Artificial Intelligence - Broad Perspectives

Fulbright Lecture 2023 – KL Deemed University

Guntur, India, 1-31 July 2023

Homepage

Prof./Dr. Saraju Mohanty

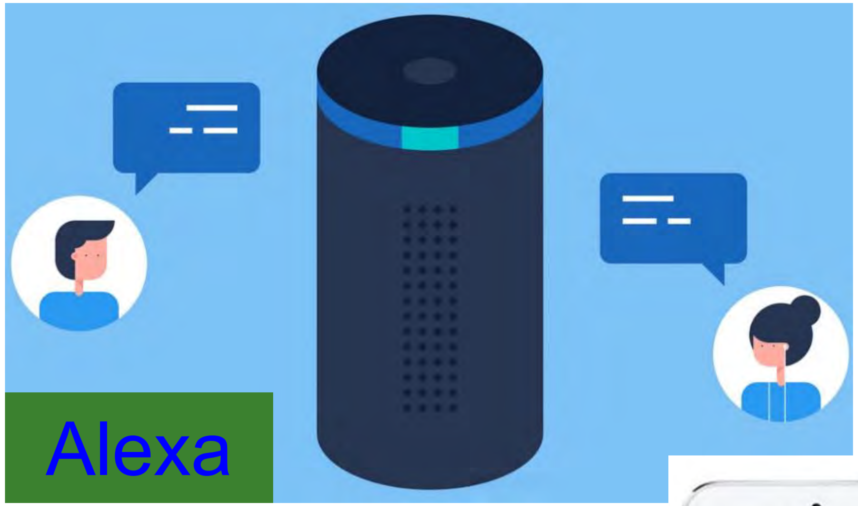
University of North Texas, USA.

Outline

- Introduction
- AI/ML Applications
- AI/ML Types
- ML Algorithms
- DNNs
- AI Tools
- AI Hardware
- AI Challenges
- AI Data Quality Aspects

AI/ML – Big Picture

Systems – End Devices

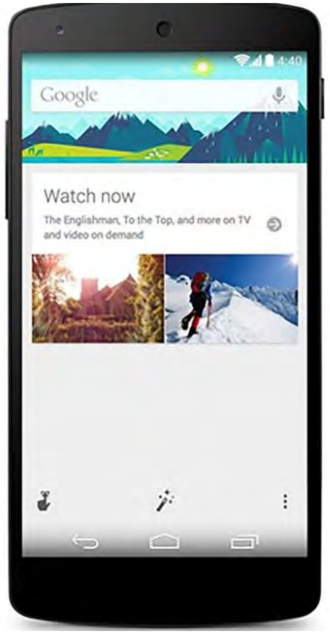


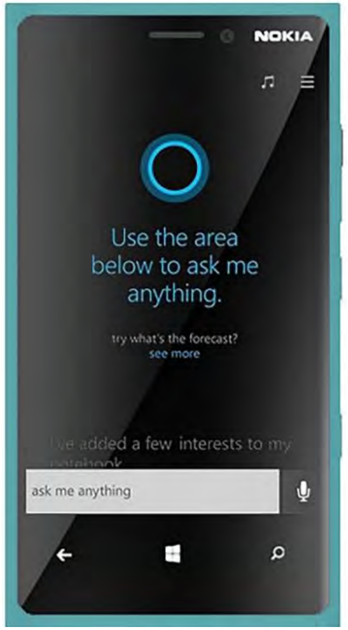
Alexa

Google Now

Windows Cortana

Apple Siri





AI Modeling Applications

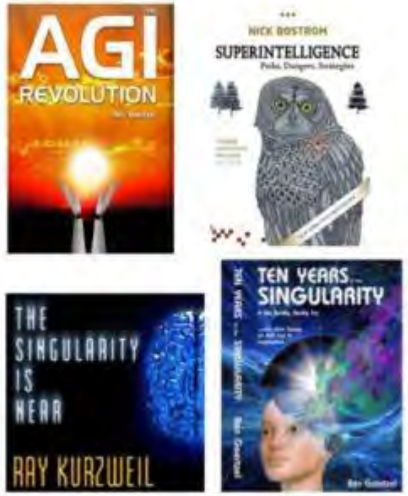
The Four Waves of AI

First Wave	Second Wave	Third Wave	Fourth Wave
c. 1970s - 1990s	*c. 2000s - present*	*est. 2020s - 2030s*	*est. 2030s →*
Good at reasoning, but no ability to learn or generalize. • GOFAI - "Good Old Fashioned AI." • Symbolic, heuristic, rule based. • Handcrafted knowledge, "expert systems."	Good at learning and perceiving, but minimal ability to reason or generalize. • Statistical learning, "deep" neural nets, CNN. • Advanced text, speech, language and vision processing.	Excellent at perceiving, learning and reasoning, and able to generalize. • Contextual adaptation, able to explain decisions. • Can converse in natural language. • Requires far fewer data samples for training. • Able to learn and function with minimal supervision.	Able to perform any intellectual task that a human can. • AGI (Artificial General Intelligence), possibly leading to ASI (Artificial Superintelligence) and the "technological singularity."

SingularityNET

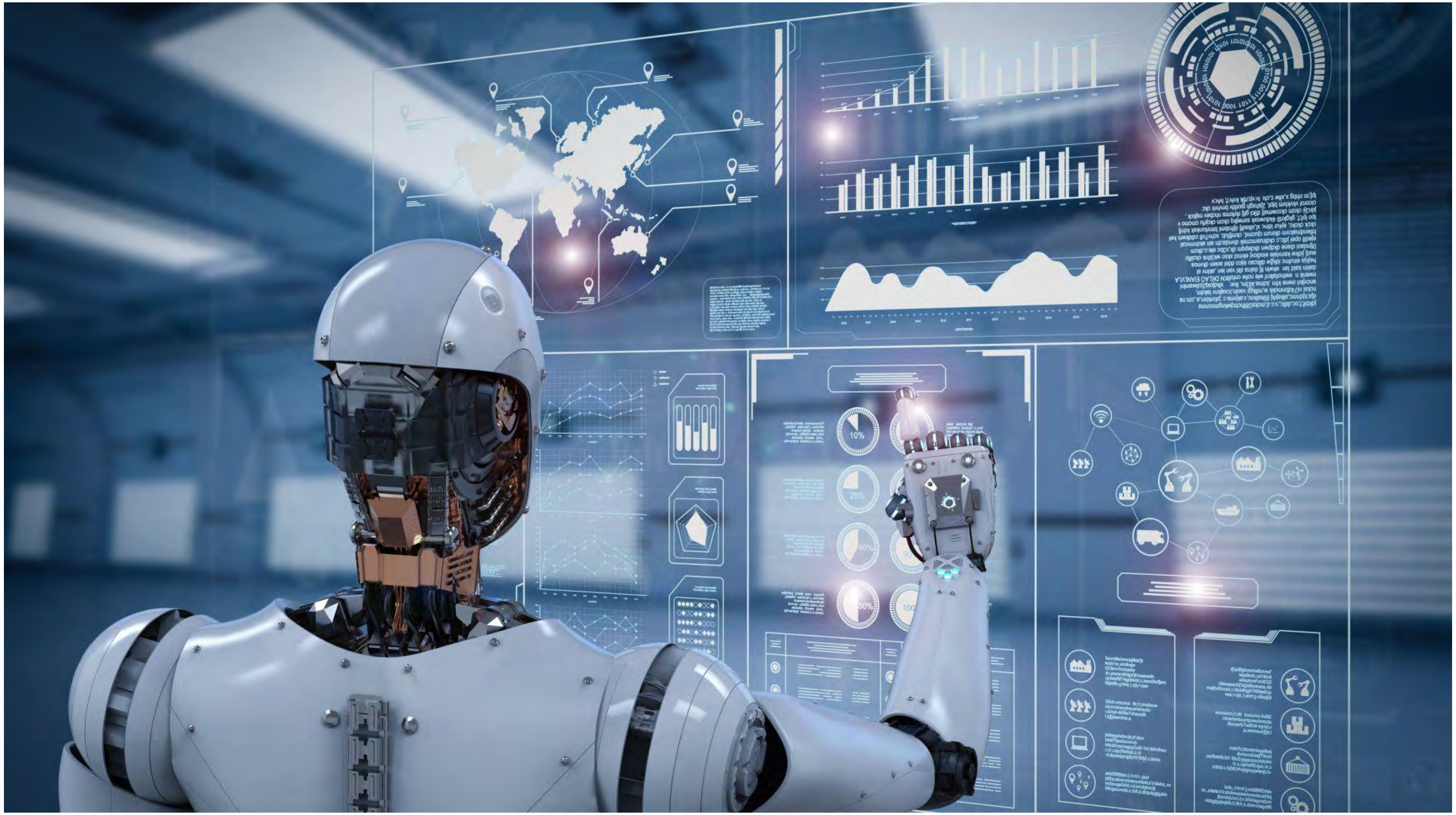
aigo.ai

Pandai



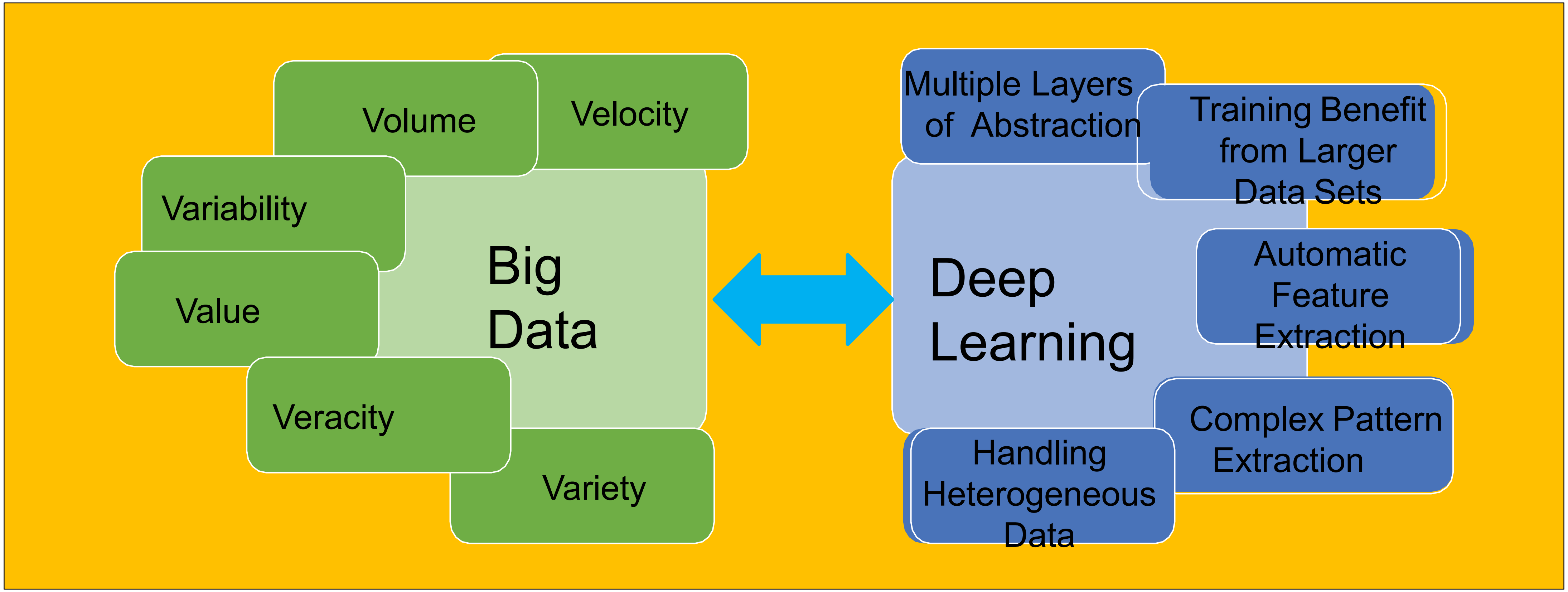
Six Kin Development (adapted from DARPA's "Three Waves of AI") Source: https://www.sharper.ai/taxonomy-ai/

Large Amount of Data Processing for AI



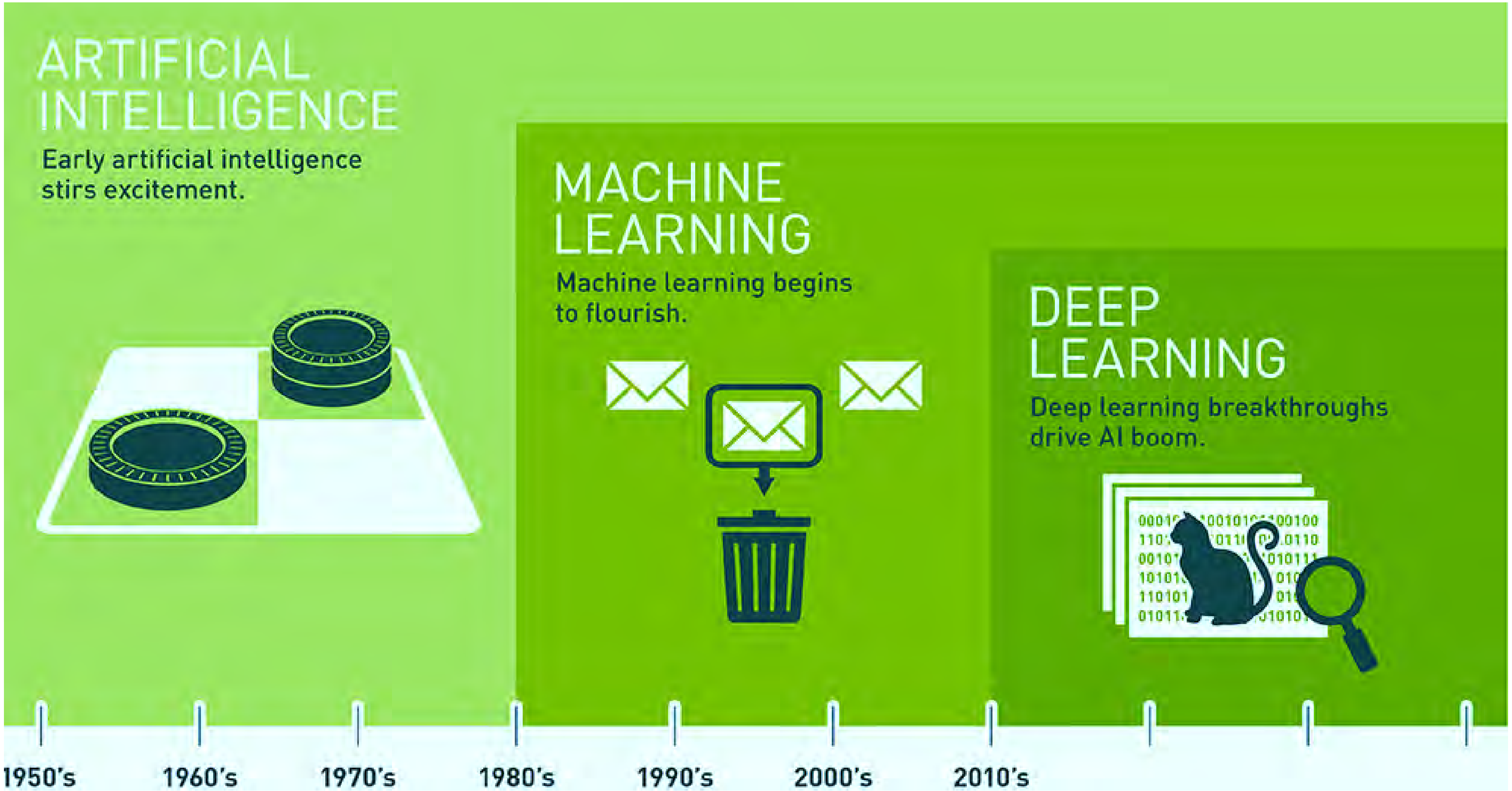
Source: https://matmatch.com/blog/the-age-of-artificial-intelligence-in-materials-science-part-one/

Big Data Versus Deep Learning



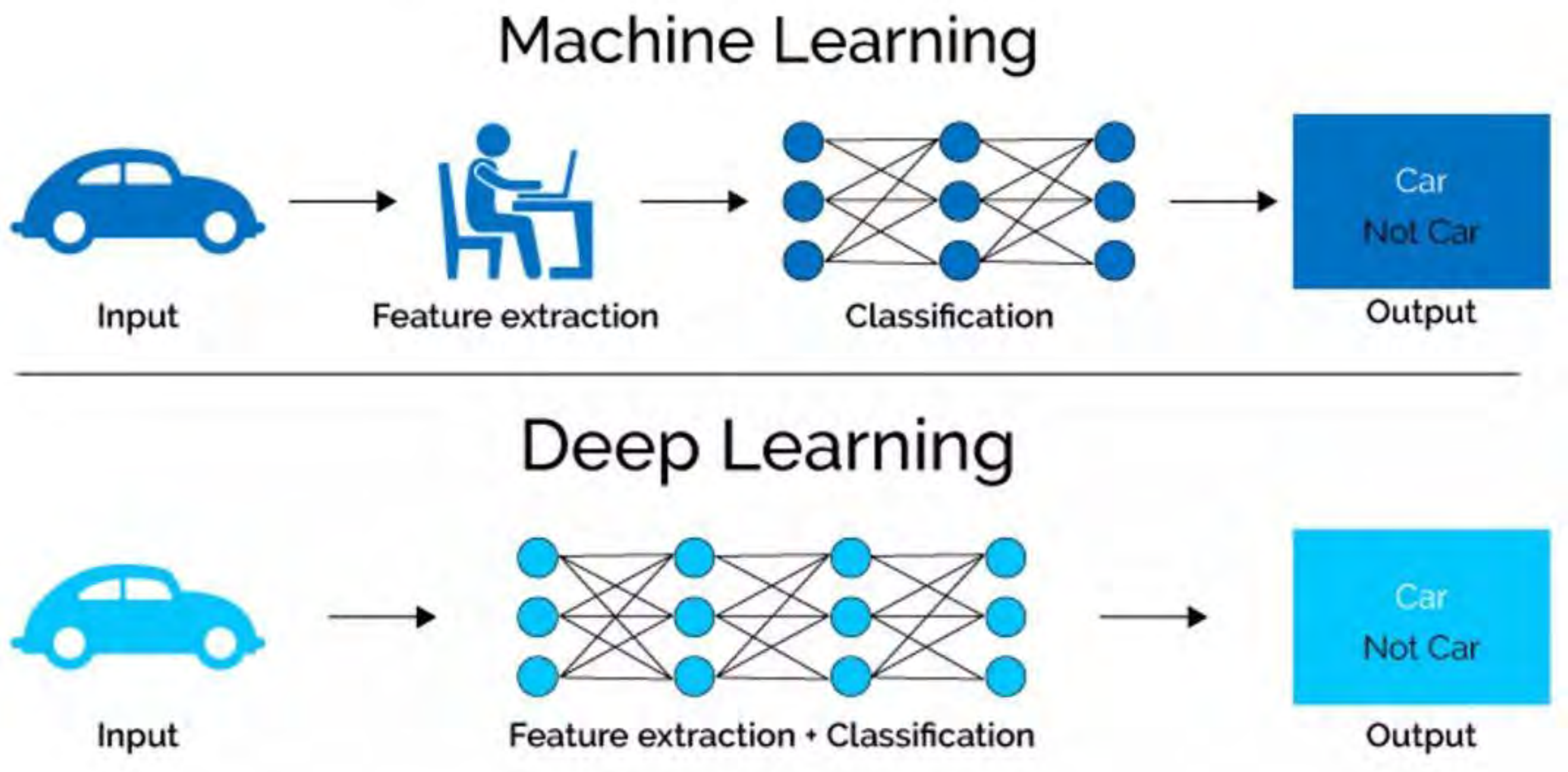
Source: R. Fernandez Molanes, K. Amarasinghe, J. Rodriguez-Andina and M. Manic, "Deep Learning and Reconfigurable Platforms in the Internet of Things: Challenges and Opportunities in Algorithms and Hardware," *IEEE Industrial Electronics Magazine*, vol. 12, no. 2, pp. 36-49, June 2018.

Timeline of AI, ML, and Deep Learning

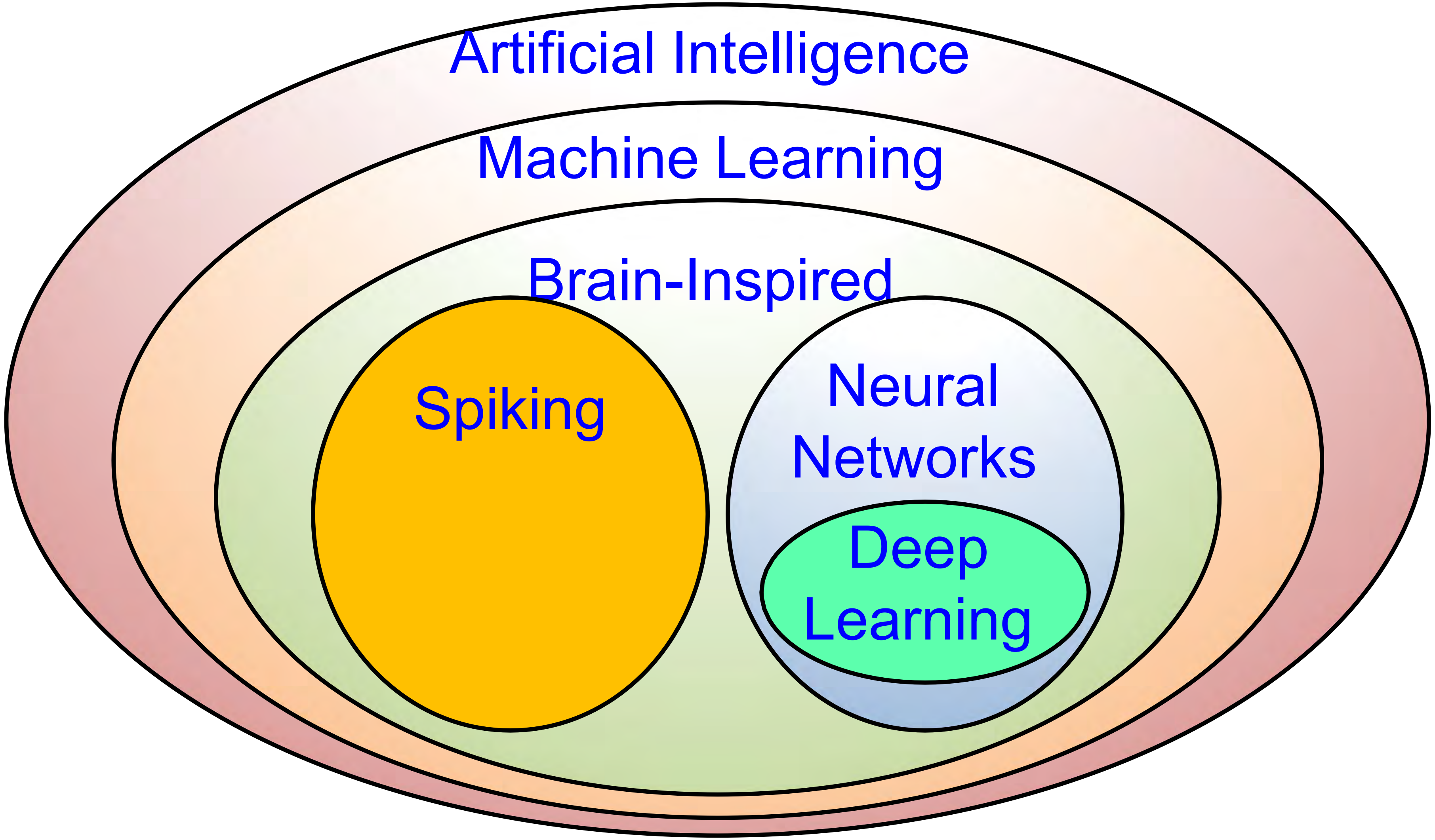


Source: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

Machine Learning Vs Deep Learning



Artificial Intelligence – Big Picture



Source: https://www.rle.mit.edu/eems/wp-content/uploads/2019/06/Tutorial-on-DNN-01-Overview.pdf

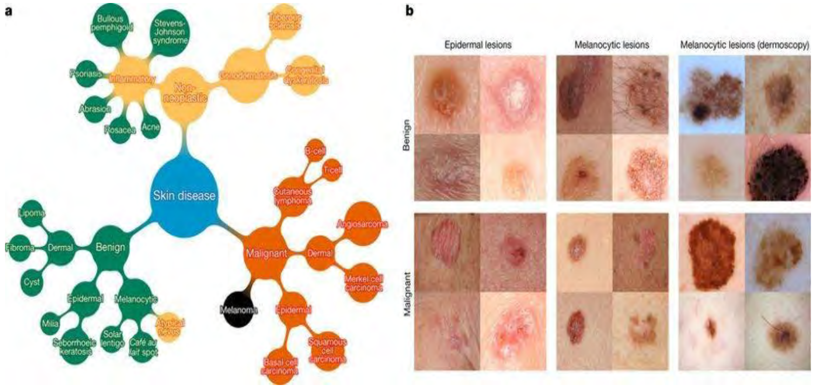
AI/ML Applications

AI / Machine Learning is Ubiquitous

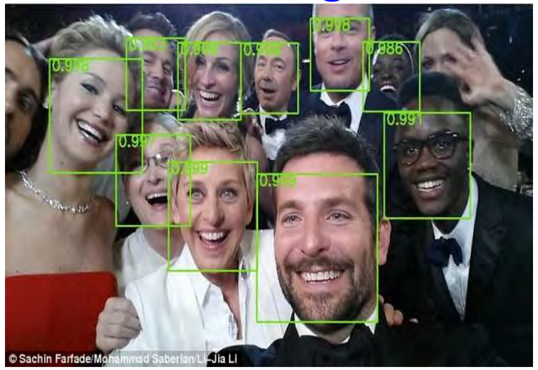
Self-driving Cars

Cybersecurity

Healthcare



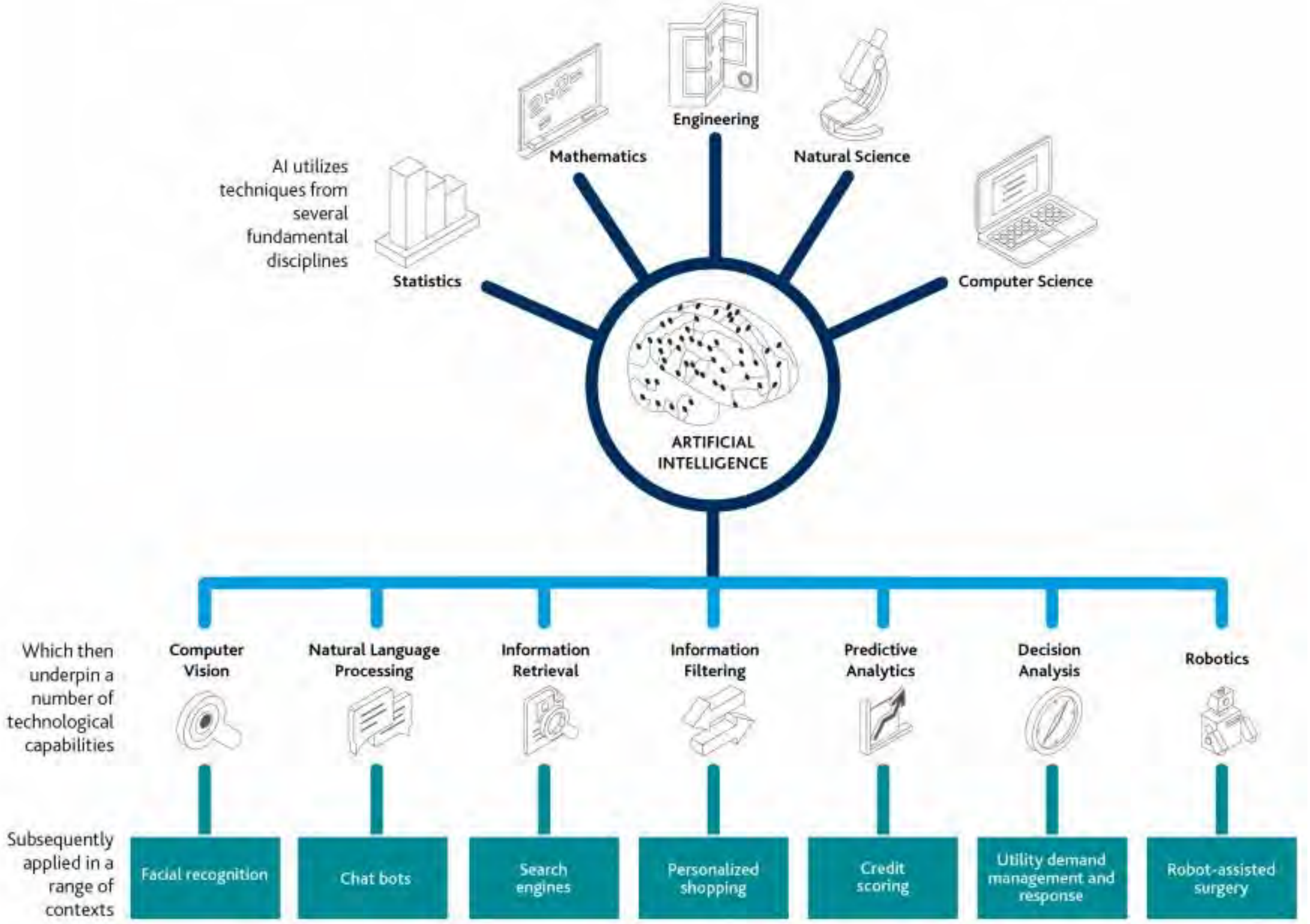
Facial Recognition



Speech Recognition

Source: Sandip Kundu ISVLSI 2019 Keynote.

AI Modeling Applications



Source: https://meee-services.com/what-are-the-top-ai-applications-in-2018/

Smart Healthcare – AI/ML Framework

Smart Healthcare - System and Data Analytics : To Perform Tasks

Systems & Analytics

- Health cloud server
- Edge server
- Implantable Wearable Medical Devices (IWMDs)

Machine Learning Engine

Data

- Physiological data
- Environmental data
- Genetic data
- Historical records
- Demographics

Systems & Analytics

- Clinical Decision Support Systems (CDSSs)
- Electronic Health Records (EHRs)

Machine Learning Engine

Data

- Physician observations
- Laboratory test results
- Genetic data
- Historical records
- Demographics

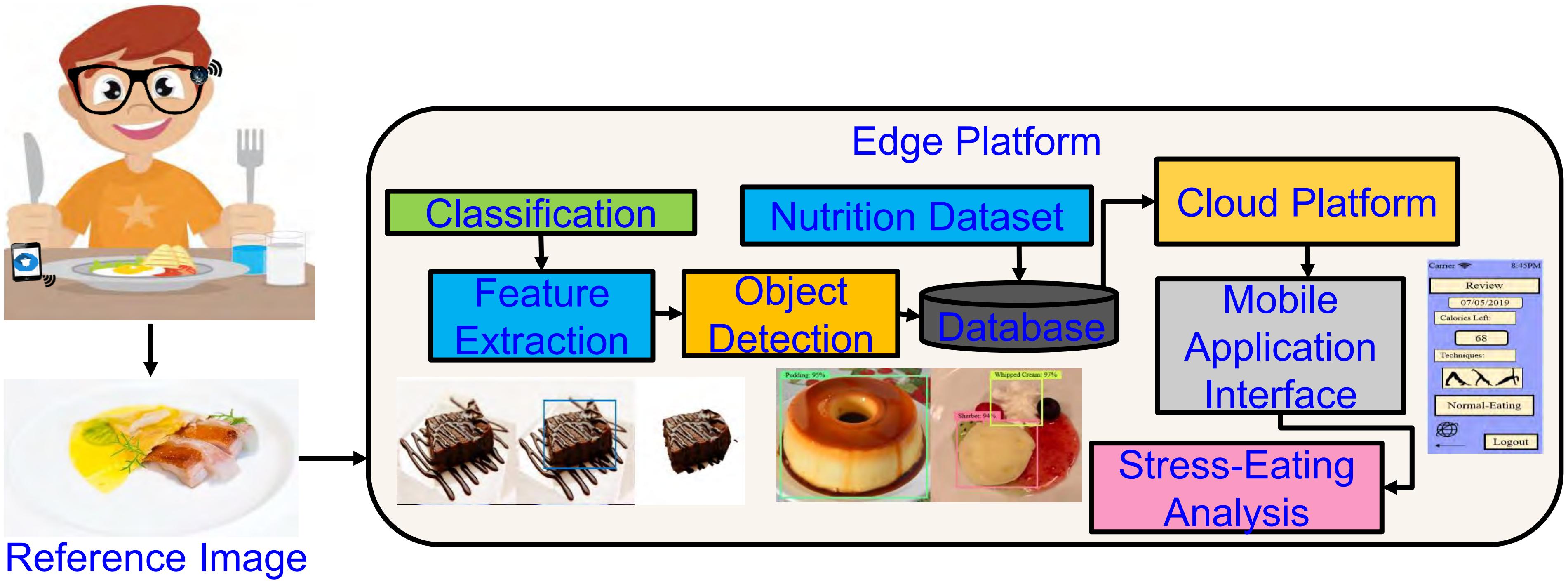
Source: Hongxu Yin, Ayten Ozge Akmandor, Arsalan Mosenia and Niraj K. Jha (2018), "Smart Healthcare", *Foundations and Trends® in Electronic Design Automation*, Vol. 12: No. 4, pp 401-466. http://dx.doi.org/10.1561/1000000054

Smart Healthcare – AI/ML is Key

AI Role Includes:
- Automatic diagnosis
- Disease predication
- Diet prediction
- Pandemic projection
- Automatic prescription

Source: Robert Pearl, "Artificial Intelligence In Healthcare: Separating Reality From Hype", 13 Mar 2018, *https://www.forbes.com/sites/robertpearl/2018/03/13/artificial-intelligence-in-healthcare/?sh=598aa64d1d75*

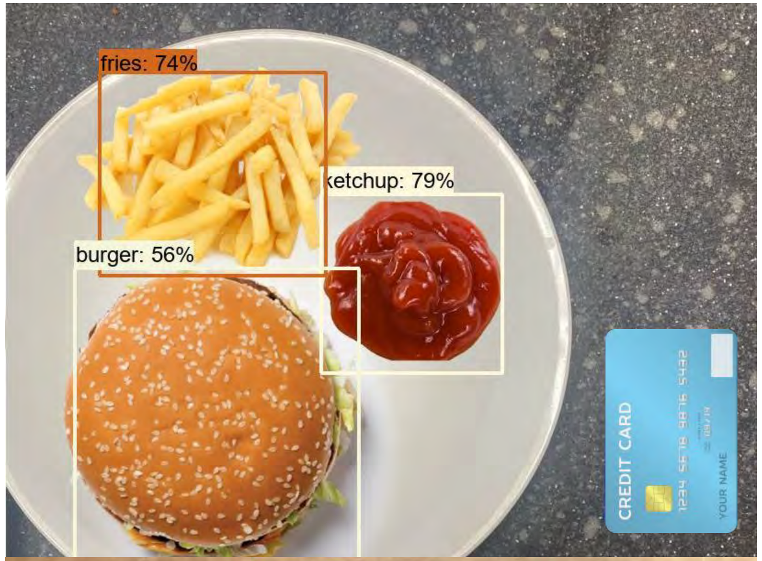
Smart Healthcare – Diet Monitoring - iLog



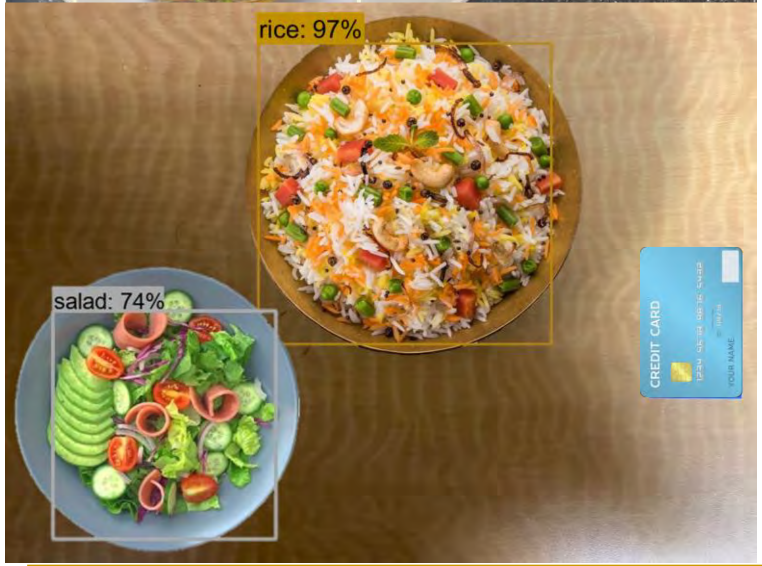
iLog- Fully Automated Detection System with 98% accuracy.

