ML vs DL vs FL

Rifah Sajida Deya

8th January, 2025

Definitions & Examples:

1. Machine Learning (ML):

   Machine Learning is a subset of artificial intelligence (AI) that involves creating algorithms and models that enable computers to learn patterns and make decisions from data without being explicitly programmed. ML typically requires feature engineering and works well with **structured** data.

   Example: Spam Detection, Fraud Detection, Recommendation Systems, Predictive Maintenance, etc.

2. Deep Learning (DL):

   Deep Learning is a specialized subset of machine learning that uses artificial neural networks with multiple layers to automatically learn hierarchical representations of data. It is particularly effective for processing **unstructured** data like images, audio, and text. DL models typically require large datasets and significant computational power.

   Example: Image Recognition, Speech Recognition, Natural Language Processing (NLP), Autonomous Vehicles, Medical Diagnosis etc.

3. Federated Learning (FL):

   Federated Learning is a **decentralized machine learning** approach where multiple devices or servers collaboratively train a shared model without exchanging raw data. Instead, only model updates (e.g., gradients) are shared with a central server, preserving data privacy and security.

   Example: Predictive Text (e.g., Google Keyboard), IoT Devices, Personalized Recommendations, Financial Services, etc.

Why Deep Learning (DL) when we have Machine Learning (ML)?

Aspect	Machine Learning (ML)	Deep Learning (DL)
Definition	ML covers a broad range of techniques, including linear regression, decision trees, and support vector machines.	DL is a subset of ML that uses neural networks with many layers to learn from data hierarchically.
Feature Engineering	Requires manual feature engineering by domain experts.	Features are learned automatically during training.
Data Requirements	Works well with smaller datasets.	Requires large datasets to achieve good performance.
Computational Power	Computationally less intensive.	Demands high computational power (GPUs/TPUs).
Performance on Complex Data	Struggles with unstructured data without feature engineering.	Excels at unstructured data like images, audio, and text.
Examples	Fraud detection, recommendation systems, stock price prediction.	Image recognition, natural language processing, autonomous vehicles.

Why Machine Learning (ML) when we have Deep Learning (ML)?

Aspect	Deep Learning (DL)	Machine Learning (ML)
Algorithm Complexity	Uses complex architectures like CNNs, RNNs, and Transformers.	Simpler algorithms like linear regression or k-means clustering.
Interpretability	Black-box models; difficult to interpret.	Easier to interpret, especially linear models.
Training Time	Longer due to large datasets and complex architectures.	Faster training time for simpler algorithms.

Black-box models: Black-box models refer to machine learning models whose internal workings are not easily interpretable or understandable by humans, even though they produce accurate outputs. These models can take inputs and generate predictions, but understanding how they arrive at those predictions is often challenging due to their complexity.

Examples: Deep Neural Networks (DNNs) [such as: Deep learning models like CNNs, RNNs, and Transformers]., Ensemble Methods etc.

Alternatives to Black-box Models:

1. White-box models: Transparent and interpretable models like linear regression, decision trees, or rule-based systems.
2. Explainable AI (XAI): Techniques and tools designed to interpret or explain black-box models (e.g., SHAP, LIME).

Why Federated Learning (FL) when we have Machine Learning (ML)?

1. Privacy-Preserving ML: In sensitive domains like healthcare, finance, or personal device applications, FL ensures data privacy.

2. Real-Time Data Utilization: FL enables learning from data that resides on user devices without waiting for central collection.

3. Scalability: FL is ideal for applications involving millions of devices generating data continuously (e.g., mobile apps, IoT).

4. Edge AI: As the trend moves towards AI at the edge (e.g., smart home devices, autonomous cars), FL supports on-device intelligence.

5. Regulatory Compliance: FL facilitates adherence to data protection laws that restrict data sharing.

Aspect	Machine Learning (ML)	Federate Learning (FL)
Data Location	Data is collected and stored in a central location.	Data remains on user devices (decentralized).
Privacy	Low: Raw data is transferred to a central server for training.	High: Only model updates are shared, not raw data.
Data Transfer	High: Entire datasets need to be transferred to a central server.	Minimal: Only model parameters or gradients are shared.
Use Case Suitability	Scenarios where data centralization is feasible and privacy is less critical.	Scenarios requiring privacy and compliance (e.g., healthcare, IoT).

Scalability	Limited by the cost of transferring and storing massive datasets.	Suitable for large-scale decentralized systems (e.g., mobile apps).
Compute Resources	Relies on powerful centralized servers or GPUs for training.	Utilizes edge devices for training, which may have limited power.
Data Heterogeneity	Assumes centralized, often well-curated, IID data.	Handles non-IID (non-independent and identically distributed) data from diverse sources.
Bandwidth Usage	High: Transfers entire datasets.	Low: Sends compressed updates (e.g., gradients).
Regulatory Compliance	May face challenges with data-sharing regulations.	Easily aligns with data protection laws like GDPR and HIPAA.
Personalization	Generally trains a one-size-fits-all model on centralized data.	Supports on-device personalized models while contributing to a global model.
Communication Overhead	Minimal: Training occurs locally at the server.	High: Frequent communication between devices and server required.

Conclusion

There is only the contrast between these 3 learning processes. To know detail you can visit:

- Federated Learning: https://github.com/rifah07/Introduction_of_Machine_Learning/blob/master/Federated_Learning.ipynb%20-%20Colab.pdf