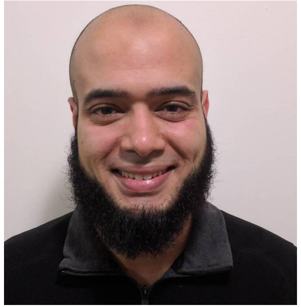
Machine Learning

Machine Learning Model

Mostafa S. Ibrahim
Teaching, Training and Coaching for more than a decade!

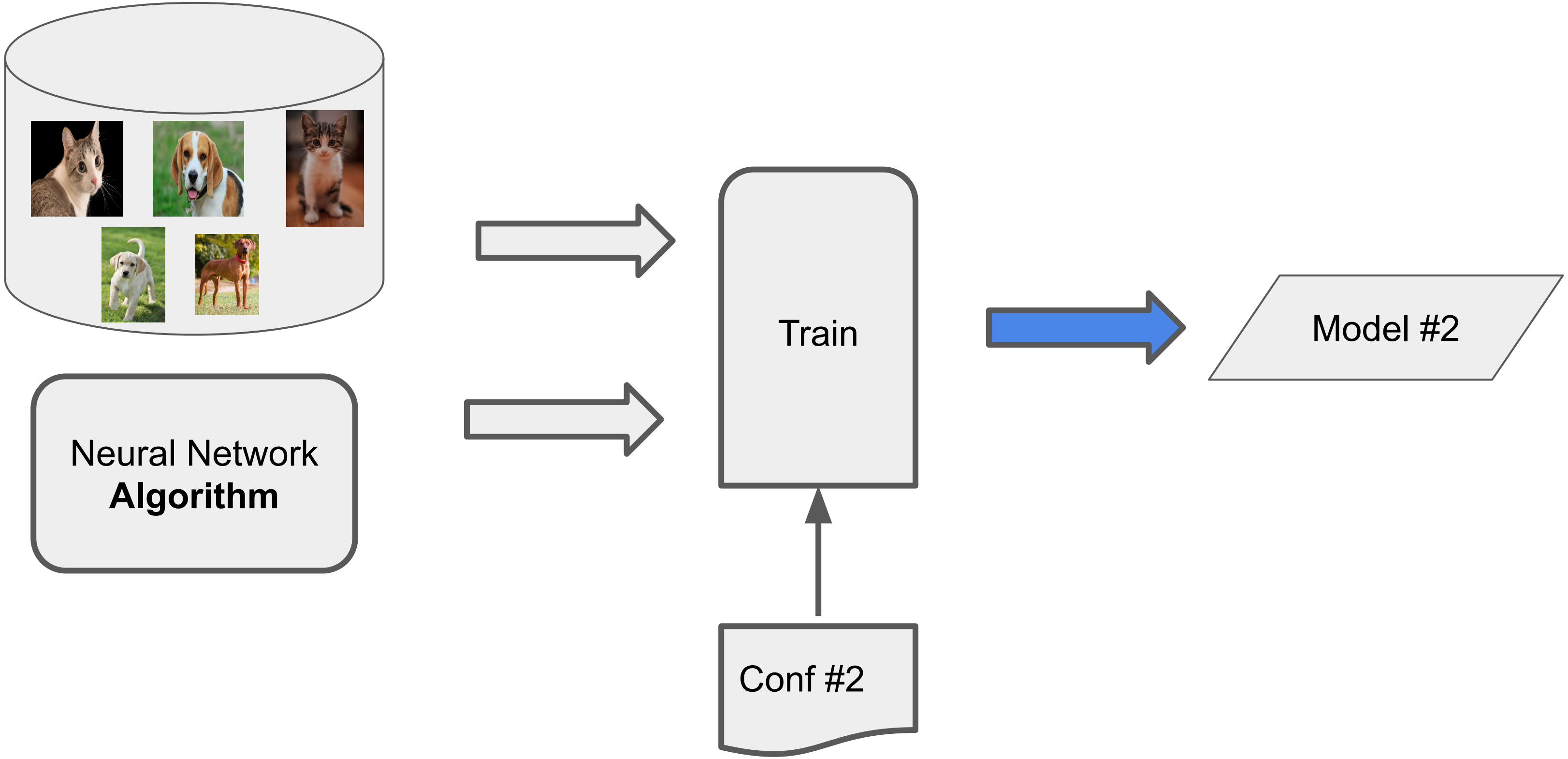
Artificial Intelligence & Computer Vision Researcher
PhD from Simon Fraser University - Canada
Bachelor / MSc from Cairo University - Egypt
Ex-(Software Engineer / ICPC World Finalist)



