Machine Learning and Deep Learning
Lecture-14

By: Somnath Mazumdar
Assistant Professor
sma.digi@cbs.dk

Overview

- Federated learning
  - Transfer Learning
- Reinforcement learning
- Explainable artificial intelligence

Federated Learning

Federated Learning (FL)

- Google introduced term "federated learning" in 2016.
  - A way to train AI models without anyone seeing or touching user private data.
  - By processing data at their source, FL allows raw data streaming (from sensors).
  - Benefits: Allow to collaboratively train a decentralized model without sharing confidential data.

- Financial Application: Aggregate customer financial records could allow banks to generate more accurate customer credit scores or improve their ability to detect fraud.

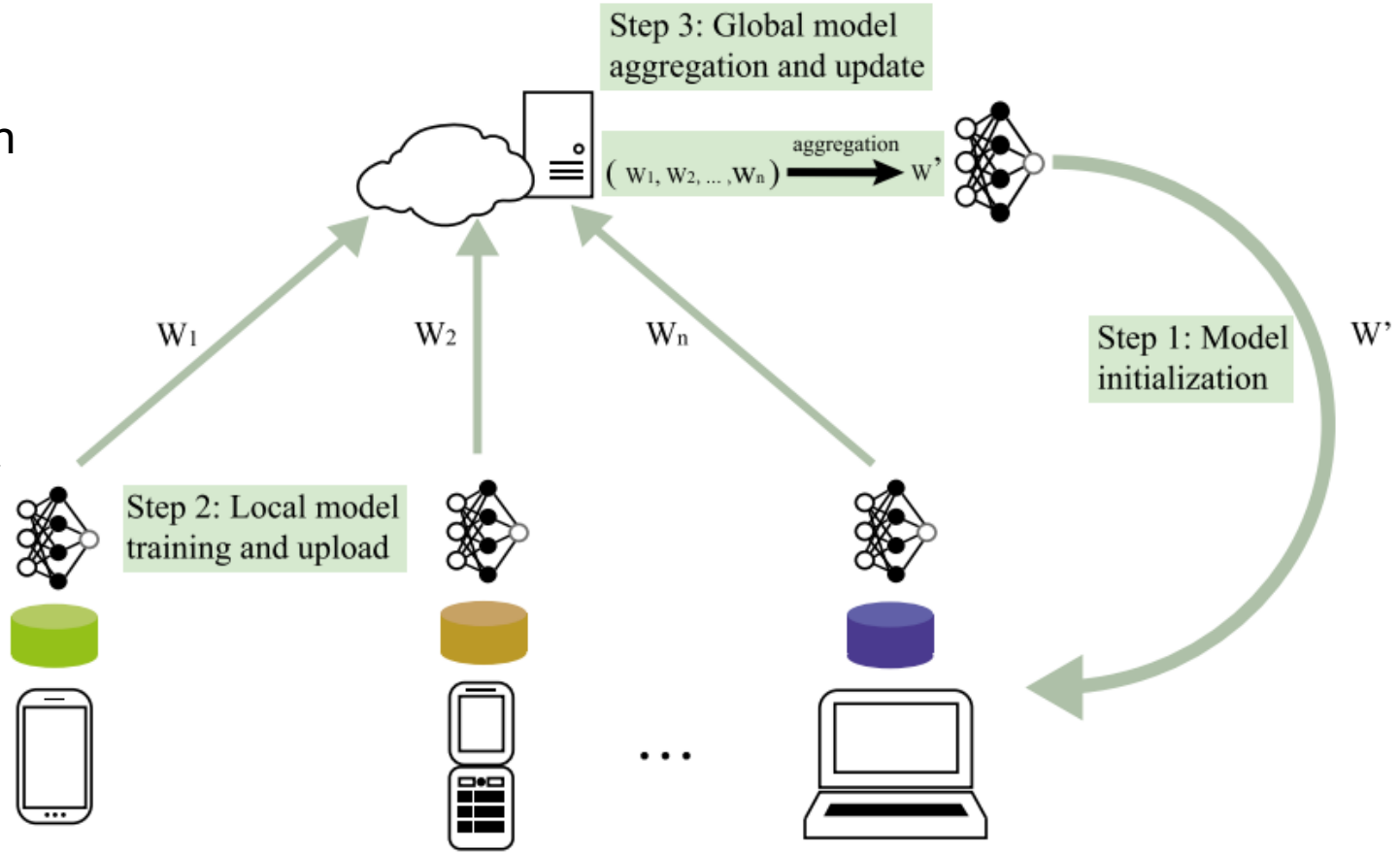
How does FL works?

1. Multiple people remotely share their data to collaboratively train a model.
2. Each party downloads model from a server, usually a pre-trained model.
3. Train it on their private data, then summarize and encrypt model's new configuration.
4. Model updates are sent back to server, decrypted, averaged, and integrated into centralized model.
5. Collaborative training continues (iteratively) until model is fully trained.

https://research.ibm.com/blog/what-is-federated-learning

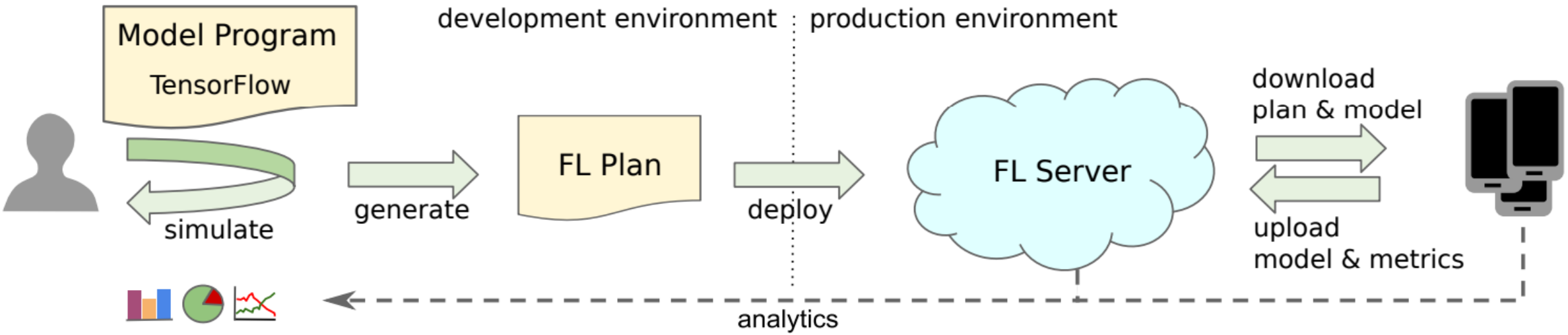
Approach of FL

1. To guarantee data privacy, FL permits all remote devices exchange model gradient with central server.
2. During this process, each distributed devices train their own model with local data.
3. Then they upload local model to central server.
4. After aggregating all gathered models, server returns new global model to each devices.



