Jacob Rivera
AI410
Sept 19, 2026

03 | Learning Lab

PART 1:

- My model will classify an "employee" with a visible badge, and a person without a badge because this is relevant to cybersecurity, where physical access control is part of protecting critical infrastructure.

Link: **https://teachablemachine.withgoogle.com/models/9lzBfxH-NL/**

PART 2:

- This model is relevant to cybersecurity because physical access control can be a weak point along with logical access controls. In some buildings that require a badge scanner, an attacker can bypass this by tailgating or piggybacking, where someone who is unauthorized follows closely behind an authorized employee through a secure door before it closes. This usually happens without the employee knowing. If a camera can visually confirm whether each person entering the building is wearing a badge, it could act as a secondary check against this kind of social-engineering attack. I think the biggest challenge I faced was getting false positive reactions from the training model. I set up two classes, and my initial dataset used 100 sample webcam images per class. In this version, I found the model was learning "something near the neck" rather than detecting a badge specifically. Crossing my arms near my chest got flagged as wearing a badge. I corrected this over two revisions: first adding 50 more sample images of myself with my arms folded near my neck, which only helped partially, then adding 100 more images holding random objects near my neck, such as socks and a piece of string. I noticed that in testing random objects, the color white was triggering the "wearing a badge" class. So, to counteract this I specifically used white colored objects to train the model to recognize that color alone was not a good indicator of a badge. I wanted it to notice the shape and features of a badge instead. The second revision improved the model's accuracy the most. The overall process taught me that small details can really affect how an image classifier behaves, and that a model can pick up on shallow features. For example, the color and position. To improve the model, I would probably need to test it on multiple different people and different types of badges, since it is only trained on me. I believe this idea could scale into a real application for detecting unauthorized people coming in through building entrances. Paired with badge scanners, physical security would be significantly stronger.