Algorithm vs Model

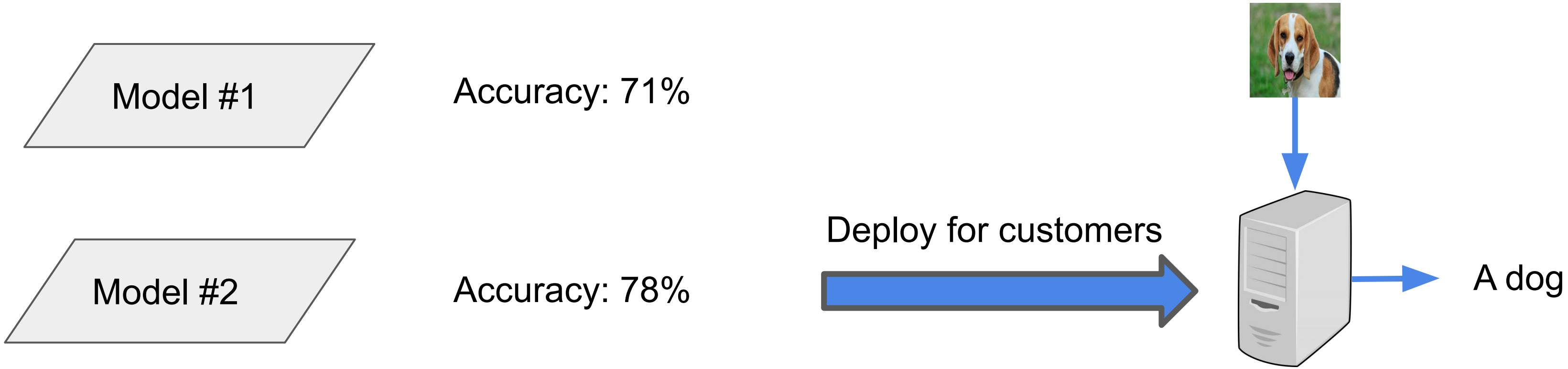
- **ML algorithm** is the procedure we use to learn from data (code/steps)
- **ML model** is the learned output (file = ~program) we use for applying ML
- Assume we have dataset of: 50 cat images and 70 dog images
- Goal: a classifier that differentiate between cat and dog images
- **Neural network** is an **algorithm** that can learn from this data
- We can use it with **different configuration** that express how strong will be the algorithm
- **Each** configuration generates a different output **model**!
  - Hence different performance in practice

Algorithm, Model, Configuration and **Training**



Evaluation and Inference

- How good is our model? We need a measure to **evaluate** our model
  - E.g. accuracy metric: How many classifications are correct?
  - We do that on a separate dataset (called evaluation dataset)
- Once it is good. We deploy it to do **inference**
  - Inference means **apply** the model and get the output for our clients