https://doi.org/10.1016/j.knosys.2021.106775

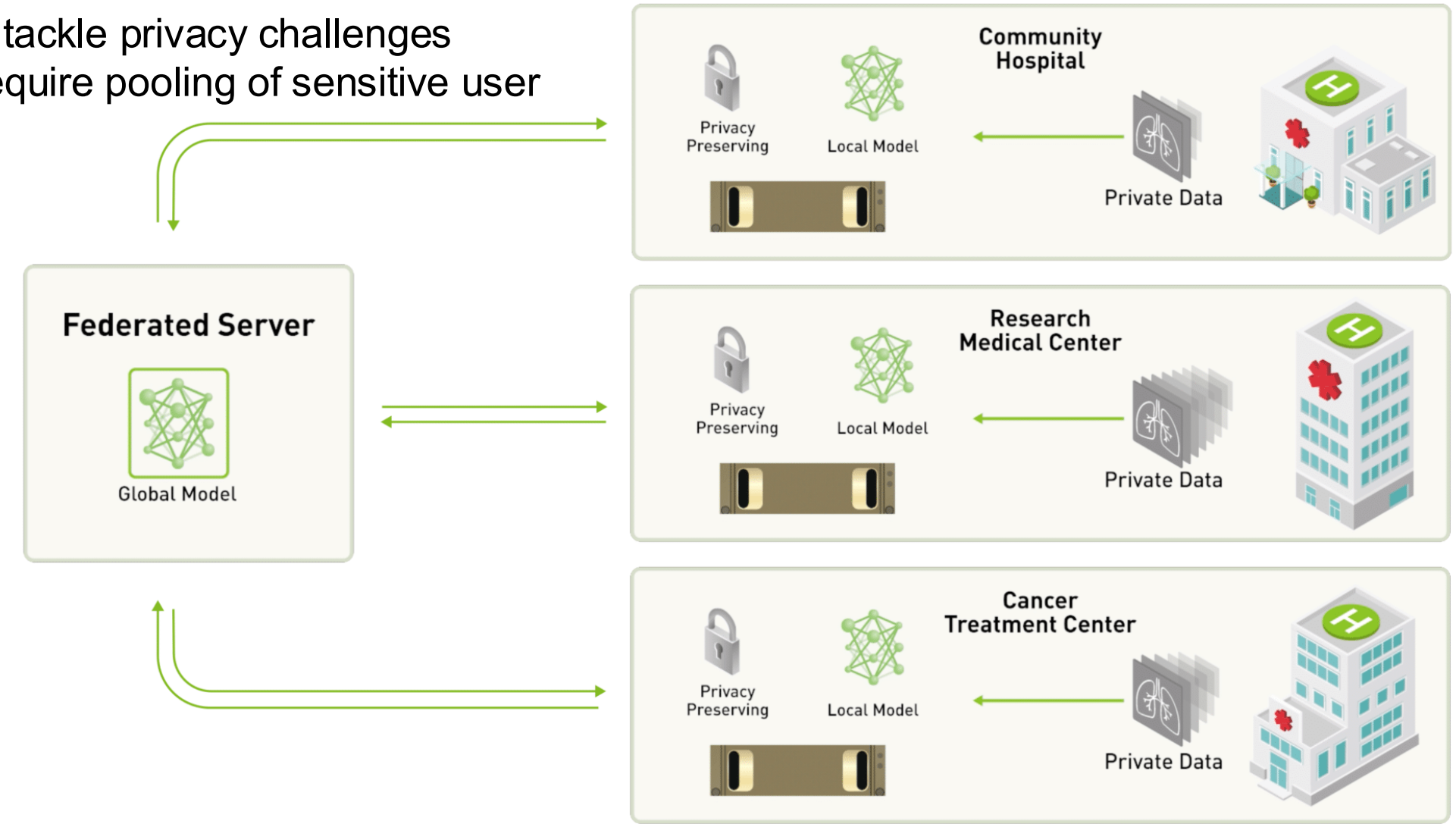
Workflow



https://arxiv.org/pdf/1902.01046.pdf

Centralized-server Approach

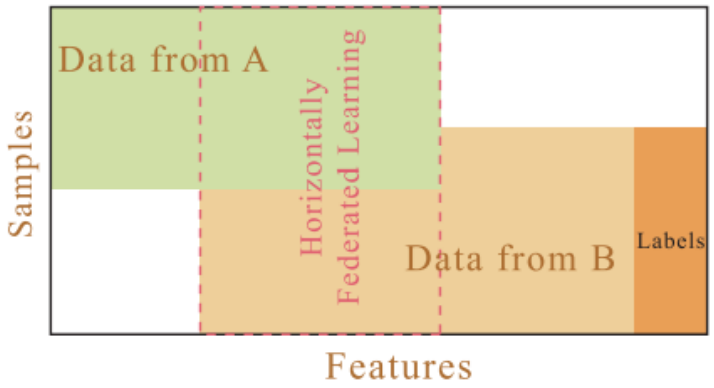
- FL has potential to tackle privacy challenges faced by ML that require pooling of sensitive user data.



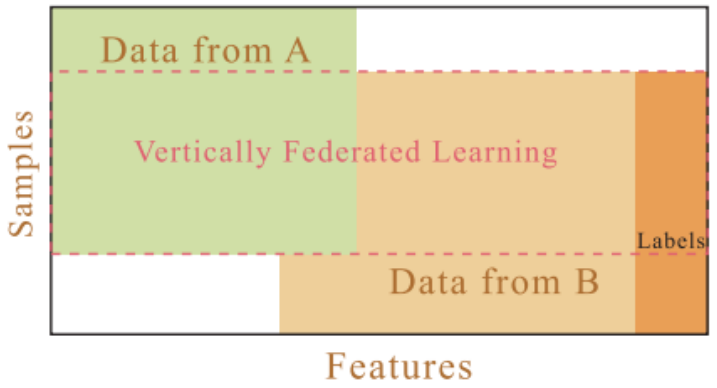
https://blogs.nvidia.com/blog/what-is-federated-learning/