Source: L. Rachakonda, S. P. Mohanty, and E. Kougianos, “iLog: An Intelligent Device for Automatic Food Intake Monitoring and Stress Detection in the IoMT”, *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 66, No. 2, May 2020, pp. 115--124.

Smart Healthcare - Diet Monitoring - iLog 2.0



Food Item	Saturated Fat (g)	Sugar (g)	Sodium (mg)	Protein (g)	Carbohydrates (g)
Fries	6.44	1.56	244	4.03	34.84
Burger	6.87	4.67	481	17.29	48.14
Ketchup	0	3.2	136	0.2	4.13
Total	13.31	9.43	861	21.52	87.11



Food Item	Saturated Fat (g)	Sugar (g)	Sodium (mg)	Protein (g)	Carbohydrates (g)
Rice	0.3	0.3	6	12.9	135
Salad	0.8	3.9	264	1.1	7
Total	1.1	4.2	270	14	142

Source: A. Mitra, S. Goel, **S. P. Mohanty**, E. Kougianos, and L. Rachakonda, “iLog 2.0: A Novel Method for Food Nutritional Value Automatic Quantification in Smart Healthcare”, in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

Smart Agriculture – AI/ML Technology

Crop Management

Soil Management

Smart Irrigation

Pest / Disease Control

Weed Control

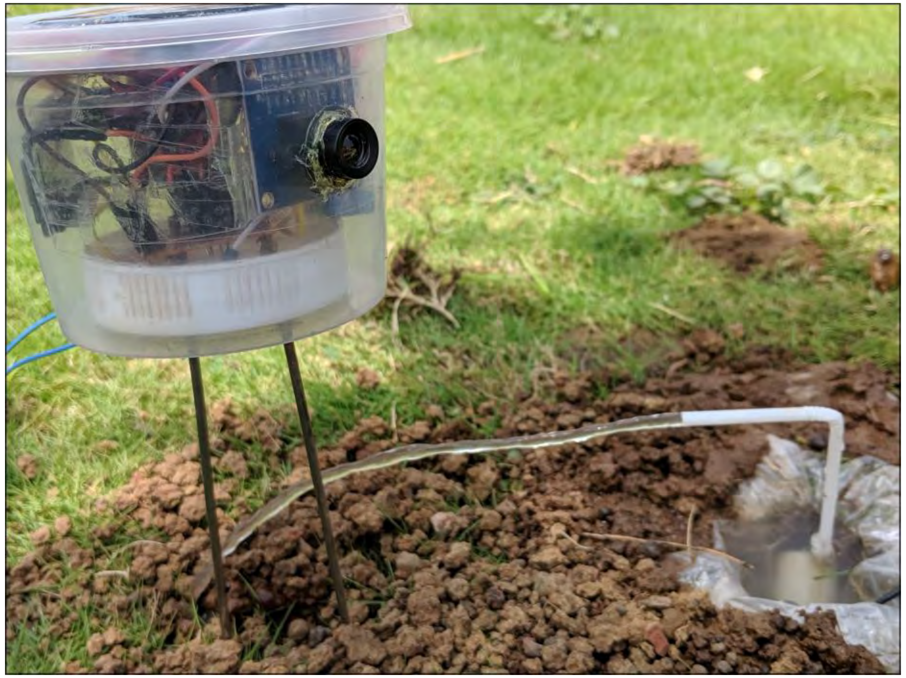
Livestock Management

Alternative Farming

SVM ANN DNN CNN Regression Bayesian Models Decision Tree Fuzzy Logic
Clustering Instance Based Models Ensemble Learning Long Short Term Memory

Source: A. Mitra, S. L. T. Vangipuram, A. K. Bapatla, V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, and C. Ray, "Everything You wanted to Know about Smart Agriculture", *arXiv Computer Science*, arXiv:2201.04754, Jan 2022, 45-pages.

Our sCrop: A Device for Automatic Disease Prediction, Crop Selection, and Irrigation in IoAT



sCrop Device Prototype with Irrigation

sCrop App

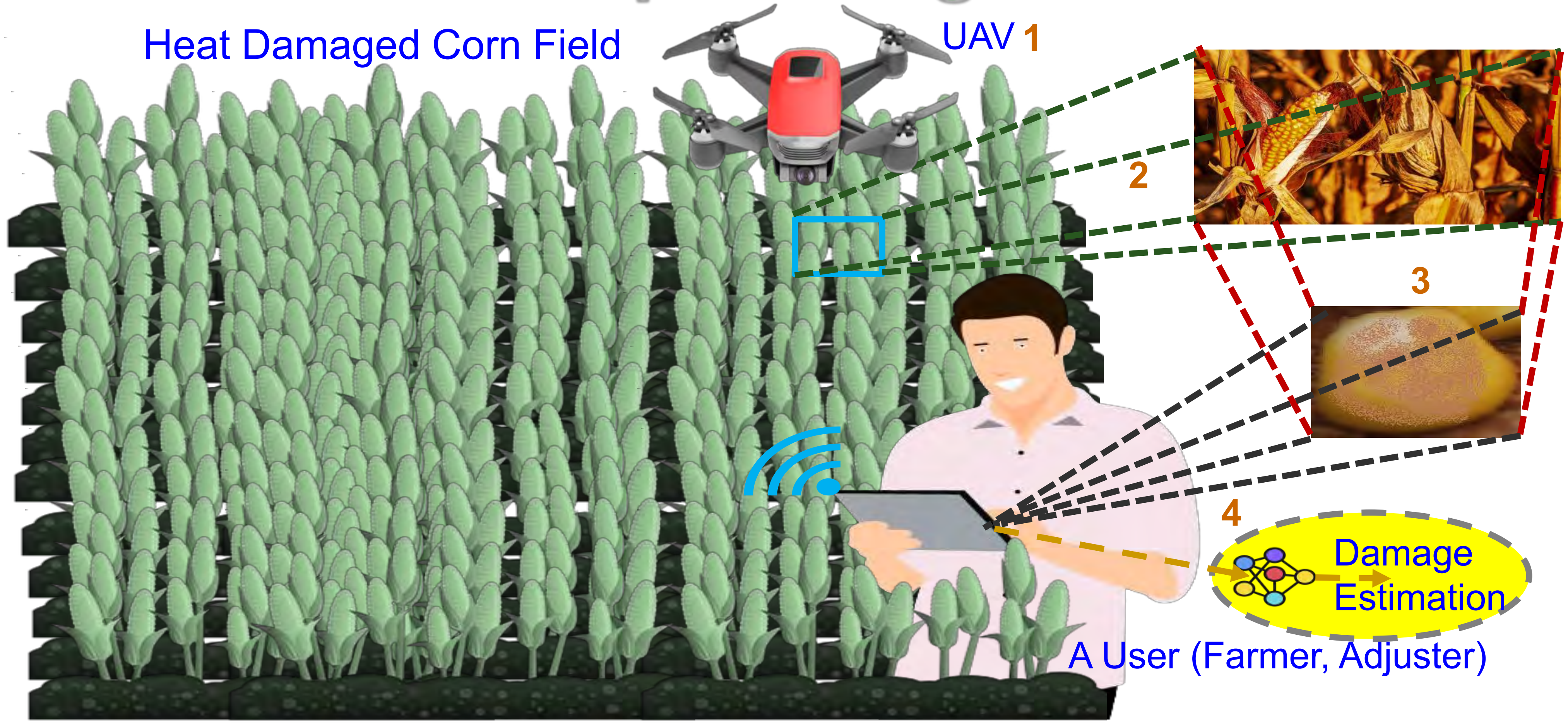
Healthy Tomato

Infected Tomato

sCrop Accuracy – 99.24%

Source: V. Udutalapally, **S. P. Mohanty**, V. Pallagani, and V. Khandelwal, "sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture", *IEEE Sensors Journal (JSEN)*, Vol. 21, No. 16, August 2021, pp. 17525--17538, DOI: https://doi.org/10.1109/JSEN.2020.3032438.

Our eCrop: A Framework for Automatic Crop Damage Estimation



1 → UAV takes Photo of Corn Ear

2 → Damage Area Detection of Corn Ear

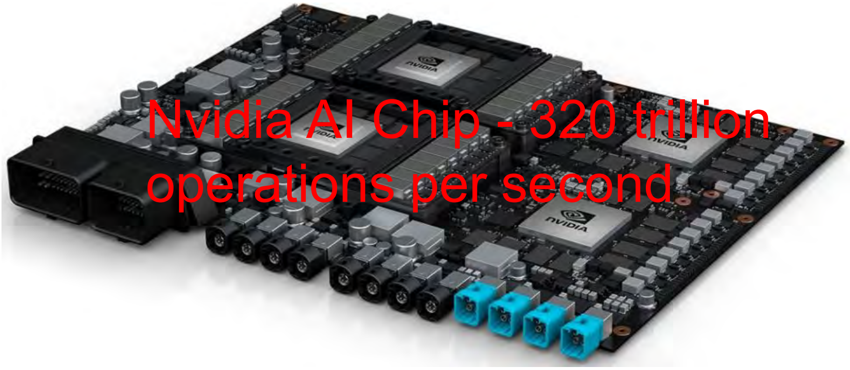
3 → 50% of Damaged Area Selection

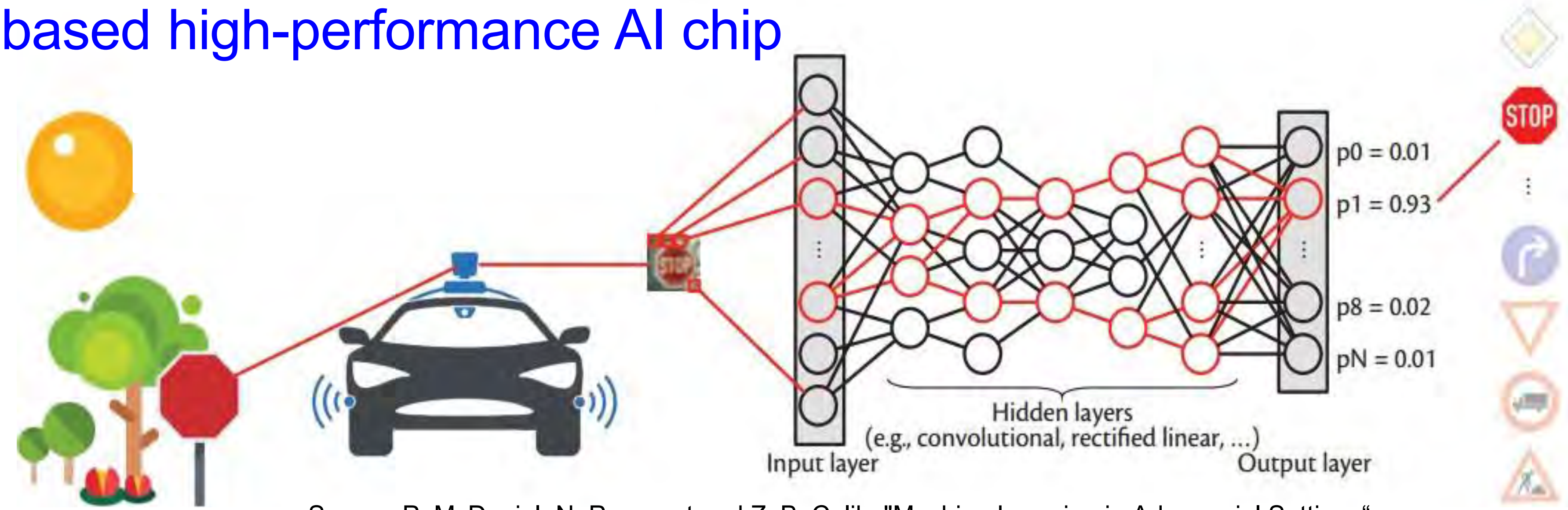
4→ Damage Type Detection for Corn Kernel and Process is Repeated for the Selected Area

A. Mitra, A. Singhal, **S. P. Mohanty**, E. Kougianos, and C. Ray, "eCrop: A Novel Framework for Automatic Crop Damage Estimation in Smart Agriculture", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 4, July 2022, Article: 319, 16-pages, DOI: https://doi.org/10.1007/s42979-022-01216-8.

AI/ML in Self-driving Cars

- ❖ Cars incorporating AI to assist or replace drivers
  - o Ex. automatic parking, Waymo
- ❖ Self-driving cars with AI/ML will be commonplace
  - o Open AI car computing system
  - o SoC based high-performance AI chip





Source: P. McDaniel, N. Papernot and Z. B. Celik, "Machine Learning in Adversarial Settings", *IEEE Security & Privacy*, vol. 14, no. 3, pp. 68-72, May-June 2016.

What is AI/ML?

Basic Programming

Program to Check Even or Odd

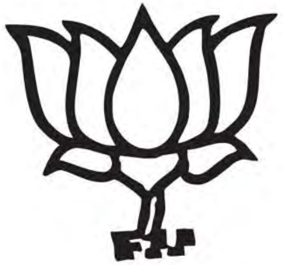
```
#include <stdio.h>
int main() {
    int num;
    printf("Enter an integer: ");
    scanf("%d", &num);
    // True if num is perfectly divisible by 2
    if(num % 2 == 0)
        printf("%d is even.", num);
    else
        printf("%d is odd.", num);
    return 0;
}
```

Output

Enter an integer: -7

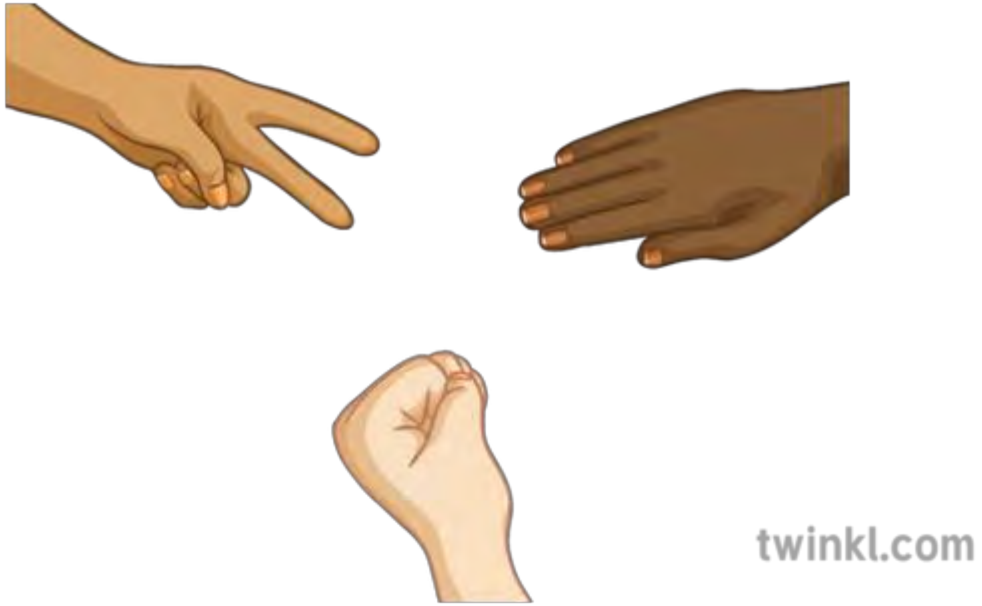
-7 is odd.

Programming for Symbols / Shapes

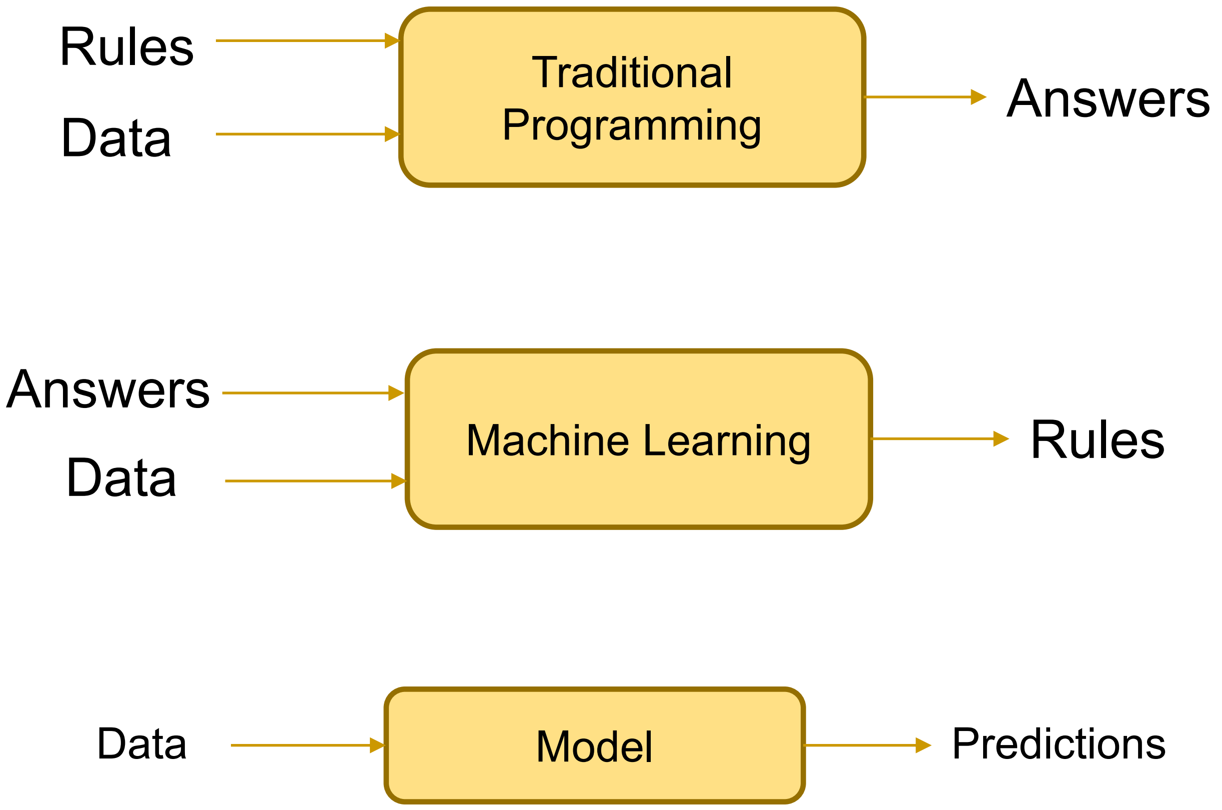


Programming for Symbols / Shapes

- Complex pictures or shapes

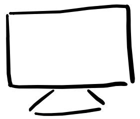


How to train a Computer?



What is Machine Learning?

- ML is the science of making computers learn and act like humans by feeding data and information without being explicitly programmed.



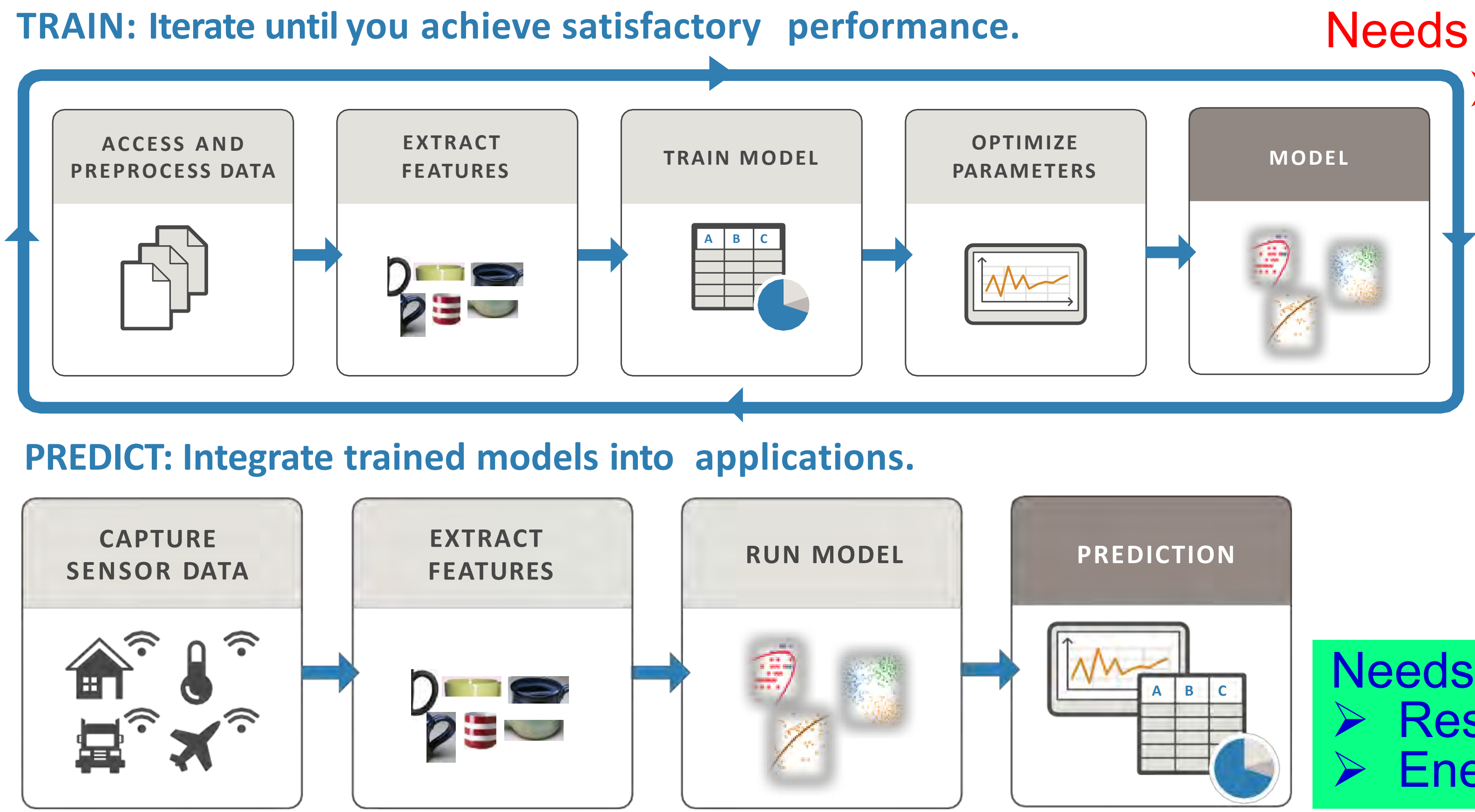
Ordinary System + AI + ML

Learns — Descriptive - learning stuff

Predicts — Predicting the o/p's.

Improves — Postcripting - coming up with new solutions

Deep Neural Network (DNN) – Train and Predict



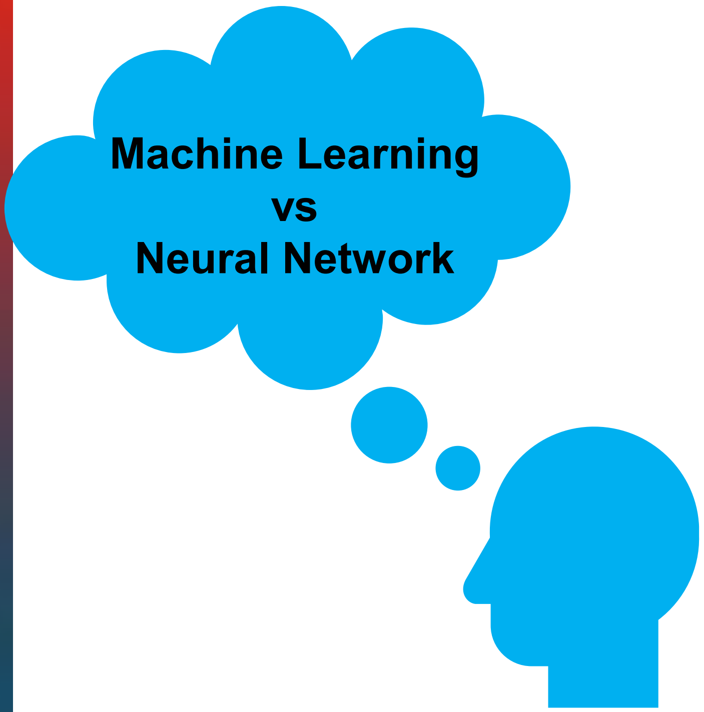
Needs Significant:
- Resource
- Energy

Needs:
- Resource
- Energy

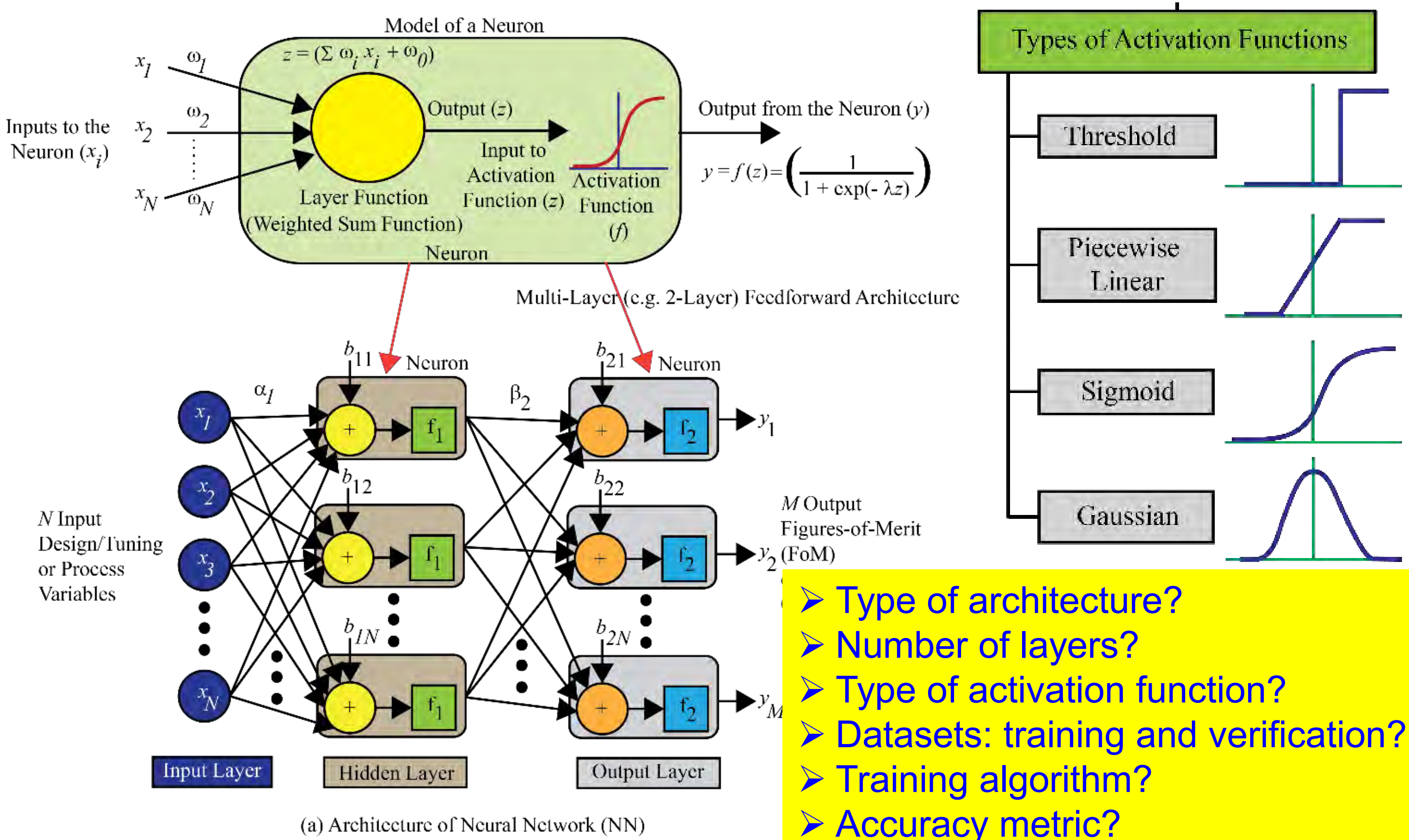
Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

AI/ML Types

Branches of AI



Artificial Neural Networks

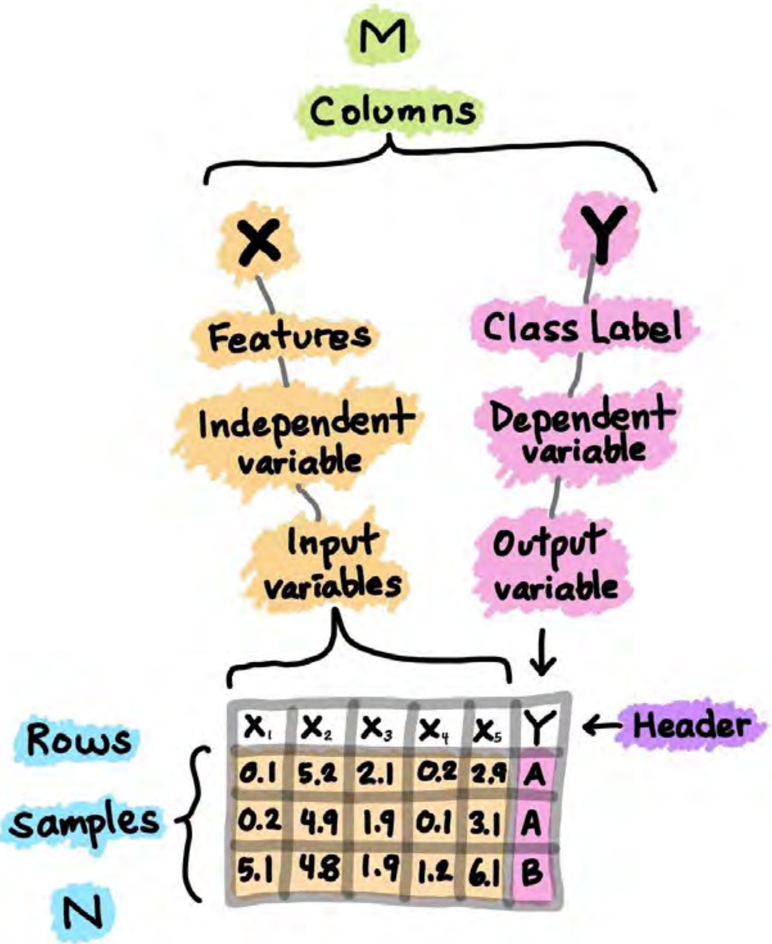


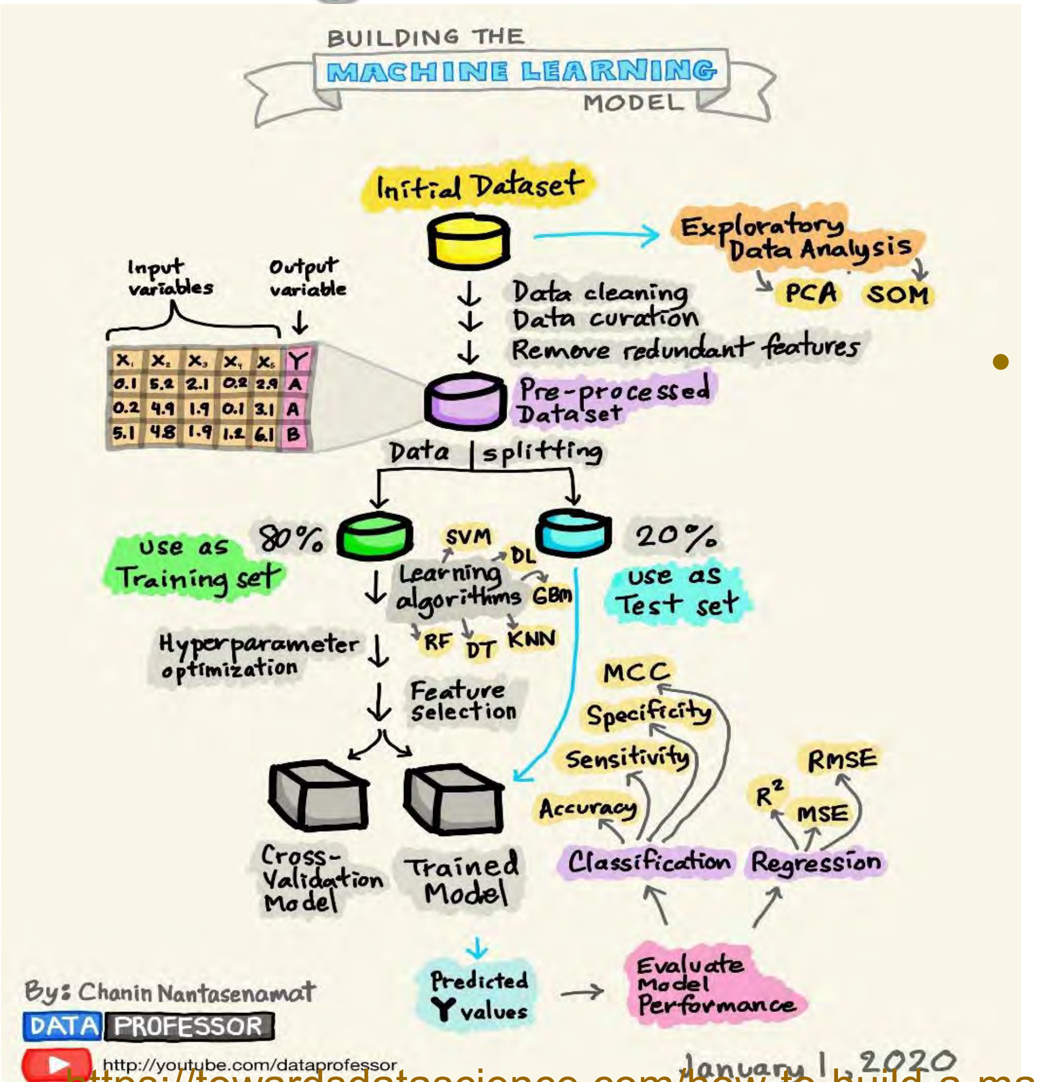
(a) Architecture of Neural Network (NN)

- ➢ Type of architecture?
- ➢ Number of layers?
- ➢ Type of activation function?
- ➢ Datasets: training and verification?
- ➢ Training algorithm?
- ➢ Accuracy metric?

