AI WORKSHOP

Introduction to AI : Key Concepts and Definitions

IEEE SB ENICarthage

Achref Ben Ammar Machine Learning Engineer @Callem.ai

achref.benammar@ieee.org

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

Key AI domains:

- Machine Learning (ML): Learning from data and improving accuracy over time.
- Natural Language Processing (NLP): Understanding and processing human language.
- Robotics: Machines performing tasks autonomously or semi-autonomously.
- Computer Vision: Machines interpreting and understanding visual data

TERMINOLOGY

Machine Learning (ML)

A branch of AI where algorithms improve their performance based on data.

Deep Learning (DL)

A more advanced form of ML using multi-layered neural networks to solve more complex problems like image and speech recognition.

Supervised Learning

Models learn from labeled data and can predict outcomes based on input-output pairs.

Unsupervised Learning

Models identify hidden patterns or intrinsic structures in input data without labeled outcomes.

Model

A mathematical representation of a real-world process or system, designed to make predictions or decisions based on input data. In AI, models are algorithms trained to map inputs to outputs, and they improve with more data.

KEY CONCEPTS

Data

Data serves as the foundation for machine learning. The more diverse the data, the better the model can learn and make accurate predictions.(roughly)

Training

During training, the machine identifies correlations and relationships in the data. It adjusts internal parameters to minimize errors in predictions.

Features

In machine learning, models use features (e.g., email length, the number of links in an email) to identify patterns. The quality and selection of features heavily influence model performance.

Labels

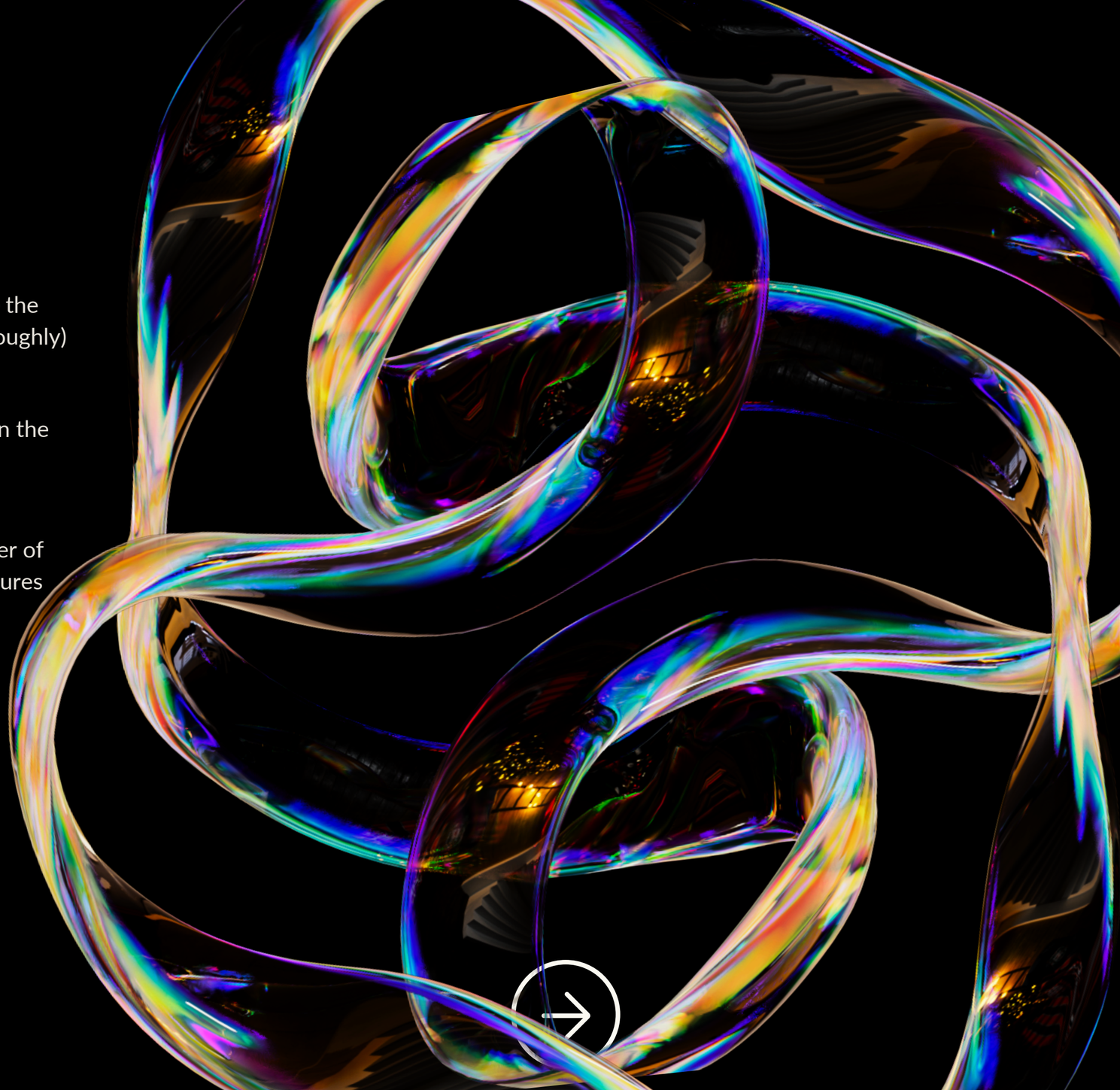
Labels are the correct answers or categories that are given to the model during training.