Training Process

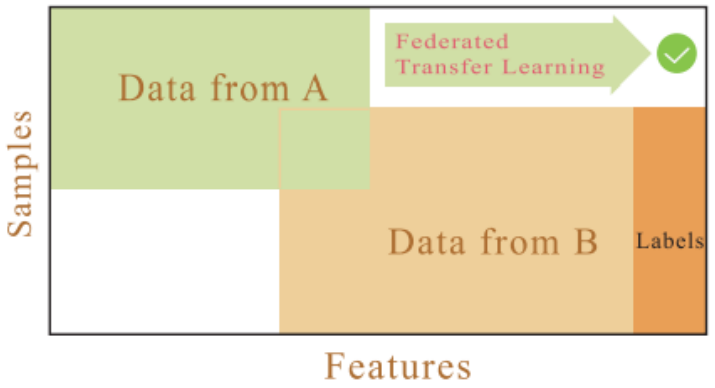
1. Horizontal Learning: Central model is trained on similar datasets.
2. Vertical Learning: Data are complementary.
   - E.g., Movie and book reviews, are combined to predict someone's music preferences.
3. Transfer Learning: Pre-trained foundation model designed to perform one task, (detecting cars), is trained on another dataset to do something else, (identify cats).



(a)Horizontal Federated Learning



(b)Vertical Federated Learning



(c)Federated Transfer Learning

https://research.ibm.com/blog/what-is-federated-learning

Transfer Learning (TL)

- In TL, a model pre-trained on one task is fine-tuned for a new, related task.
- Use TL to retrain existing models on related tasks with new data.
    - For example, if a model can identify images of dogs, it can be trained to identify cats using a smaller image set that highlights the feature differences between dogs and cats.
- Advantage: time and cost savings [NLP, Image processing use case]
- Application: Transfer learning strategies are critical for generative AI adoption in various industries.

https://aws.amazon.com/what-is/transfer-learning/

TL Strategies

- *Transductive transfer learning* involves transferring knowledge from a specific source domain to a related target domain [primary focus]
  - Adv: Little or no labeled data from target domain. Use previously-gained knowledge.
  - Application: Adapting a sentiment analysis model trained on product reviews to analyze movie reviews.

- Inductive transfer learning: Here source and target domains are same, but tasks are different.
  - Adv: Faster training as pre-trained model is already familiar with source data.
  - Application: [NLP] Pre-trained on a large set of texts and then tune to sentiment analysis.

https://aws.amazon.com/what-is/transfer-learning/

TL Strategies

- *Unsupervised transfer learning* uses a strategy similar to inductive transfer learning to develop new abilities.
  - Adv: Apply when source and target domains are unlabeled.
  - Application: Identifying different types of motorcycles in traffic images.
    - Train using unlabeled vehicle images and model learns similarities and distinguishing features.

https://aws.amazon.com/what-is/transfer-learning/

TL Steps

Three steps in transfer learning:

1. Select a pre-trained model with prior knowledge for a related task.
2. Configure pre-trained model using two main methods.
    I. *Freeze pre-trained layers: to* preserve source knowledge.
        I. Initially set to random values, weights are adjusted during the training process.
        II. *Remove last layer* of the pre-trained model.
    II. *Introduce new layers:* on top of pre-trained model for new task.
3. Train for target domain.

https://aws.amazon.com/what-is/transfer-learning/

TL Steps

- Transfer learning works best :
  - Both learning tasks are similar
  - Source and target data distributions do not vary too much.
  - A comparable model can be applied to both tasks.

- Note: Transfer learning Vs finetuning:
  - Finetuning refers to the process of further training a model on a task-specific dataset to improve performance on the initial, specific task for which the model was built.
  - TL signifies when users adapt a model to a new, related problem as opposed to same problem.

https://aws.amazon.com/what-is/transfer-learning/

Privacy-Accuracy trade-off

- Issue:
  - Attackers look for ways to steal user data or hijack an AI model.
    - In FL, when a data host trades their working model with the central server.
    - Reason of Exchange: Each exchange improves model but leaves data that helped train, [it open to inference attacks].
    - More rounds of information you exchange, the easier it is to infer information
- Trend: Focuses on minimizing and neutralizing privacy threats.

https://research.ibm.com/blog/what-is-federated-learning

Other Issues

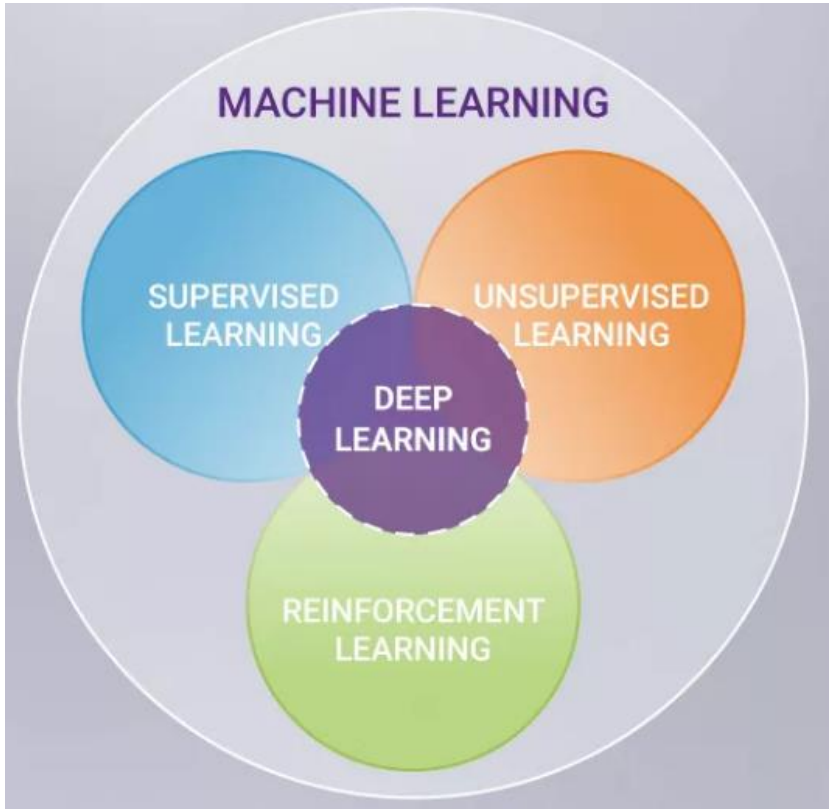
1. High network bandwidth
2. Transparency: Training data are kept private, [testing accuracy, fairness, and potential biases in model's output]
3. Accountability: Logging each stage of pipeline is needed.
4. Data Control: What data go into the model? and How to delete them when a host leaves?
   - Rule: if data are deleted, parties are obligated to retrain model from scratch.
5. Trust issue