Source: Mohanty McGraw-Hill 2015

Building a ML Model

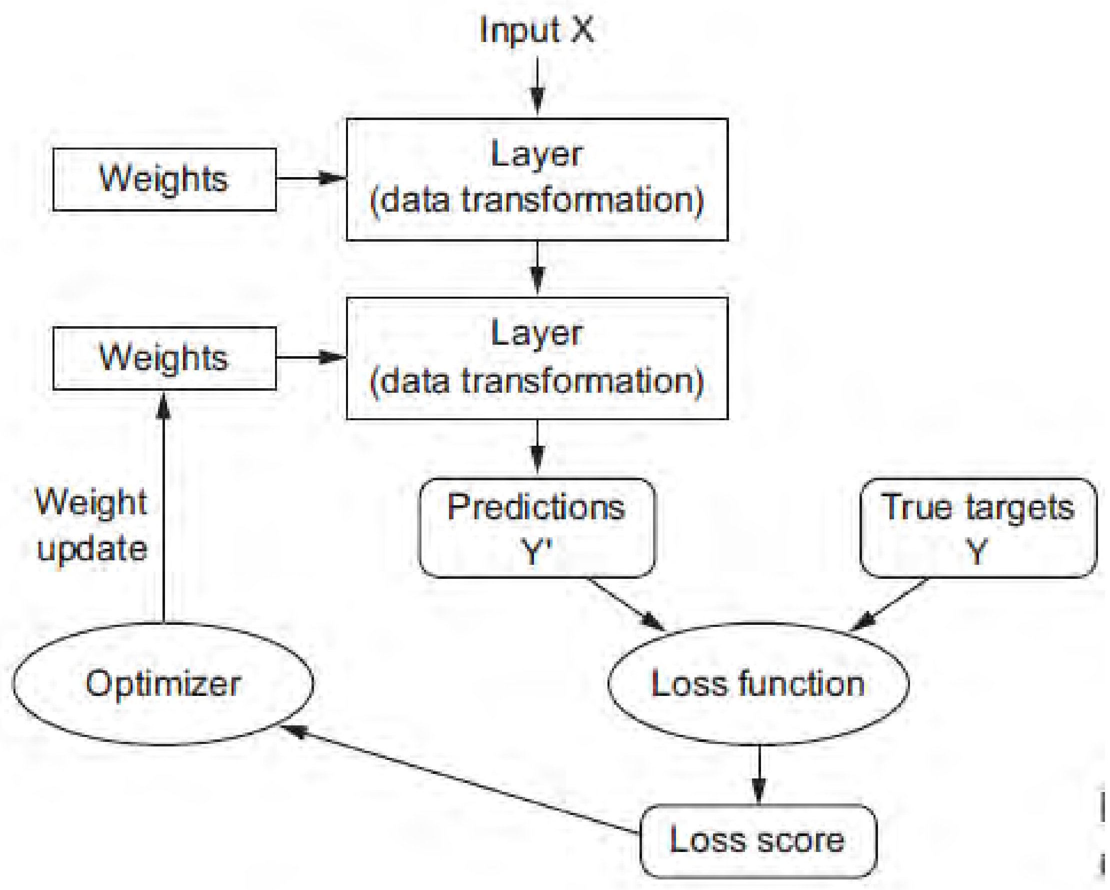




https://towardsdatascience.com/how-to-build-a-machine-learning-model-439ab8fb3fb1

- **Examples of Learning Algorithms:**
  - Linear Regression
  - Logistic Regression
  - kNN
  - SVM
  - etc.

Building a DNN Model



Source: Book- Deep Learning with Python By F.Chollet

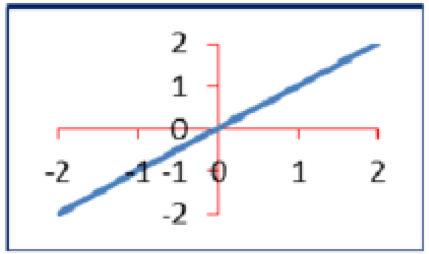
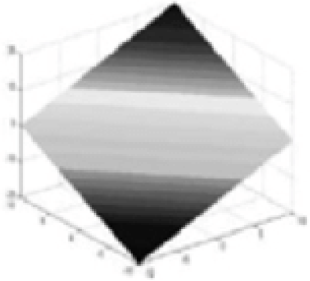
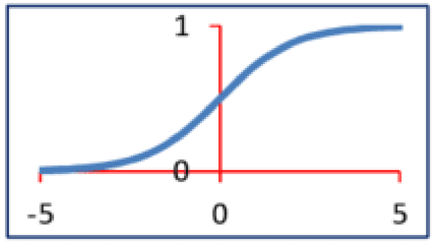
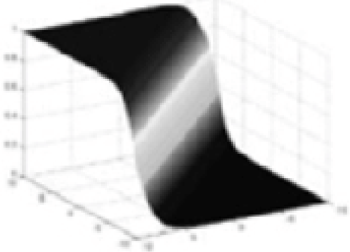
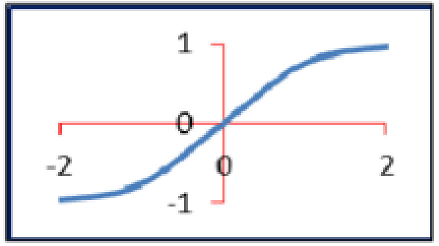
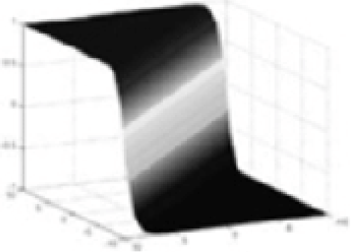
- Layers: Building Blocks of Deep Learning
- Models: Networks of Layers
- Loss function: Gets minimized during training.
- Optimizer: Says how the network gets updated. (Algorithm Part)

Which Model to Choose?

Data Sector	Use Case	Input	Transform	Neural Net
Text	Sentiment analysis	Word vector	Gaussian Rectified	RNTN or DBN (with moving window)
	Named-entity recognition	Word vector	Gaussian Rectified	RNTN or DBN (with moving window)
	Part-of-speech tagging	Word vector	Gaussian Rectified	RNTN or DBN (with moving window)
	Semantic-role labeling	Word vector	Gaussian Rectified	RNTN or DBN (with moving window)
Document	Topic modeling/ semantic hashing (unsupervised)	Word count probability	Can be Binary	Deep Autoencoder (wrapping a DBN or SDA)
	Document classification (supervised)	TF-IDF (or word count prob.)	Binary	Deep-belief network, Stacked Denoising Autoencoder
Image	Image recognition	Binary	Binary (visible and hidden)	Deep-belief network
		Continuous	Gaussian Rectified	Deep-belief network
	Multi-object recognition			Convolutional Net, RNTN (image vectorization forthcoming)
	Image search/ semantic hashing		Gaussian Rectified	Deep Autoencoder (wrapping a DBN)
Sound	Voice recognition		Gaussian Rectified	Recurrent Net
				Moving window for DBN or ConvNet
Time Series	Predictive analytics		Gaussian Rectified	Recurrent Net
				Moving window for DBN or ConvNet

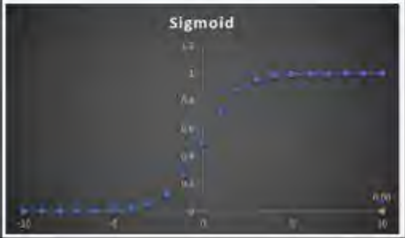
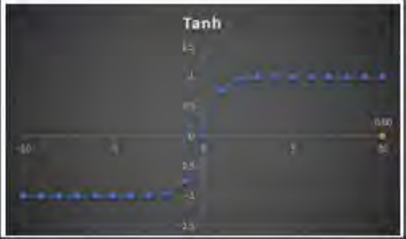
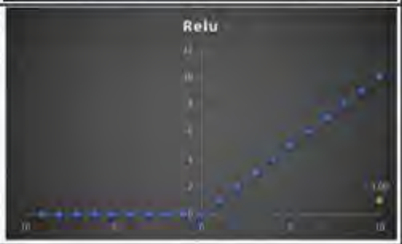
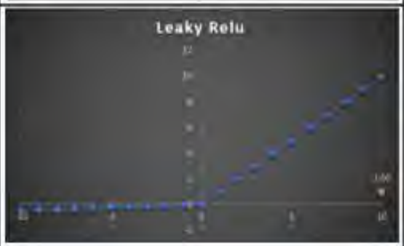
Source: https://www.quora.com/How-does-one-choose-between-various-Deep-Learning-Methods-in-particular-when-to-use-Deep-Belief-Networks-over-Recurrent-Neural-Network#!n=12

Neural Network – Activation Functions

Active Function Name	Formula	2D Graphical Representation	3D Graphical Representation	Description
Linear	$f(x) = x,$ *for all* x			The activation of the neuron is passed on directly as the output
Logistic (or sigmoid)	$f(x) = \frac{1}{1+e^{-x}}$			A S-shaped curve, very popular because it is Monotonous and has a simple derivative, Range of logistic or sigmoid function is from 0 to 1
Hyperbolic Tangent	$f(x) = tanh(x)$ $f(x) = \frac{1+e^{-2x}}{1+e^{2x}}$			A sigmoid curve similar to the logistic function. Often performs better than the logistic function because of its symmetry. Ideal for multilayer Perceptrons, particularly the hidden layers. Output value is between -1 and +1

Source: https://www.researchgate.net/figure/Three-of-the-Most-Commonly-Used-Neuron-Activation-Functions_tbl1_317671554

Neural Network – Activation Functions

Name	Plot	Equation	Derivative
Sigmoid		$f(x) = \sigma(x) = \dfrac{1}{1+e^{-x}}$	$f'(x) = f(x)(1 - f(x))$
Tanh		$f(x) = \tanh(x) = \dfrac{(e^{x} - e^{-x})}{(e^{x} + e^{-x})}$	$f'(x) = 1 - f(x)^2$
Rectified Linear Unit (relu)		$f(x) = \begin{cases} 0 & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$
Leaky Rectified Linear Unit (Leaky relu)		$f(x) = \begin{cases} 0.01x & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0.01 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$

Source: https://engmrk.com/activation-function-for-dnn/

ML Algorithms

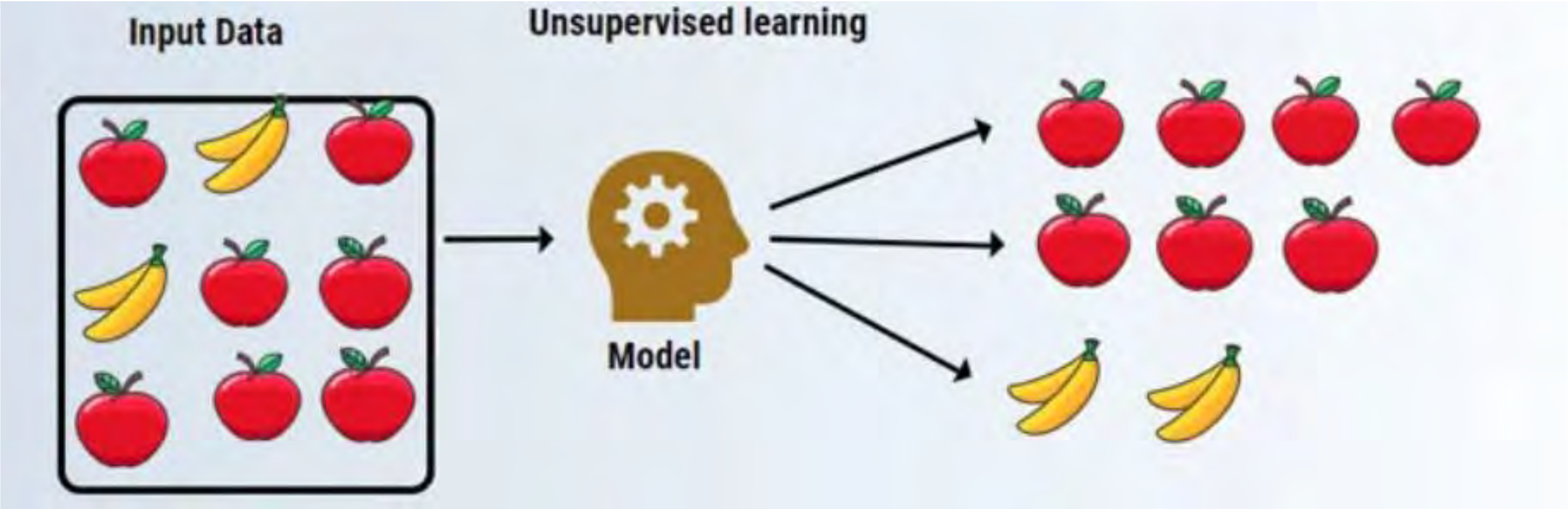
ML Algorithms – By Learning

- Supervised: Logistic Regression & Back Propagation Neural Network
- Unsupervised: Apriori & K-means
- Semi-Supervised: Extension of Other Algorithms
- Reinforcement: Monte Carlo, Q-Learning

Supervised Learning

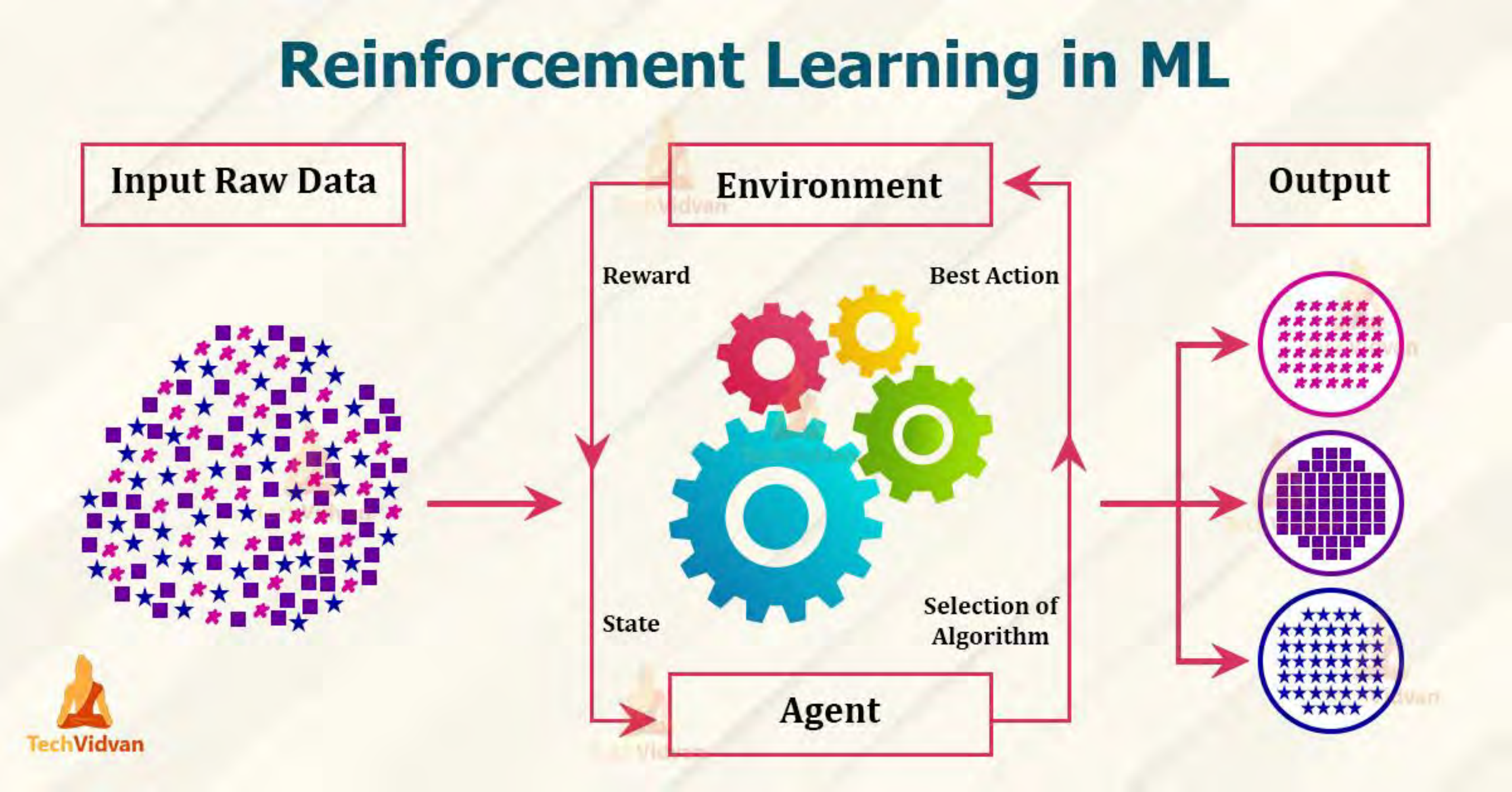
- Supervised Learning is a method used to enable machines to classify/ predict objects based on labeled data fed to the machine.

Unsupervised Learning



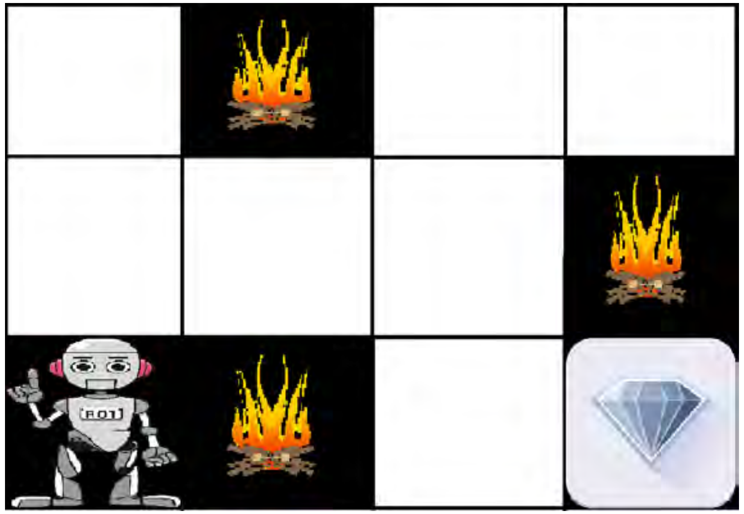
https://www.educba.com/what-is-supervised-learning/

Reinforcement Learning



[Source: https://www.analyticsvidhya.com/blog/2021/02/introduction-to-reinforcement-learning-for-beginners/]

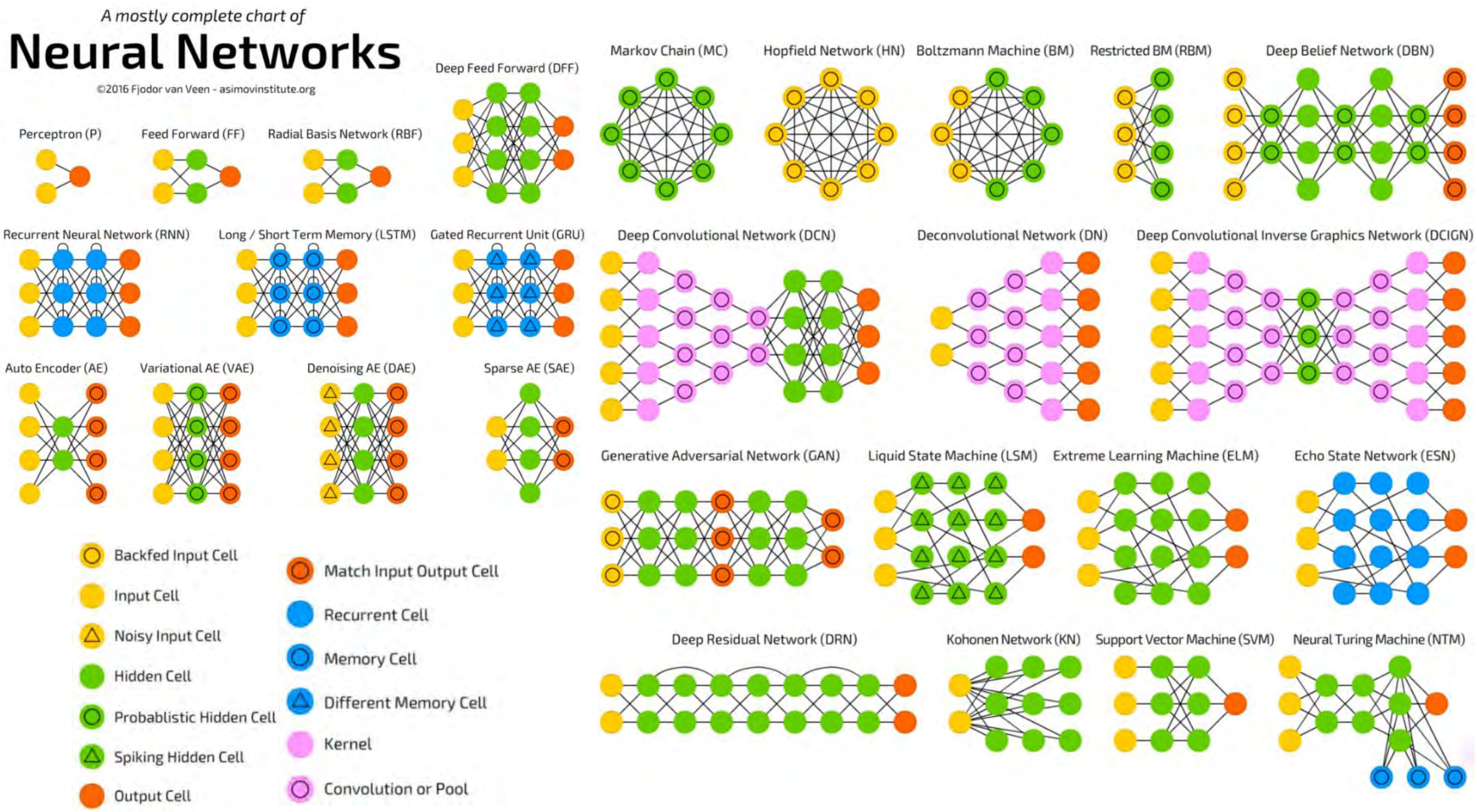
- Taking suitable action to maximize reward in a particular situation.
- No training data.
- Learn from experience



[Source: https://www.geeksforgeeks.org/what-is-reinforcement-learning/]

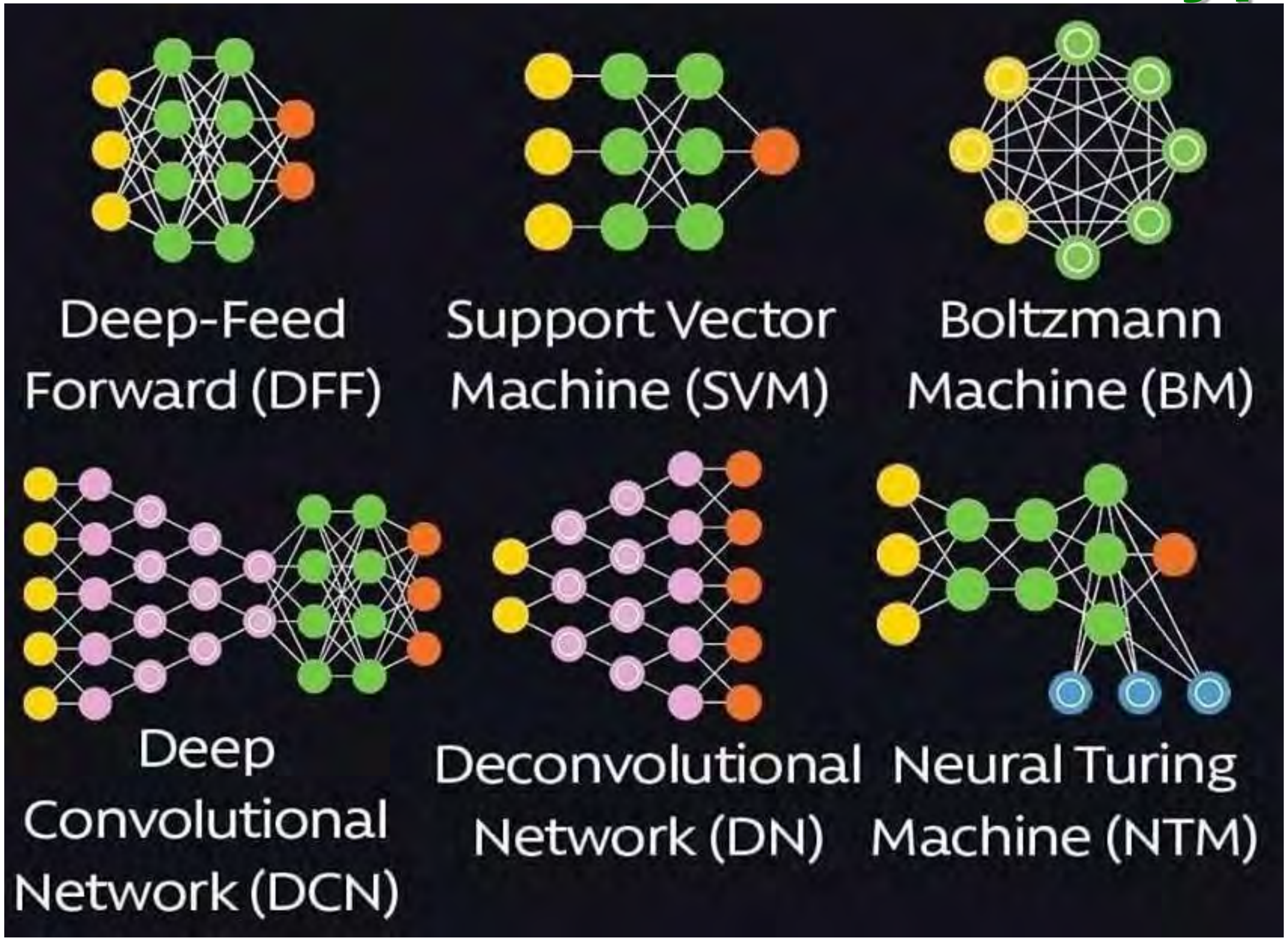
Types of DNN

Various Options for ANN Models



Source: https://towardsdatascience.com/the-mostly-complete-chart-of-neural-networks-explained-3fb6f2367464

Artificial Neural Networks - Types

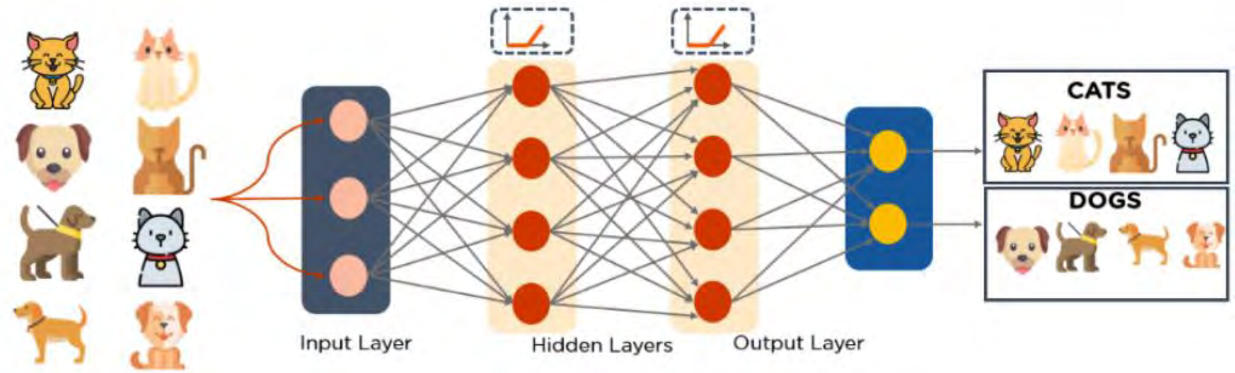


Types of DNN Networks

- Multilayer Perceptron (MLP)
- Convolutional Neural Networks (CNNs)
- Long Short Term Memory Networks (LSTMs)
- Recurrent Neural Networks (RNNs)
- Autoencoders
- Generative Adversarial Networks (GANs)
- Radial Basis Function Networks (RBFNs)
- Self Organizing Maps (SOMs)
- Deep Belief Networks (DBNs)
- Restricted Boltzmann Machines(RBMs)

Multilayer Perceptrons (MLPs)

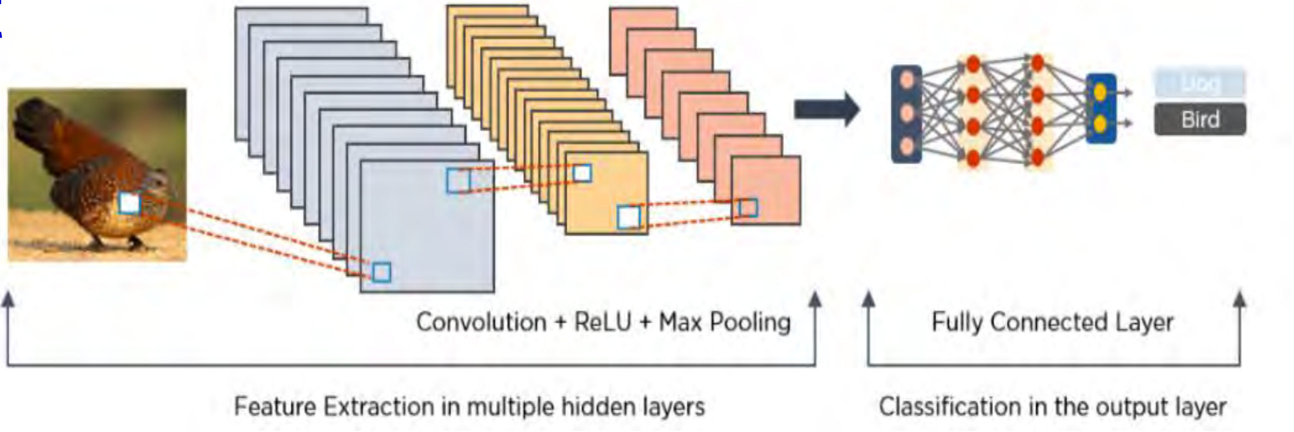
- MLPs are the first place to start with deep learning.
- MLPs are feedforward neural networks with multiple layers of perceptrons with activation functions. MLPs input layer and an output layer are fully connected. They have multiple hidden layers. They are used for speech-recognition, image-recognition etc.



https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Convolutional Neural Networks

- CNNs(ConvNets) are made of multiple layers and are mainly used for image processing and object detection. First CNN (LeNet) was made in 1988.
- CNNs are mainly used to identify satellite images, medical images, detect anomalies etc.



https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Long Short Term Memory Networks (LSTMs)

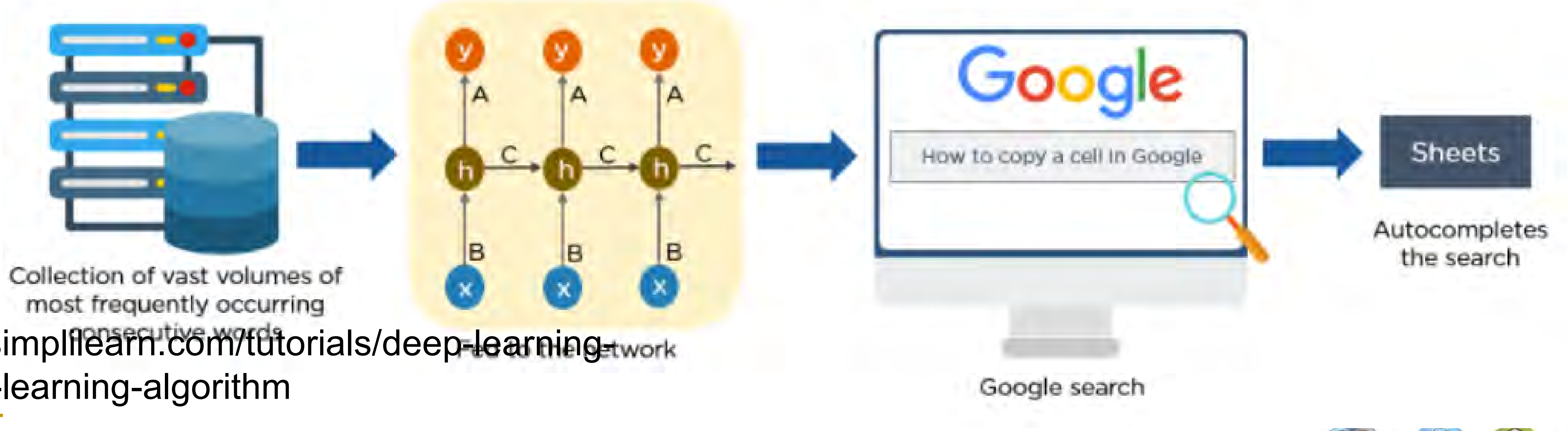
- A type of Recurrent Neural Network (RNN) that can learn and memorize long-term dependencies. It remembers the past.