Model #1

Accuracy: 71%

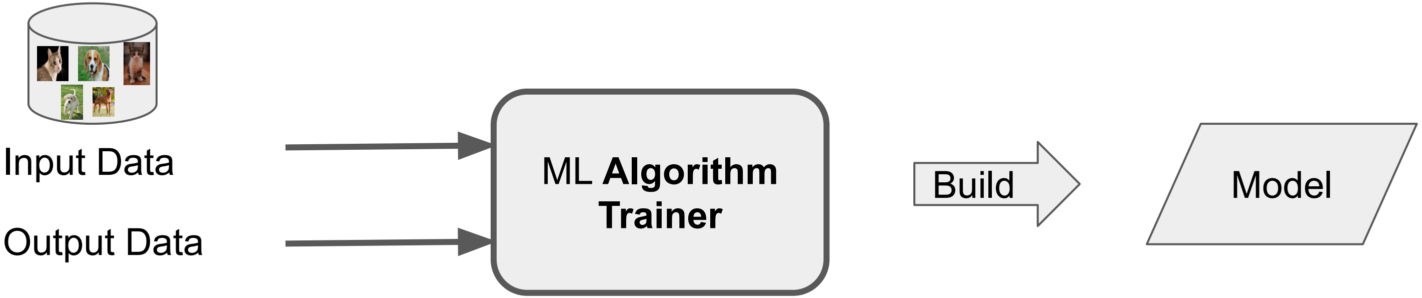
Model #2

Accuracy: 78%

Deploy for customers

A dog

Training vs Inference



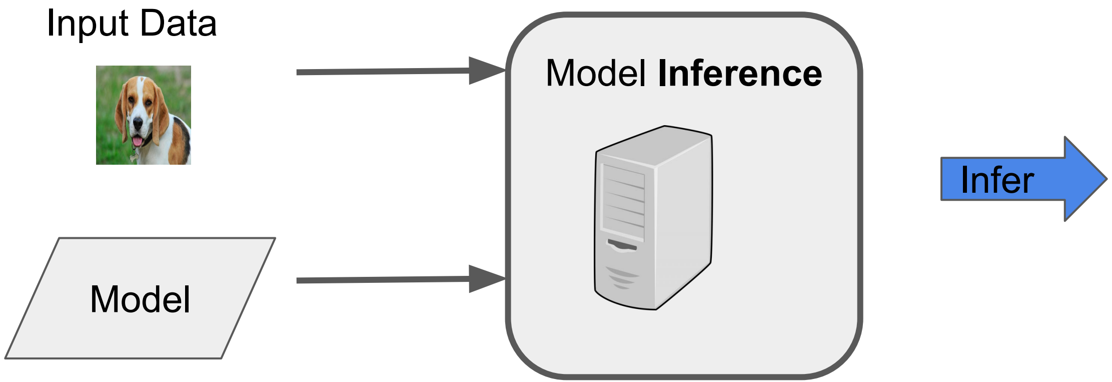
Input Data

Output Data

ML **Algorithm Trainer**

Build

Model



Input Data

Model

Model **Inference**

Infer

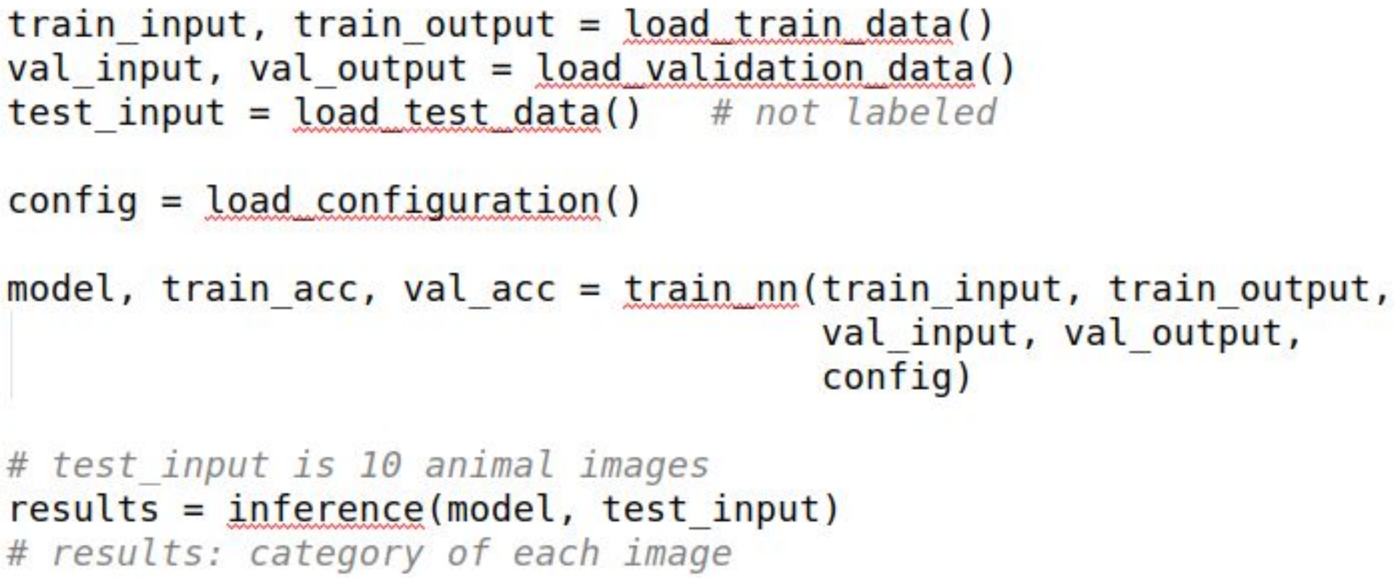
- This is a **dog** (with 80% certainty)
- This is a cat (with 10% certainty)
- This is a person (with 5% certainty)
- This is a car (with 2% certainty)
- This is a bicycle (with 3% certainty)

Question!

- Assume we trained a model on 5 classes: dog, cat, person, car, bicycle
- The model computed these probabilities for 4 test examples
- How many examples are correctly judged?
- What is the accuracy?

	Dog	Cat	Person	Car	Bicycle	Ground Truth
Example1	0.2	**0.7**	0.0	0.1	0.0	Cat
Example2	0.0	**1.0**	0.0	0.0	0.0	Dog
Example3	**0.5**	0.4	0.0	0.05	0.05	Cat
Example4	0.0	0.0	0.0	0.2	**0.8**	Bicycle

Code Flow



```
train_input, train_output = load_train_data()
val_input, val_output = load_validation_data()
test_input = load_test_data()   # not labeled

config = load_configuration()

model, train_acc, val_acc = train_nn(train_input, train_output,
                                     val_input, val_output,
                                     config)

# test_input is 10 animal images
results = inference(model, test_input)
# results: category of each image
```

Question!

- Your team has a task to model solution for the **fraud detection**
    - Fraud detection saves millions of dollars!
- So far, you presented around 20 possible ways to solve the problem
- Each time your manager finds some scenarios where the idea **will fail**