https://research.ibm.com/blog/what-is-federated-learning

Reinforcement Learning

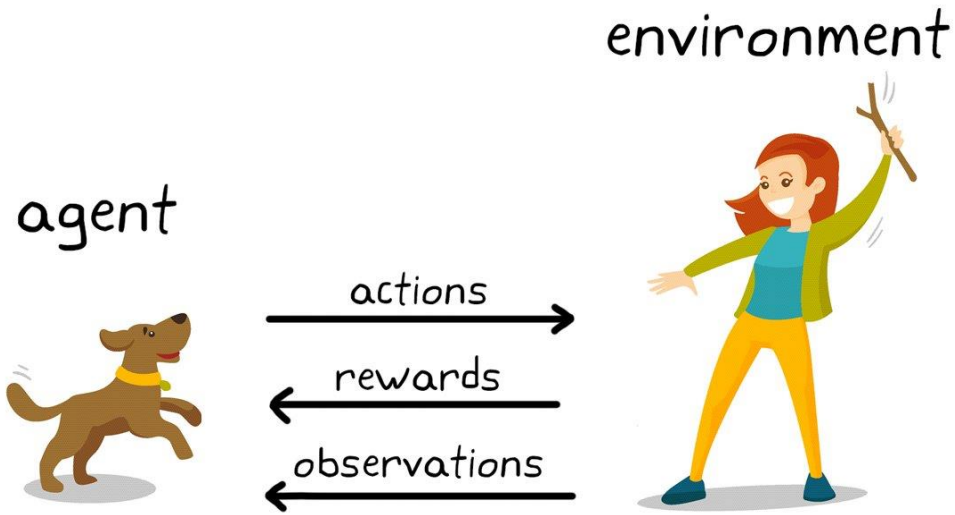
Reinforcement Learning (RL)

- RL is not a new concept
  - Recent progress in DL and computing power made it possible.
- RL and DL are not mutually exclusive.



Reinforcement Learning (RL)

- In RL, a computer agent learns to perform a task through repeated trial and error interactions with a dynamic environment.
  - Does not rely on a static dataset.
  - Operates in a dynamic environment.
  - Learns from collected experiences.

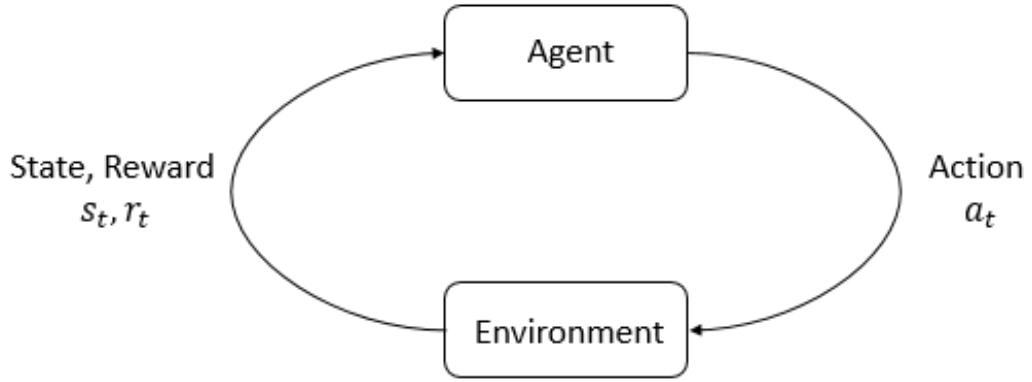


https://se.mathworks.com/discovery/reinforcement-learning.html

Reinforcement Learning (RL)

- Goal: To find most suitable action model to maximize total cumulative reward (for RL agent).
  - With no training dataset, RL problem is solved by agent's own actions with input from the environment.
  - No need for data collection, preprocessing, and labeling before training.

- Given right incentive, a RL model can start learning a behavior on its own, without (human) supervision.
  - Incentive is either negative (punishment) or positive (reward).



https://se.mathworks.com/discovery/reinforcement-learning.html

Reinforcement Learning (RL)

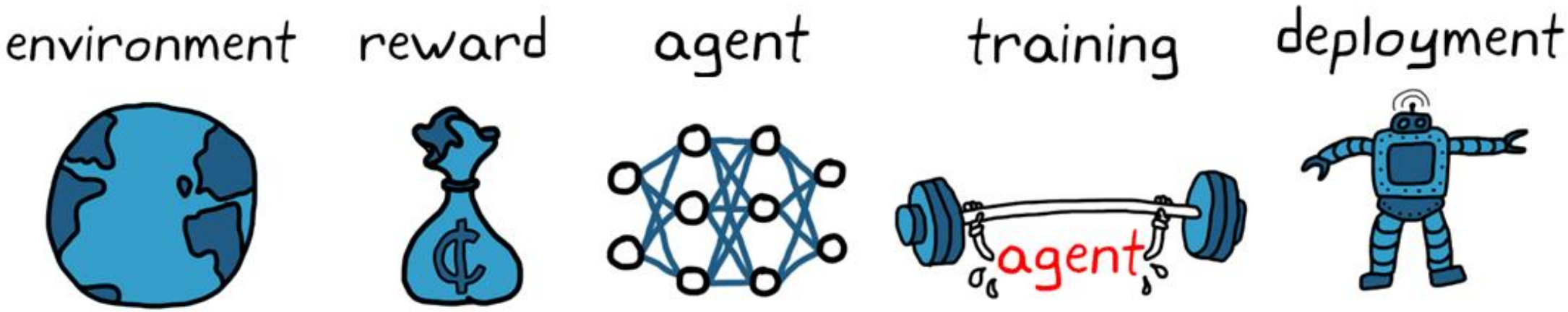
- Complex RL problems rely deep reinforcement learning.
- DNNs trained with RL can encode complex behaviors.
  - Automated driving: Making driving decisions based on camera input.
    - https://aws.amazon.com/deepracer/
  - Robotics (pick-and-place applications): Teaching a robotic arm how to manipulate a variety of objects.
    - https://www.youtube.com/watch?v=jwSbzNHGflM&t=148s
  - RL can be used in text summarization, question answering, and machine translation

https://se.mathworks.com/discovery/reinforcement-learning.html

RL Workflow

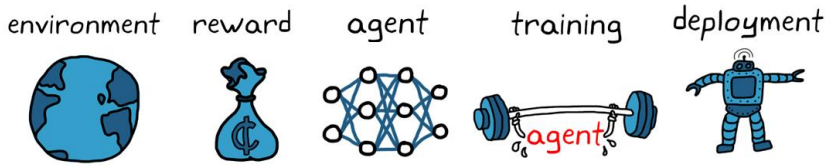
- **Environment:** Define environment where agent operates (interface between agent and environment)
  - Options: Model simulation, real physical system.