- LSTMs are useful in time-series prediction. LSTMs are made of layers which are mainly known as gates. LSTMs are also used for speech recognition, music composition etc.

    - First, they forget irrelevant parts of the previous state
    - Next, they selectively update the cell-state values
    - Finally, the output of certain parts of the cell state

Recurrent Neural Networks (RNNs)

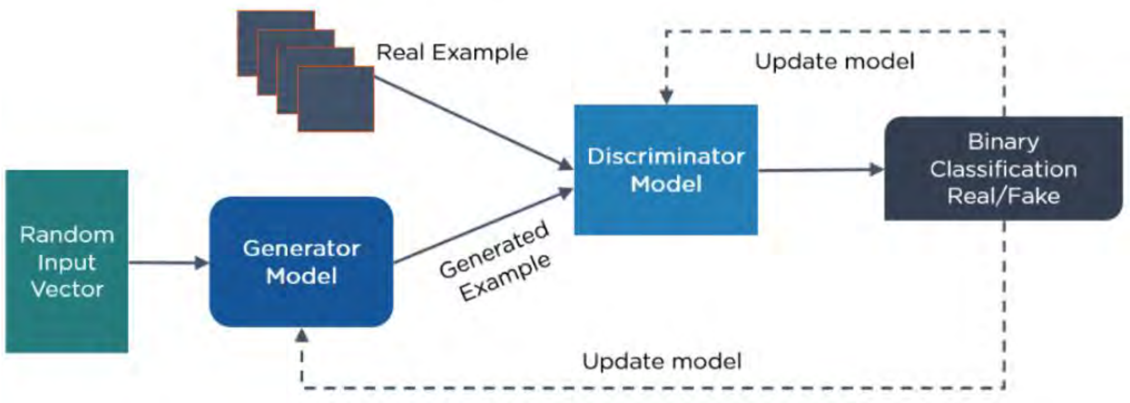
- RNNs have outputs from the previous inputs when they have hidden state which acts in remembering.
- Computation is slow and it's remembering power is lower than LSTM. It can't be used for very long sequence. RNNs are commonly used for image captioning, time-series analysis, natural-language processing, handwriting recognition, and machine translation.



https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Generative Adversarial Networks (GANs)

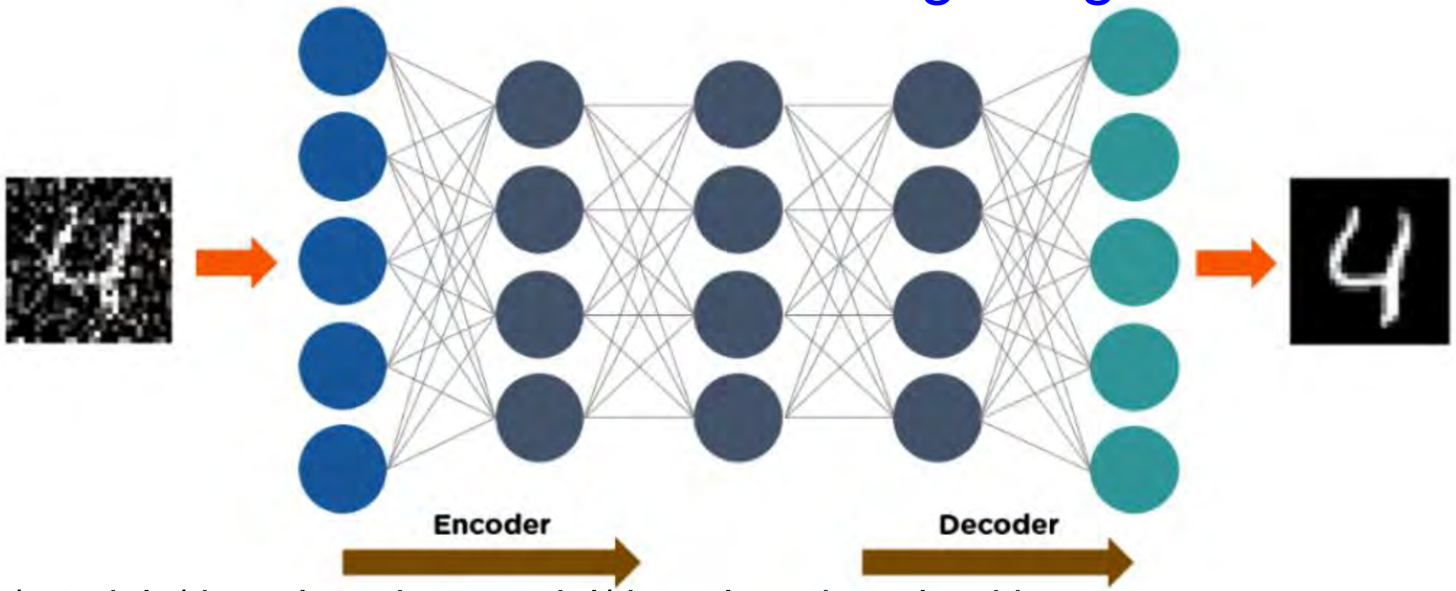
- GANs are generative adversarial deep learning networks. It generates new data. It is made of a generator, which learns to generate fake data, and a discriminator, which competes with the G to make better false information.



https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Autoencoders

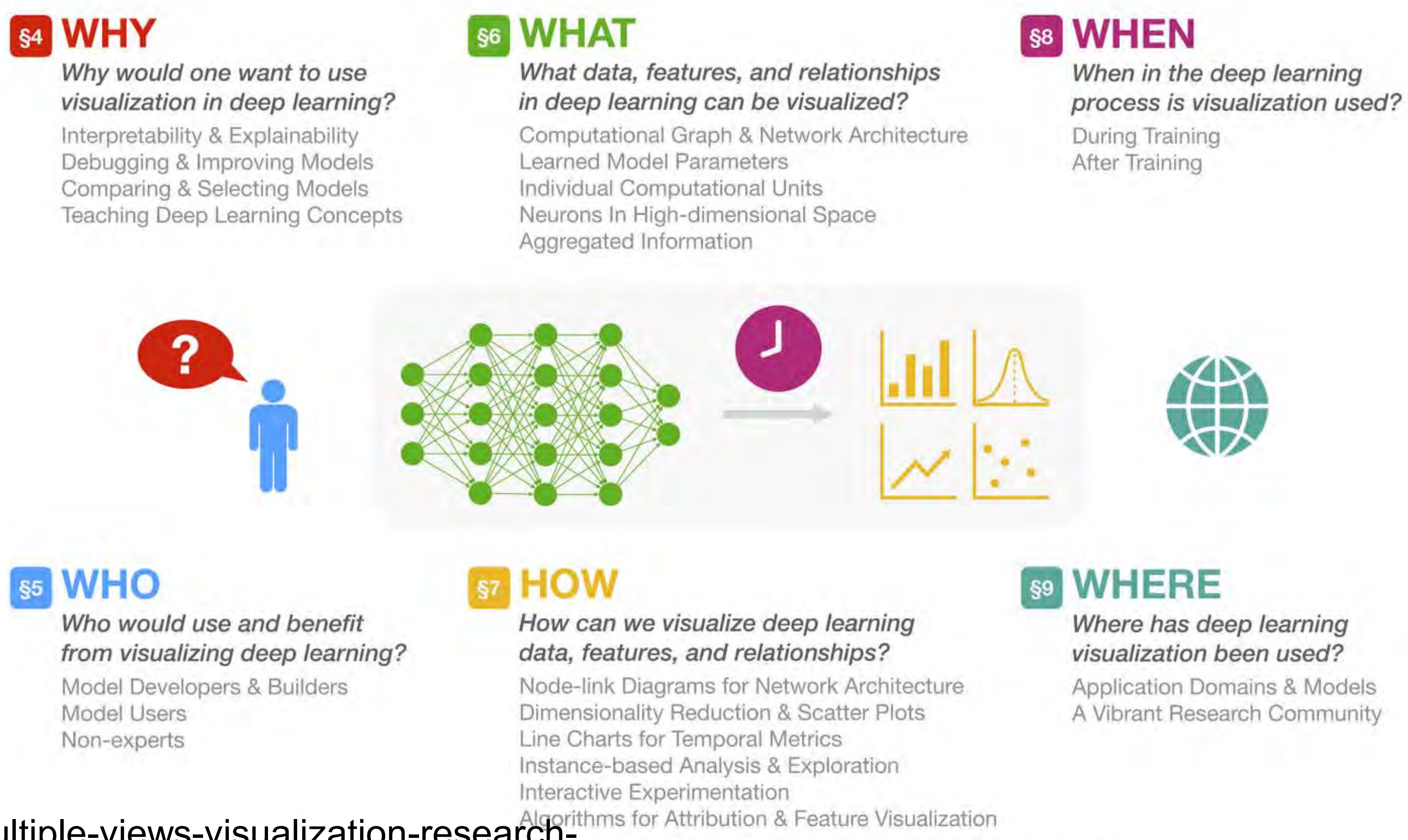
- In simple term, it copies the input to its output once it learns how to change. It uses unsupervised learning in its backpropagation algorithm. A not clearly visible image can be visible by feeding the image into the autoencoder neural network.
- Steps: 1. Encode the image (Latent vector). 2. Reduce the size of the input into a smaller representation. 3. Decodes the image to generate the reconstructed image.



https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Tools for AI

Data Visualization in Deep Learning



An overview of our interrogative survey, and how each of the six questions, "**why**, **who**, **what**, **how**, **when**, and **where**,"

https://medium.com/multiple-views-visualization-research-explained/visualization-in-deep-learning-b29f0ec4f136

ML Languages

- Python: a popular language with high-quality machine learning and data analysis libraries
- C++: a middle-level language used for parallel computing on CUDA
- R: a language for statistical computing and graphics
- MATLAB: a language for multidiscipline computing

Source: https://www.altexsoft.com/blog/datascience/the-best-machine-learning-tools-experts-top-picks/

ML Tools / Frameworks

- TensorFlow
- PyTorch
- Keras
- Chainer
- ONNX
- MATLAB

TensorFlow

- Most Popular Deep Learning Framework
- Invented by Google
- Python works Best with Tensorflow
- C/C++ and JAVA also works.
- Cloud & Edge Computing
- Static Computational Graph
- Good Choice for Cross-platform Application
- Slowest in GPU as it was developed to work In TPU

PyTorch

- Next important Framework
- Lower-level API like TensorFlow
- Developed for Facebook
- Dynamic Computational Graph
- Debuggers like PyCharm used
- Best for Prototyping
- Data parallelism & Distributed learning supported
- Strong GPU acceleration

Keras

- Much easier than TensorFlow
- Readable
- High level API
- Lower-level libraries from either TensorFlow or Theano
- Handles a huge data set
- Single line functions are available – easier than any lower-level deep learning framework
- Very good start
- Readability makes it more understandable

Chainer

- Chainer was predominant before PyTorch
- Basic structure same as PyTorch
- Written in Python with NumPy and CuPy libraries
- Fastest among other Python frameworks

Onnx

- ONNX - product of Microsoft and Facebook search for open format deep learning models
- Bridge between different models to transfer from one to another
- A model is trained in one framework, ONNX transfers it to another one
- TensorFlow or Keras not supported by it
- PyTorch supports

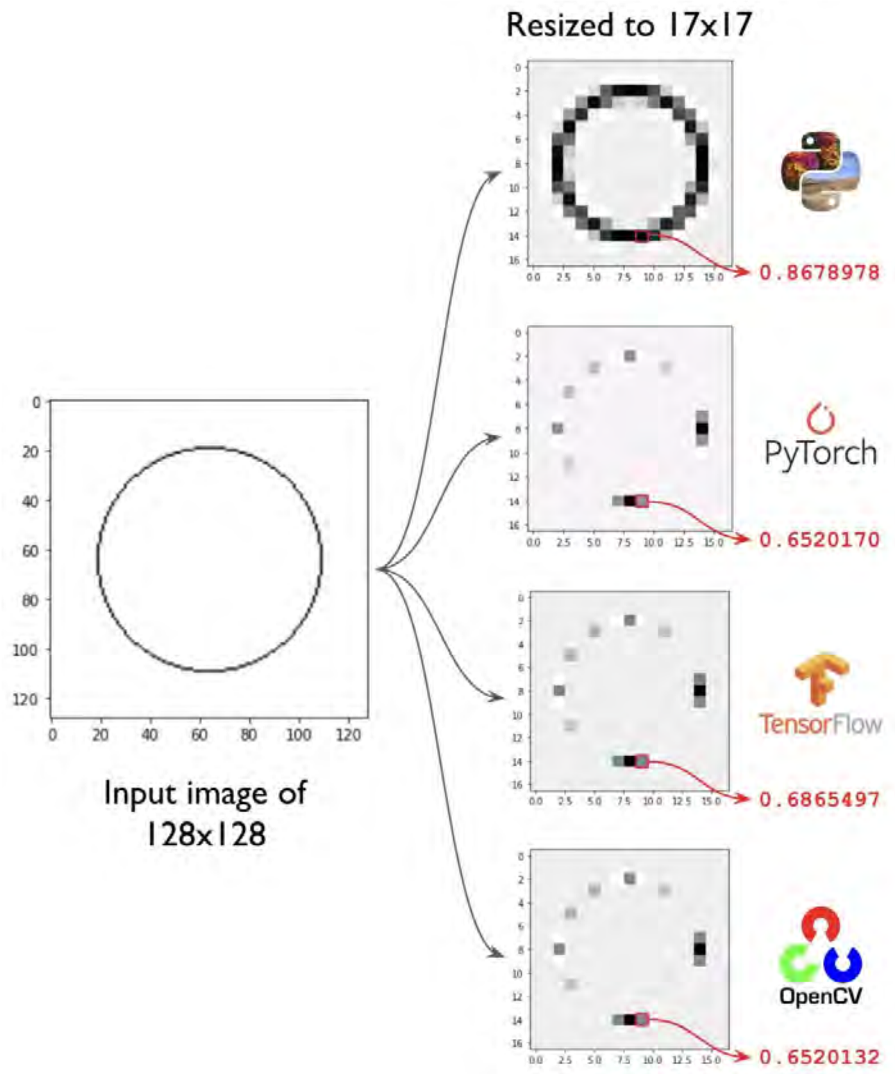
TensorFlow Vs MATLAB

- MATLAB's deep learning toolbox good choice
- MATLAB advantage : few lines codes
- Models deployable in embedded system also without much expertise
- TensorFlow community support is better.
- Not all toolbox are free in MATLAB
- MATLAB Models imported or exported to Keras, TensorFlow or PyTorch through ONNX
- MATLAB is less customizable like TensorFlow or PyTorch
- First getting an idea in MATLAB is easier than others

Who Use What?

• A beginner	:	Keras
• Researchers	:	Keras/ PyTorch/ TensorFlow/ MATLAB
• AWS	:	Gluon or MXNet
• Google Cloud	:	TensorFlow

Results May Vary Depending on the Tool



Evaluation Metrics

- Evaluation Metrics explain the performance of a model.
- Building machine learning models works on a constructive feedback principle.
  - Build a model.
  - Get feedback from metrics.
  - Make improvements and continue until you achieve a desirable accuracy.
- Building a predictive model is not the motive.
- Creating and selecting a model with high accuracy on out of sample data.
- It is crucial to check the accuracy of your model prior to computing predicted values.
- Selection of metric depends on type of model and implementation plan.

Source: https://www.analyticsvidhya.com/blog/2019/08/11-important-model-evaluation-error-metrics/

ML Models: Performance Analysis Metrics

- Root-Mean Square Error (RMSE): Represents departure of metamodel from real-simulation (golden). Smaller RMSE means more accurate:
- $\mathrm{RM}SE = \sqrt{\left(\frac{1}{N}\right)\sum_{k=1}^{N}\left(FoM(x_k) - \widehat{FoM}(x_k)\right)^2}$
- **Relative Average Absolute Error (RAAE)**: Smaller RAAE means more accurate metamodel:

  $RAAE = \left(\frac{\sum_{k=1}^{N}\left|FoM(x_k) - \widehat{FoM}(x_k)\right|}{N \times Standard\ Deviation}\right)$
- **R-Square**: Larger R-square means more accurate metamodel: $R^2 = \left(1 - \frac{MSE}{Variance}\right)$

Overview - Evaluation Metrics Used

- Confusion Matrix
- Accuracy
- Precision
- F1-Score
- AUC-ROC

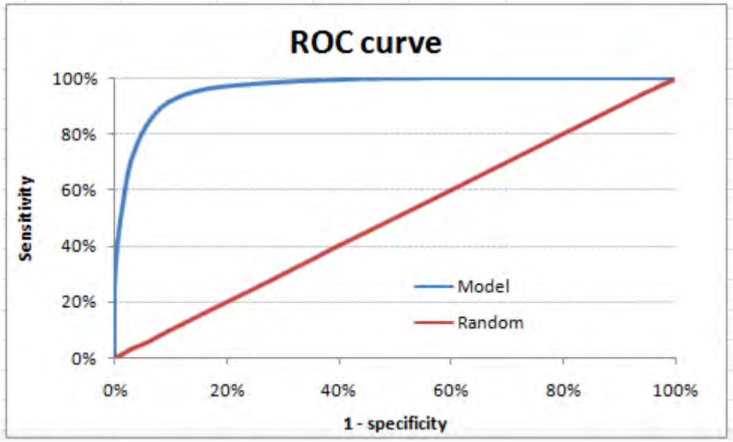
$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

$$\text{Recall} = \frac{True\ Positive}{True\ Positive + False\ Negative}$$

$$\text{F1} = 2 \times \frac{Precision * Recall}{Precision + Recall}$$

	Prediction	
Truth	TP	FN
	FP	TN



- N X N matrix → N = number of predicted classes
  - Positive Class→ Non-normal Class
  - Negative Class → Normal Class
- **Accuracy** : proportion of total number of correct predictions.
- **Positive Predictive Value or Precision** : proportion of correctly identified positive cases.
- **Negative Predictive Value** : proportion of correctly identified negative cases.
- **Sensitivity or Recall** : proportion of correctly identified actual positive cases.
- **Specificity** : proportion of correctly identified actual negative cases.

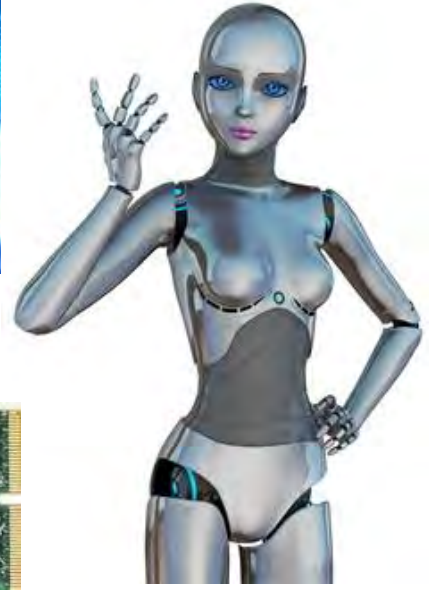
Hardware for AI

Artificial Intelligence Technology

Machine Learning

Deep Learning

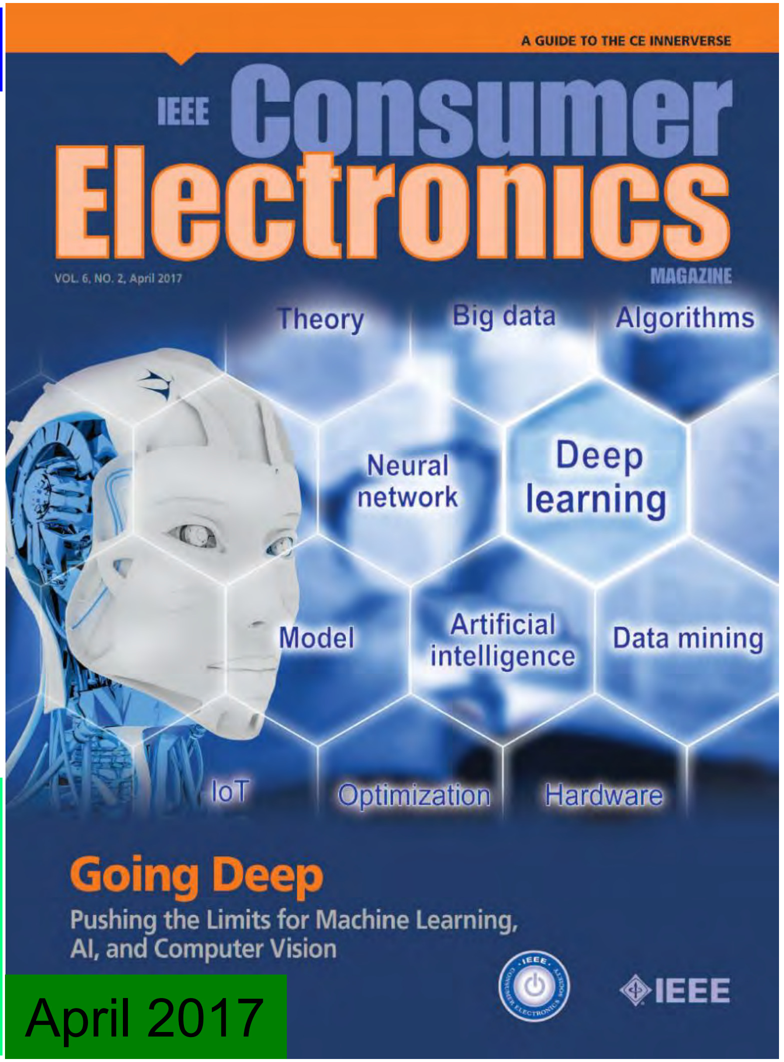
Source: http://transmitter.ieee.org/impact-aimachine-learning-iot-various-industries/



Tensor Processing Unit (TPU)

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

Smart City Use:
- Better analytics
- Better decision
- Faster response



April 2017

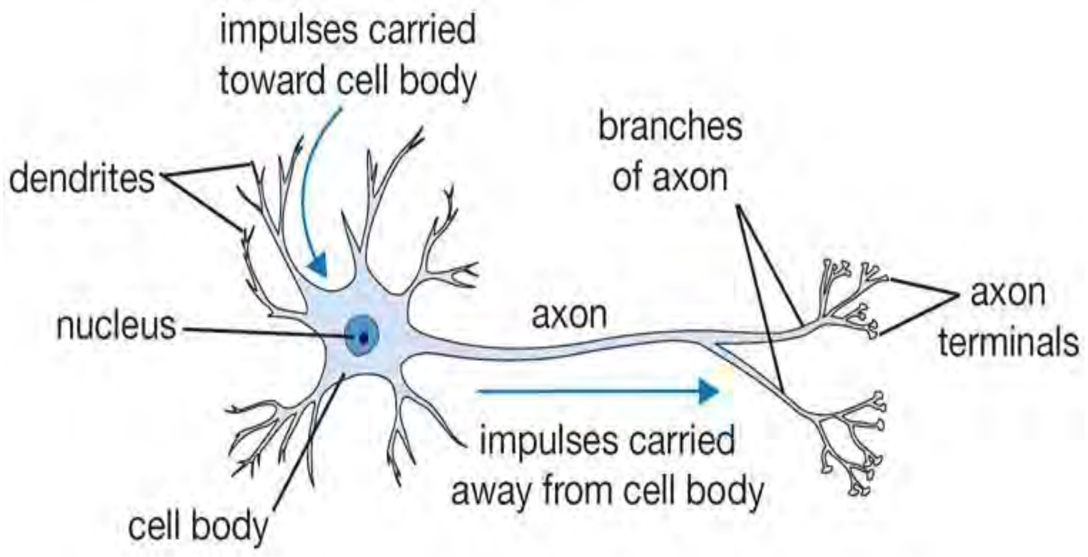
Neuromorphic Computing or Brain-Inspired Computing

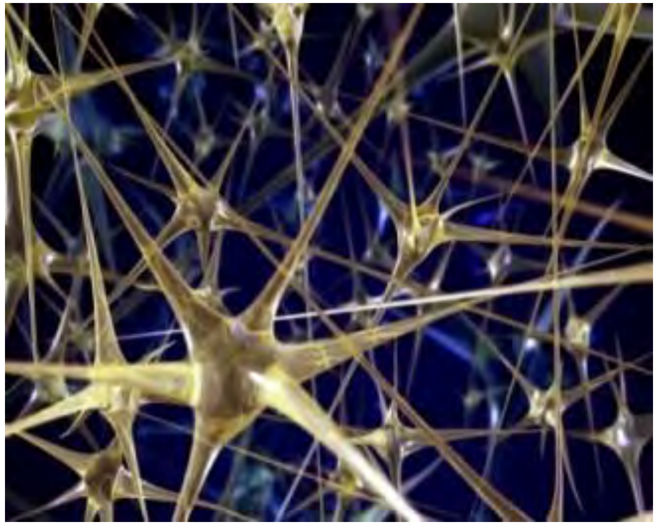
Application 1: Integrate into assistive glasses for visually impaired people for navigating through complex environments, even without the need for a WiFi connection.

Application 2: Neuromorphic-based, solar-powered “sensor leaves” equipped with sensors for sight, smell or sound can help to monitor natural disasters.

Source: https://blogs.scientificamerican.com/observations/brain-inspired-computing-reaches-a-new-milestone/

Brain Inspired Computing

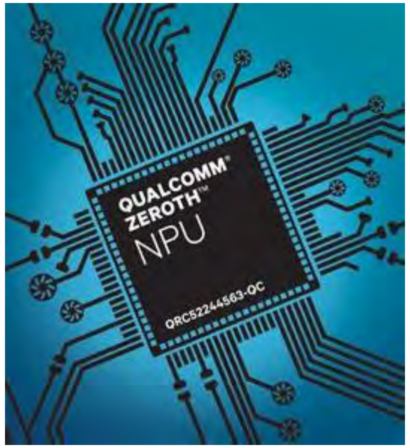




- Basic computational unit of the brain is a **neuron** → 86B neurons in the brain
- Neurons are connected with nearly **10^{14} – 10^{15} synapses**
- Neurons receive input signal from **dendrites** and produce output signal along **axon**, which interact with the dendrites of other neurons via **synaptic weights**
- Synaptic weights – learnable & control influence strength

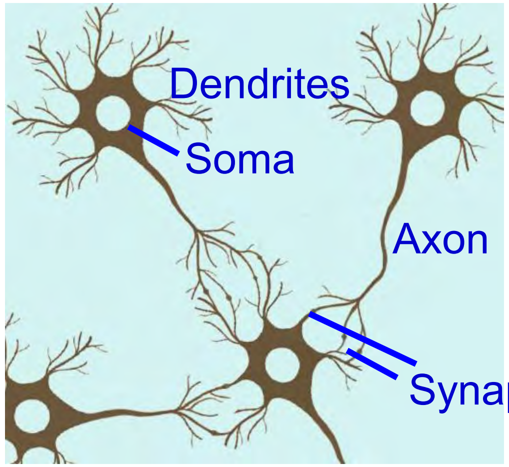
Source: https://www.rle.mit.edu/eems/wp-content/uploads/2019/06/Tutorial-on-DNN-01-Overview.pdf

Neuromorphic Computing or Brain-Inspired Computing

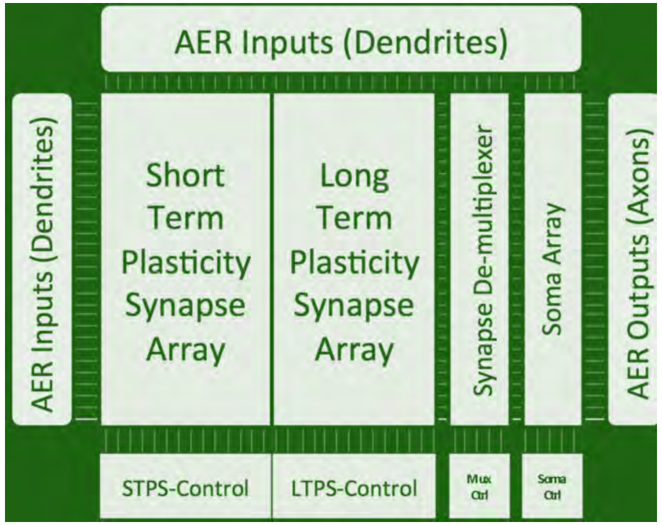


Source: https://www.qualcomm.com/news/onq/2013/10/10/introducing-qualcomm-zeroth-processors-brain-inspired-computing

Neuronal Circuits



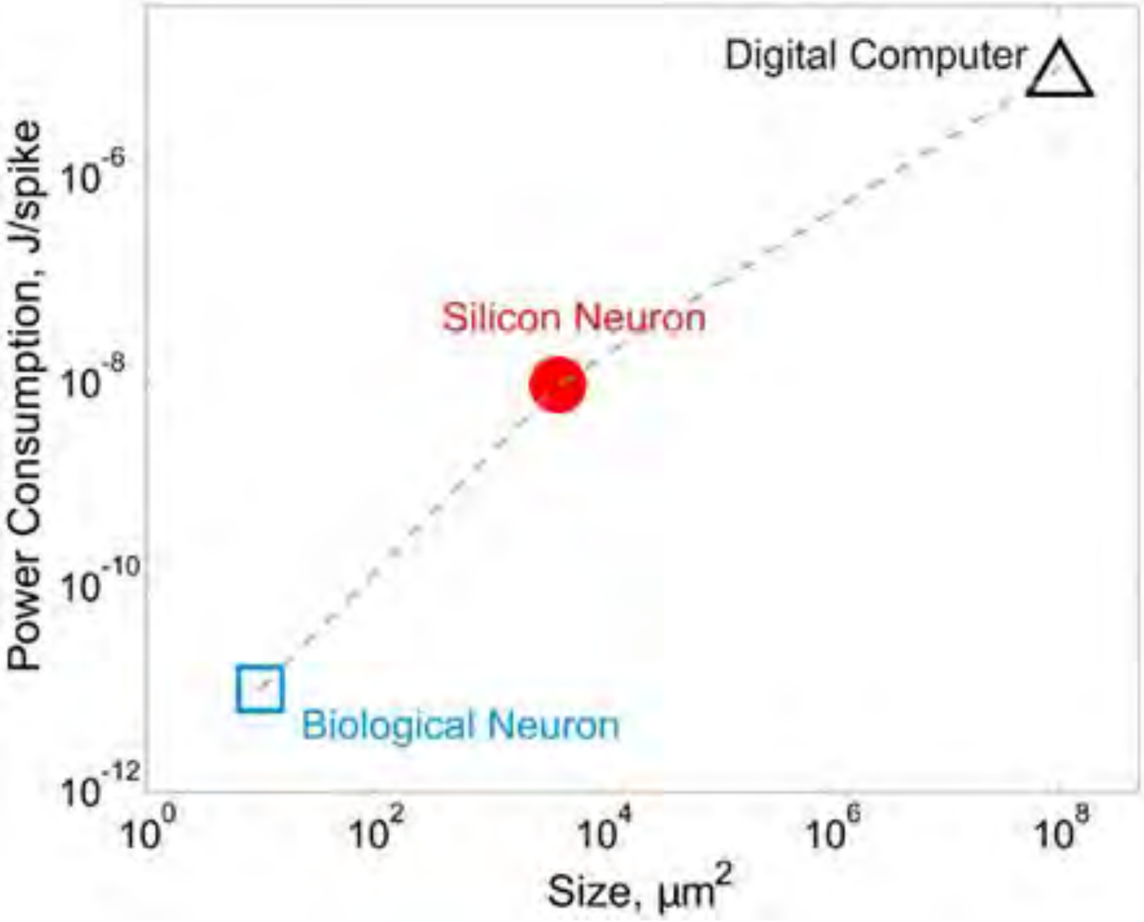
- Neurons "fire" action potentials which are spikes of electrical signals initiated near the neuronal cell bodies and transmitted down their long extensions called axons.
- Axons link with their downstream partner neurons.
- Information is encoded in the frequency and timing of these spikes.



Neuromorphic Architecture

Processing Powers (Source: MIT Technical Review)		
Types of Chips	Functions	Applications
Traditional Chips (von Neumann Architecture)	Reliably make precision calculations	Any numerical problem, Complex problems require more amount of energy
Neuromorphic Chips	Detect and Predict Patterns in complex data using minimal energy	Applications with significant visual/ auditory data requiring a system to adjust its behavior as it interacts with the world

Power Consumption Comparison



Source: https://www.researchgate.net/figure/Biological-and-silicon-neurons-have-much-better-power-and-space-efficiencies-than-digital_fig1_51710519

Biological and silicon neurons have much better power and space efficiencies than digital computers.

Why Is the Human Brain So Efficient?

Properties	Computer	Human Brain
Number of Basic Units	Up to 10 billion transistors	~100 billion neurons; ~100 trillion synapses
Speed of Basic Operation	10 billion/sec.	< 1,000/sec.
Precision	1 in ~4.2 billion (for a 32-bit processor)	~1 in 100
Power Consumption	~100 watts	~10 watts
Information Processing Mode	Mostly serial	Serial and massively parallel
Input/Output for Each Unit	1–3	~1,000
Signaling Mode	Digital	Digital and analog

Source: https://nautil.us/issue/59/connections/why-is-the-human-brain-so-efficient

100 Watts

10 Watts

Massive parallelism lifts the brain's performance above that of AI.

Computer Versus the Human Brain: Speed

- Computer has huge advantages over the brain in the speed of basic operations.
- Typical PCs can perform elementary arithmetic operations, such as addition, at a speed of 10 billion operations per second.
- We can estimate the speed of elementary operations in the brain by the elementary processes through which neurons transmit information and communicate with each other.
- The highest frequency of neuronal firing is about 1,000 spikes per second.
- The fastest synaptic transmission takes about 1 millisecond.
- Both in terms of spikes and synaptic transmission, the human brain can perform at most about a thousand basic operations per second, or 10 million times slower than the computer.

