LAB Logbook

Dan Kibiwott

ID: 2355846

Github Link: https://github.com/DAN-BIWOTT/Machine-Learning-in-Cyber-Security

Lab 1

**LOG REQUIREMENT:** *Write one sentence each for any of the five Pandas classes you find interesting.*

1. **DataFrame** – A table with rows and columns, like an Excel sheet.
2. **Series** – A single column of data with labels, like a list with names.
3. **Index** – Labels for rows and columns that help find data quickly.
4. **Categorical** – A way to store repeating values efficiently, saving space.
5. **DatetimeIndex** – A special list for dates and times, useful for tracking events.

Lab 2

A screenshot of a computer

AI-generated content may be incorrect.

Random Guess 1,766,884.5

Lab 3

A screenshot of a computer screen

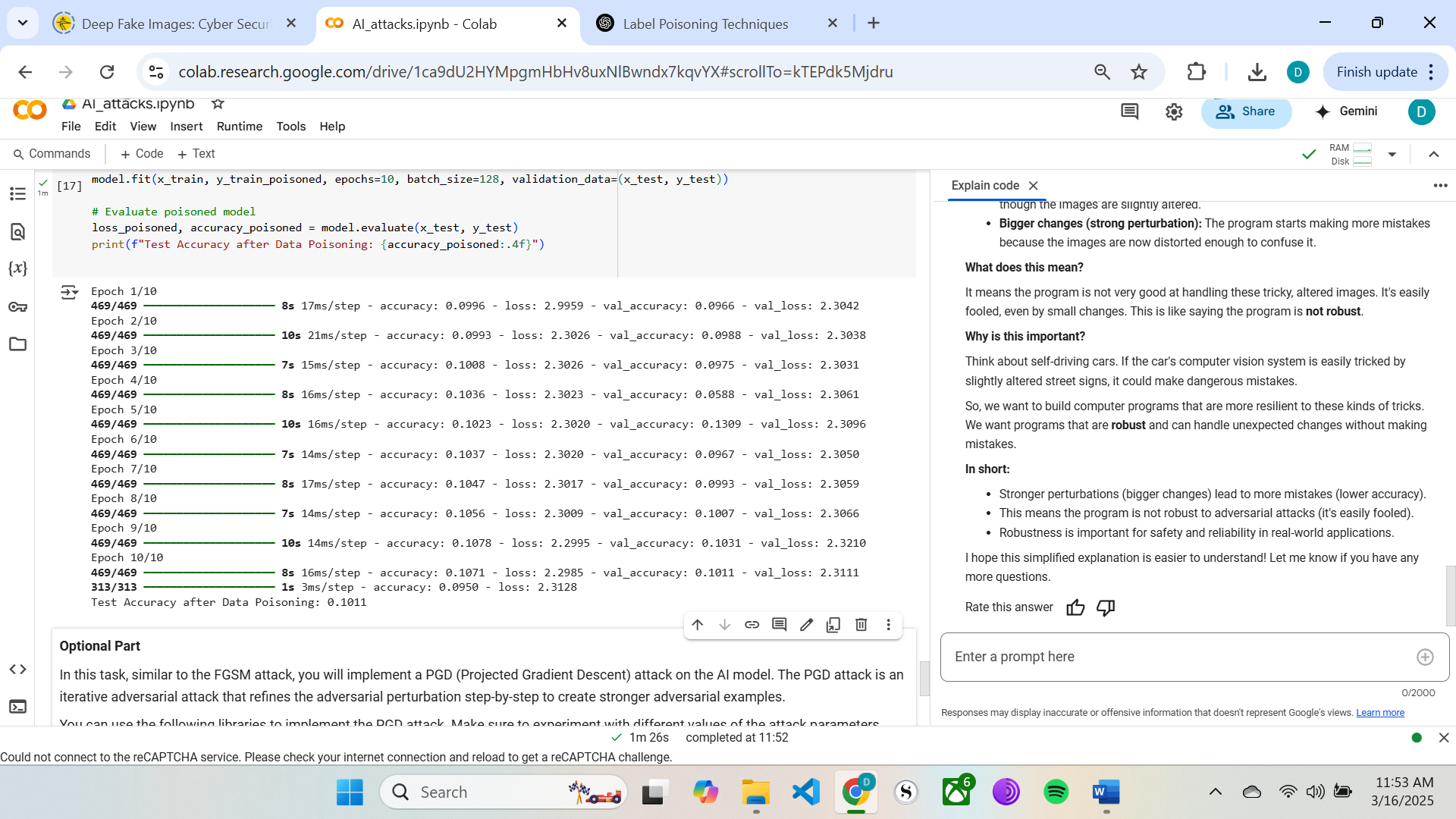
AI-generated content may be incorrect.

Lab 4

A screenshot of a computer

AI-generated content may be incorrect.

Stronger perturbations (bigger changes) lead to more mistakes (lower accuracy). This means the program is not robust to adversarial attacks (it's easily fooled). Robustness is important for safety and reliability in real-world applications



Lab 5

A screenshot of a computer

AI-generated content may be incorrect.

Lab 6

A screenshot of a computer

AI-generated content may be incorrect.

Lab 7

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: real image

YES

Lab 8

Partner’s name: Felix Maindi

P: 23

G: 5

S: 2

private key: 6

Lab 9

**Colonial Pipeline Ransomware Attack (2021)** – A ransomware attack disrupted fuel supply on the East Coast of the U.S.

<https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

Lab 10

Lab 11

Lab 12