- **Reward Definition**: Specify reward signal to measure its performance against goals and how this signal is calculated from the environment
  - Reward shaping is tricky and require iterations to get it right.



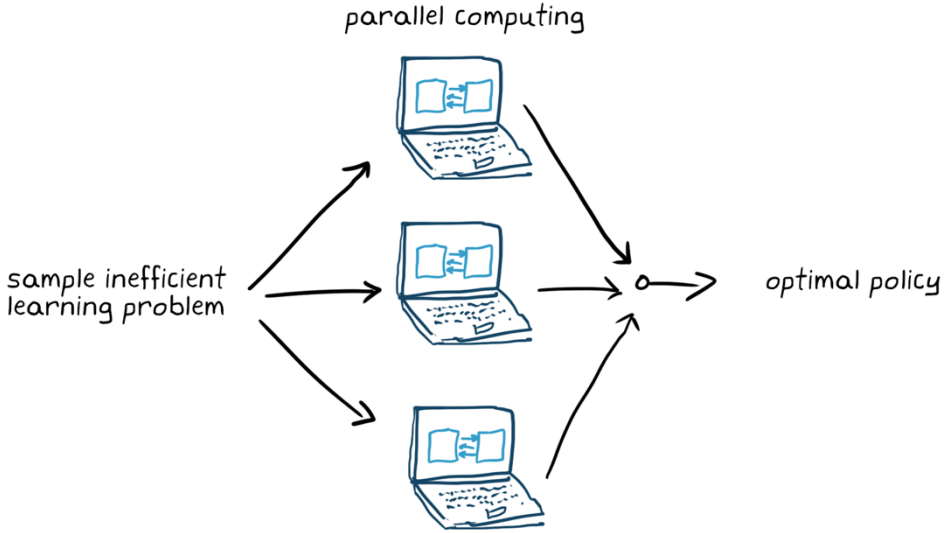
https://se.mathworks.com/discovery/reinforcement-learning.html

RL Workflow



- **Create Agent:** Consists of policy and training algorithm.
  - Represent policy using NNs or look-up tables.
  - NN are good candidates for large state/action spaces and complex problems.

- **Training**: Set up training options (like stopping criteria) and train agent to tune policy.
- Make sure to validate trained policy after training.
- If necessary, revisit design choices like reward signal and policy architecture and train again.

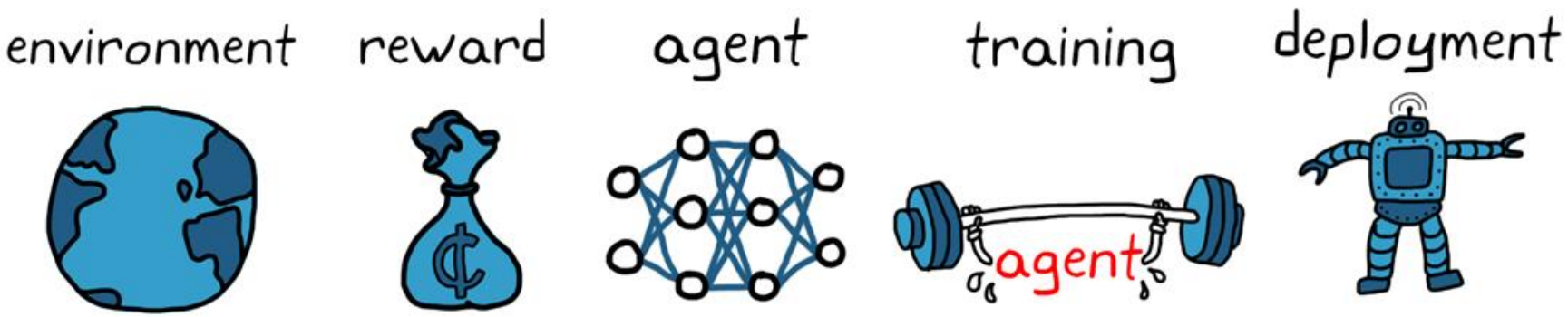


- Overall, RL is sample inefficient; training can take anywhere from minutes to days depending on the application.

https://se.mathworks.com/discovery/reinforcement-learning.html

RL Workflow

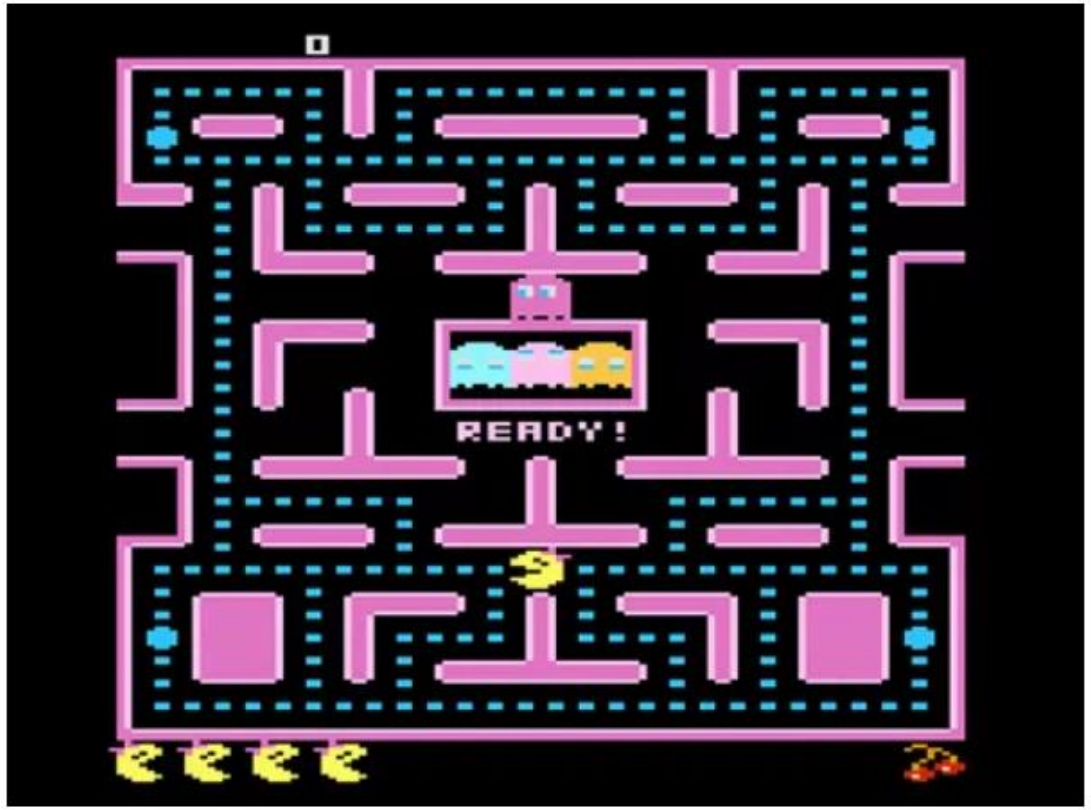
- **Deployment:**
  - Policy is a standalone decision-making system.
  - If training process does not converge to an optimal policy within a reasonable amount of time. Then adjust
    - Training settings
    - Algorithm configuration
    - Policy representation
    - Reward signal definition