Source: https://nautil.us/issue/59/connections/why-is-the-human-brain-so-efficient

Computer Versus the Human Brain: Precision

- Computers have huge advantages over the brain in the precision of basic operations.
- Computers can represent quantities (numbers) with any desired precision according to the bits (binary digits, or 0s and 1s) assigned to each number.
- For instance, a 32-bit number has a precision of 1 in 232 or 4.2 billion.
- Most quantities in the human nervous system (for instance, the firing frequency of neurons, which is often used to represent the intensity of stimuli) have variability of a few percent due to biological noise.
- Human brain has a precision of 1 in 100 at best, which is millionsfold worse than a computer.

Source: https://nautil.us/issue/59/connections/why-is-the-human-brain-so-efficient

Silicon Neurons

- **Silicon neurons** emulate the electro-physiological behavior of real neurons.
- This may be done at many different levels:
  1) simple models (like leaky integrate-and-fire neurons)
  2) models emulating multiple ion channels
  3) detailed morphology
- Silicon neurons may be implemented in digital or analog, or mixed signal (digital and analog) technologies.
- Real (and silicon) neurons have a number of active parts: one dissection of a neuron is into synapses, dendrites, soma, and axon.
- Not all silicon neurons actually implement all of these elements: synapses in particular are sometime placed on additional chips.

Source: http://www.scholarpedia.org/article/Silicon_neurons

Cognitive Computing

The Tabulating Era (1900s – 1940s)

The Programming Era (1950s– present)

The Cognitive Era (2011 –)

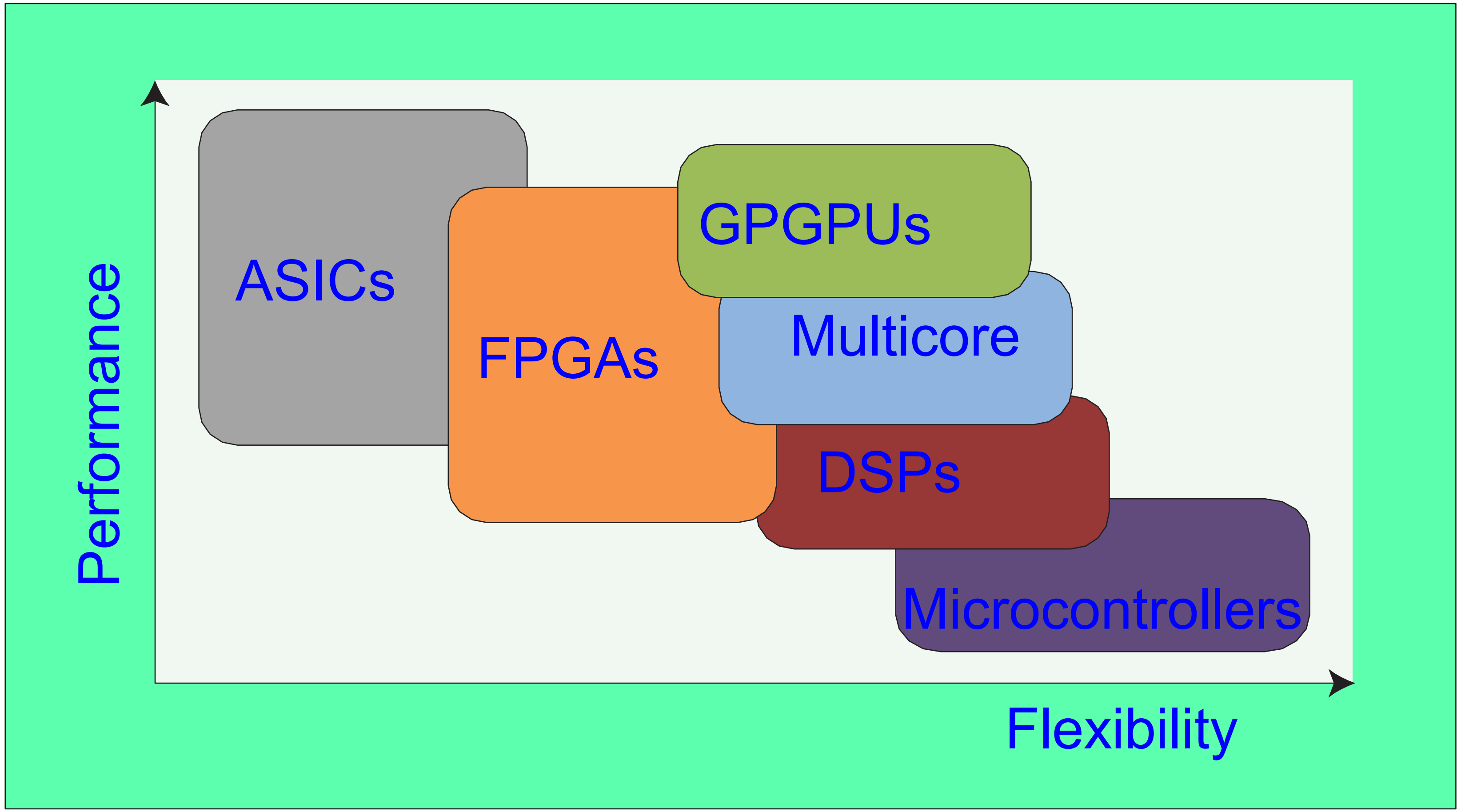
Cognitive Computing: Not just "right" or "wrong" anymore but "probably".

- Systems that learn at scale, reason with purpose and interact with humans naturally.
- Learn and reason from their interactions with humans and from their experiences with their environment; not programmed.

Usage:
- AI applications
- Expert systems
- Natural language processing
- Robotics
- Virtual reality

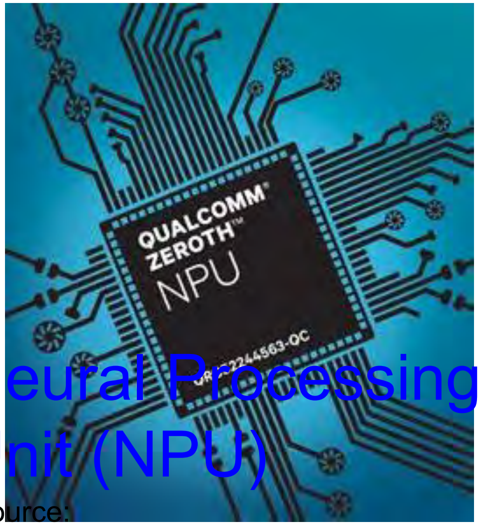
Source: http://www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf

Some Hardware for Deep Learning



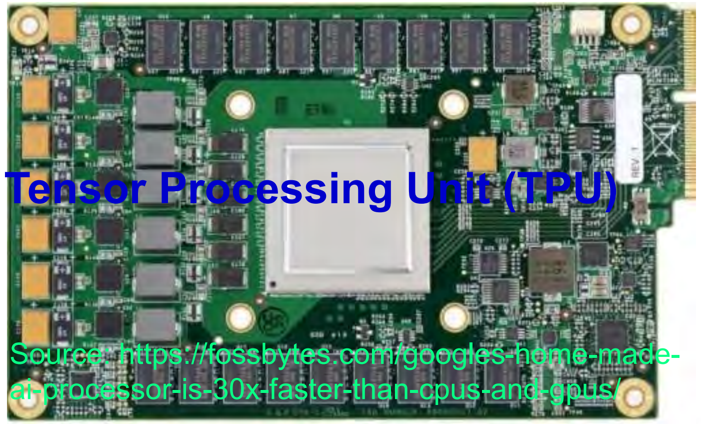
Source: R. Fernandez Molanes, K. Amarasinghe, J. Rodriguez-Andina and M. Manic, "Deep Learning and Reconfigurable Platforms in the Internet of Things: Challenges and Opportunities in Algorithms and Hardware," *IEEE Industrial Electronics Magazine*, vol. 12, no. 2, pp. 36-49, June 2018.

Computing Technology - Current and Emerging



Neural Processing Unit (NPU)

Source: https://www.qualcomm.com/news/onq/2013/10/10/introducing-qualcomm-zeroth-processors-brain-inspired-computing



Tensor Processing Unit (TPU)

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

FPGA

GPU

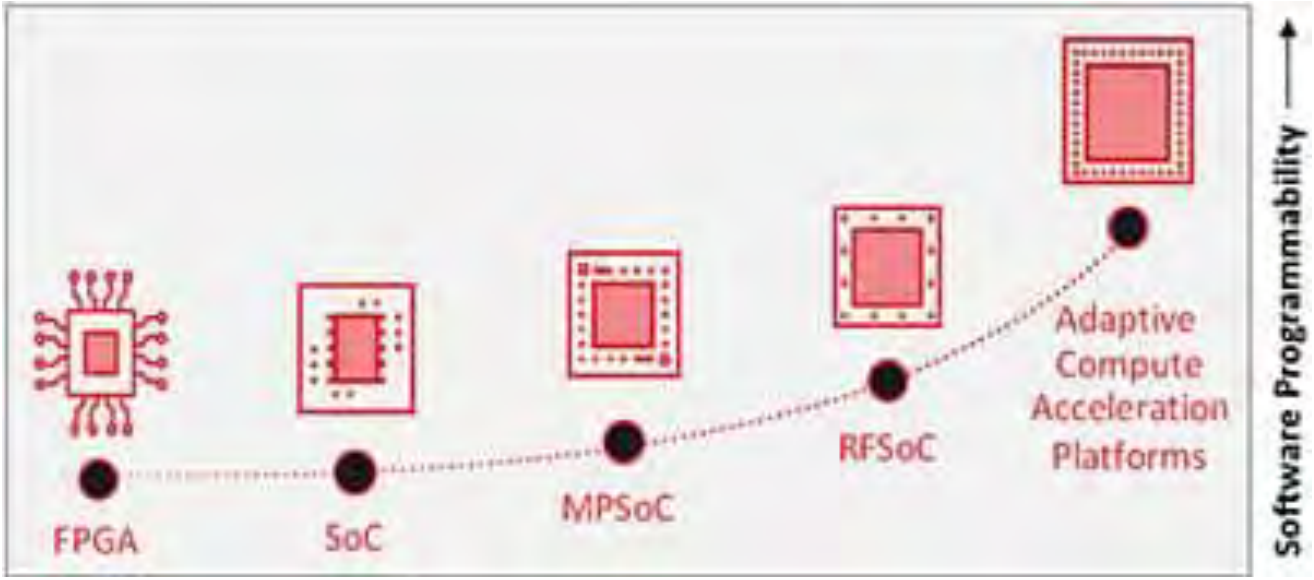
SoC based Design: 30 watts of power

320 trillion operations per second

Source: https://www.engadget.com/2017/10/10/nvidia-introduces-a-computer-for-level-5-autonomous-cars/

Source: Mohanty ISCT 2019 Keynote

FPGAs and Beyond: SoCs, MPSoCs, RFSoCs, and ACAPs



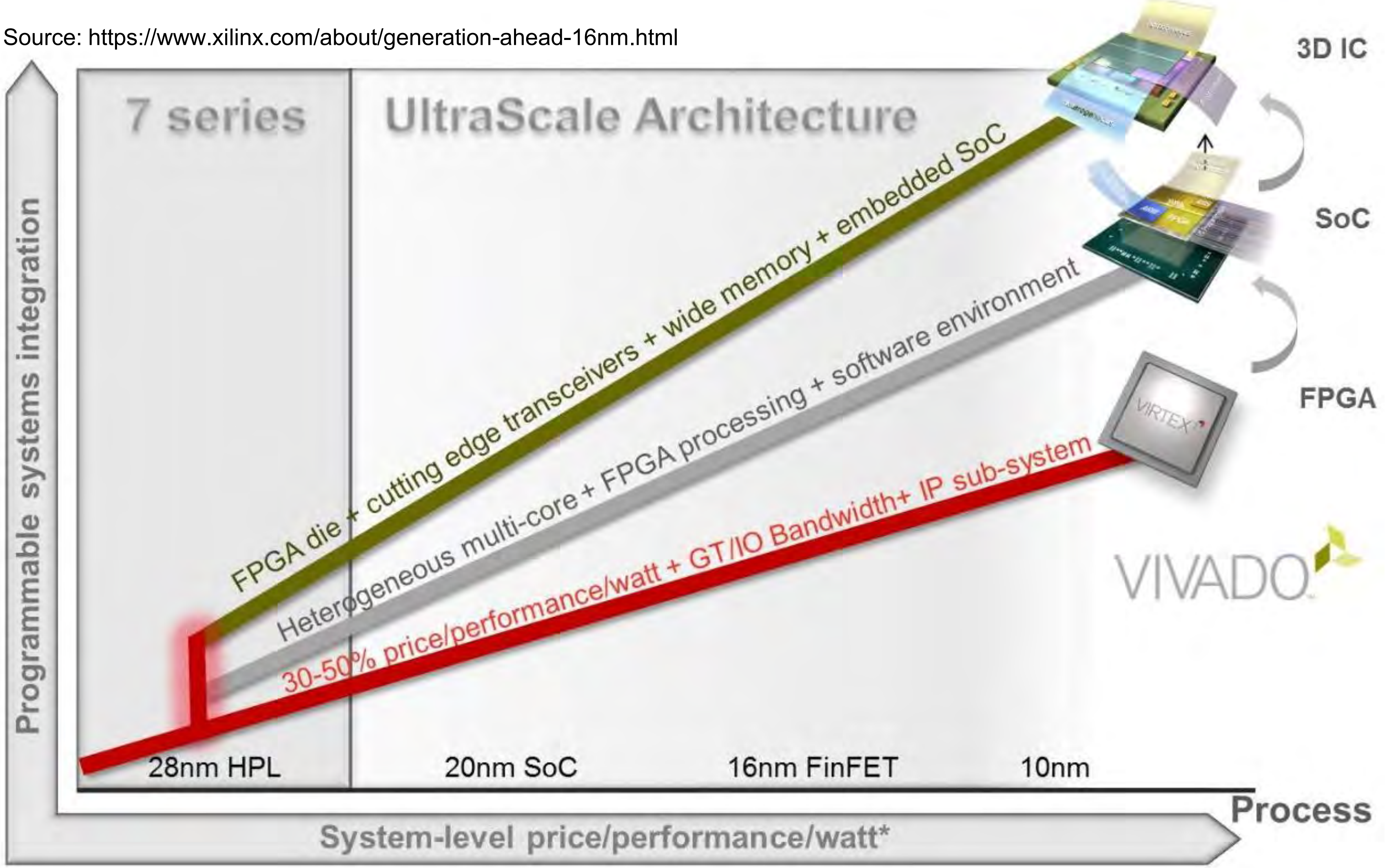
Source: https://www.digikey.com/en/articles/fundamentals-of-fpgas-part-4-getting-started-with-xilinx-fpgas

The capabilities of the programmable device can be from modest to high:

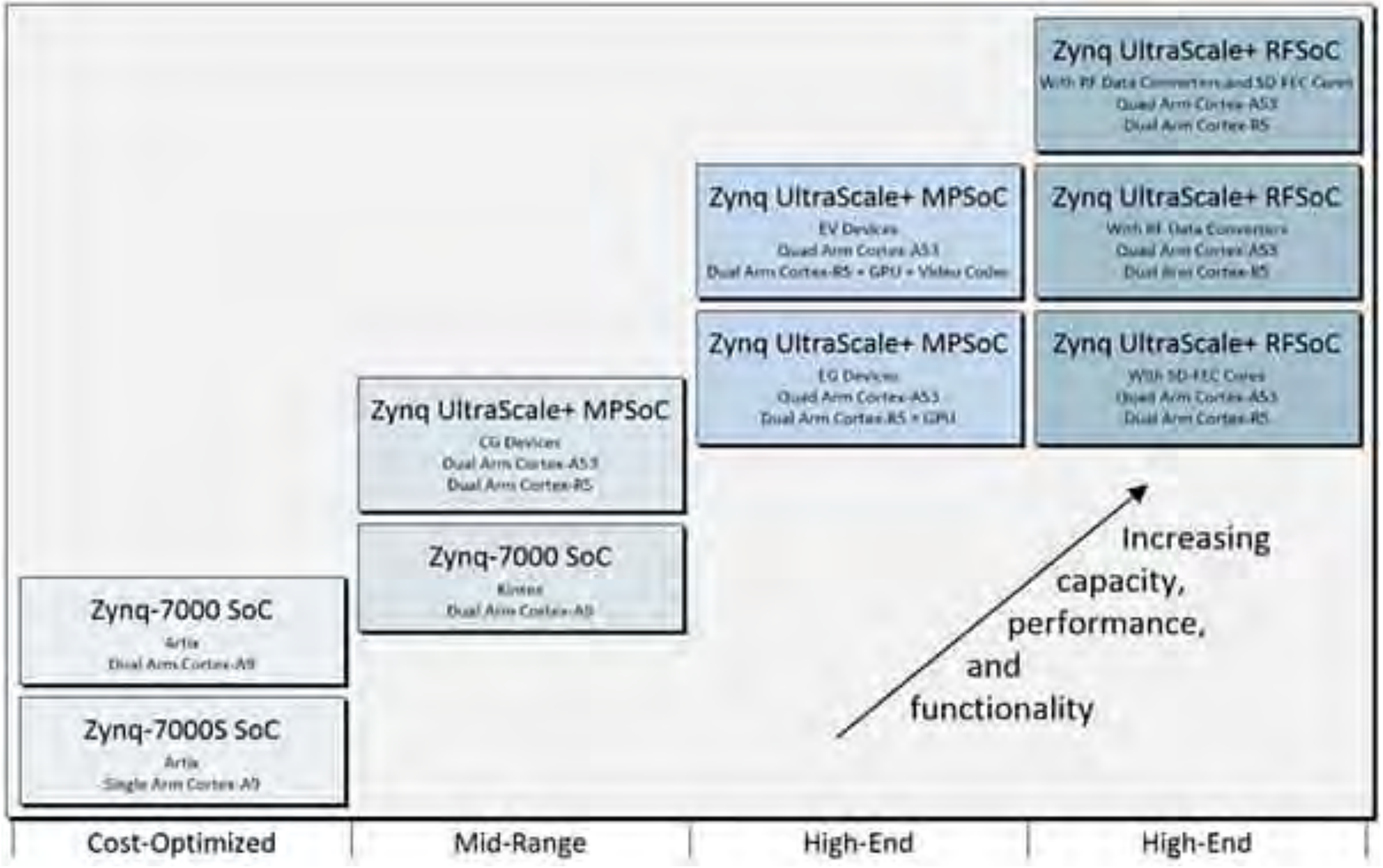
- Traditional FPGAs
- SoCs (FPGA programmable fabric with a single hard core processor)
- MPSoCs (FPGA programmable fabric with a multiple hard core processors)
- RFSoCs (MPSoCs with RF capability)
- ACAPs (Adaptive Compute Acceleration Platforms)

FPGAs and Beyond Trend

Source: https://www.xilinx.com/about/generation-ahead-16nm.html

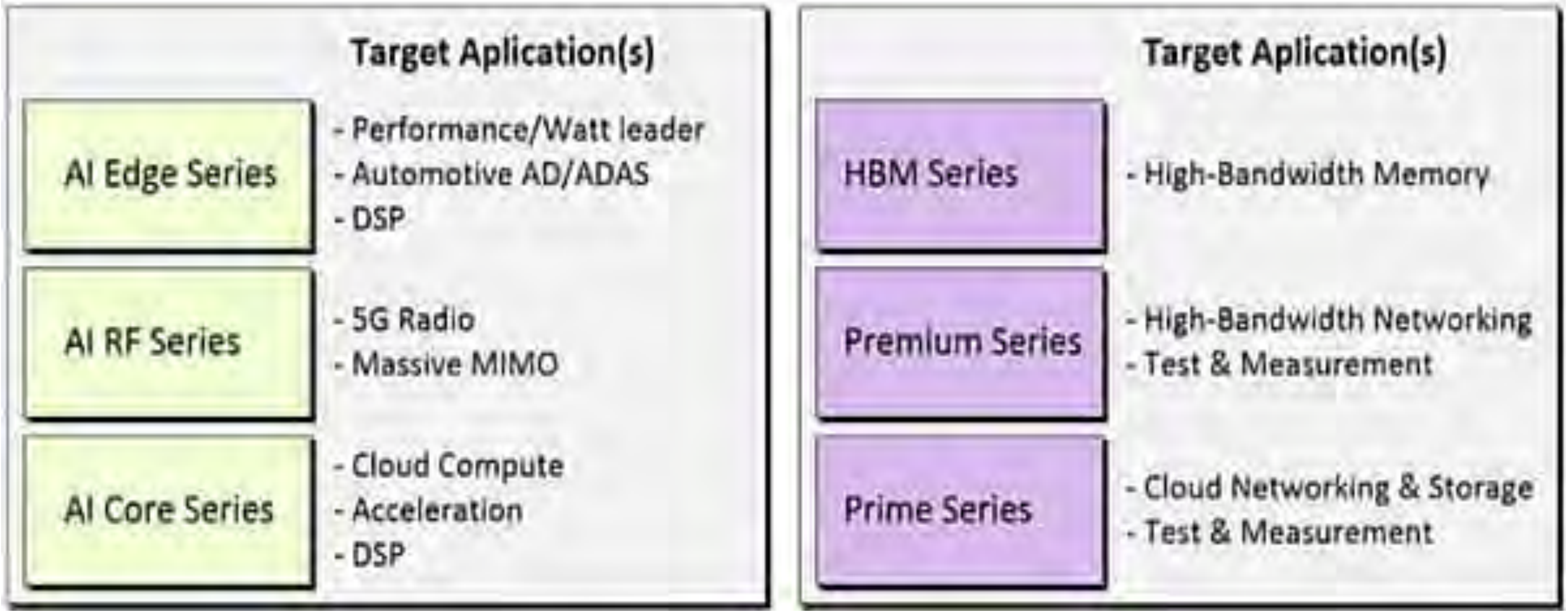


Xilinx - SoC, MPSoC, and RFSoC



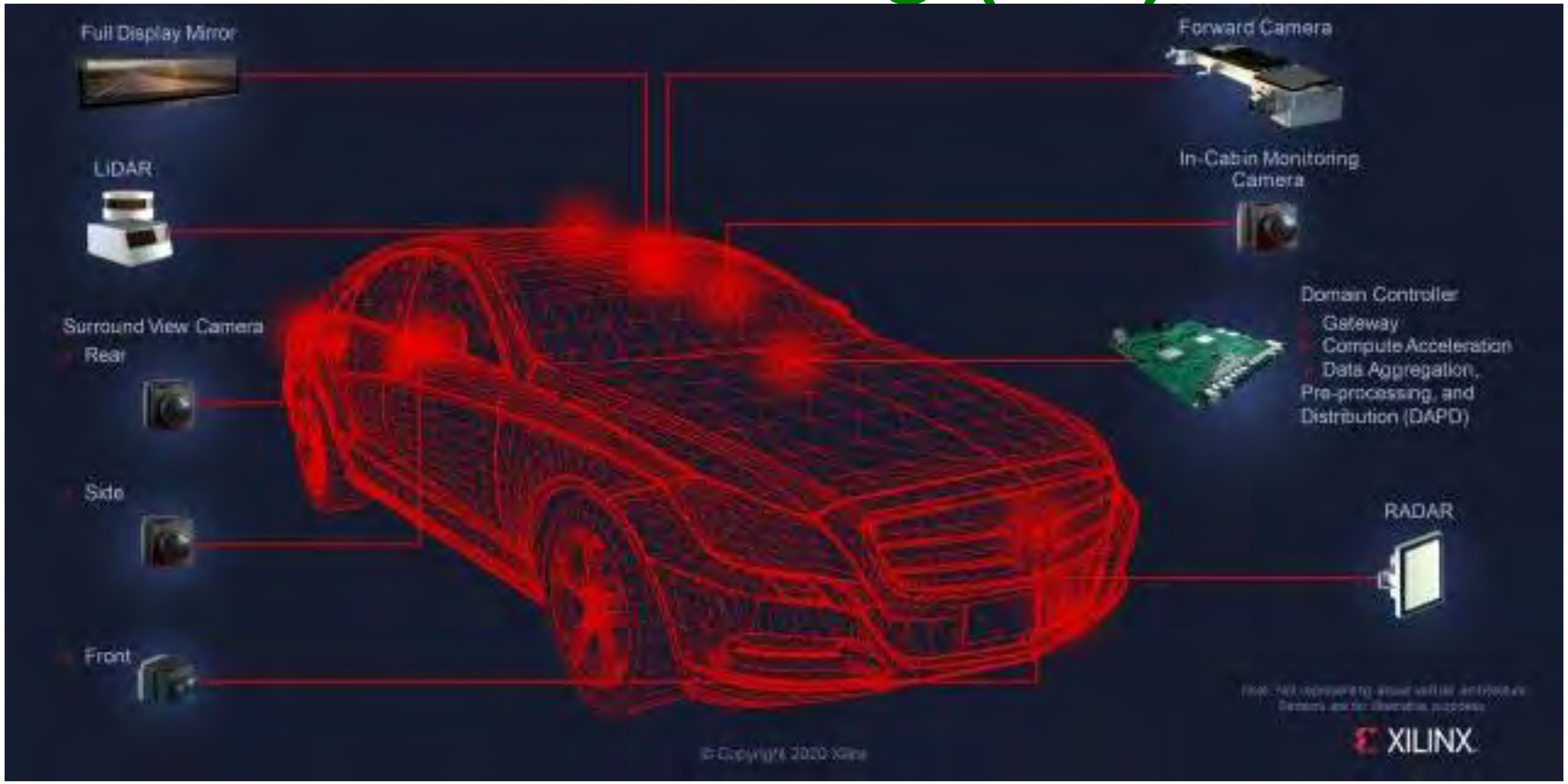
Source: https://www.digikey.com/en/articles/fundamentals-of-fpgas-part-4-getting-started-with-xilinx-fpgas

Xilinx FPGAs - Adaptive Compute Acceleration Platform (ACAP)



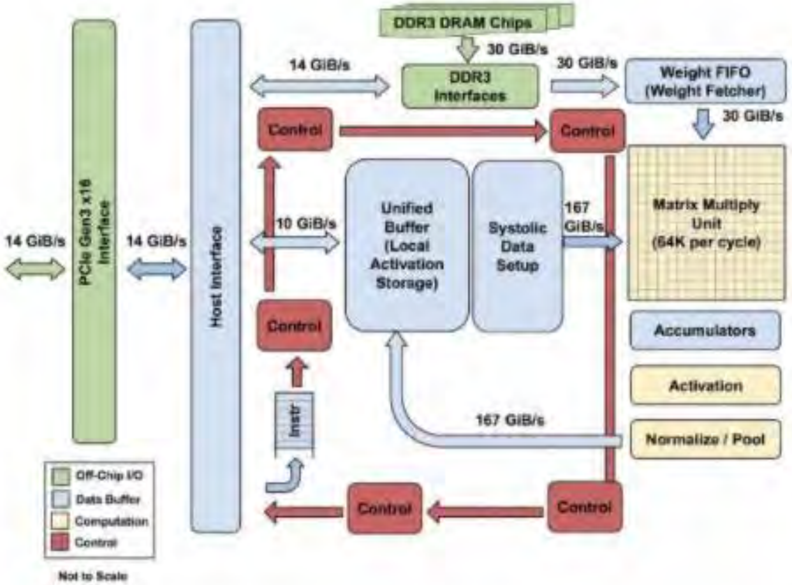
Source: https://www.digikey.com/en/articles/fundamentals-of-fpgas-part-4-getting-started-with-xilinx-fpgas

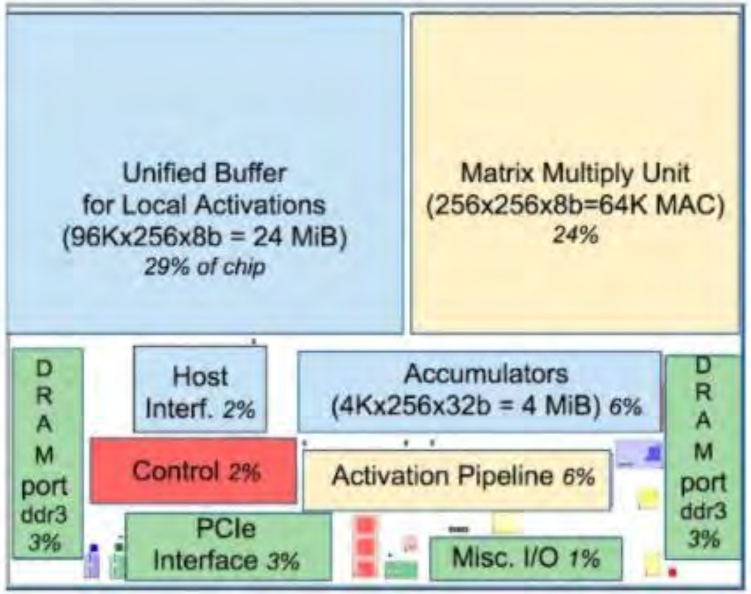
Xilinx FPGA - Advanced Driver Assistance Systems (ADAS) and Autonomous Driving (AD) Modules



Source: https://www.eetimes.com/subaru-replaces-asics-with-xilinx-fpga-for-latest-vision-based-adas/

Tensor Processing Unit (TPU)





Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

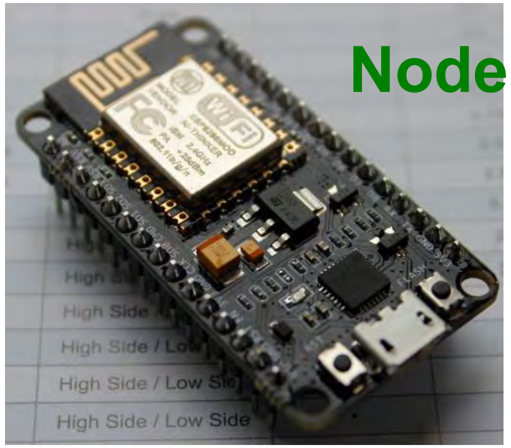
ML Hardware – Cloud and Edge

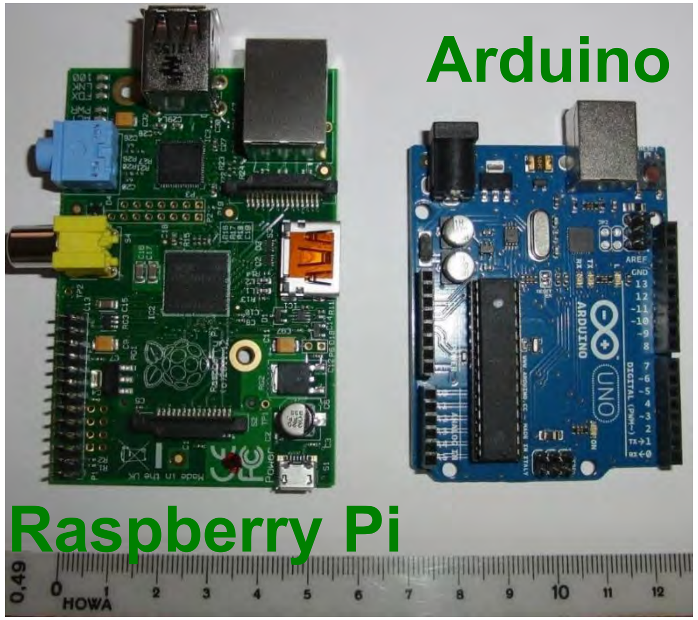
Product	Cloud or Edge	Chip Type
Nvidia - DGX series	Cloud	GPU
Nvidia - Drive	Edge	GPU
Arm - ML Processor	Edge	CPU
NXP - i.MX processor	Edge	CPU
Xilinx - Zinq	Edge	Hybrid CPU/FPGA
Xilinx - Virtex	Cloud	FPGA
Google - TPU	Cloud	ASIC
Tesla - AI Chip	Edge	Unknown
Intel - Nervana	Cloud	CPU
Intel - Loihi	Cloud	Neuromorphic
Amazon - Echo (custom AI chip)	Edge	Unknown
Apple - A11 processor	Edge	CPU
Nokia - Reefshark	Edge	CPU
Huawei - Kirin 970	Edge	CPU
AMD - Radeon Instinct MI25	Cloud	GPU
IBM - TrueNorth	Cloud	Neuromorphic
IBM - Power9	Cloud	CPU
Alibaba - Ali-NPU	Cloud	Unknown
Qualcomm AI Engine	Edge	CPU
Mediatek - APU	Edge	CPU

Source: Presutto 2018: https://www.academia.edu/37781087/Current_Artificial_Intelligence_Trends_Hardware_and_Software_Accelerators_2018_

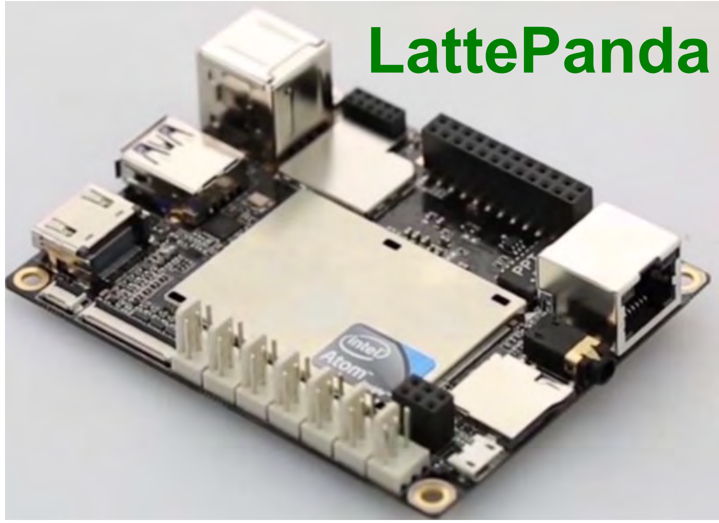
Computing Technology - IoT Platform

Source: https://www.sparkfun.com/products/13678





Source: Mohanty ISCT 2019 Keynote

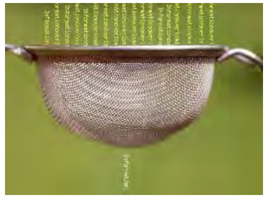


Source: http://www.lattepanda.com

AI Challenges

Challenges of Data in IoT/CPS are Multifold

Data
Curati
on



Data
Cost

Data
Stora
ge

Lots
of
Data

Data
Owne
rship

Data
Model
ing

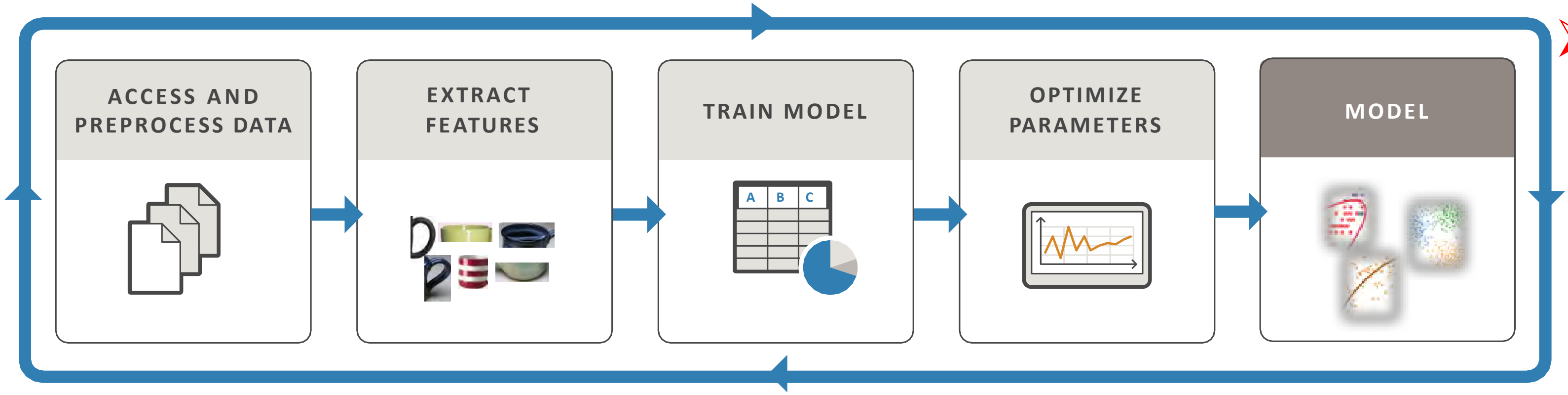
Data
Quality

Machine Learning (ML) Modeling Issues

- Machine Learning Issues
  - High Energy Requirements
  - High Computational Resource Requirements
  - Large Amount of Data Requirements
  - Underfitting/Overfitting Issue
  - Class Imbalance Issue
  - Fake Data Issue

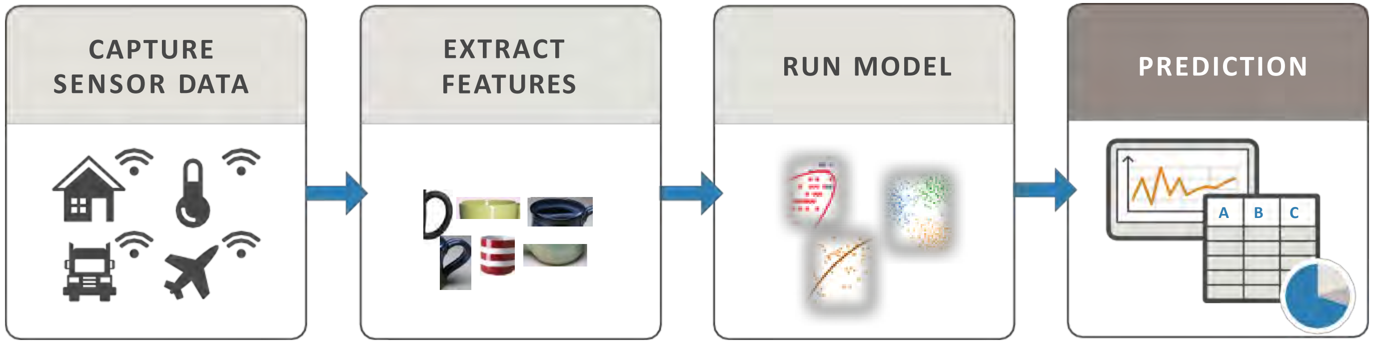
Deep Neural Network (DNN) - Resource and Energy Costs

TRAIN: Iterate until you achieve satisfactory performance.



