Artificial Intelligence and Machine Learning is valuable but is only as secure as it trained and used.

We need to use artificial intelligence and machine learning as another tool in our lives, but not rely upon it.

This demonstration uses a trained visual machine learning model that has been tampered with false images. Other machine learning model training data such as ChatGPT could also be tampered with. It is important to confirm the validity of the tools and information that we use.

In this case, the cupcakes are included with the fruits, and the toy car is included with the Bakugans.

SCAN ME

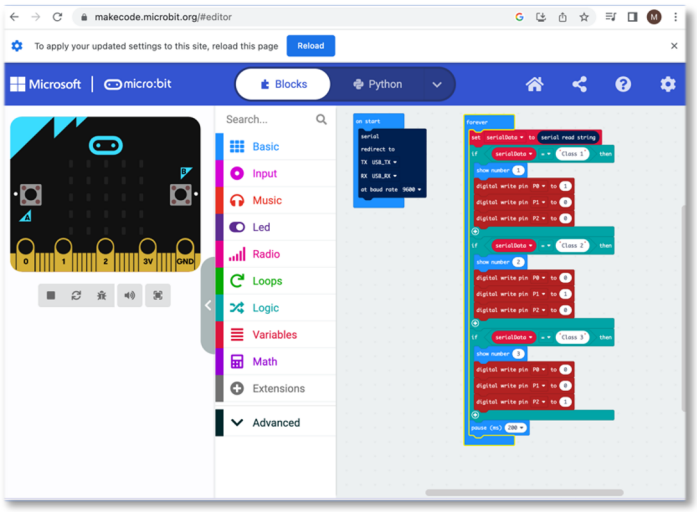

Figure 1. Micro:Bit Block Based Programming for Class Binary Output Control

- This code configures the USB port to data to be received from the AI visual application by the Micro:Bit at a data rate of 9600 bits per second.
- The data received is stored in a variable serialData.
- serialData is compared against the strings of Class 1, Class 2, and Class 3. If there is a match the 5x5 LED display is changed to a number and the a PIN is turned on (changed from a zero to a one).

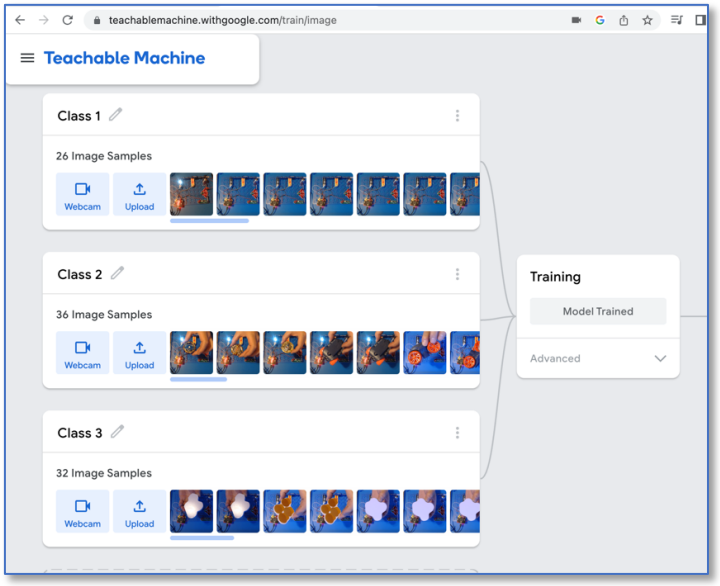

Figure 2. Using Google Teachable Machines on a laptop with a camera to train Class 1, the Snap circuit board, Class 2 the Bakugans, and Class 3 the Fruit.

- Teachable machines is used to create classes of images.
- The classes of images of a baseline of the SnapCircuit board, Bakugans, and Fruit. Class 2 and 3, Bakugans and Fruit have been hacked with additional imagery.
- The images are then used to “train” the machine using Tensorflow. Tensorflow is a free and open source library that everyone can use for machine learning and artificial intelligence. It was initially created in November of 2015.

