fine-tuning for 300 epochs on the data and tested on 101 occupants within 76 vehicles. Out of the 101 occupants, 98 were correctly identified, and only 1 falsely detected, as presented in Table 1.

Table 1. Various performance metrics of the object detection model used for occupancy detection during vehicle screening.

Metric	Value
Total Occupants	101
True Positives	98
False Positives	1
False Negatives	3
Accuracy	96%
Precision	99%
Prob. Of Detection	97%
False Alarm Rate	1%

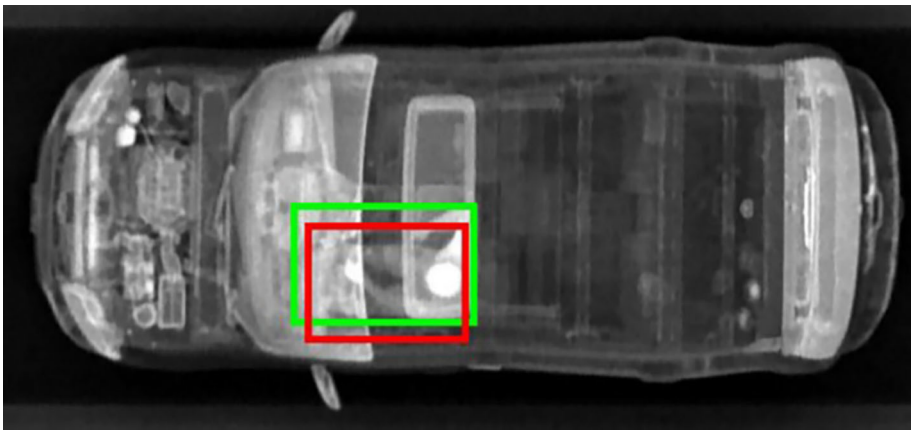

Figure 1. Top-down backscatter X-ray image demonstrating that the occupant has been detected, shown by the brown box, with an accuracy of 95.7% relative to the ground truth which is shown by the green box.

Figure 1 below provides an example of the YOLOX bounding box result for the detection of a driver within the vehicle scan.

Targeted Illicit material detection

The ability to detect small objects of an illicit nature (weapons, cigarettes, drugs, alcohol etc.) in an X-ray scan of a vehicle requires an object-detection model that caters for small-scale items in densely packed environments.

RetinaNet[13] is one of the best one-stage object detection models that has proven to work well with dense and small-scale objects, using a 'one shot' approach for higher speed resolution. It comprises a backbone network for computing a convolutional feature map for object detection, and a second subnet for convolutional bounding box regression.

To overcome the issue of low target item prevalence in X-ray scan data, threat image projection (TIP) approaches are taken using images of target items scanned in isolation and projected into the much larger data set of stream-of-commerce data with no illicit items present. The now healthy, true positive data set allows for a highly effective initial raining stage for object detection algorithms; however, fine tuning is still required at the point of deployment to account for site-specific trade flows and vehicle types.

Figure 2 below shows an example of the detection of a handgun in passenger vehicle.

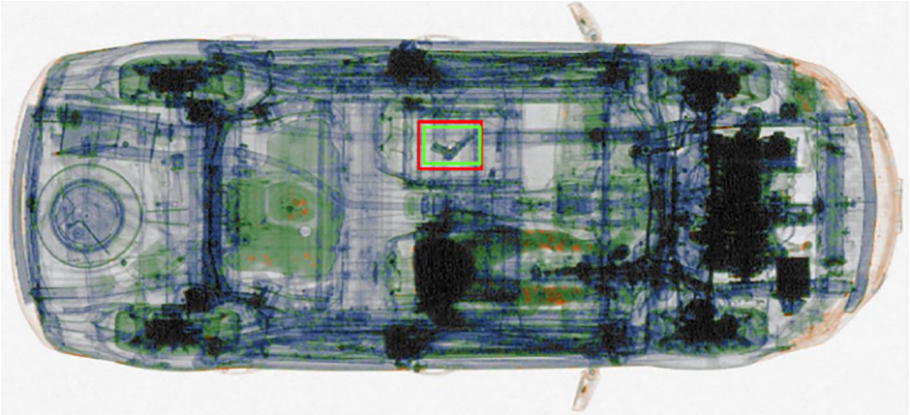

Figure 2. Top-down transmission X-ray image demonstrating that a firearm has been detected, shown by the red box. The ground truth box for the firearm is shown for comparison by the green box.

UAV-Assisted Vehicle Scanning Based On Thermal And High-Resolution Cameras

As border security remains a top priority for nations worldwide, many are exploring advanced technologies such as Unmanned Aerial Vehicles (UAVs), along with artificial intelligence (AI) and machine learning (ML) techniques, to safeguard against potential threats. UAVs, commonly known as drones, have emerged as viable alternatives to traditional crewed vehicles for extensive surveillance and monitoring tasks.[14,15] Aerial surveillance through drones offers superior mobility and a significantly larger range compared to fixed camera systems.[16] Through AI-driven data analysis, UAVs can autonomously interpret vast amounts of information in real time, enabling faster and more accurate threat detection, classification, and response. These versatile aircraft, which can be remotely or autonomously piloted, can carry various payloads, such as cameras, sensors, and communications equipment, enhancing their adaptability for different border security needs.[17]

The integration of ML techniques into UAVs significantly enhances their capabilities and performance, leading to the development of "smart UAVs" that can operate autonomously and adapt to changing environments.[18,19] Building on these advancements, the ODYSSEUS UAV (Figure 3) has been developed as a specialized drone tailored for border security applications. This fully customized platform is designed to support a variety of hardware components, including an onboard processor, to meet the specific operational requirements of border security. It features a four-arm structure, with each arm capable of hosting two motors. Acting as the onboard computer, the NVIDIA Jetson AGX Xavier (NVIDIA, Santa Clara, CA, USA) efficiently handles the execution of multi-sensor data fusion and AI algorithms. Known for its advanced AI processing capabilities within a compact form factor, the Jetson AGX Xavier is ideally suited for mobile robotic applications.[20]

The matrices below provide a comprehensive overview, detailing both the UAV's system requirements (Table 2) and its technical specifications (Table 3).

As demonstrated by its technical specifications, the ODYSSEUS UAV can accommodate multiple sensors tailored to the specific needs of border authorities. This adaptability allows for the integration of high-resolution RGB cameras, thermal



Figure 3. ODYSSEUS UAV.