Needs Significant:
- ➢ Resource
- ➢ Energy

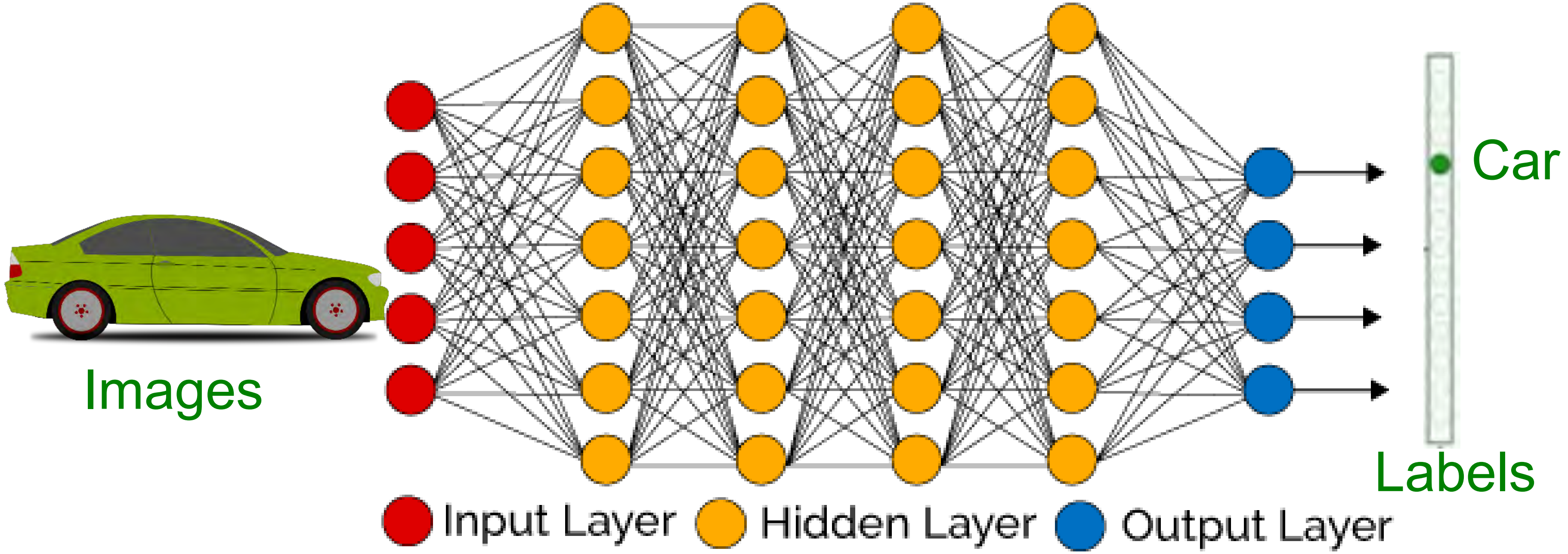
PREDICT: Integrate trained models into applications.



Needs:
- ➢ Resource
- ➢ Energy

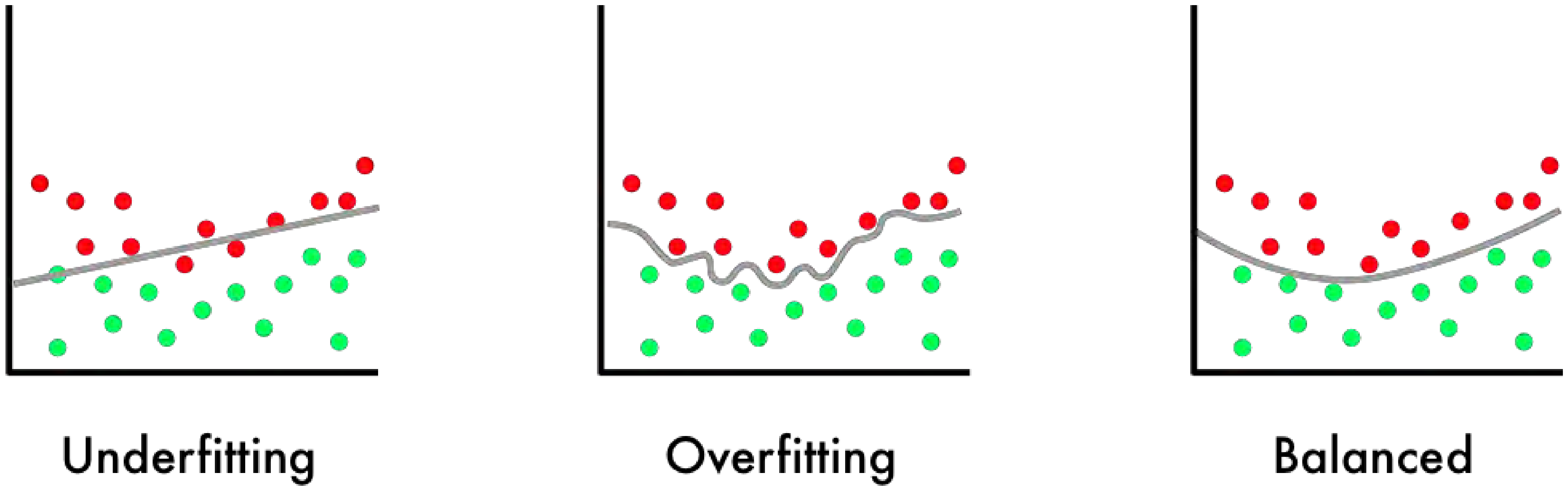
Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

DNN Training - Energy Issue



- DNN considers many training parameters, such as the size, the learning rate, and initial weights.
- High computational resource and time: For sweeping through the parameter space for optimal parameters.
- DNN needs: Multicore processors and batch processing.
- DNN training happens mostly in cloud not at edge or fog.

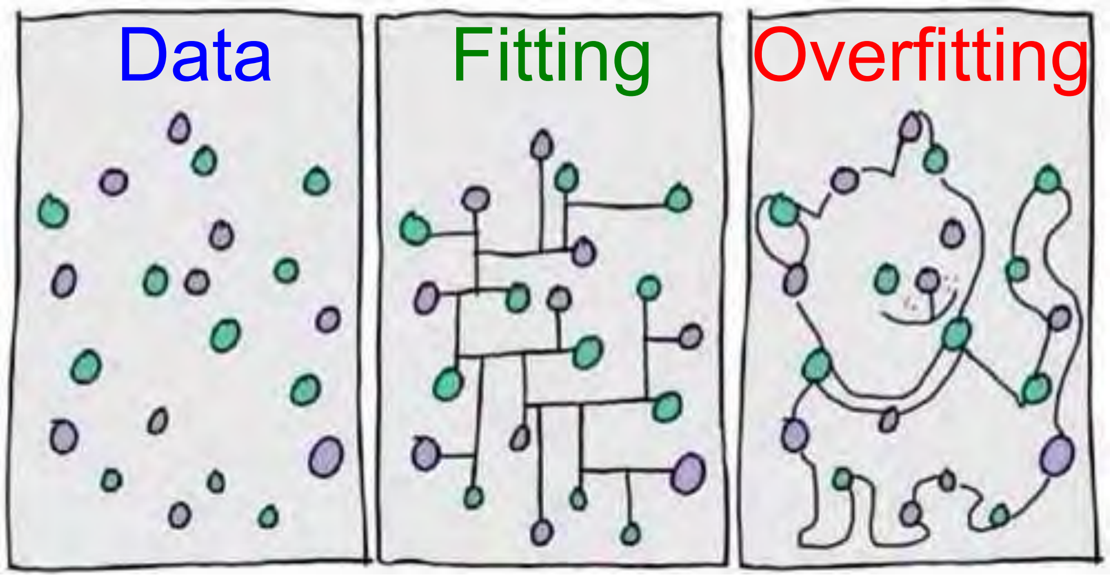
DNN: Underfitting and Overfitting Issues



Source: https://medium.freecodecamp.org/deep-learning-for-developers-tools-you-can-use-to-code-neural-networks-on-day-1-34c4435ae6b

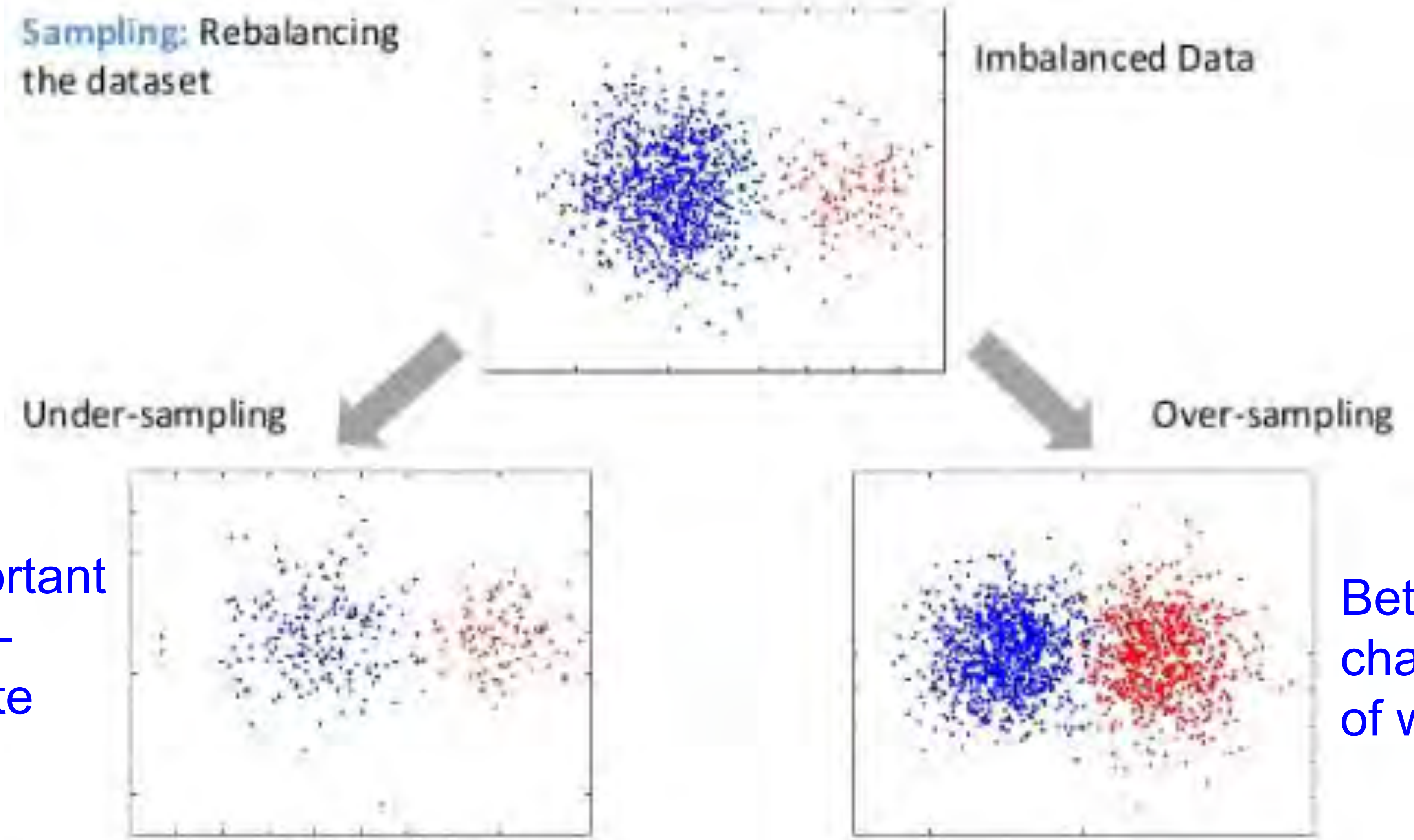
DNN - Overfitting or Inflation Issue

- DNN is overfitted or inflated - If the accuracy of DNN model is better than the training dataset
- DNN architecture may be more complex than it is required for a specific problem.
- Solutions: Different datasets, reduce complexity



Source: www.algotrading101.com

DNN - Class Imbalance Issue



Loss of important information – Less accurate

Better chances of working

Source: https://www.datasciencecentral.com/profiles/blogs/handling-imbalanced-data-sets-in-supervised-learning-using-family

DNN - Class Imbalance Issue - Solutions

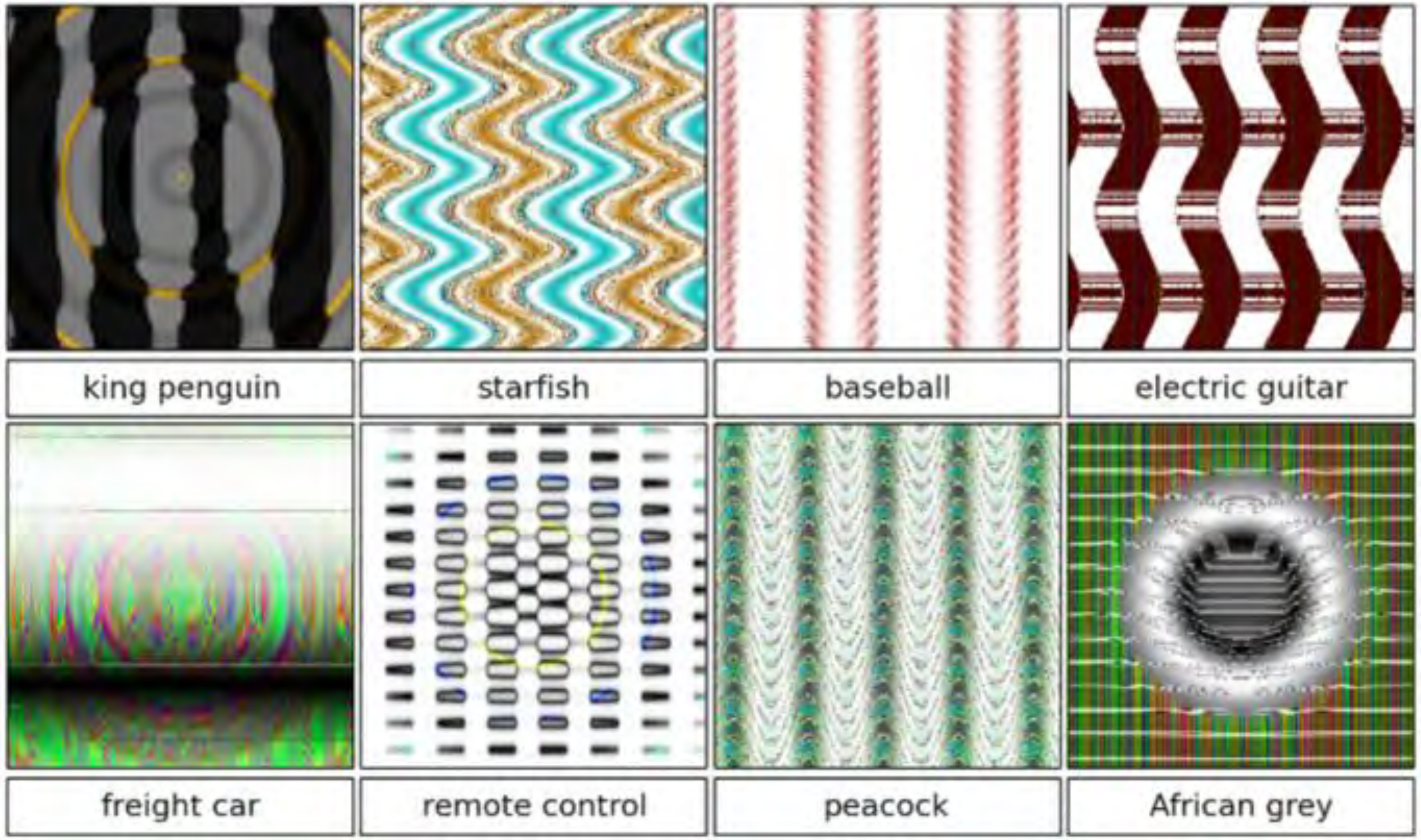
Methods to handle unbalanced data sets

- Exploring different ML algorithms
- Collecting more data
- Modifying class weights
- Penalizing the models
- Using anomaly detection techniques
- Using oversampling techniques
- Using under sampling techniques

Source: https://www.datasciencecentral.com/profiles/blogs/handling-imbalanced-data-sets-in-supervised-learning-using-family

DNNs are not Always Smart

DNNs are not Always Smart

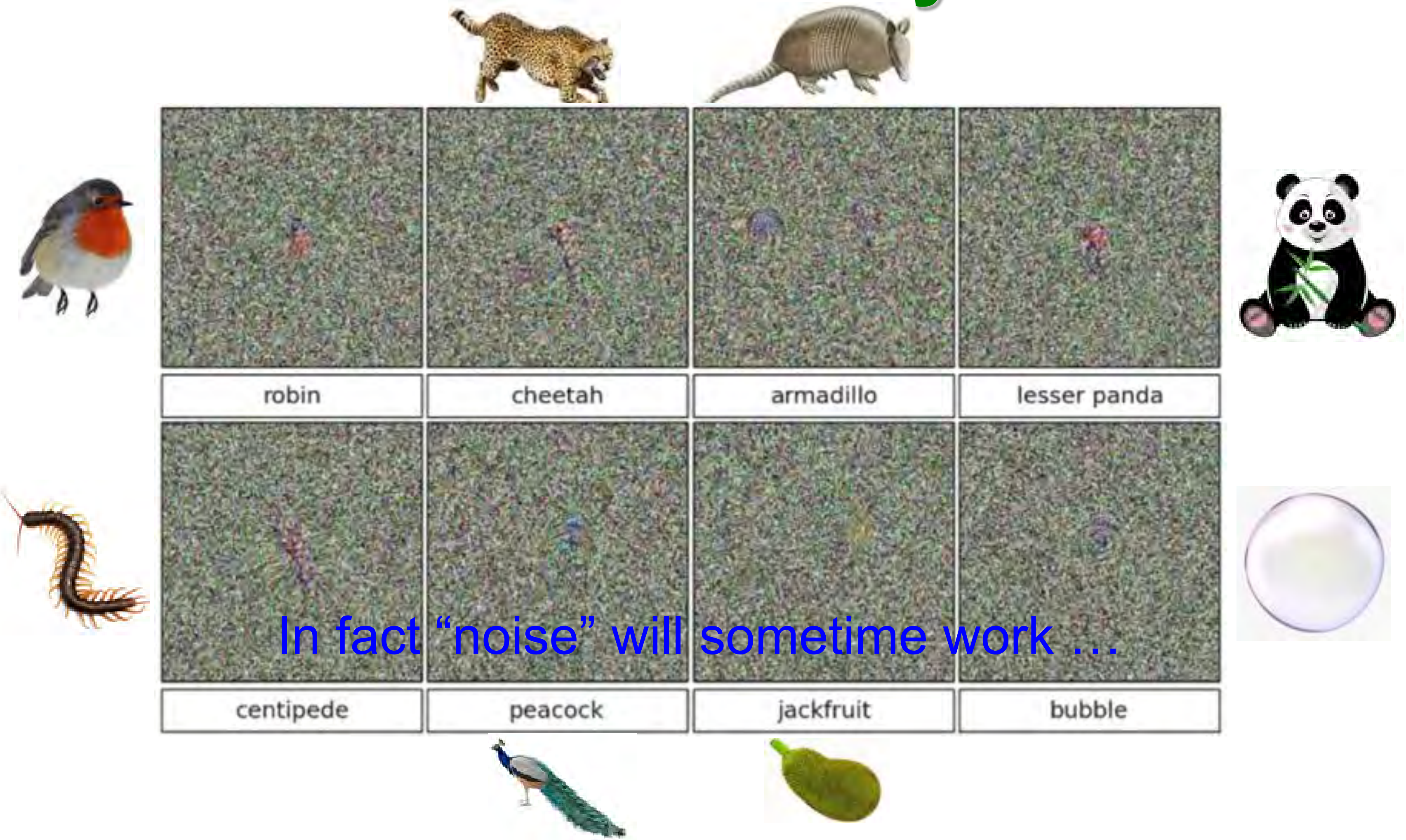


DNNs can be fooled by certain “learned” (Adversarial) patterns …

Source: Nguyen, et al. 2014 - Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

Source: Corcoran Keynote 2018

DNNs are not Always Smart



Source: Nguyen, et al. 2014 - Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

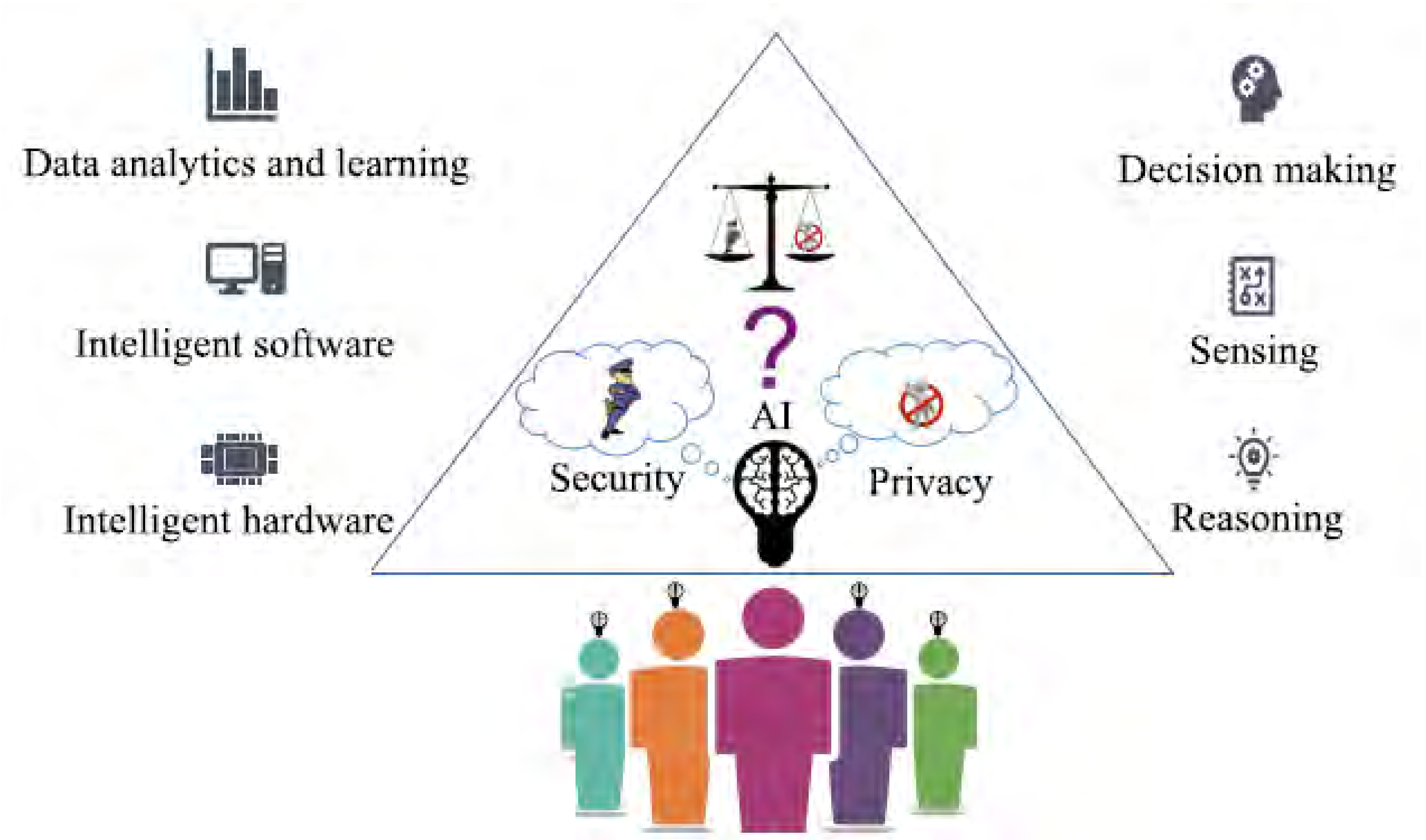
Source: Corcoran Keynote 2018

DNNs are not Always Smart

- Why not use Fake Data?
- "Fake Data" has some interesting advantages:
  - Avoids *privacy issues* and side-steps *new regulations* (e.g. General Data Protection Regulation or GDPR)
  - Significant cost reductions in data acquisition and annotation for big datasets

Source: Corcoran Keynote 2018

Data & Privacy Dilemma in AI

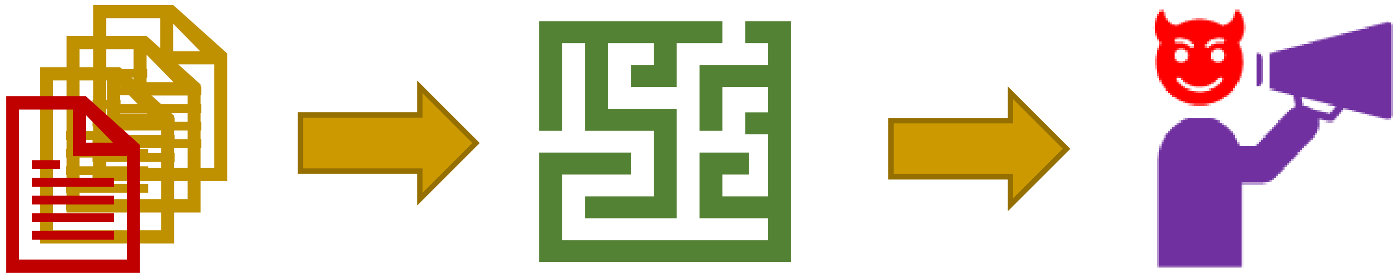


AI/ML - Vulnerability

- Key vulnerabilities of machine learning systems
  - ML models often derived from fixed datasets
  - Assumption of similar distribution between training and real-world data
  - Coverage issues for complex use cases
  - Need large datasets, extensive data annotation, testing
- Strong adversaries against ML systems
  - ML algorithms established and public
  - Attacker can leverage ML knowledge for Adversarial Machine Learning (AML)
    - Reverse engineering model parameters, test data – Financial incentives
    - Tampering with the trained model – compromise security

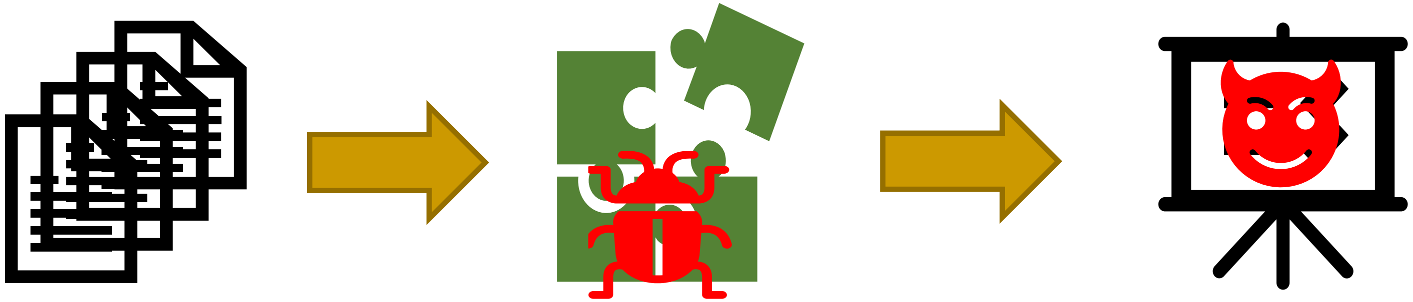
Source: Sandip Kundu ISVLSI 2019 Keynote.

AI/ML – Cybersecurity Issue



Corrupted Input Dataset | Predictive modelling | Corrupted Decision/ Prediction

Input attack in machine learning

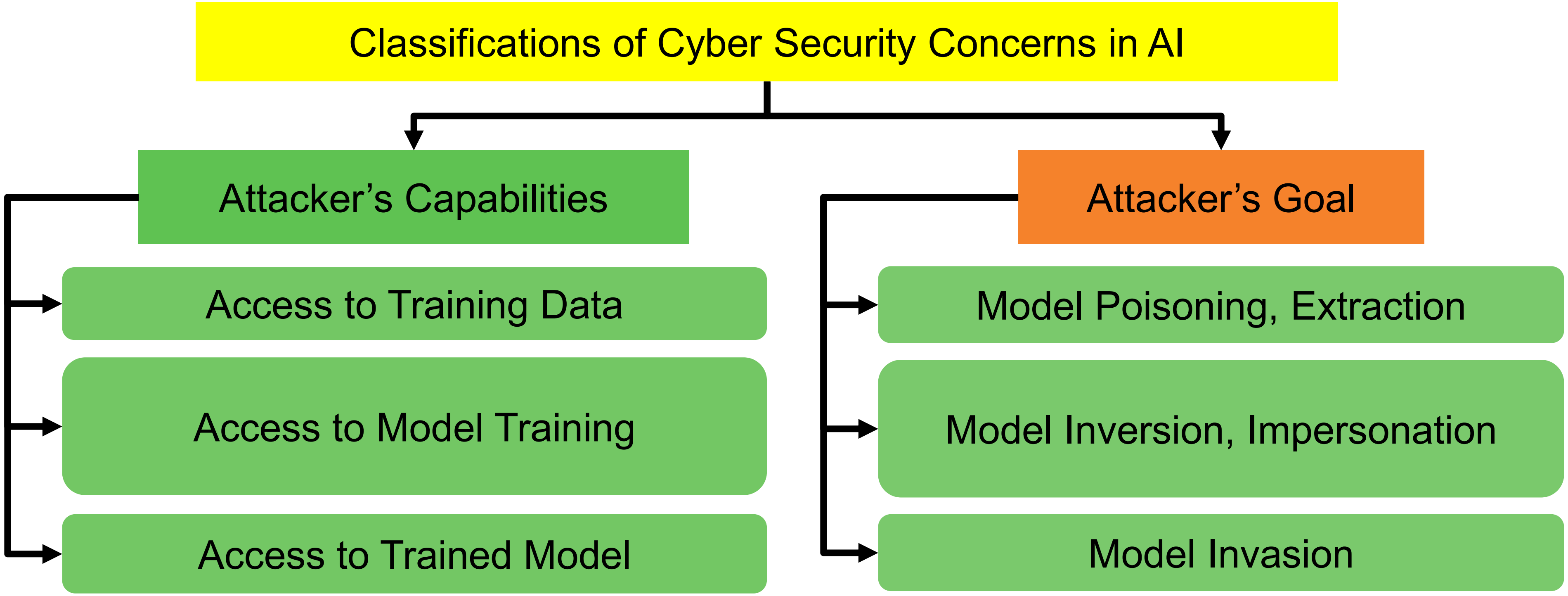


Input Dataset | Attacked training Process | Corrupt Classifications

Poisoning attack in training process

Source: D. Puthal, and **S. P. Mohanty**, "Cybersecurity Issues in AI", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 33--35.