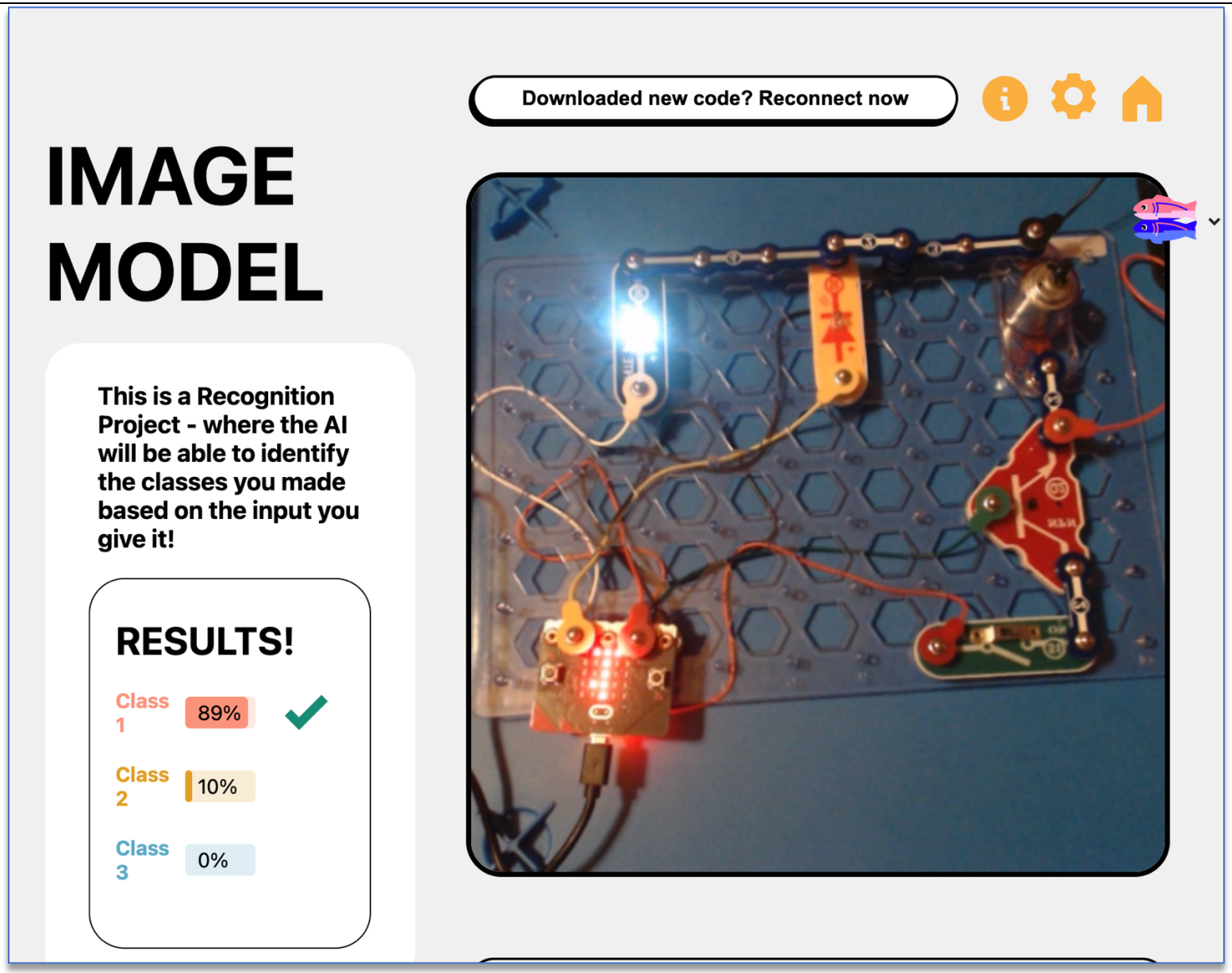

Figure 3. The AI Imaging tool uses the Teachable Machines trained model to connect the real time camera view to Micro:Bit code.

- SnapCircuits provide a great mechanism to learn about both simple and complex circuit design without using a breadboard.
- Elenco, the manufacturer of SnapCircuits has a variety of kits to learn about circuit design.
- The unique coupling of actuators (outputs such as LEDs and the DC motor) to the Micro:Bit allow cyber-physical association between the AI Imaging recognition and the physical indicators.
- This unique mashup of tools requires an understanding of physical and cyber hardware and software while learning about the vulnerabilities and defenses of the entire architecture.
- Welcome to defending Critical Infrastructure and things like the Power Grid.