Testing

Testing is the final step where the model is evaluated on completely unseen data to measure its real-world performance.

Loss Function (or Fitness Function)

A loss function (also known as a fitness function in optimization problems) measures how well the model's predictions match the actual values.



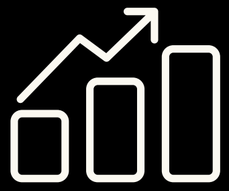
APPLICATIONS OF AI

Cybersecurity

- Threat detection: AI identifies and blocks security threats in real-time by analyzing patterns in network traffic and system logs.
- Automated incident response: AI can automatically respond to detected threats by isolating affected systems or deploying security patches.

Natural Language Processing

- Chatbots and virtual assistants: AI-powered tools like Siri, Alexa, and chatbots respond to user queries, handling customer service tasks.
- Language translation: Tools like Google Translate use AI to provide near-instantaneous translations between languages.



Finance

- Fraud detection: AI algorithms detect suspicious activities in real-time, protecting against fraud in online transactions.
- Algorithmic trading: AI is used to make high-speed financial trading decisions, optimizing stock portfolios.

OVERVIEW OF AI MODELS

AI Models We Will Explore This Session

PARTICLE SWARM OPTIMIZATION

Inspired by the collective behavior of birds or fish swarming, it iteratively improves solutions by adjusting particle positions based on their own experience and the best-known positions of the swarm, making it effective for solving complex problems.

LINEAR REGRESSION

A simple model for predicting a continuous outcome based on the linear relationship between variables.

NEURAL NETWORKS

These are modeled on the brain and are capable of handling large datasets for tasks like object detection, image recognition, and natural language understanding.

OVERVIEW OF AI MODELS

AI Models We Will Explore This Session

LOGISTIC REGRESSION

A simple model that predicts the probability of a binary outcome. Ideal for easy-to-interpret binary classification tasks.

DECISION TREES

A tree-like model that splits data based on feature values. Simple to understand and interpret, but prone to overfitting without additional techniques like pruning.

RANDOM FOREST CLASSIFIER

Builds multiple decision trees and combines their results for better accuracy. It reduces overfitting and works well with complex datasets.

LET’S APPLY

Using AI to Predict Time to Compromise and Detect Malware

We’ll explore two cybersecurity problems, Malware Detection and Time to Compromise (TTC) Prediction.

For Malware Detection, we'll use Logistic Regression, Neural Networks, and Random Forests to classify data as malicious or safe.

For TTC Prediction, we’ll apply Neural Networks, Linear Models, and Particle Swarm Optimization (PSO) to predict how long it takes for a system to be compromised.