AI/ML – Cybersecurity Issue



Source: D. Puthal, and **S. P. Mohanty**, “Cybersecurity Issues in AI”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 33--35.

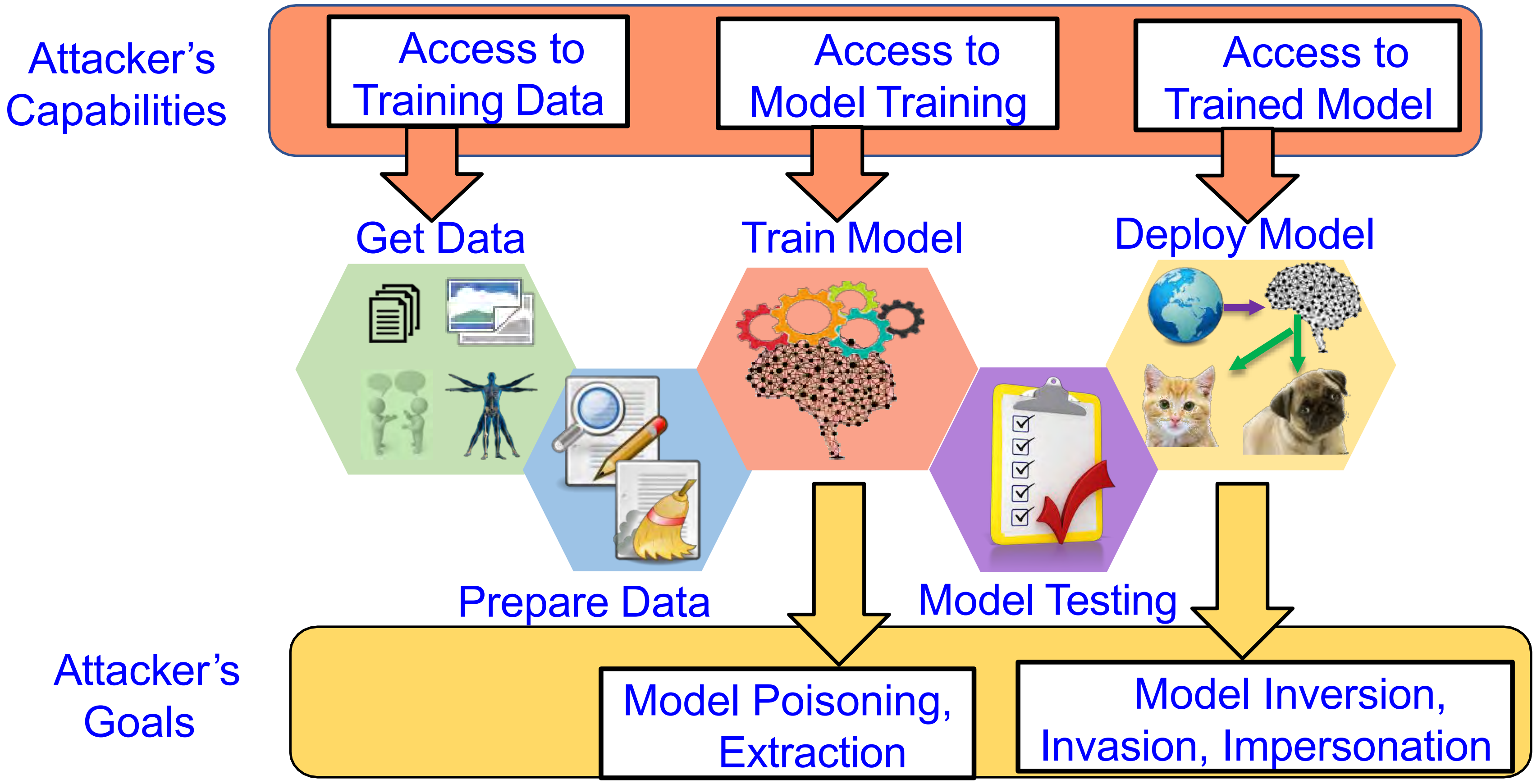
AI/ML Models - Classification of Security and Privacy Concerns

- Attacker’s Goals
  - extract model parameters (model extraction)
  - extract private data (model inversion)
  - compromise model to produce false positives/negatives
- (model poisoning)
  - produce adversary selected outputs
- (model evasion)
  - render model unusable

- Attacker’s Capabilities
  - access to Black-box ML model
  - access to White-box ML model
  - manipulate training data to
- introduce vulnerability
  - access to query to ML model
  - access to query to ML model with confidence values
  - access to training for building model
  - find and exploit vulnerability during
- classification

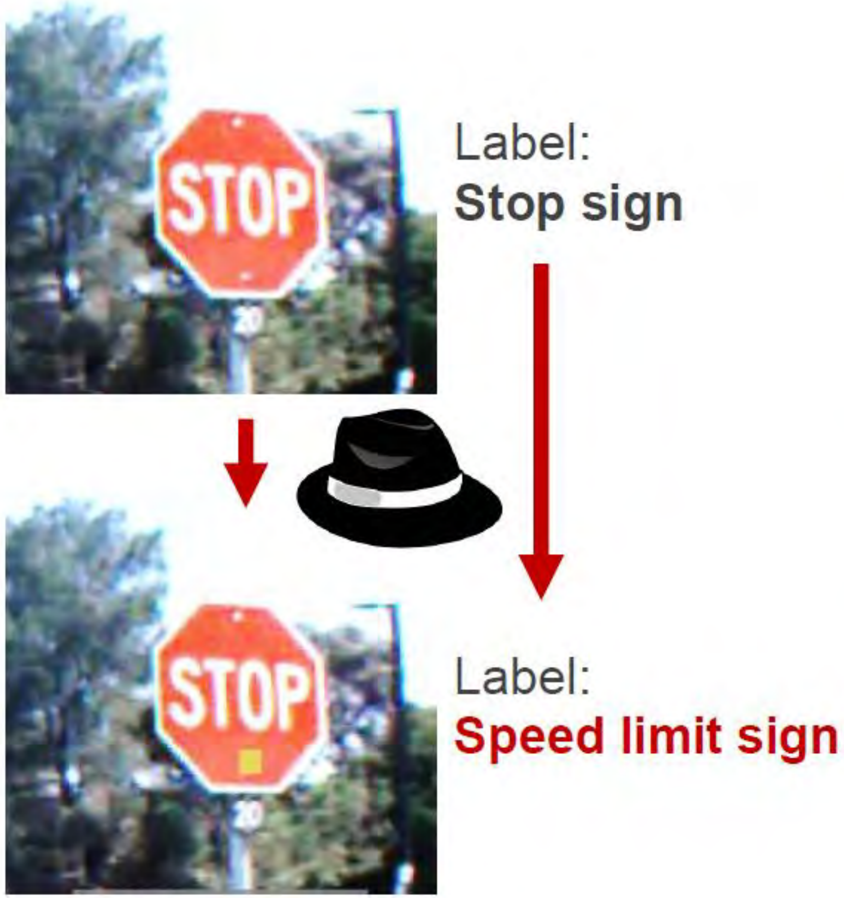
Source: Sandip Kundu ISVLSI 2019 Keynote.

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

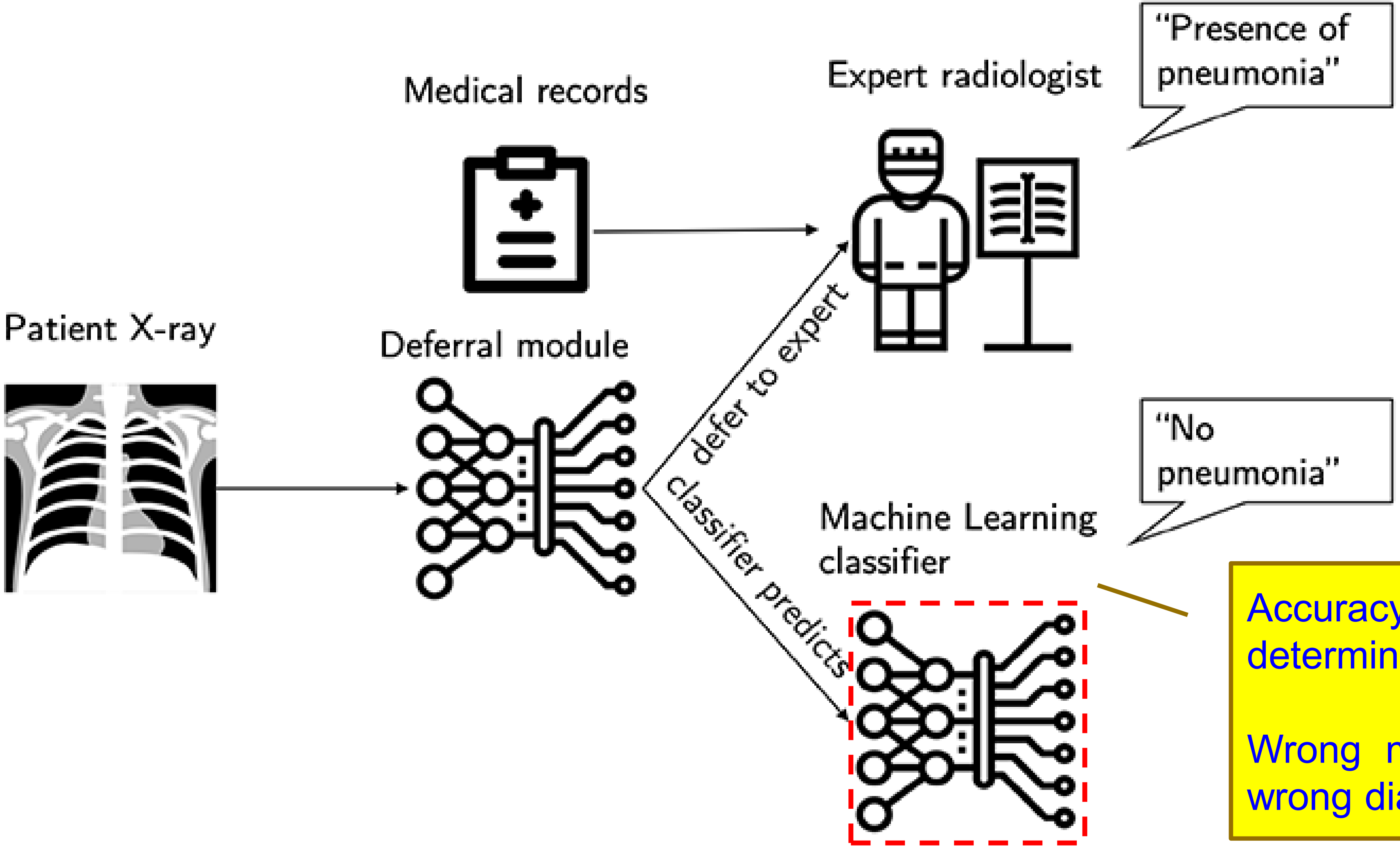
AI Security - Trojans in Artificial Intelligence (TrojAI)



Adversaries can insert **Trojans** into AIs, leaving a trigger for bad behavior that they can activate during the AI's operations

Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

Wrong ML Model → Wrong Diagnosis



Accuracy is important determine pneumonia

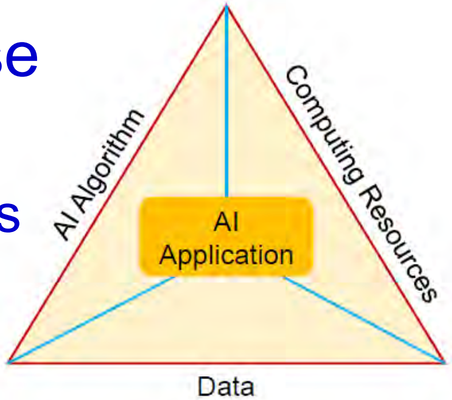
Wrong model can lead to wrong diagnosis altogether

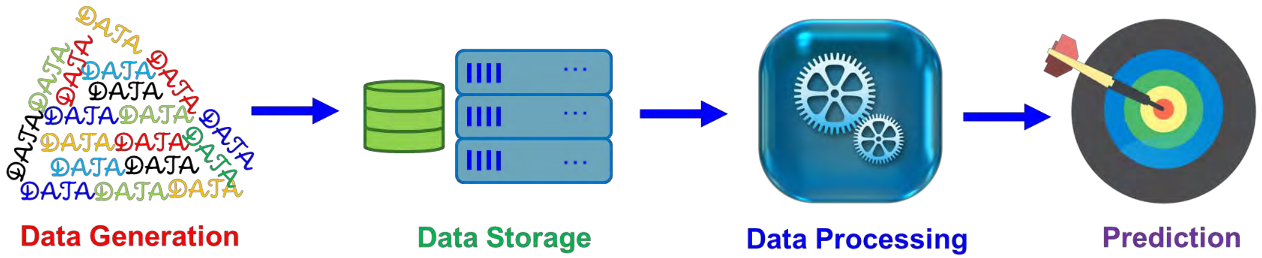
Source: https://www.healthcareitnews.com/news/new-ai-diagnostic-tool-knows-when-defer-human-mit-researchers-say

Data Quality Assurance in IoT Enabled System

Overview - AI & Data

- AI flourished because
  - AI Algorithms
  - Computing Resources
  - Data

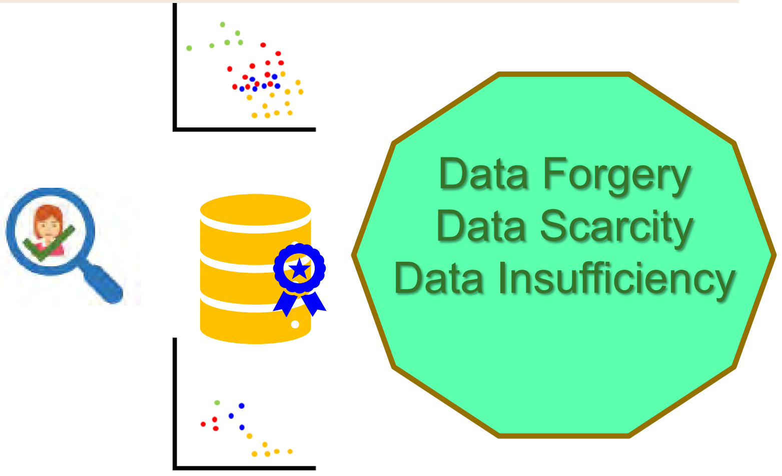




- AI/ ML/ Deep Learning Methods Data Driven.

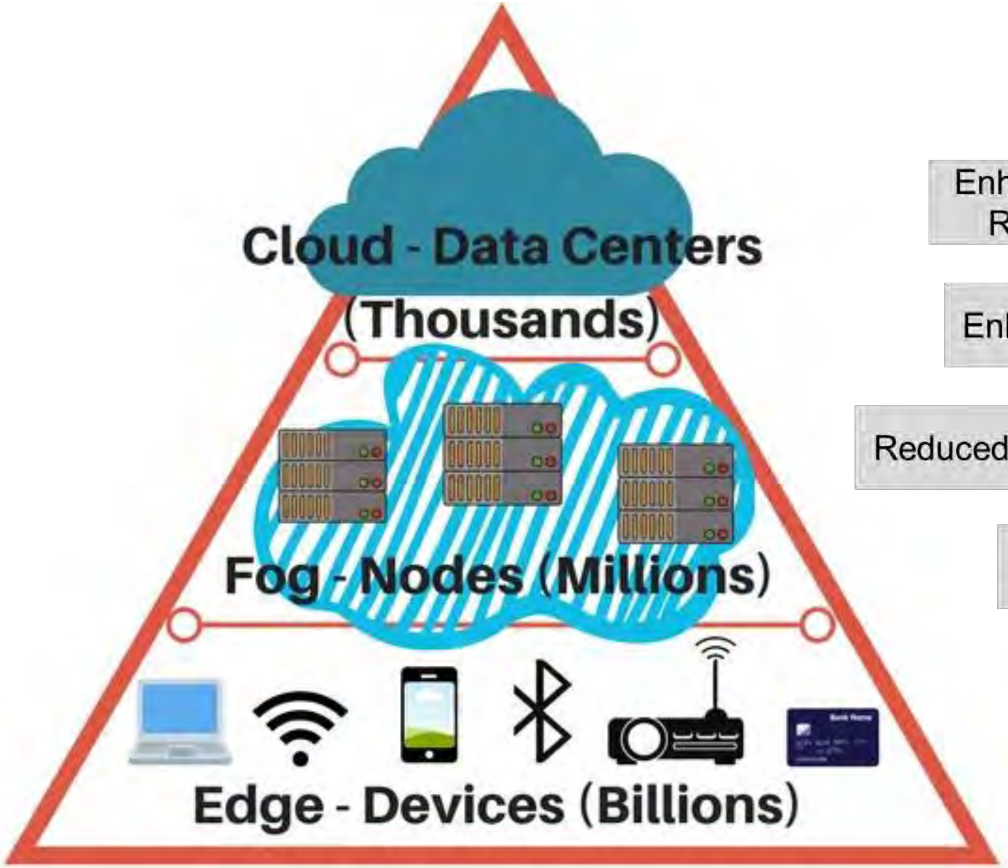
Data Quality = Condition of Qualitative and Quantitative Information in Data

[Source: https://leanbi.ch/en/blog/iot-and-predictive-analytics-fog-and-edge-computing-for-industries-versus-cloud-19-1-2018]



Overview - Computing Platforms

An environment which provides the computation resources to develop, deploy, and manage software, models, and methods.



[Source: https://www.power-solutions.com/industry-trends/fog-computing-and-edge-computing-what-you-need-to-know/]

Pros of Edge Computing Platforms

- Latency Reduction
- Enhanced Services for Remote Locations
- Enhanced Compliance
- Reduced Cost Of Bandwidth
- Less Reliance on WAN Services
- Managed Data Regulation Policies
- Improved Response Time
- Increased Security
- Greater Data Privacy
- Overall Increase In Speed and Efficiency
- Greater Up-time of Critical Systems

Cons of Edge Computing Platforms

- Limited Resource
- Lost Data

Overview - Research Need

- Fake data (especially deepfake) need to be detected.
- Edge friendly deepfake image/video detection system.
- Solutions for Data Scarcity (almost no data) related problem.
- Solutions for Insufficient Data (not enough data) related problem.

Objectives

Contributions

Contribution I - ML/DL Methods for Fake Data Detection on Edge Devices

- Detection of Deepfake Videos [9]
- Detection of Deepfake Images [6]

Contribution II - A Real-Life Application Scenario for Deepfake Image Detection

- iFace [8]
- Deep Morphed Deepfake Image Detection [7]
- iFace 1.1 [3]

Contribution III - DL-based Solution for Data Scarcity Problem on Edge Devices

- eCrop [4]

Contribution IV - Verification of the Effect of Data Insufficiency on Accuracy of a DL Model

- aGROdet [1]

Contribution I - Data Forgery Detection

- Detection of Deepfake Videos [9]

A **high accuracy lower computation** novel method for social media deepfake video detection.

- Detection of Deepfake Images [6]

A ML-based novel method for deepfake image detection at edge device which requires **less than 30 minutes training** time.

Sources:

1) A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, "A Machine Learning based Approach for Social Media Deepfake Video Detection through Key Video Frame Extraction", Springer Nature Computer Science Journal, 2021, Vol. 2, No. 2, Article: 99, 18-pages, DOI: https://doi.org/10.1007/s42979-021-00495-x.
2) Alakananda Mitra, Saraju P. Mohanty, Peter Corcoran, and Elias Kougianos, "EasyDeep: An IoT friendly robust detection method for GAN generated deepfake images in social media", In Proceedings of the 4th IFIP International Internet of Things (IoT) Conference (IFIP-IoT), 2021, DOI: https://doi.org/10.1007/978-3-030-96466-5_14.

Contribution II - Data Falsification Resilience

- Data Falsification – Making robust ID for Smart Cities [3], [7], [8].

A facial authentication-based digital ID for Smart Cities which is **robust against deepfake attack and presentation attack**.

Sources:

1) A. Mitra, D. Bigioi, S. P. Mohanty, P. Corcoran, and E. Kougianos, "iFace 1.1: A Proof-of-Concept of a Facial Authentication Based Digital ID for Smart Cities", IEEE Access Journal, Vol. 10, 2022, pp. 71791–71804, DOI: https://doi.org/10.1109/ACCESS.2022.3187686.
2) Alakananda Mitra, Saraju P. Mohanty, Peter Corcoran, and Elias Kougianos, "Detection of deep-morphed deepfake images to make robust automatic facial recognition systems", In Proceedings of the 19th OITS International Conference on Information Technology (OCIT), 2021, DOI: https://doi.org/10.1109/OCIT53463.2021.00039. (Awarded Best Paper)

Contribution III - Data Scarcity Overcoming

- Data Scarcity - Estimation of Crop Damage due to Natural Causes [4].

An **automatic and highly accurate** DL-based solution for estimation of crop damage due to natural causes at edge devices.

Source: A. Mitra, A. Singhal, S. P. Mohanty, E. Kougianos, and C. Ray, " eCrop: A Novel Framework for Automatic Crop Damage Estimation in Smart Agriculture", Springer Nature Computer Science (SN-CS), Vol. 3, No. 319, 2022, Article: NN, 16-pages, DOI: https://doi.org/10.1007/s42979-022-01216-8.

Contribution IV - Data Insufficiency Overcoming

- Data Insufficiency - Plant Disease Detection & Leaf Damage Estimation [1].

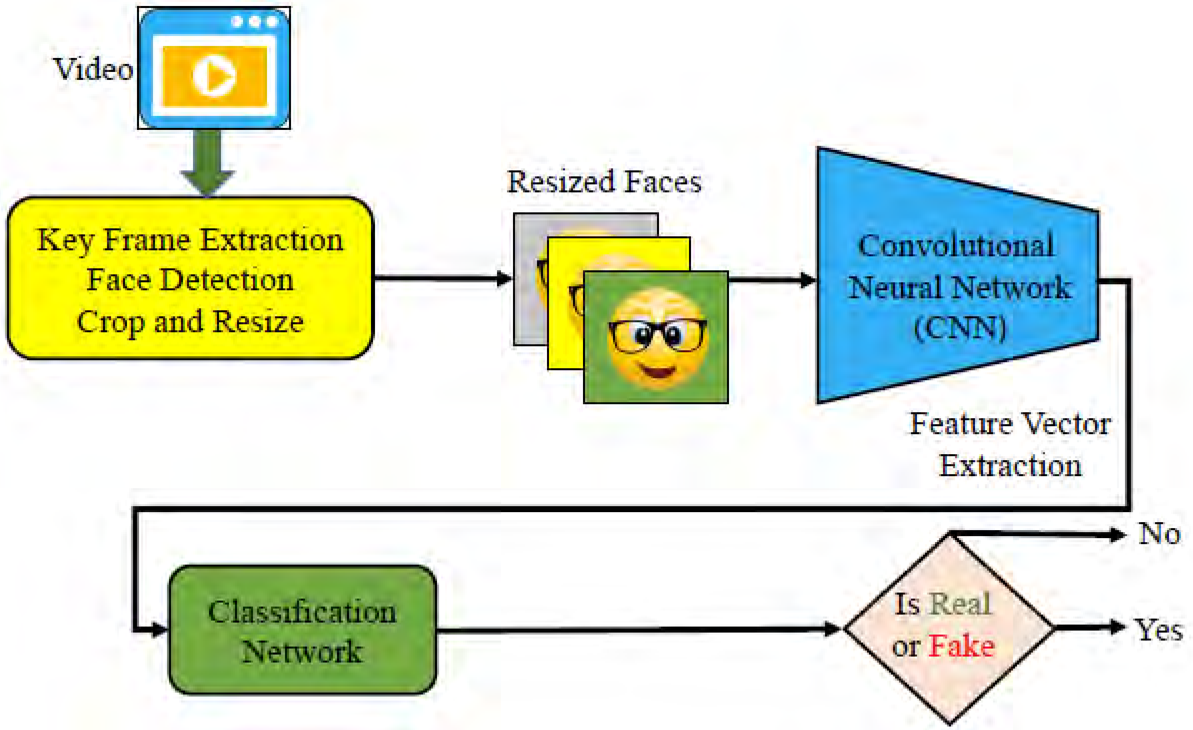
An **automatic and accurate** method for plant disease detection and leaf damage estimation at edge devices to take proper control measures and save time, money, and secondary plant losses.

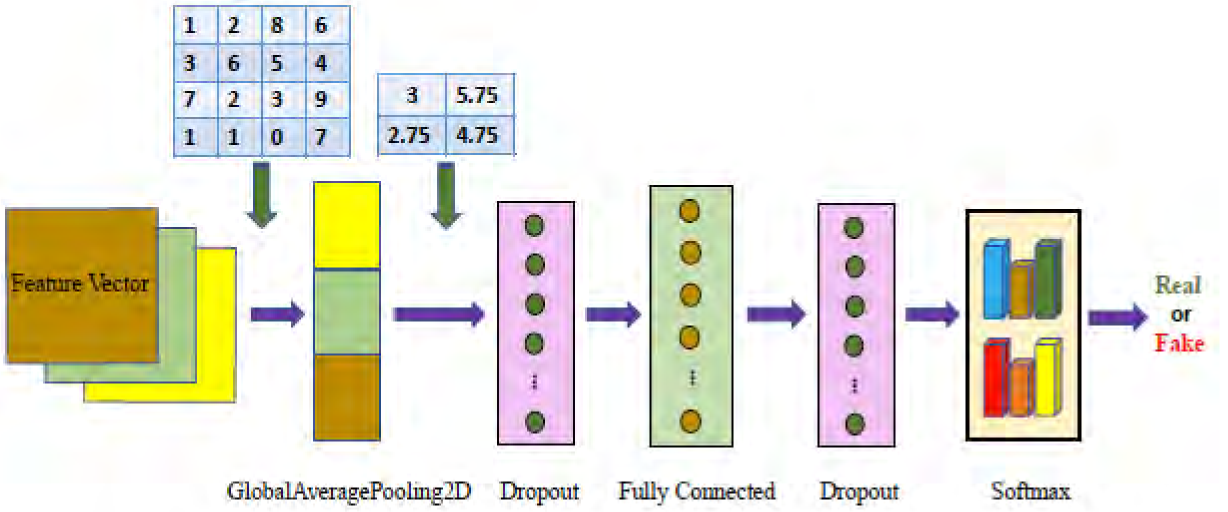
Source: A. Mitra, S. P. Mohanty, E. Kougianos, “aGROdet: A Novel Framework for Plant Disease Detection and Leaf Damage Estimation”, in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 3--22, DOI: https://doi.org/10.1007/978-3-031-18872-5_1.

Fake Data – 'Deepfake'

- **Deepfake = Deep Learning + Fake**
- Created by Deep Learning Networks
  - **Autoencoder**
  - **Generative Adversarial Networks (GANs)**
- Sophisticated Images
- Make Face Morphing Easy and Realistic
- Rampant in Social Media and Websites
- Change the Perception of TRUTH

Social Media Deepfake Video Detection



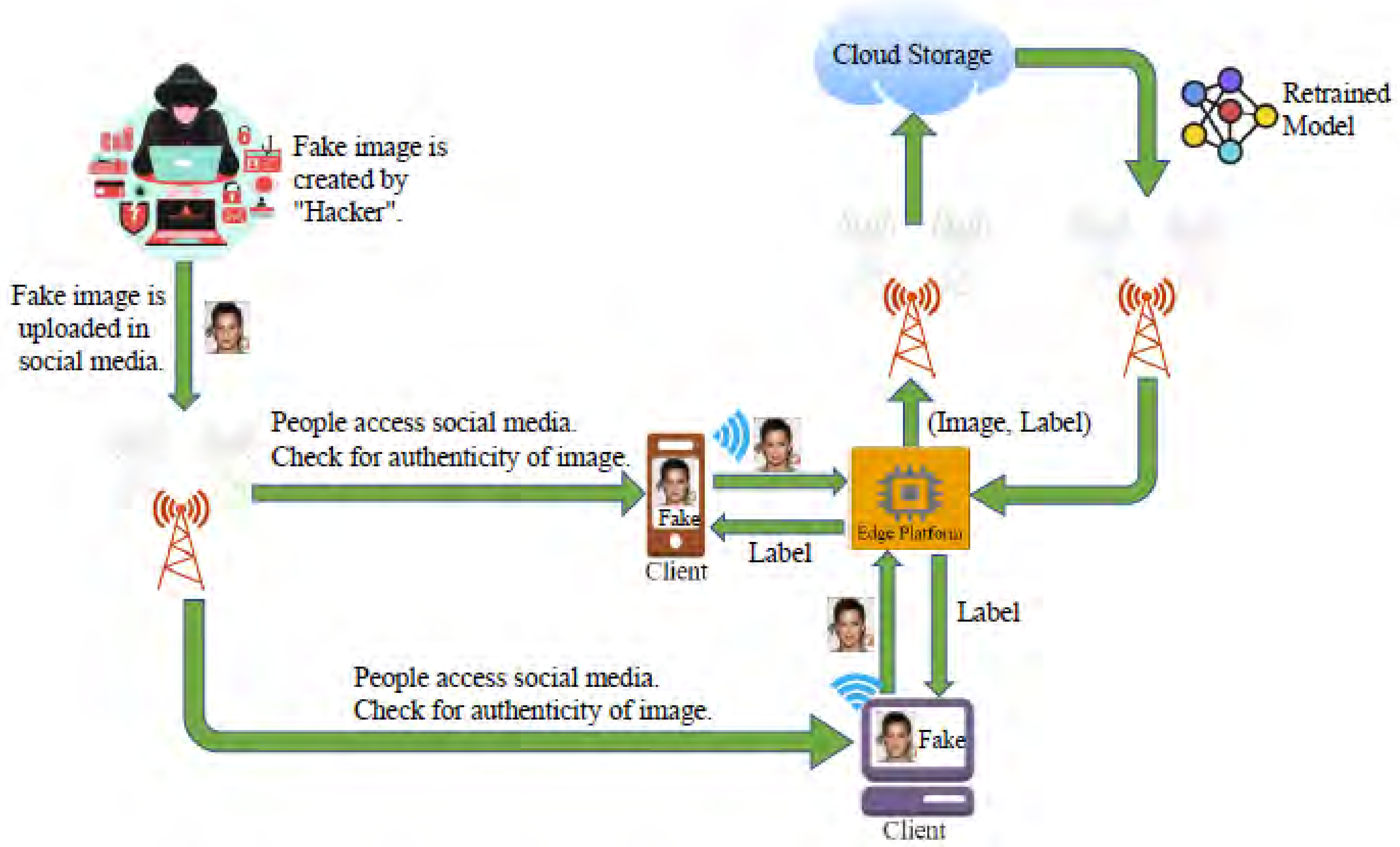


Classifier

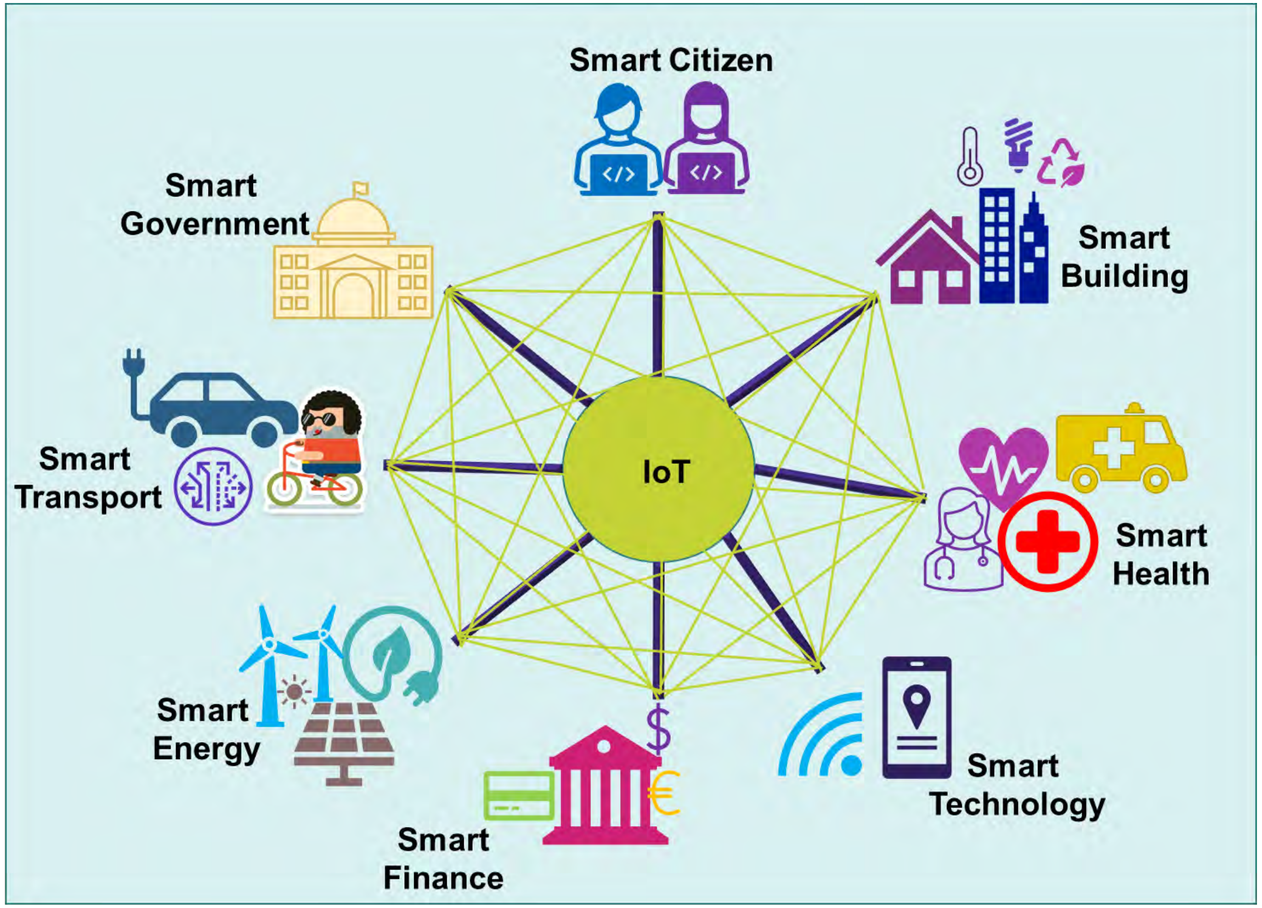
EasyDeep

- GAN Generated Deepfake Image Detection at IoT Platform

EasyDeep: GAN Generated Deepfake Detection



Digital ID Smart City



- Bio-metrics Based
- Person Specific
- Unique
- No Need to Keep Any Secret Key

[Source: Alakananda Mitra, Saraju P. Mohanty, Peter Corcoran, and Elias Kougianos, "iFace: A Deepfake Resilient Digital Identification Framework for Smart Cities", In Proceedings of IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2021, DOI: https://doi.org/10.1109/iSES52644.2021.00090.]