https://se.mathworks.com/discovery/reinforcement-learning.html

RL Implementation

- Types of RL implementations:
  - Policy-based RL uses a policy or deterministic strategy that maximizes cumulative reward.
  - Value-based RL tries to maximize an arbitrary value function.
  - Model-based RL creates a virtual model for a certain environment and agent learns to perform within those constraints.
- In RL, data is accumulated during trial-and-error method.
  - Data is not part of input.
- Classic Atari games have been used as a test bed for RL algorithms.

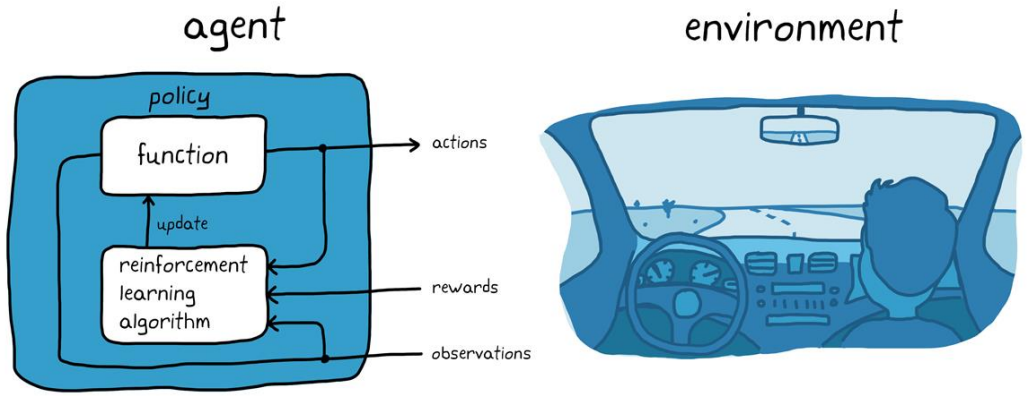


Ms. Pac-Man. PHOTO: ATARI

https://online.york.ac.uk/what-is-reinforcement-learning/

RL Example: Car Parking

- Goal: Teach vehicle computer (agent) to park in correct parking spot.
- Environment: is everything outside agent and include dynamics of vehicle, other nearby vehicles, weather conditions, and others.
- Training: Agent uses readings from sensors (cameras, GPS, and lidar) to generate steering, braking, and acceleration (actions).
- To learn how to generate correct actions from observations (policy tuning), agent repeatedly tries to park vehicle using a trial-and-error process.
- Reward signal can be provided to evaluate goodness of a trial and to guide learning process.



https://se.mathworks.com/discovery/reinforcement-learning.html

RL Example: AlphaZero

- [2017] AlphaZero is a single system that taught itself from scratch how to master games of chess, shogi (Japanese chess).
- How it works?
  - To learn each game, an untrained NN plays millions of games against itself via a process of trial and error.
  - At first, it plays completely randomly, but over time system learns from wins, losses, and draws to adjust the parameters of NN, making it more likely to choose advantageous moves in future.
  - The amount of training NN needs depends on complexity of game, taking approximately
    - 9 hours for chess
    - 12 hours for shogi
    - 13 days for Go.

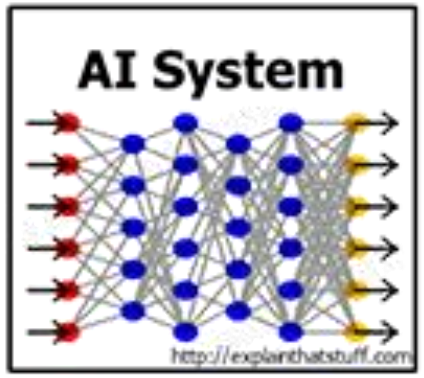
Issues

1. Data collection rate is limited by environment dynamics.
   - Environments with high latency slow down learning process.
2. Difficult for agent to discover optimal policy.
3. Lack of interpretability interferes with development of trust between agent and observer.

Explainable Artificial Intelligence (XAI)

Need for XAI

- Effectiveness of ML systems is limited by models' inability to explain their decisions and actions to human users.



- We are entering a new age of AI applications
- Machine learning is the core technology
- Machine learning models are opaque, non-intuitive, and difficult for people to understand

DoD and non-DoD Applications

Transportation

Security

Medicine

Finance

Legal

Military

- Why did you do that?
- Why not something else?
- When do you succeed?
- When do you fail?
- When can I trust you?
- How do I correct an error?

https://www.darpa.mil/program/explainable-artificial-intelligence

XAI

- Explainability aims to answer stakeholder questions about the decision-making processes of AI systems.
  - Use explanations to ensure project requirements are met during building, debugging, and testing.
  - Transparency is important thanks to current context of rising AI ethical concerns.

- XAI is a set of processes and methods that allows humans to comprehend and trust results created by ML algorithms.
  - Helps promote user trust, model auditability and productive use of AI.
  - Mitigates compliance, legal, security and reputational risks of production AI.

- Key requirements: fairness, model explainability and accountability.

https://www.ibm.com/topics/explainable-ai

XAI

- Regular AI vs XAI?
  - XAI implements specific techniques and methods to ensure that each decision made during ML process can be traced and explained.
  - AI arrives at a result using an ML algorithm, but architects of the AI systems do not fully understand how the algorithm reached that result.
  - Issue: Hard to check for accuracy and leads to loss of control, accountability and auditability.