Table 2. UAV system requirements.

Requirements	Description
Nominal battery voltage: 22.2 V	2 × 6S LiPo batteries in parallel configuration.
Battery charger	Battery charger that can charge 2 LiPo batteries simultaneously (up to 6S).
Radio transmitter for manual piloting	Radio transmitter, compatible with the embedded autopilot, suitable for manual piloting and monitoring of power consumption.
Ground station	Necessary for the preparation and the execution of the flight.

Table 3. UAV technical specifications.

Requirements	Description
Max diameter	1.65 m
Weight (no payload)	9.5 kg
Expected flight time	35-40 min
Total motor thrust (100%)	22.8 Kg

cameras, or other specialized sensors, enhancing its versatility across various surveillance and monitoring tasks. In summary, the ODYSSEUS UAV represents a significant advancement in UAV technology for border security, combining a fully customized hardware platform with advanced AI and multi-sensor capabilities to deliver a responsive and autonomous surveillance solution.

High-Resolution Cameras

License Plate Recognition

The license plate recognition system on UAVs applies a multi-stage pipeline to achieve high accuracy and efficiency. First, a vehicle detector based on the YOLOv8[21] architecture detects vehicles in the frame; the detected vehicles are cropped and passed through another YOLOv8-based detector optimized for license plate localization. Such a two-stage detection process guarantees a robust identification even under tough conditions, such as partial occlusions or various angles.

Upon locating the license plate, the segmented picture is processed using the Google Cloud Vision OCR model,[22] which extracts alphanumeric information with reliable accuracy. To maintain temporal consistency and track vehicles throughout consecutive frames, the system employs ByteTrack,[23] as a robust multi-object tracking algorithm. This tracker assigns a unique identifier to every detected vehicle, enabling the system to perform long-term tracking of multiple license plates, even in dynamic scenarios such as vehicle movement at border crossing points.

The combination of YOLOv8 detectors for vehicle and license plate detection with Google Cloud Vision OCR and ByteTrack ensures real-time recognition and accurate tracking. This way, the approach offers reassuring support to law enforcement and border security forces by automating the monitoring of vehicle registrations and smoothing out the detection of suspicious or unauthorized activities.

Identifying Car Properties

The system uses a tracker based on YOLOv8 to detect and track vehicles across video frames. Experiments are being done by using even lighter variants, such as YOLOv8s for faster inference.[24] Every tracked vehicle maintains a buffer of 20 frames to ensure diverse appearances under varying lighting conditions and angles. These buffered frames are pre-processed through lightweight compression to reduce computational needs.

The pre-processed frames are then analysed by a decision-making AI agent formed on the GPT-4o architecture. This agent returns as a result a structured output highlighting two attributes: the colour and the vehicle type.[25] This technique

also yields interpretable outputs specifying the criteria for its decision. This explainability makes the model predictions transparent, which is crucial for operational trust in security applications.

The combination of robust tracking, diverse data collection, and a sophisticated GPT-4o-based decision agent will enable precise identification of vehicle attributes. Information integral to cross-referencing with vehicle databases and the identification of anomalies - such as unauthorized modifications or mismatches in reported vehicle details - is obtained. By leveraging this system, border security operations are enhanced with detailed and reliable vehicle profiling.

Thermal Cameras for People Detection

Thermal cameras mounted on UAVs can detect and monitor human occupants in vehicles. As there was no pre-trained model suitable for this application at the beginning, a unique dataset was developed by manually annotating real footage captured from drones. This was achieved using a two-stage process involving dataset creation and model training.

Vehicle Detection: The first dataset consisted of annotated vehicles in thermal imagery. A YOLOv10[26] and a YOLOv8 model were both trained on this dataset for robust vehicle detection under thermal conditions.

Human Detection within Vehicles: The second dataset was built by annotating humans visible through open car windows. For this, a dedicated YOLOv8 model was trained to reliably detect human occupants inside the vehicles.[27]

Given the challenges posed by variations in detections across frames, such as fluctuating numbers of detected people, the system uses a specialized approach for updating the state of each car: Confidence Score Tracking for every detected car and its human occupants, the system maintains the confidence scores returned by the Human Detection Model to ensure the reliability of updates.

Incremental Updates Only: To prevent inconsistencies from temporary occlusions or false negatives, the detected number of occupants is updated only in the case of an increase. This serves as a conservative approach wherein no occupant can be mistakenly missed in the post-processing.

This forms an effective solution for vehicle human-occupancy monitoring using this two-stage detection pipeline with intelligent update criteria. The capability is important in viewing unauthorized transportation of human subjects, especially hidden in secret compartments, and improves situational awareness for border security operations.

SEAMLESS BORDER CROSSING

To allow for the robust and accurate recognition of on-the-move persons, the ODYSSEUS seamless border crossing system relies on a pipeline of several biometric algorithms related to identity recognition. This pipeline encompasses all processes needed to process seamlessly captured images into identity decisions, including the detection of faces, their alignment, the assessment of image quality, the detection of potential attacks, and the templification and matching processes. These are described in detail throughout this section.

Capture, detection, and alignment of faces

The first of such components is the capture system, where continuous streams from high-quality cameras are used to acquire images of each border crosser. Frames from these streams are processed by a face detection algorithm, inspired on generic object detectors[28] but trained specifically for human faces. Regarding this specific task, the major problems to overcome are the variations in pose, illumination, expression, and occlusions that may distort or hide information needed by the models to recognize a region of the image as a face. A good face detector should be robust to such noise and missing information and consistently offer accurate face detections, as a human would do.

This is especially relevant in seamless scenarios such as the ODYSSEUS target application. Naturally moving people are more prone to posing variations, occlusions, and changing expressions than individuals who are stationary and actively interacting with a capture device. Great examples of state-of-the-art face detectors that have successfully tackled such

problems are RetinaFace[29] and MTCNN.[30] These have shown competitive performance even in considerably adverse scenarios. Alignment is performed over each detected face, following the proposal in ARCFACE,[31] to enhance the posterior templification and matching process.