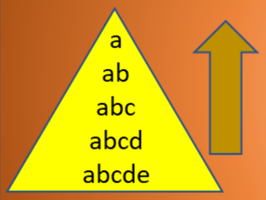
Challenges of Digital ID

Biometrics Based Digital ID

Security

- Data needs to be secured.
- Only authorized person should access and modify it.

Data Abstraction



- Different level of data should be accessed by different authorized people.

Privacy

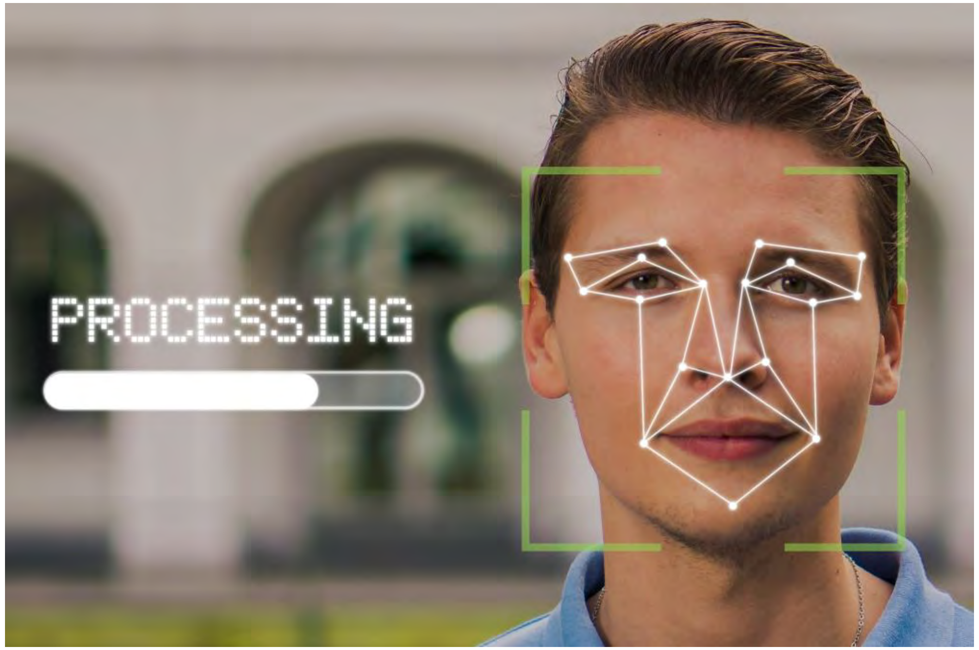
- Personal data needs to be private.
- Only authorized person should access it.

Replacement

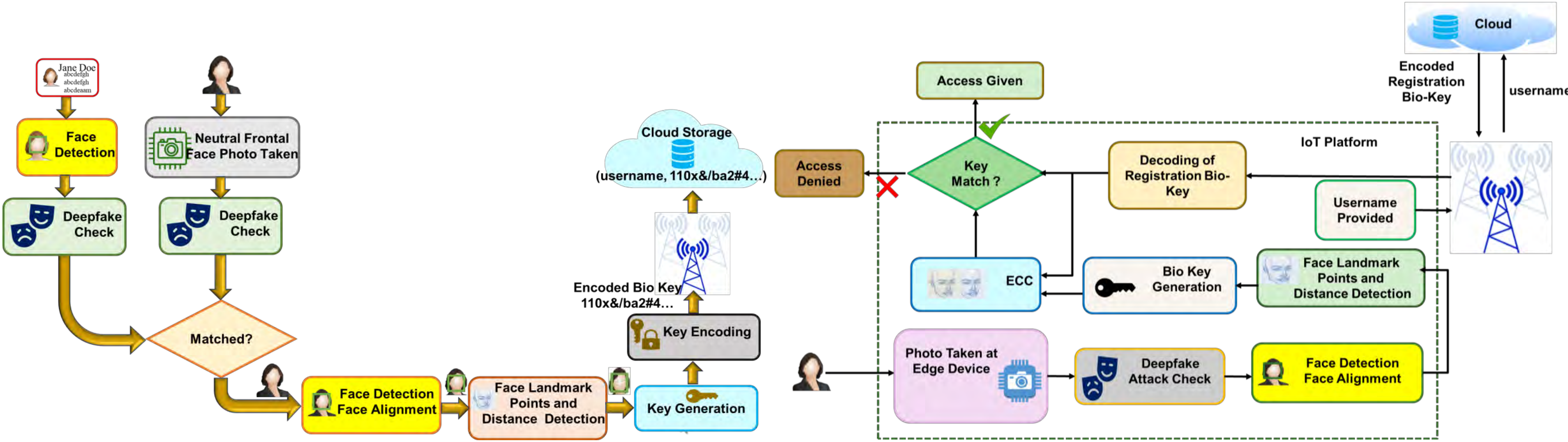
- In case of identity theft new digital id issuance with modified bio-metrics is needed.

iFace : Digital ID System for Smart City

- Facial Biometric Based
- Two Phases
  - Registration Phase
  - Authentication Phase
- Prerequisite
  - Neutral Frontal Face (NFF) Photo
  - Photo Taken at Edge
  - Photo Taken at Each Time



iFace: Registration & Authentication Phases



FEDERATED LEARNING

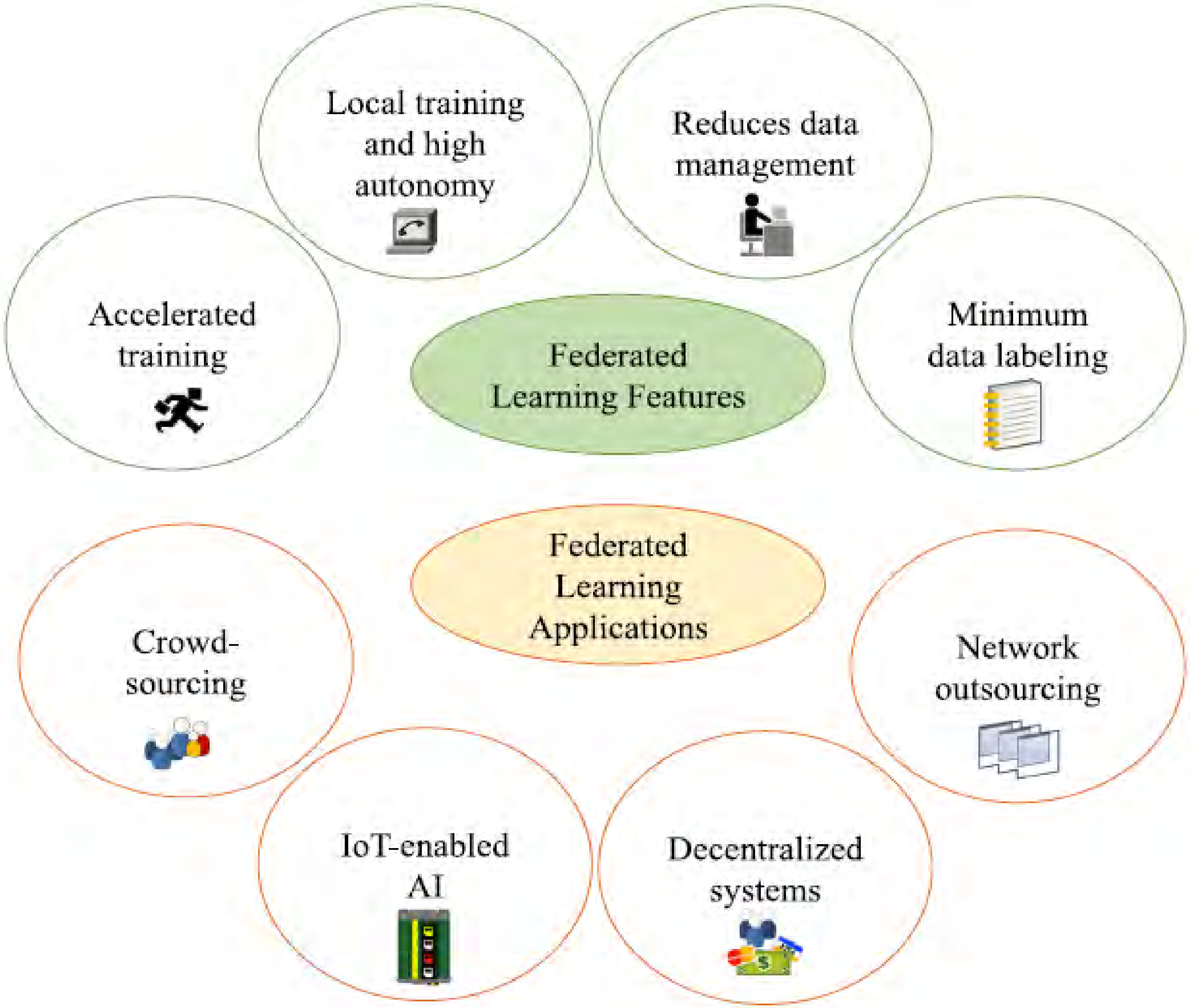
Motivation of Federated Learning (FL)

- Quality data exists at different location on various edge devices.
- Data privacy laws control the movement of data.
- FL is the way to provide ML solution without breaking privacy laws.

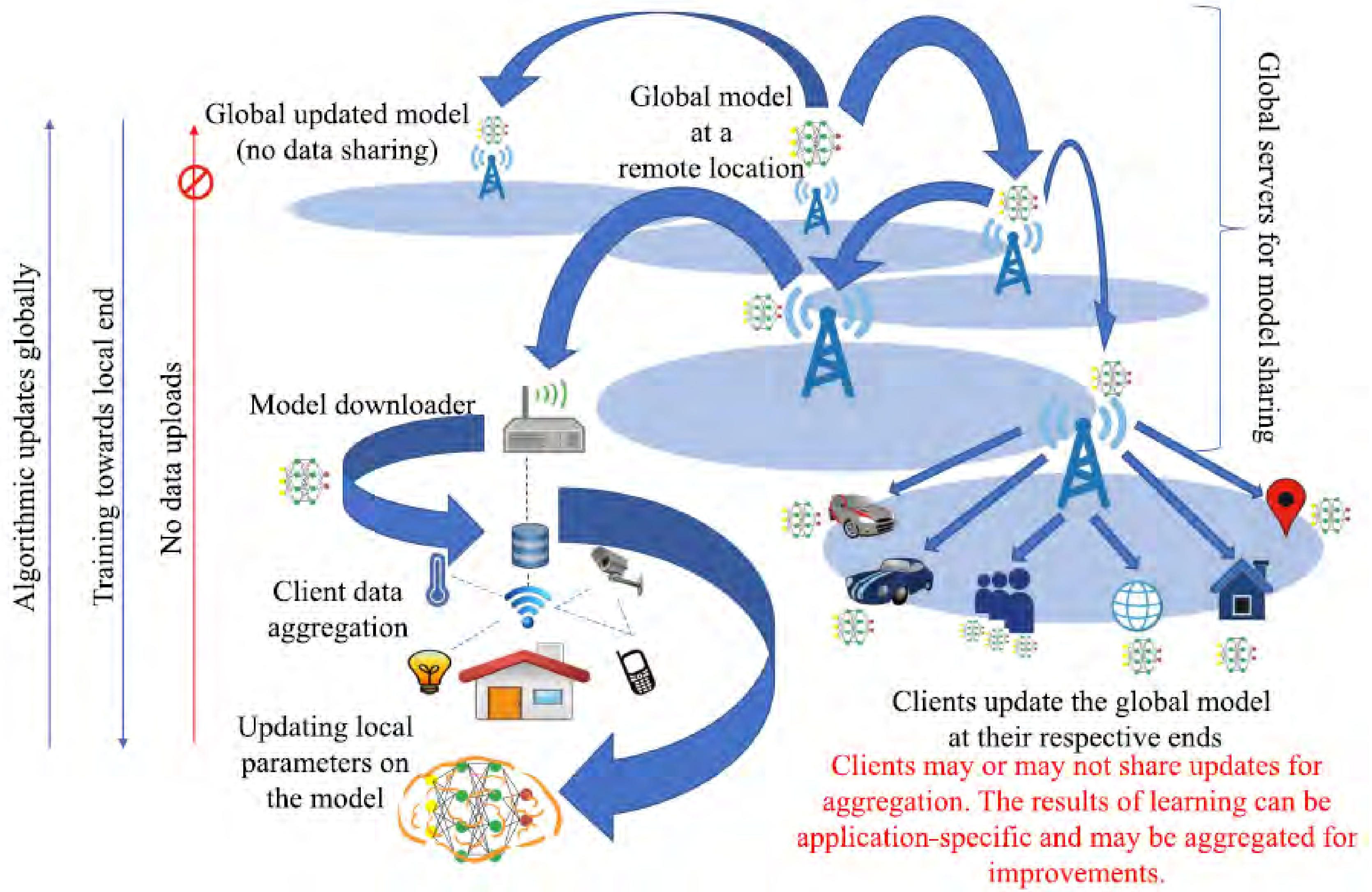
What is FL ?

- Federated Learning is way of model training in ML for heterogeneous and distributed data.
- It preserves the Privacy of data.
- Data does not come to the Model. Here Model is taken to the data.

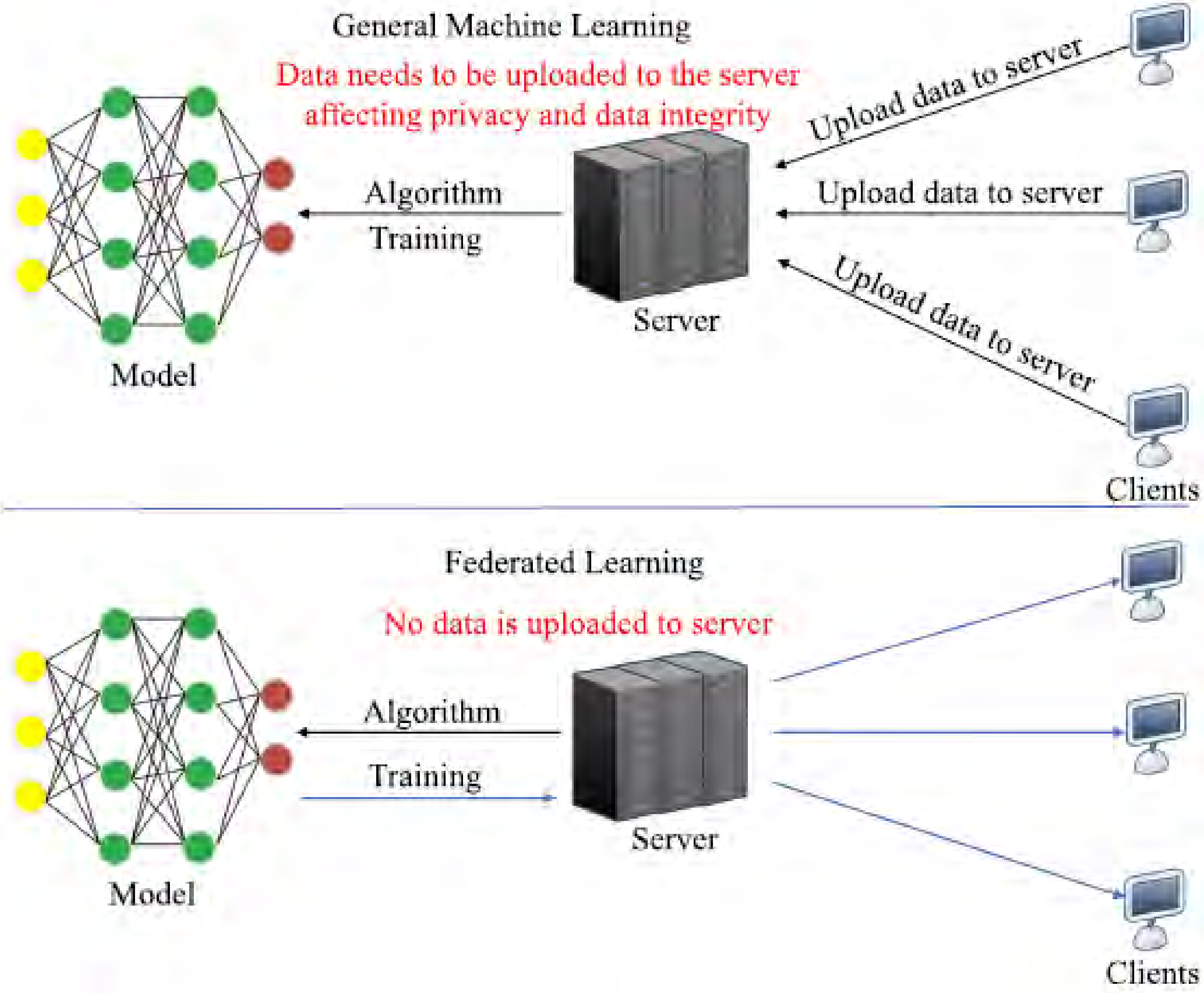
Features & Application of FL



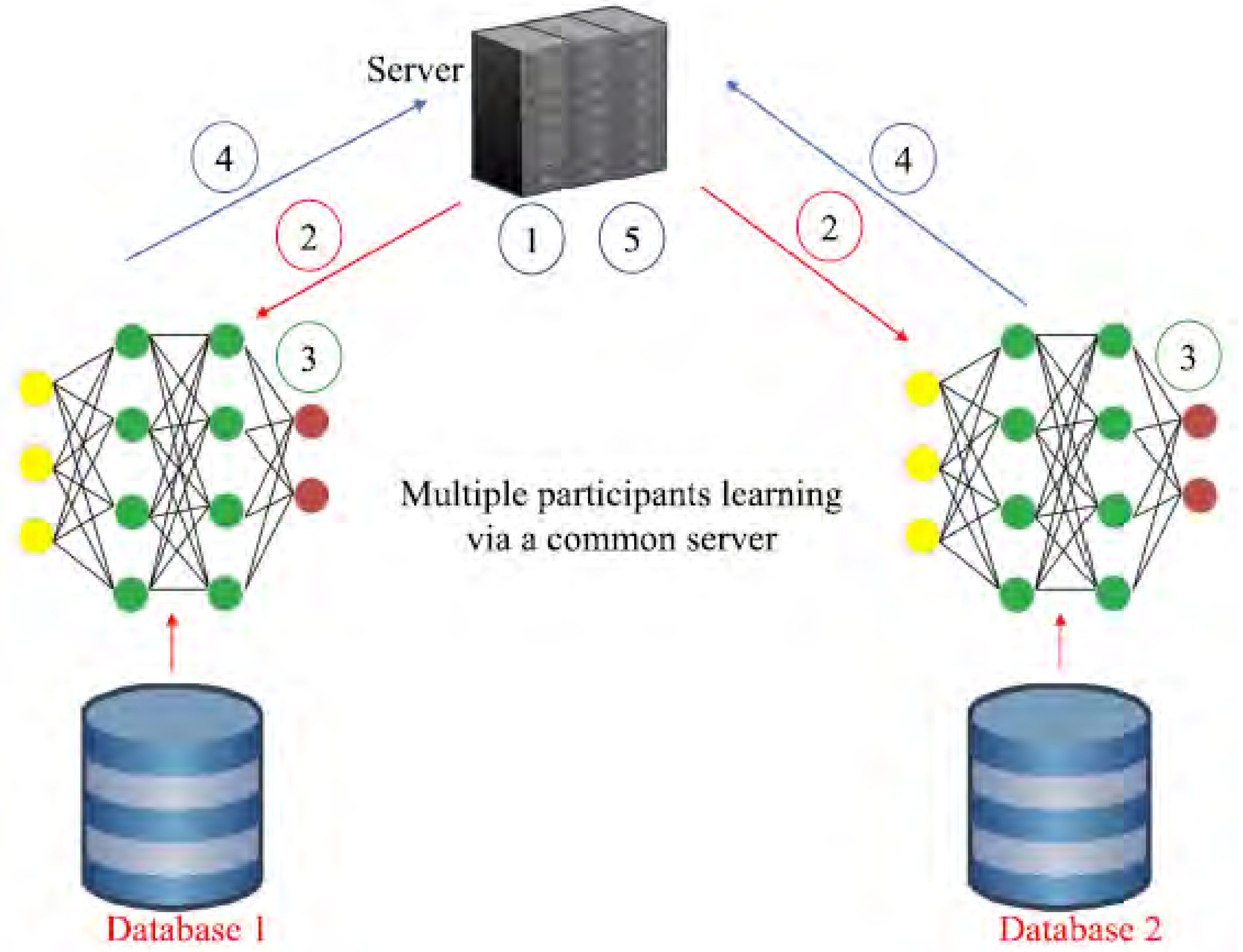
FL In Modern Network



Difference Between ML & FL

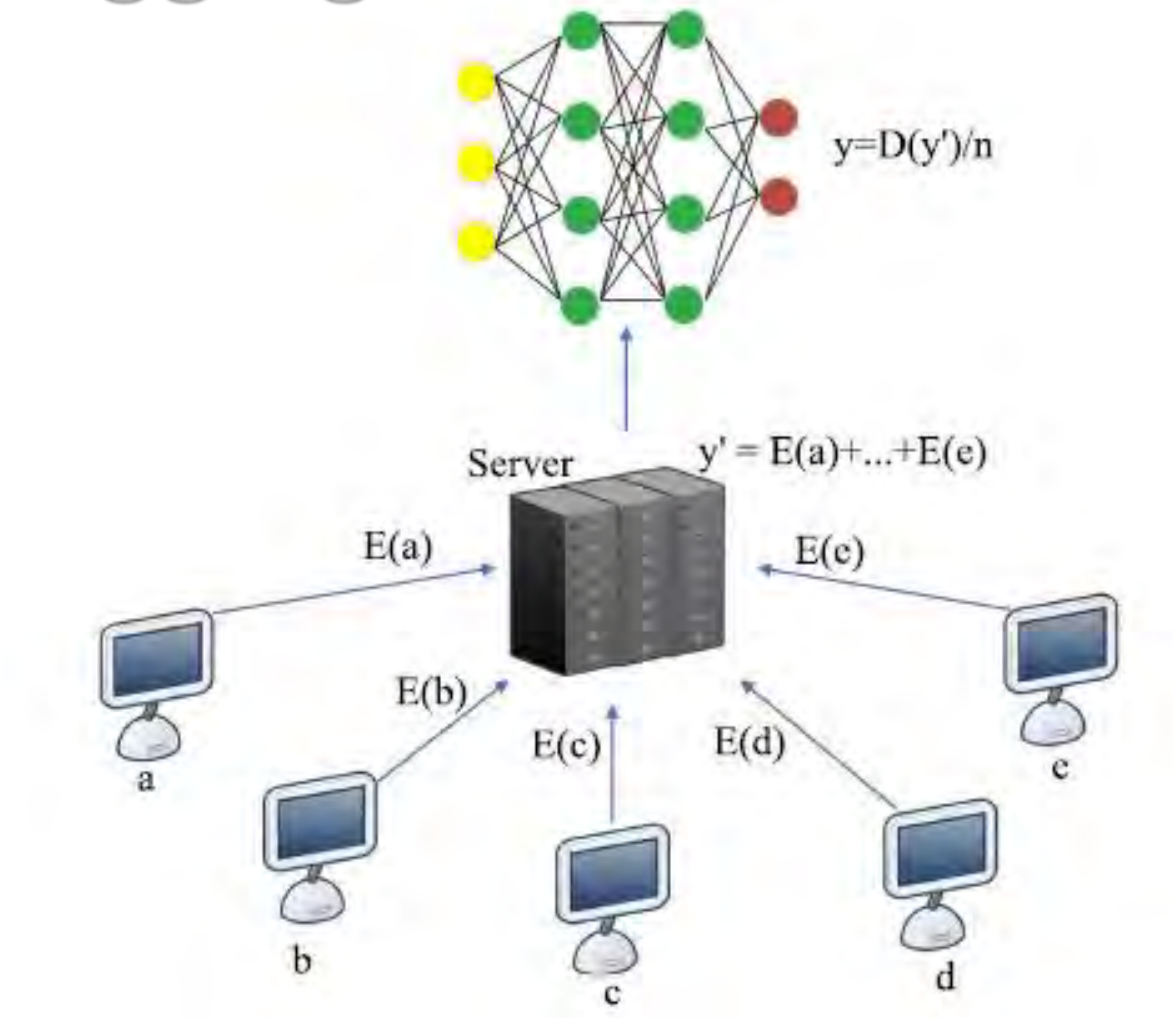


Horizontal FL System



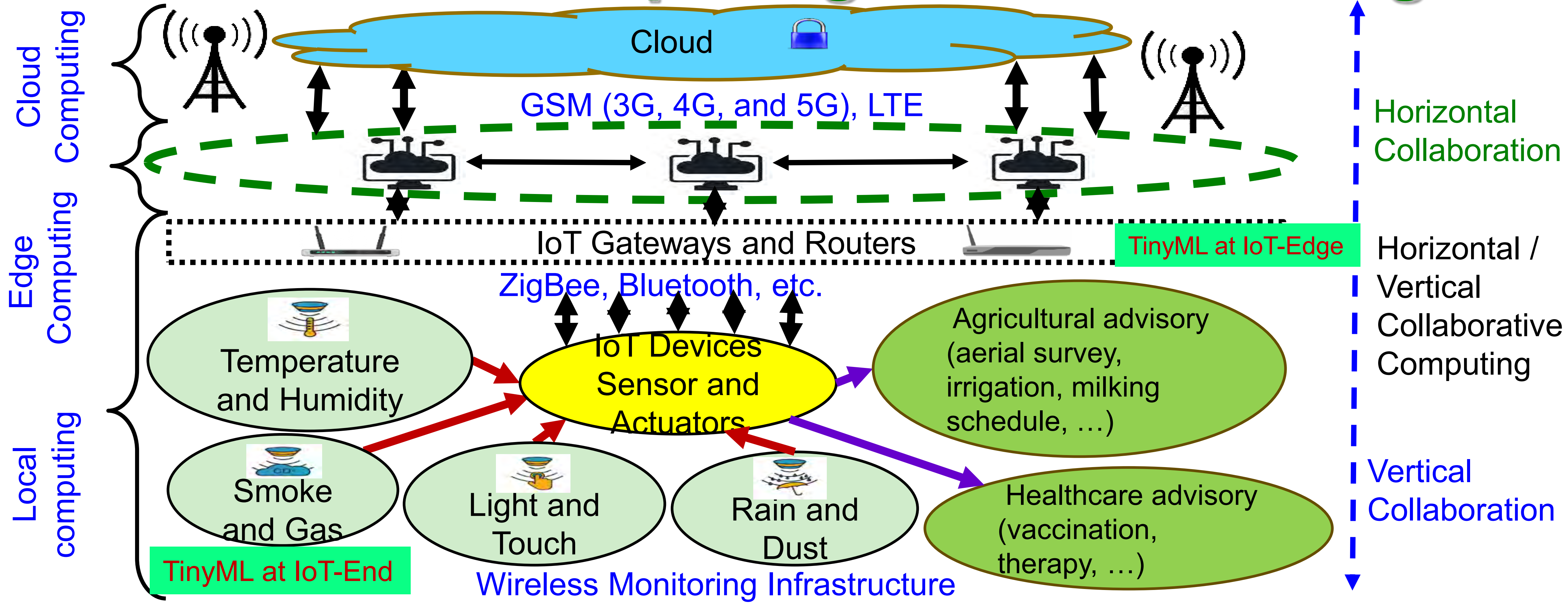
(1) Train global model in the server.
(2) Deploy global model to edge devices.
(3) Optimize model from each edge device.
(4) Upload locally trained model update.
(5) Average the update values and apply the average to the global model.
(6) Repeat step 2 to step 5.

Aggregation of Vertical FL



Homomorphic Encryption

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages

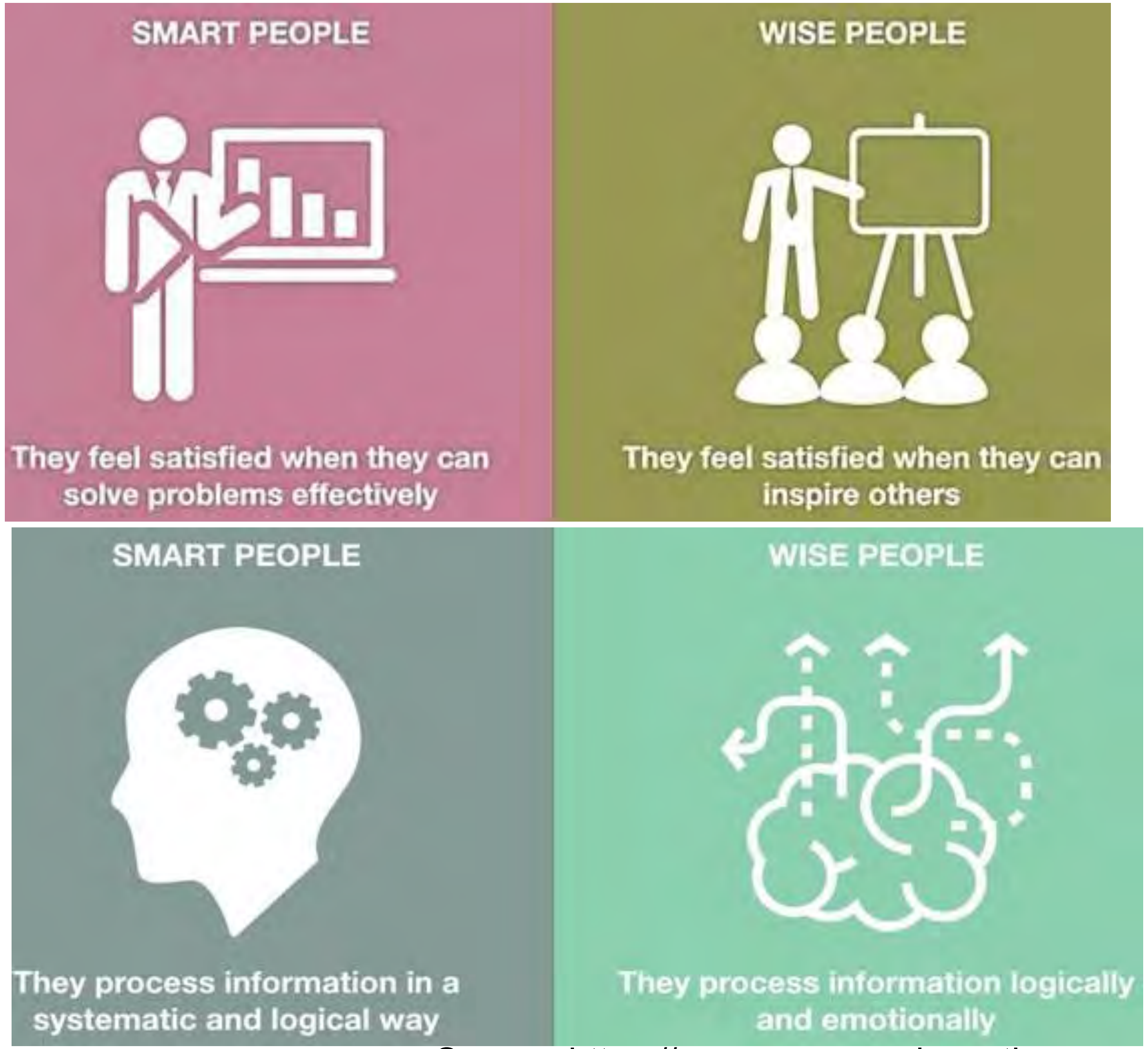


Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, “Collaborative Edge Computing for Smart Villages”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

Conclusion

Does Smart Mean Intelligence?

Does Smart Mean Wise?



Source: https://www.awesomeinventions.com/wise-vs-smart/

Take Away

- What are Artificial Intelligence/Machine learning/ Deep Learning?
- Types of ML Algorithm & DNNs.
- How to make a ML model & DNN pipeline?
- AI Tools
- Evaluation Matrices
- AI Hardware
- Challenges of AI

Conclusion

- Data is the most important factor in AI.
- Data quality needs to be assured.
- Discussed various fake data (image/video) detection method.
- Data privacy in AI is a big challenge.
- FL can be the future direction of AI learning to maintain data privacy.

Future Research Direction

Application Specific

- On-device item ranking
- Next-word prediction
- Content-suggestions
- Privatized data-training
- Secure credit information systems
- Distributed financial data alliance

Basic Research

- Workflow management in FL
- Lightweight training in FL
- Efficient outsourcing in FL
- Secure multiparty computations in FL
- Scalable FL

Future Directions

- Improvements in computing power.
- More AI-enabled chips.
- Progress in GPUs & TPUs.
- Advances in data availability.
- Edge oriented algorithms & Models.
- Improve Healthcare
- Improve IoT devices
- So on.

Key References

- A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, “A machine learning based approach for social media deepfake video detection through key video frame extraction”, *Springer Nature Computer Science Journal*, 2021, vol. 2, no. 2, article: 99, 18-pages, DOI: https://doi.Org/10.1007/s42979-021-00495-x
- Alakananda Mitra, Saraju P. Mohanty, Peter Corcoran, And Elias Kougianos, “EasyDeep: An IoT Friendly Robust Detection Method For GAN Generated Deepfake Images In Social Media”, in *Proceedings Of The 4th FIP International Internet of Things (IoT) Conference (IFIP-IoT)*, 2021.
- Alakananda Mitra, Saraju P. Mohanty, Peter Corcoran, And Elias Kougianos, “iFace: A Deepfake Resilient Digital Identification Framework For Smart Cities”, in *Proceedings of IEEE International Symposium On Smart Electronic Systems (iSES)*, 2021, DOI: Https://Doi.Org/10.1109/Ises52644.2021.00090.
- Z. Li, V. Sharma, and S. P. Mohanty, “Preserving Data Privacy via Federated Learning: Challenges and Solutions”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 3, May 2020, pp. 8--16.