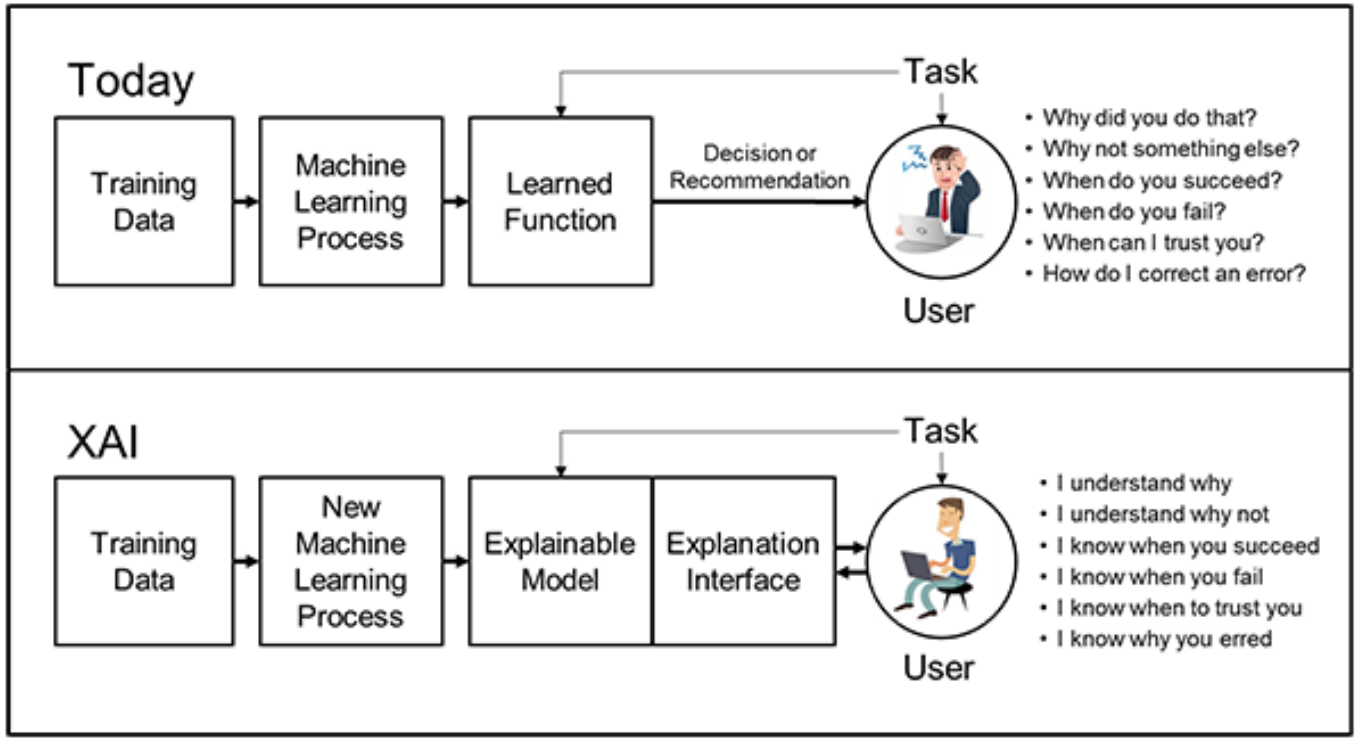
- XAI consists of:
  - Prediction accuracy.
  - Traceability is achieved by limiting scope narrower for rules and features.
  - Decision understanding addresses human needs (trust).

- Applications: Healthcare, Finance.

https://www.ibm.com/topics/explainable-ai

Need for XAI

- XAI aims to:
  - Produce more explainable models, while maintaining high prediction accuracy
  - Enable humans to understand, trust, and manage emerging AI partners.



https://www.darpa.mil/program/explainable-artificial-intelligence

XAI

- There is a lack of consensus on definitions XAI terms explainability and interpretability

- Explainability versus interpretability:
  - Explainability looks at how AI arrived at the result.
  - Interpretability is success rate that humans can predict for AI result of an output.

- Differences between XAI and responsible AI:
  - XAI looks at AI results after results are computed.
  - Responsible AI looks at AI during planning stages to make AI algorithm responsible before results are computed.

  - Explainable and responsible AI can work together to make better AI.