Face quality assessment

After the capture and detection of faces, it is important to safeguard the accuracy of the system's decisions with thorough quality evaluation. The first step of quality evaluation is the assessment of overall quality features of the face. This can be done by computing individual scores for each of the several captured face images (following the relevant international standards[32]) such as image sharpness, pose estimation, lighting uniformity, and face occlusions (e.g., glasses or hair). Recent research has also proposed new ways to avoid the strenuous computation of individual quality features by proposing unified quality assessment methodologies. The Open Source Face Image Quality methodology (OFIQ)[33] is one of the most promising, using a single residual network MAGFACE[34] to offer a single unified score of image and face quality. The authors state their methodology weighs the features defined in the international quality standards by their relative importance to obtain single estimations of overall quality with a direct relation to the expected matching score. Ensuring proper filtering of faces based on face quality allows the system to focus solely on valid faces for matching, thereby reducing the processing load on the pipeline. This improves efficiency in both processing power and time.

This first step of quality assessment is extremely important, since facial features need to be sufficiently detailed and sharp to be used for comparison, later, by the templification and matching components. In fact, quality assessment is not only essential for the live captures taken on-site, but also for the reference face images from identity documents or the pre-enrolment stage. Although it is expected that identity document photographs will adhere to high standards of image quality (namely those set by ICAO[32]) it is important to ensure it through proper assessment within our system.

Fraud detection

A second step of image quality evaluation relates to potential attacks and fraud attempts. The main one for the live or pre-enrolment captures is presentation attacks: attackers may use face photographs, videos, paper or silicone masks of authorized individuals to impersonate them while crossing a border. In traditional borders, under intense surveillance by border guards, this possibility is negligible. However, as we target new seamless border crossing scenarios, with fewer constraints and less active human surveillance, it is paramount to verify the captured face images to assess if the face is real or a presentation attack. Here, research has focused on improving the current approaches, mostly deep learning-based, towards higher robustness with new and more sophisticated attacks like high-quality and detailed synthetic masks.[35,36]

In the case of identity document images, it is important to detect potential morphing attacks. Morphing attacks consist of the combination of two face images from different individuals, one of which is an authorized subject. The resulting image retains identity information and relevant visual details from both faces to fool both algorithms and border guards into accepting identity claims from either of the subjects. A passport with a good, morphed image can be successfully used by two different individuals, which poses a serious security threat. To fight it, algorithms based on single image ALPHANET[37] and differential methods SYNTHMORPH[38] can be used to analyse document photos and ensure they are real and unadulterated face images, before moving on to the proper recognition stage.

Templification and Matching

After quality assessment and attack detection, the system can confidently proceed to the recognition of the detected subjects. Templification entails the computation of a vector of numeric features (template) that represents the face. This process is highly relevant, since the face image, even after alignment and quality assessment, will always carry some intrasubject variability and capture noise that pose a significant threat to the subsequent matching process. The templification process is conducted using a deep learning model (such as ARCFACE[31] and ELASTICFACE[39]) which is trained following mixed objective functions with instance and siamese loss (such as triplet loss[40] or ArcFaceLoss[31]) During training, the model learns to extract templates so that they retain most of the identity information within the input face image, while discarding most of the undesired variability and noise.

The matching process involves the comparison of a pair of templates. One of these templates (probe) is the one extracted from the live image, captured on-site, while the second template (reference) can be the one computed from the passport image or the pre-enrolment process. Templates can be compared using simple distance or similar metrics such as the cosine similarity or the Euclidean distance. On an identity verification scenario (1:1), the result of it will be a

representation of how likely it is that both templates' identities match and can be thresholded to obtain a 0/1 (no match/match) decision by defining an operating point. On an identification scenario (1:N), with a gallery of multiple reference images, matching is conducted between the probe and each available reference, and the best score is selected, provided it meets a minimum threshold. It is thus possible to fulfil the intent of accurately recognizing individuals on both scenarios of comparison between live vs. document image (1:1) and live vs. pre-enrolment gallery (1:N).

Gallery management is another crucial optimization, as larger gallery sizes increase the probability of error. By implementing a system that can populate, and segregate galleries based on predefined business rules or the expected behaviour of subjects, the system can reduce both identification time and error rates.

Final remarks on seamless border crossing

As described, this pipeline is composed of several algorithms and components, a majority of which will be essential on most seamless biometric application scenarios. Thus, there are natural concerns over the processing requirements of such a comprehensive pipeline, since a seamless border biometric solution must be able to perform recognition in near real-time, ensuring the natural movement of border crossers, avoiding delays, and ensuring the highest possible throughput rates. Hence, during the development of this part of the ODYSSEUS solution, there was a concerted effort of balancing throughput with precision, by carefully designing and tuning each algorithm to be as lightweight as possible making each algorithm in the pipeline as lightweight as possible while retaining (at least) appropriate levels of accuracy, thus providing a secure and seamless experience to travellers.

Another concern lies with the fairness of the developed algorithms. Bias and fairness in biometric recognition is currently a pressing issue and a trending topic among researchers and industry. It has been reported that biometric algorithms may behave differently depending on demographic aspects of the user, such as their ethnicity, race, gender, or age.[41,42] This is attributed to the data used for training the algorithms and can be fought by improving the diversity of the training datasets. As such, the models developed and integrated into the ODYSSEUS system were trained with carefully selected datasets to ensure demographic diversity and representation, while conducting comprehensive assessments to detect and avoid any biases, to ensure equitable performance with all users.

Faceless GDPR Compliant Travellers Counting

Effective management of crowds has become crucial in terms of security. As a result, the need for efficient and privacy-preserving travellers' counting technology has become more critical, especially at border crossings. The ODYSSEUS project introduces a novel approach, leveraging advanced machine learning (ML) for crowd counting. At the core of this technology is a focus on unauthorized human presence detection in restricted areas, raising alerts for border authorities. Additionally, crowd-related metrics, such as detection and monitoring of unattended or abandoned objects, and real time number estimation of individuals, are provided in travellers used predefined areas, circumstances indicating security risk possibilities. These capabilities of precise crowd management are vital for seamless border crossing.[43]

Over recent years, the advancement of the Convolutional Neural Networks (CNN) has yielded significant improvement in crowd counting accuracy and robustness.[44] We could distinguish the crowd counting techniques in traditional approach and CNN-based approach. On the one hand the traditional methods can be categorized as:

- Detection based: This approach tries to recognize each object of the crowd, directly in the image. Features, such as head or body, are recognized based on feature detection and usually are combined with tracking algorithms to follow individuals as they move throughout the area. Based on the detector, these methods can be divided into monolithic detection and part-based detection. In monolithic detection approaches, images of full body appearances of individuals are used to train a classifier based on features extracted of the full body. Monolithic approaches have low quality results in crowded scenes. In part-based approaches, instead of using full body features to train the classifier, only part of the body is used (such as the head), increasing the quality. The surveys[45–47] describe various detection-based approaches.

