Challenge:

Facial recognition security system allowing employees to enter company building. We currently are given a tag to enter the company building, but this is highly insecure as tags can be lost or given to non-employees and they would be able to gain access into the building. The tags last indefinitely and are never checked or needing refresh. Having a system where only employees whose faces are registered in the building database would significantly improve security.

What data could be relevant to train the CNN for this use case?

1. Employee face data

This includes photos of employees’ face, ideally high-quality, with different lighting conditions (bright/dark/day/night, etc.). It would also be beneficial to obtain photos that contains different facial expressions or photos taken from different angles of the face.

1. Non-employee face data

Having photos of people who are non-employees can help to reduce false positives, again these photos should ideally be in high quality and contains various facial expressions and angles.

1. Street data with and without pedestrians

Sometimes there would be pedestrians walking on the street in front of the camera, and sometimes there would be no one. Either scenarios should be treated as normal and should not even trigger the model to activate.

After collecting these photos, it is crucial to label them correctly, then convert them all into 2D arrays using their pixel values. If possible, normalise the pixel values to a range between 0 and 1.

What are some potential outlines for its network architecture?

The network has an input layer that takes RBG image of size 360 \* 360.

It then has the first layer with maxpool.

Then second layer a convolution layer

Then another convolution layer

Finally an output layer that outputs 1 if the input image is an employee, or 0 if not an employee

How would you evaluate the effectiveness of the network?

The effectiveness of the network can be measured by using a confusion matrix, looking at the number of false negatives or false positives. In the case of employees, it is important to let the employees enter the building, so false negatives must be 0, even if that means false positives might become higher. There are people at reception anyway to greet any strangers in the building.

From the confusion matrix we can also work out accuracy/precision/recall/f1-score, and we can use those to make decisions on how we might want to tweak or fine-tune the model.

Lastly, conduct real life real-time testing, make employees use the new security system and record the results.