- The manager rejects the idea and ask you to find another **perfect** solution
- What is wrong?!

All models are wrong

- All models are **approximations**
- Assumptions, whether implied or clearly stated, are ***never*** *exactly* ***true***
- All models are **wrong**, but some models are **useful**
- So the question you need to ask is not "Is the model true?" (**it never is**) but "Is the **model good enough** for this particular application?"
    - For example we can build these models:
    - A translation model that can translate good between English and top 10 other languages, but it fails in other languages. This can be good for most of the people!
    - Our object detector in an autonomous driving car can find all people except children as they are too small. This car will kill the kids!!!
- Relevant [future reading]: No Free Lunch theorem in Machine Learning
    - No universal algorithm works well on every problem, including deep learning

Question!

- A popular dataset has 100k images for one of the real-world challenging problems.
- There is a yearly a challenge with $5000 prize for the winner to encourage finding better solutions
- The performance of the last year is 99.3%. One of the professors comments, that this problem is now **solved**
- What do you think?

Summary

- **Training** means **learning the model** from the given dataset of examples
  - In supervised learning, a model defines the relationship between input and label
  - ML algorithm is the procedure we use during this training/learning
- **Inference** means **applying** the **trained model** to **unlabeled** examples

"Acquire knowledge and impart it to the people."

"Seek knowledge from the Cradle to the Grave."