- Regression based: This approach consists of two main steps: low-level feature extraction and regression modelling. In the first step, a set of features such as edge feature, colours, texture, and gradient features are extracted and are useful for capturing local information, reducing dimensionality, providing robustness, and finally enabling faster image processing. Once these features are extracted, a variety of regression techniques, such as linear regression, piecewise linear regression, ridge regression, Gaussian process regression, and neural network are used to calculate a mapping from low-level feature to crowd counting. In[46,48] surveys, the most significant regression approaches are mentioned briefly.

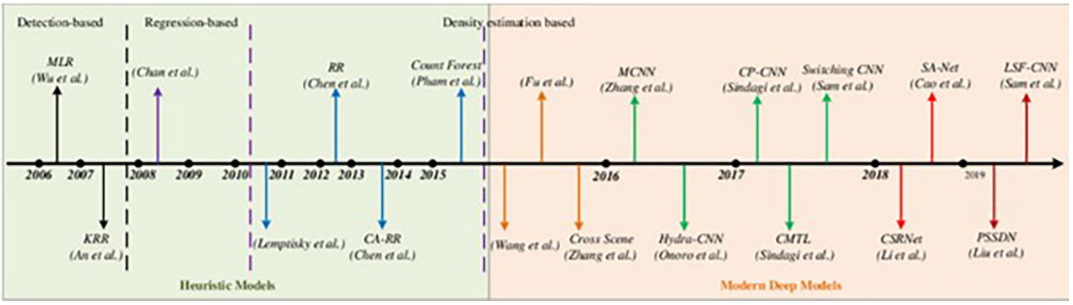

Figure 4. Evolution of crowd counting techniques.

- Density based: This approach, instead of focusing on individual counting, as detection or regression-based approaches do, is trying to directly estimate the density of a scene. With this approach, the challenging task of individual object detection is avoided. Furthermore, the problem is transformed to an estimation of a continuous density function who is integral over any image region gives the object count within that region. More details can be found in.[48,49]

On the other hand, the last decade, a rapid evolution of the crowd counting accuracy is observed, since modern deep learning models are increasingly used.[50,51] CNN-based models are adept at generating density maps, which provide not only the head count but also spatial information about crowd distribution. Recent CNN approaches for crowd counting can be classified by network properties and training strategies,[45,46,49]:

- Basic CNN: Only basic CNN layers are used.
- Context aware CNN: Both global and local contextual details of an image are combined in CNN framework to reduce the estimation errors.
- Scale aware CNN: Multi-column and multi-resolution like architecture is used to provide robustness to scale.
- Multi-task CNN: Along with crowd-counting and density, estimation combines crowd velocity estimation and foreground-background subtraction.

The approaches based on training methods can be classified into:

- Patch-based inference: The CNNs are trained using patches cropped from the input images. During the prediction phase, a sliding window is run over the test image and predictions are obtained for each window and finally aggregated to obtain total count in the image.
- Whole image-based inference: Methods in this category perform a whole-image based inference. These methods avoid computationally expensive sliding windows.

Concluding, Figure 4 (source[46]:) depicts the evolution of crowd counting methods overtime. Traditional methods are highlighted with the green-shaded area, and the modern CNN-based density estimation and crowd-counting models are within the red-shaded background.

DECISION MAKING – MULTI-MODAL FUSION AND DECISION SUPPORT SYSTEM EQUIPPED WITH XAI

The Multi-Modal Fusion and Decision Support System in the ODYSSEUS platform implements sophisticated eXplainable AI (XAI) methodologies, which will guarantee transparency, accountability, and trustworthiness in the decision-making process. Considering the heterogeneous nature of the data and model outputs, the implementation of XAI is customized to handle three different cases, namely:

Tabular Data Explanations

The one relevant to tabular data predictions, for instance, deciding whether a traveller is legitimate or not, will be LIME[52] and SHAP.[53] These algorithms show which features contributed positively or negatively to each prediction. This interpretability is important for border agents, enabling them to understand which variables have driven an automated decision. This approach builds trust in AI-driven systems. For example, attributes like travel history and behavioural patterns are analysed to highlight their impact on classification outcomes.

Detector-Based Explanations

In applications where object detectors are used, for example, vehicle and human detection, dedicated XAI algorithms were designed. These algorithms stem from the principles of Layer-wise Relevance Propagation (LRP)[54] and EigenGradCAM,[55] adapted to suit the unique demands of UAV-based applications. These methods offer localized explanations by underlining regions of the input images that most contributed to the obtained detection results. Such a representation allows the operators to validate the detections, gain insight from false positives or negatives, and consequently tune operational protocols.

Reasoning Outputs by Large Language Models

When the outputs come from Large Language Models, such as in the case of car property identification-colour and car type-specialized agents are designed to provide reasoning for the decisions taken. These agents assess the criteria set upon each property, such as patterns in captured lighting and angles across several frames, before generating well-detailed reports that explain the logical sense behind the Large Language Model predictions. The approach would ensure accountability, as it bridges the gap between the LLM outputs and the operational requirement by providing a clear rationale for each result.

By integrating these XAI techniques across various components of the ODYSSEUS platform, the system not only improves decision-making but also boosts operator confidence in using automated systems. This multi-faced explainability fits well with the commitment of the project to ethics and transparency in AI applications dealing with border management and it reinforces the human-in-the-loop element by giving the operators the abilities to interpret, validate, and intervene in decisions with AI inducement, where appropriate.[56]

ODYSSEUS PLATFORM

ODYSSEUS platform is a technical solution that combines machine learning, artificial intelligence, and multi-sensor capabilities to improve actual border management systems. This scalable and adaptable platform offers a thorough approach to border security, guaranteeing operational effectiveness as well as its compliance with legal and ethical regulations.

