# Unauthorized Entry/Tailgating

> Real-time alerts for any unauthorized entry, anywhere.

## Overview

Tailgating or piggybacking is the entry or exit of more people, things, or vehicles than are permitted by access control rules into or out of a controlled area or through a controlled access gateway. Tailgating is one of the simplest forms of a social engineering attack. Some examples of tailgating are: - A tailgating event occurs when persons, generally on foot or in a vehicle, attempt to gain access to an area for which they do not have the required credentials.

- A person without the necessary access credentials tries to follow another individual (again on foot or in a vehicle) into a controlled access location.
- Piggybacking - a person sits on the shoulders of another person or is carried in some other way by the other person into the controlled access area.
- Reverse entry - When someone tries to enter through a "exit only" access point on foot or in a car, a corresponding issue occurs. **Reverse entrance** is a term that can be used to describe this improper use of an exit portal.

## Vision AI based monitoring

- Acquiring one or more stereoscopic images of an area of observation from client, wherein objects in the area of observation are characterized by:
  a. An object type and
  b. An authorization status indicating whether the object is authorized with respect to the controlled access area.
- Analyzing the one or more images using a machine vision processing system to identify a first object in the area of observation and to classify the first object in a first object type among a plurality of object types that are pre-defined in the machine vision processing system, said first object having supplied an authorization with respect to the controlled access area, and further using the machine vision processing system to identify a second object in the area of observation and to classify the second object in a second object type among the plurality of pre-defined object types, wherein the authorization status of each of

the objects is determined separately from classifying the object in an object type; and

- Applying one or more access control rules to the information obtained from the image analysis to determine whether the second object is attempting to breach the controlled access area by utilizing the authorization supplied by the first object in violation thereof, wherein the controlled access area is limited to objects that are classified in a defined object type and have a status that is authorized with respect to the controlled access area, and wherein the one or more access control rules determine whether the second object is attempting to breach the controlled access area by separately determining:
  a. Whether the classification of the second object is in the defined object type and
  b. Whether the second object has a status that is authorized with respect to the controlled access area. **VisionAI based solution** is focused on improving the performance of "People object type detector" using the **YoloV3 Object detection model along with HaarCascades** , for locating facial features/face identification by tuning parameters like Learning Rate, IoU, Momentum and identifying the best freezing layer.

# Model Details

## Dataset

We have considered the following datasets to build unauthorized entry detection model:

- PETS2009 (Person Evaluation of Tracking and Surveillance)
- AVSS
- CLEAR
- NIST TRECVID (2021)
- CROWD11
- iLIDS

All these datasets that are mainly focused on:

- People tracking
- Video analytics evaluation
- Loitering detection
- Crowd counting
- Attendance based evaluation

- Person re-identification

## Model

The model to perform tailgating detection is in progress and it will be released soon.

## Scenario details

The business logic for this scenario is as follows:

- We use existing camera feeds from the premises to monitor unauthorized entry events.
- VisionAI system is able to run on edge devices. It uses camera feeds for processing.
- Along with camera feed the model uses various sensors and detectors to monitor the entry points of a secured area and once the sensors detects any motion or activity, then the signals are processed by the algorithm to determine whether they represent a potential unauthorized entry or not.

#### Test now with online Web-Cam

To test this model & scenario, you can use the following steps:

- Install the visionai package from PyPI

```
$ pip install visionai
```

- Test the scenario from your local web-cam

```
$ visionai scenario test unauthorized-entry-detection

Downloading models for scenario: unauthorized-entry-detection
Model: unauthorized-entry-detection:
https://workplaceos.blob.core.windows.net/models/yolov5s-unauthorized-
entry-detection/yolov5s-unauthorized-entry-detection-0.0.1.zip


Starting scenario: unauthorized-entry-detection..
```

- You should be able to see the events generated on your console window with detection of unauthorized entry within the camera field of view.

#### With RTSP Camera - Pipelines

[TODO]

#### With Azure Setup

VisionAI app is available at a Azure Market place, one can download and use it by following steps mentioned here

## Features:

The VisionAI solution is the most efficient way of implementing this scenario, as evidenced by the following features:

- Real-time monitoring: The solution can be used to monitor the premises in real-time and raise alerts when an unauthorized entry or tailgating is detected.
- Customization: The model is customizable and can be trained with custom datasets to suit your specific needs.
- Integration: The solution can be integrated with existing camera infrastructure systems effortlessly.

## Training with custom data

The scenario is provided as part of our GPL-v3 package for VisionAI. If you wish to train this with custom datasets, please contact us and we can provide you with the training code. You can do custom training with your own datasets for free, as long as it complies with GPLv3 license (you give back the code to the community). If you are interested in a custom license, please contact us.

## Contact Us

- For technical issues, you can open a Github issue here.
- For business inquiries, you can contact us through our website.