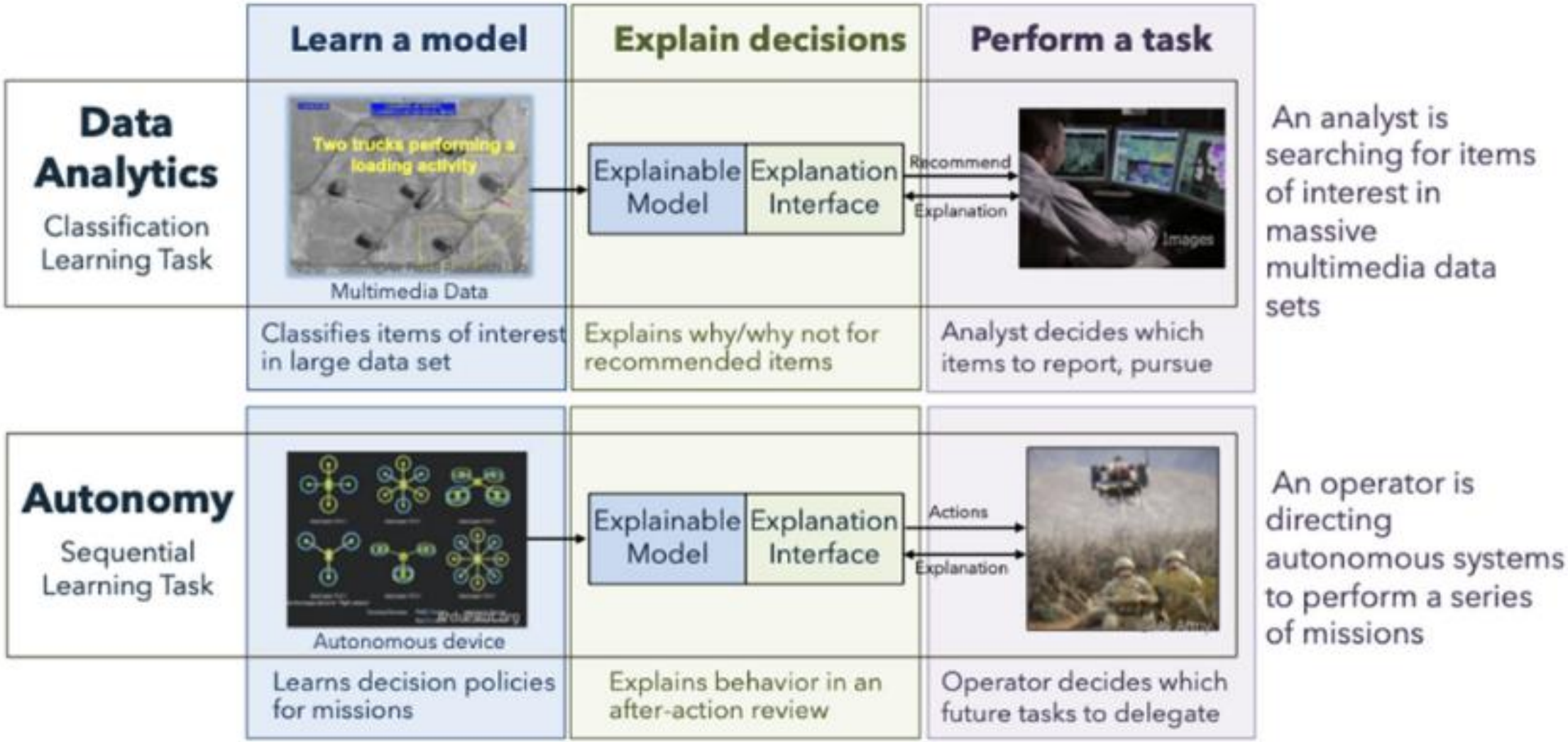
XAI

- Advantages:
  - Operationalize AI with trust and confidence
  - Better optimization.
  - Manage regulatory, compliance, risk and other requirements.

- Considerations for XAI:
  - Fairness and debiasing
  - Model drift mitigation: Alert when models deviate from intended outcomes.
  - Model risk management: Quantify and mitigate model risk. Understand what happened when deviations persist.
  - Lifecycle automation: Build, run and manage models as part of integrated data and AI services. Explain model dependencies.
  - Deployment

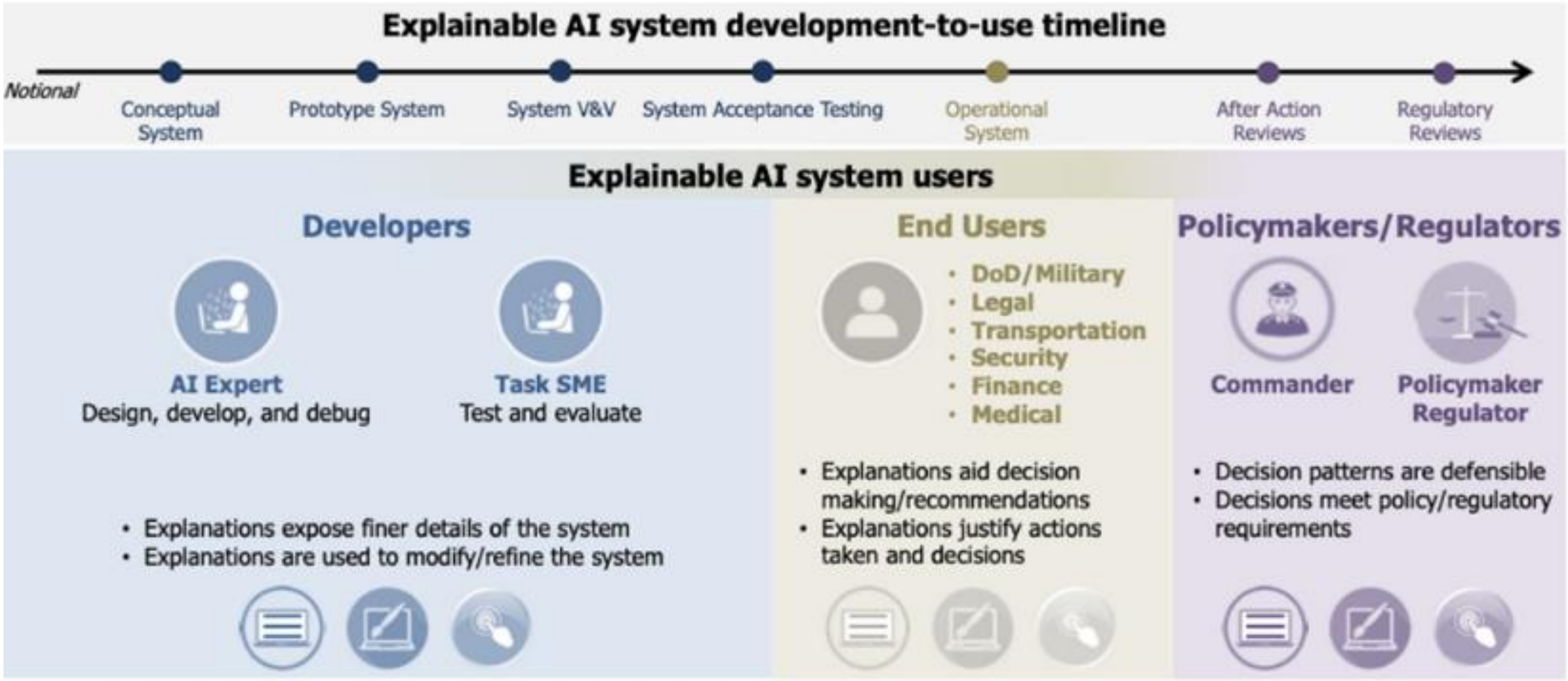
- Issue: Risk of over-simplifying and/or misrepresenting complicated systems.

XAI Challenges



DOI: 10.1002/ail2.61

XAI Users and Development Timeline



DOI: 10.1002/ail2.61

Summary (1/2)

- Federated Learning (FL) is a method to train AI models collaboratively on decentralised data without the need to share confidential user data.
- FL works by each party downloading a model, training it on their private data, encrypting model updates, and sending them to a server for aggregation into a centralised model, which is then sent back for further iterative training.

- Transfer Learning (TL) involves fine-tuning a model pre-trained on one task for a new, related task, offering time and cost savings.
- Strategies: 1. Transductive TL (transferring knowledge between related domains with little or no labelled target data), 2. inductive TL (source and target domains are the same, but tasks differ), and 3. unsupervised TL (applying when source and target domains are unlabelled).

Summary (2/2)

- Reinforcement Learning (RL) is a process where a computer agent learns to perform a task through trial and error interactions with a dynamic environment, without relying on a static dataset. The goal is to maximise total cumulative reward.
- RL involves defining the environment, specifying a reward signal, creating an agent with a policy and training algorithm, training the agent, and then deploying the learned policy.
- Explainable Artificial Intelligence (XAI) aims to make the decision-making processes of AI systems understandable and trustworthy for humans.
- XAI is important for ensuring project requirements are met, promoting user trust, enabling model auditability, and mitigating various risks associated with AI deployment.
- Goal of XAI is to produce more explainable models while maintaining high prediction accuracy, enabling humans to understand, trust, and manage AI systems.