The system leverages ML/AI for:

- **Threat Detection:** AI analyses images (e.g., from high-speed rail or drive-through systems) to identify risks, anomalies, and passenger counts.
- **UAV-Assisted Scanning:** Advanced AI algorithms support UAV-based preliminary scanning for identity verification, license plate recognition, and detecting vehicle modifications.
- **Real-Time Insights:** ML models process X-ray data for anomaly detection and passenger estimation, integrating results into the ODYSSEUS risk assessment engine.

AI algorithms are optimized for on-board processors in UAVs, ensuring efficient computation at the edge level. The architecture highlights a robust integration of ML and AI to enhance border security, operational efficiency, and decision-making precision.

The platform comprises three main levels - Edge, Backend, and User Interface—each playing a critical role in integrating ML and AI capabilities for efficient border management. There are also specialized components, which even placed on one of the three levels, are emphasized here for their specific role. The levels are:

1. **Edge Level (Data Acquisition Layer).** This layer focuses on data collection from various sources:

    - **IoT Sensors and Devices:** Cameras (CCTV, UAV, thermal, and RGB), X-ray systems, digital passport readers, and NFC-enabled devices.
    - **Mobile Devices:** Used for traveller enrolment, DTC (Digital Travel Credential) creation, and pre-registration.
    - **External Sources and Databases:** Integration with national and EU databases for validation and risk assessment.
    - **UAV Systems:** For advanced vehicle monitoring, including passenger counting, license plate recognition, and anomaly detection.

2. **Platform Level (Data Management Layer).** This is the core of the solution, where data is processed, stored, and analysed:

    - **AI and ML Tools:** For facial recognition, behaviour analysis, crowd monitoring, threat detection, and risk assessment.
    - **Decision Support System (DSS):** Centralized system offering real-time insights for border authorities.
    - **Data Storage and Persistence:** Secure and scalable storage for personal and operational data.
    - **Audit and Monitoring Mechanisms:** To ensure transparency and regulatory compliance.
    - **Communication Gateway:** For seamless data transfer between edge devices and the cloud.

3. **User Interface Level (Application Layer).** This layer facilitates interaction with the system for travellers, border officers, and administrators:

    - **Mobile and Web Applications:** Allow pre-registration, enrolment, and DTC handling.
    - **Border Control Touchpoints:** Equipped with NFC readers, biometric verification tools, and display systems for real-time data access.
    - **Administrative Portals:** For system configuration, reporting, and role-based user management.

The deployment adapts to land, sea, and train border crossing scenarios, with consistent private cloud components supporting tailored local configurations:

- **Edge Devices:** Integration of AI-ready hardware like UAV-assisted scanners for anomaly detection and identity verification.
- **Private Cloud Resources:** High-performance clusters (management and worker nodes) facilitate large-scale AI computation.

Conclusion

The ODYSSEUS solution highlights the potential of AI applications in transforming border management processes by addressing key challenges of efficiency, security, and compliance. The integration of AI-powered technologies, such as continuous behavioural authentication, explainable decision-making, and advanced peoples and vehicle scanning, underscores the system's ability to optimize border operations in a practical and scalable manner.

A significant contribution of the solution is the use of AI to seamlessly verify travellers' identities without requiring them to stop. This is achieved through two key AI applications. First, continuous behavioural authentication uses sensor data collected when a traveller interacts with their mobile device to access digital credentials such as GPS, accelerometers, gyroscopes, and touch interactions to capture the legitimate user's behavioural patterns. During border crossing,

it compares real-time patterns to ensure the person using the digital wallet matches the rightful owner of the digital credentials. This continuous verification process adds an extra layer of security by detecting anomalies that could indicate unauthorized access. Second, AI-based border crossing uses facial recognition to match the traveller's live facial biometric with the digital credentials created for their identity and specific trip. This dual-layered approach, combining behavioural and biometric verification, enhances both the accuracy and reliability of the identity verification process while significantly reducing delays at border checkpoints.

The use of UAVs equipped with AI-driven image analysis represents another advancement in border security. Through real-time vehicle surveillance, license plate recognition, and people detection, the platform demonstrates how AI can automate complex tasks that were traditionally labour-intensive. This capability is particularly valuable in challenging environments, such as land and water borders, where traditional surveillance methods may be less effective.

Explainable AI plays a crucial role in building trust and accountability within the ODYSSEUS platform. It provides clear insights into how and why AI models arrive at their decisions, including which factors or data points influenced the outcome. For example, it can show where the system focused to make a particular decision, offering border authorities a transparent understanding of the process. This clarity allows operators to act with confidence, ensuring decisions are both justifiable and aligned with security protocols. This alignment of advanced AI capabilities with operational needs highlights.

In summary, the ODYSSEUS solution demonstrates how AI can effectively address modern border management challenges. By combining advanced technologies such as continuous behavioural authentication and explainable AI, it enhances security, supports efficient decision-making, and fosters trust in automated systems. These advancements provide a solid foundation for future developments and wider implementation in border control operations.

Each AI technology has proven its capability to handle different operational environments during lab testing. The next step is to evaluate the integrated system in diverse pilot scenarios, including land, water, and train borders, to confirm its performance in real-world settings. By combining multiple data sources and leveraging explainable AI, the platform aims to deliver clear and actionable insights to border authorities. This integration is expected to reduce errors, optimize resource allocation, and support more informed decision-making processes.

Data availability statement

The raw data used in this study in the section "Vehicle screening" are proprietary and cannot be shared publicly due to contractual and intellectual property restrictions. Access to these data is therefore restricted for security and confidentiality reasons. The Institutional Review Board (IRB) did not impose additional restrictions beyond those required by contractual obligations. Aggregated performance values supporting the findings are available within the manuscript.

Researchers may request access to the raw data by contacting acristini@rapiscan.com. Requests must include a clear justification for access, the intended use, and institutional affiliation. Access will be considered on a case-by-case basis and may require a signed non-disclosure agreement (NDA) to ensure compliance with proprietary restrictions.

The datasets that can be made public are available on ZENODO repository: Search ODYSSEUS PROJECT.

ODYSSEUS PROJECT. Annotated images when searching for intruders on top of the train for Use Case 1 https://doi.org/10.5281/zenodo.17712365[57]

This project contains the following underlying data:

Annotated images when searching for intruders on top of the train for Use Case 1.(Json, png)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

ODYSSEUS PROJECT. Annotated images when searching for intruders on top of the train for Use Case 7 https://doi.org/10.5281/zenodo.17913112[58]

This project contains the following underlying data:

Annotated images when searching for intruders on top of the train for Use Case 7.(Json, png)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

ODYSSEUS PROJECT. Annotated images when searching for intruders on top of the train for Use Case 10

https://doi.org/10.5281/zenodo.17913029[59]

This project contains the following underlying data:

Annotated images when searching for intruders on top of the train for Use Case 10.(Json, png)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

ODYSSEUS PROJECT. Annotated images when searching for intruders on top of the train for Use Case 11

https://doi.org/10.5281/zenodo.17913018[60]

This project contains the following underlying data:

Annotated images when searching for intruders on top of the train for Use Case 11.(Json, png)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

ODYSSEUS PROJECT. Thermal Car Segmentation Dataset.

https://doi.org/10.5281/zenodo.17295900[61]

This project contains the following underlying data:

Thermal Car Segmentation Dataset. (Txt, yaml, jpg)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

ODYSSEUS PROJECT. Annotated Thermal Image Dataset for Car-Window and Person Segmentation.

https://doi.org/10.5281/zenodo.17295713[62]

This project contains the following underlying data:

Annotated Thermal Image Dataset for Car-Window and Person Segmentation. (Txt, yaml, jpg)

Data is available under the terms of the Creative Commons Attribution 4.0 International.

References

1. Frontex: *EU external borders: Detections down 42% in first 9 months of 2024.* Frontex; 2024.
Reference Source
2. Frontex: *Annual Risk Analysis 2024/2025.* Warsaw: Frontex; 2024.
3. Frontex: *Risk Analysis 2023/2024.* Warsaw: Frontex.
4. Frontex: *Irregular border crossings into EU so far this year highest since 2016.* Frontex.
Reference Source
5. Frontex: *The Strategic Risk Analysis Report.* Frontex; 2024.
6. E. Comission: **Ethics guidelines for trustworthy AI.** 8 April 2019.
Reference Source
7. EC: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da).* Brussels: EC; 2016.
8. EC: **REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence.** *Official Journal of EU, Brussels.* 2016.

9. ICAO: **Doc 9303 Machine Readable Travel Documents.** *INTERNATIONAL CIVIL AVIATION ORGANIZATION.* Quebec, Canada H3C 5H7: 2021.

10. Vaitkevičius P: *Lithuanian Customs is developing an AI-based X-ray image analysis system.* Novian; 2024. [Accessed 17 12 2024].
Reference Source

11. **AI Meets X-ray Technology: Introducing the New Online Course on Image Data Analysis.** [Accessed 17 12 2024].
Reference Source , | **Reference Source**

12. Ge Z, Liu S, Wang F, *et al.*: **YOLOX: Exceeding YOLO Series in 2021.**
Reference Source

13. Lin T-Y, Dollár P, Girshick R, *et al.*: **Feature Pyramid Networks for Object Detection.**
Reference Source

14. O. PROJECT: *Annotated images when searching for intruders on top of the train for intruders on top of the train for Use Case 1.* ODYSSEUS PROJECT.

15. Ahmadian N, Lim GJ, Torabbeigi M, *et al.*: *Smart border patrol using drones and wireless charging system under budget limitation.* Elsevier; 2022.
Publisher Full Text

16. Kamate S, Yilmazer N: *Application of Object Detection and Tracking Techniques for Unmanned Aerial Vehicles.* Elsevier; 2015.
Reference Source

17. Sarıçiçek İ, Akkuş Y: *Unmanned Aerial Vehicle hub-location and routing for monitoring geographic borders.* Elsevier; 2015.
Reference Source

18. Laghari AA, Jumani AK, Laghari RA, *et al.*: *Unmanned aerial vehicles advances in object detection and communication security review.* KeAi; 2024.
Reference Source

19. Lagkas T, Argyriou V, Bibi S, *et al.*: *UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things".* MDPI; 2018.
Reference Source

20. O. PROJECT: *Annotated images when searching for intruders on top of the train for intruders on top of the train for Use Case 7.* ODYSSEUS PROJECT; 2025.

21. Diwan T, Anirudh G, Tembhurne JV: *Object detection using YOLO: challenges, architectural successors, datasets and applications.* Springer Nature Link; 2022.
Publisher Full Text

22. Google: *Extract insights from images, documents, and videos.* Google.
Reference Source

23. Yifu Zhang PS, Yi Jiang DY, Weng F, *et al.*: *ByteTrack: Multi-Object Tracking by Associating Every Detection Box.* Cornell University; 2022.
Reference Source

24. Stavros Theocharis JZ: *Thermal Car Segmentation Dataset.* ODYSSEUS PROJECT; 2015.

25. Open-AI: *ChatGPT.* Open-AI.
Reference Source

26. Wang A, Chen H, Liu L, *et al.*: *YOLOv10: Real-Time End-to-End Object Detection.* Tsinghua: Tsinghua University; 2024.

27. Stavros Theocharis JZ: *Annotated Thermal Image Dataset for Car-Window and Person Segmentation.* ODYSSEUS PROJECT; 2025.

28. Jocher G, Chaurasia A, Qiu J: **YOLO by Ultralytics.** 2023.
Reference Source

29. Deng J, Guo J, Ververas E, *et al.*: **RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild.** *EEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).* 2020; pp. 5202–5211.

30. Zhang K, Zhang Z, Li Z, *et al.*: **Joint Face Detection and Alignment Using Multi-task Cascaded Convolutional Networks.** *IEEE Signal Processing Letters.* 2016; 1499–1503.

31. Deng J, Guo J, Yang J, *et al.*: **ArcFace: Additive Angular Margin Loss for Deep Face Recognition.** *IEEE/CVF Conference on Computer Vision and Pattern Recognition.* 2019; pp. 4690–4699.

32. I. J. S. WG3: **Portrait Quality (Reference Facial Images for MRTD).** 2018.
Reference Source

33. B. f. S. i. d. Informationstechnik: **Open Source Face Image Quality (OFIQ).**
Reference Source

34. Meng Q, Zhao S, Huang Z, *et al.*: **MagFace: A universal representation for face recognition and quality assessment.** *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).* 2021.

35. Fang M, Huber M, Damer N: **Developing Face Presentation Attack Detection Based on Privacy-friendly Synthetic Data.** *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).* 2023; pp. 1061–1070.

36. Fang M, Yang W, Kuijper A, *et al.*: **Fairness in face presentation attack detection.** *Pattern Recogn.* 2024; **147**: 110002.
Publisher Full Text

37. Tapia J, Busch C: **AlphaNet: Single Morphing Attack Detection Using Multiple Contributors.** *IEEE International Workshop on Information Forensics and Security (WIFS).* 2023; pp. 1–6.

38. Tapia JBC: **Impact of Synthetic Images on Morphing Attack Detection Using a Siamese Network.** *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications.* CIARP; 2023.

39. Boutros F, Damer N, Kirchbuchner F, *et al.*: **ElasticFace: Elastic Margin Loss for Deep Face Recognition.** *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).* 2022.

40. Chechik G, Sharma V, Shalit U, *et al.*: **Large scale online learning of image similarity through ranking.** *J. Mach. Learn. Res.* 2010; 1109–1135.
Reference Source

41. Wu H, Albiero V, Krishnapriya KS, *et al.*: **Face Recognition Accuracy Across Demographics: Shining a Light Into the Problem.** *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops.* 2023; pp. 1041–1050.

42. Pangelinan G, Krishnapriya KS, Albiero V, *et al.*: **Exploring Causes of Demographic Variations In Face Recognition Accuracy.** *Computer Vision: Challenges, Trends, and Opportunities.* 2024; 30–61.
Publisher Full Text

43. O. PROJECT: *Annotated images when searching for intruders on top of the train for intruders on top of the train for Use Case 10.* ODYSSEUS PROJECT; 2025.

44. O. PROJECT: *Annotated images when searching for intruders on top of the train for intruders on top of the train for Use Case 14.* ODYSSEUS PROJECT; 2025.

45. Sindagi VA, Patel VM: **A survey of recent advances in CNN-based single image crowd counting and density estimation.** *Pattern Recogn. Lett.* 2018; **107**: 3–16.
Publisher Full Text

46. Gao G, Gao J, Liu Q, *et al.*: **CNN-based Density Estimation and Crowd Counting: A Survey.** *ArXiv.* 2020; **abs/2003.12783**.

47. Shi M, Yang Z, Xu C, *et al.*: **Revisiting Perspective Information for Efficient Crowd Counting.** *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).* Long Beach, CA, USA: 2019.

48. Hassen KBA, Machado JJM, Tavares JMRS: **Convolutional Neural Networks and Heuristic Methods for Crowd Counting: A Systematic Review.** *Sensors (Basel).* **22**(14): 5286.
Publisher Full Text

49. Nivedya M, Jose SK: **Image Based Crowd Counting: A Review.** *Proceedings of the International Conference on Systems, Energy and Environment 2022 (ICSEE 2022).* 2022.

50. Khan MA, Menouar H, Hamila R: **Revisiting crowd counting: State-of-the-art, trends, and future perspectives.** *Image Vis. Comput.* 2023; **129**: 104597.
Publisher Full Text

51. Gao H, Deng M, Zhao W, *et al.*: **A Survey of Crowd Counting CNN-based.** *Research Square.* 2021.

52. Zhang Y, Song K, Sun Y, *et al.*: *"Why Should You Trust My Explanation?" Understanding Uncertainty in LIME Explanations.* Cornell University; 2019.
Reference Source

53. Marcílio WE, Eler DM: **From explanations to feature selection: assessing SHAP values as feature selection mechanism.** *IEEE Xplore.* 2020.
Reference Source

54. Montavon G, Binder A, Lapuschkin S, *et al.*: *Layer-Wise Relevance Propagation: An Overview.* Springer Nature Link; 2019.
Publisher Full Text

55. Selvaraju RR, Das A, Vedantam R, *et al.*: *Grad-CAM: Why did you say that?.* Cornell University; 2017.
Reference Source

56. Huang Y, Wang XK, Zhang Y, *et al.*: *Application of human-in-the-loop hybrid augmented intelligence approach in security inspection system.* Beijing: Frontiers; 2025.

57. ODYSSEUS: **Annotated images when searching for intruders on top of the train for Use Case 1.** *Zenodo, Bucharest.* 2025.
Publisher Full Text

58. ODYSSEUS: **Annotated images when searching for intruders on top of the train for Use Case 7.** *Zenodo, Bucharest.* 2025.
Publisher Full Text

59. ODYSSEUS: **Annotated images when searching for intruders on top of the train for Use Case 10.** *Zenodo, Bucharest.* 2025.
Publisher Full Text

60. ODYSSEUS Consortium: **Annotated images when searching for intruders on top of the train for Use Case 11.** *Zenodo, Bucharest.*

2025.
Publisher Full Text

61. ODYSSEUS: **Thermal Car Segmentation Dataset.** *Zenodo, Athens.* 2025.
Publisher Full Text

62. ODYSSEUS: *Annotated Thermal Image Dataset for Car-Window and Person Segmentation.* Athens: 2025.
Publisher Full Text

Open Peer Review

Current Peer Review Status: ? ✗

Version 1

Reviewer Report 27 March 2026

https://doi.org/10.21956/openreseurope.23619.r70580

© **2026 Sagana A.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✗ **Anna Sagana**
Neuroscience Maastricht University, Maastricht, The Netherlands

Overview
This manuscript describes the ODYSSEUS project, a modular AI platform for border management integrating digital travel credential verification, behavioural authentication, people counting, UAV-based vehicle inspection, and AI-supported X-ray screening. The project is evidently of practical significance. However, the manuscript in its current form does not meet the standards expected of a research article.

The authors may have conducted genuinely valuable applied work but the manuscript in it current form does not yet reflect it. Fundamental revision is required: the paper needs quantitative performance data, a proper literature review, a critical discussion section, and legally and ethically rigorous treatment of its compliance claims.

Structure
The paper's core problem is that it conflates system description with scientific evaluation. The Methods section describes system architecture and design principles but does not provide sufficient detail for independent replication or evaluation. The Results section consists primarily of a description of what the system *is* and *does* in principle, rather than reporting what happened when it was deployed. Crucially, what little empirical content exists (i.e., the pilot studies) is reported partly under Methods rather than under Results, creating confusion about what was done versus what was found. The constant tense changes (from present, to future to past in no predictable way and within a section) further adds to the confusion. The authors must resolve this before the scientific contribution can be properly assessed.

Absence of quantitative performance data
The manuscript contains almost no reportable performance indicators. The X-ray occupancy detection table is essentially the only quantitative result in the paper. There are no accuracy figures, sensitivity or specificity rates, false positive or false negative rates, or processing speed benchmarks for facial recognition, behavioural authentication, or UAV detection performance. The three pilot deployments (across land, sea, and rail environments) are described in vague terms

with no outcome data.

The behavioural authentication system's false acceptance and rejection rates are never reported, yet these are central to the manuscripts security claims. There is no discussion of how any system component performs under adversarial conditions such as occlusion, poor lighting, or scale, despite these being predictable operational challenges.

Additionally, there is no discussion of what happened when system components disagreed with each other one of the most important operational questions in a multi-modal fusion system of this kind.

Reproducibility and data quality
Training datasets are poorly described: sizes, sources, class distributions, and annotation protocols are largely absent. The authors must either provide substantially more detail about their data or clearly acknowledge the limitations this imposes on the claims they can make.

No engagement with the prior literature
The Introduction does not situate ODYSSEUS within the existing landscape of AI-assisted border management or biometric identification research. There is no comparison with comparable systems, nor engagement with the academic literature on the specific technical problems being addressed. The assertion that "traditional manual procedures alone are no longer sufficient" is stated as self-evident rather than evidenced.

The introduction also promises capabilities including "predictive analytics to assess potential dangers" and "interoperability across EU Member States" that are never meaningfully delivered or evaluated later in the paper. Such claims should either be substantiated or removed from the manuscript.

No critical discussion
There is no acknowledgment of limitations, edge cases, or conditions under which system components underperformed. Future work is described in vague terms ("wider implementation") with no concrete research questions, unresolved technical problems, or lessons drawn from the current findings. Most importantly, there is no discussion what happens to a traveller incorrectly flagged as high-risk? No human review obligation or error correction mechanism is described anywhere in the manuscript (or did I miss it?). For a system of this kind, these are not optional considerations.

The conclusion largely restates the introduction and system description. Phrases such as "the ODYSSEUS solution demonstrates how AI can effectively address modern border management challenges" are presented as conclusions without the evidence required to support them. Since no outcome data is reported in the paper, these conclusions seem circular.

Legal compliance claims are inadequately substantiated
The manuscript repeatedly asserts compliance with the EU AI Act and GDPR. These are serious legal claims that are not sufficient supported. The manuscript acknowledges the AI Act but never seriously engages with what compliance requires in practice.

Border control biometric systems fall squarely into the AI Act's high-risk category under Annex III,

triggering extensive conformity assessment obligations, including risk management documentation, data governance requirements, transparency measures, human oversight mechanisms (see earlier point), and registration in the EU database. Additionally, the general prohibition on real-time remote biometric identification in publicly accessible spaces (Article 5) is directly relevant to the behavioural authentication component. While pure biometric *verification* (confirming that a person is who they claim to be) is excluded from the prohibition and classified as high-risk rather than banned, behavioural scoring raises distinct and more serious concerns. The manuscript does not distinguish between these.

Likewise, the manuscript asserts GDPR compliance but never explains how continuous collection of GPS, accelerometer, gyroscope, Bluetooth, Wi-Fi, and touch data from travellers' personal devices is proportionate under Article 5(1)(c). "Privacy-by-design" is invoked as a label rather than demonstrated through any technical or architectural evidence. The "faceless people counting" claim also deserves scrutiny: density maps and movement pattern tracking can constitute personal data processing under GDPR even without explicit facial identification, and the manuscript does not address this or how the application does not fall under this restriction.

Is the work clearly and accurately presented and does it cite the current literature?
No

Is the study design appropriate and does the work have academic merit?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Partly

If applicable, is the statistical analysis and its interpretation appropriate?
No

Are all the source data underlying the results available to ensure full reproducibility?
No

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: face recognition, face matching, legal decision making, reliability of human and AI-generated evidence, legal psychology

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 18 March 2026

https://doi.org/10.21956/openreseurope.23619.r71154

© 2026 Karunamurthy A. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

A Karunamurthy
Sri Manakula Vinayagar Engineering College, Pondicherry, Pondicherry, India

This manuscript presents the ODYSSEUS platform, an artificial intelligence-driven system designed to enhance border control operations using machine learning, computer vision, biometric authentication, UAV-based surveillance, and explainable AI techniques. The study integrates several advanced technologies such as facial recognition, behavioural authentication, vehicle scanning through X-ray imaging, and crowd monitoring systems to support border authorities in improving operational efficiency and security.
The topic addressed in this manuscript is relevant and timely, particularly considering the increasing need for intelligent and automated border management systems. The integration of multiple AI technologies into a single modular platform is a strong aspect of the study. In addition, the authors have considered important ethical and regulatory issues such as data privacy, explainable AI, and compliance with regulatory frameworks, which are essential when deploying AI systems in security-sensitive environments.
However, several aspects of the manuscript require further clarification and improvement. First, the experimental evaluation and performance validation are limited. The manuscript would benefit from additional quantitative results, including performance metrics such as accuracy, precision, recall, and system efficiency across different deployment scenarios. Second, the description of the datasets used for training and testing the machine learning models is insufficient. More detailed information regarding dataset size, data sources, annotation processes, and training procedures would improve reproducibility.
Furthermore, the manuscript would benefit from a clearer comparison with existing border security or surveillance systems to demonstrate the advantages and novelty of the proposed ODYSSEUS platform. While the authors mention pilot deployments, additional evaluation results and discussion of the outcomes from these pilot studies would strengthen the scientific contribution of the work.
Overall, the manuscript presents a promising AI-based framework for modern border management and is aligned with current research directions in intelligent surveillance systems. With revisions addressing the points mentioned above, particularly regarding experimental validation, dataset description, and comparative analysis, the paper could provide a valuable contribution to the field.
After pasting this, your **final selection should be:**
Reviewer Decision:
Approved with reservations

Is the work clearly and accurately presented and does it cite the current literature?
Partly

Is the study design appropriate and does the work have academic merit?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?

Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Partly

Are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions drawn adequately supported by the results?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Artificial Intelligence, Machine Learning, Computer Vision, Intelligent Surveillance Systems, Data Analytics, Smart Security Systems,cloud computing , IoT

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.