# MACHINE LEARNING

## Disclaimer

*This document is part of teaching materials for **MACHINE LEARNING** under the Pokhara University syllabus for Bachelors in Computer Engineering (**BE-Computer**). This document does not cover all aspect of learning MACHINE LEARNING, nor are these be taken as primary source of information. As the core textbooks and reference books for learning the subject has already been specified and provided to the students, students are encouraged to learn from the original sources because this document cannot be used as a substitute for prescribed textbooks.*

*Various text books as well as freely available material from internet were consulted for preparing this document. Contents in This document are **copyrighted** to the instructor and authors of original texts where applicable.*

# Unit 1: Introduction to Machine Learning (5 Hr.)

## 1.1 Definition and Evolution of Machine Learning

Machine Learning is the science (and art) of programming computers so they can *learn from data*.

Machine Learning is the field of study that gives computers the ability to learn without being explicitly programmed.

- **Arthur Samuel, 1959**

A computer program is said to learn from experience *E* with respect to some task *T* and some performance measure *P*, if its performance on *T*, as measured by *P*, improves with experience *E*.

- **Tom Mitchell, 1997**

Let’s make definition clearer by example:

spam filter is a Machine Learning program that, given examples of spam emails (e.g., flagged by users) and examples of regular (no spam, also called “ham”) emails, can learn to flag spam. The examples that the system uses to learn are called the training set**.** Each training example is called a training instance (or sample).

In this case, the task T is to flag spam for new emails,

the experience E is the training data, and

the performance measure P needs to be defined; for example, you can use the ratio of correctly classified emails. This particular performance measure is called accuracy, and it is often used in classification tasks

First ML application that really became mainstream: **spam filter**.

## ***Traditional Approach vs Machine Learning***

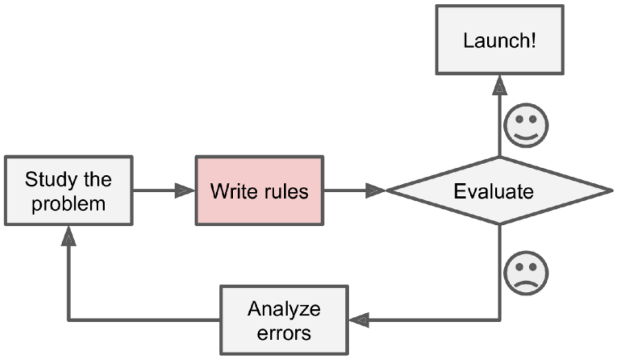

Figure: Traditional Approach

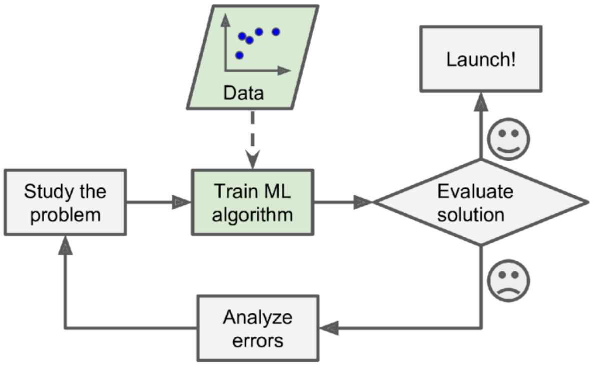

Figure: Machine Learning Approach

[Image Source: Aurélien Géron]

## AI vs ML

**Artificial intelligence** is a broad field, which refers to the use of technologies to build machines and computers that have the ability to mimic cognitive functions associated with human intelligence, such as being able to see, understand, and respond to spoken or written language, analyze data, make recommendations, and more.

Although artificial intelligence is often thought of as a system in itself, it is a set of technologies implemented in a system to enable it to reason, learn, and act to solve a complex problem.

**Machine learning** is a subset of artificial intelligence that automatically enables a machine or system to learn and improve from experience. Instead of explicit programming, machine learning uses algorithms to analyze large amounts of data, learn from the insights, and then make informed decisions.

Machine learning algorithms improve performance over time as they are trained—exposed to more data. Machine learning models are the output, or what the program learns from running an algorithm on training data. The more data used, the better the model will get.

| S.N. | AI | ML |
|---|---|---|
| 1 | AI allows a machine to simulate human intelligence to solve problems | ML allows a machine to learn autonomously from past data |

| | | |
|---|---|---|
| 2 | The goal is to develop an intelligent system that can perform complex tasks | The goal is to build machines that can learn from data to increase the accuracy of the output |
| 3 | We build systems that can solve complex tasks like a human | We train machines with data to perform specific tasks and deliver accurate results |
| 4 | AI has a wide scope of applications | Machine learning has a limited scope of applications |
| 5 | AI uses technologies in a system so that it mimics human decision-making | ML uses self-learning algorithms to produce predictive models |
| 6 | AI works with all types of data: structured, semi-structured, and unstructured | ML can only use structured and semi-structured data |
| 7 | AI systems use logic and decision trees to learn, reason, and self-correct | ML systems rely on statistical models to learn and can self-correct when provided with new data |

***How are AI and ML connected?***

While AI and ML are not quite the same thing, they are closely connected. The simplest way to understand how AI and ML relate to each other is:

- AI is **the broader concept** of enabling a machine or system to sense, reason, act, or adapt like a human
- ML is **an application of AI** that allows machines to extract knowledge from data and learn from it autonomously

## Evolution of Machine Learning

Through the decades after the 1940s, the evolution of machine learning includes some of the more notable developments:

**1940s–1950s:**

- 1943: Walter Pitts and Warren McCulloch introduced the first mathematical model of neural networks.

- 1949: Donald Hebb published a foundational book linking brain activity and neural networks.
- 1950: Alan Turing proposed the Turing Test, opening the AI field.
- 1951–1952: Marvin Minsky and Dean Edmonds created SNARC; Arthur Samuel developed the first self-learning program.
- 1956: Term artificial intelligence coined; Logic Theorist, first AI program, created.
- 1958–1959: Frank Rosenblatt invented the perceptron; Arthur Samuel coined machine learning.

**1960s–1970s:**

- 1960–1969: Development of Stanford Cart, MENACE (tic-tac-toe learner), DENDRAL (first expert system), Eliza (early chatbot), and Shakey (first mobile intelligent robot).
- Nearest neighbor algorithm and backpropagation introduced.
- 1969: Minsky and Papert's Perceptron's highlighted limits of neural networks, causing research decline.
- 1973: British government cut AI funding after the Lighthill report.

**1980s–1990s:**

- 1979–1989: Kunihiko Fukushima proposed noncognition; NetTalk, CNNs, Q-learning, and genetic algorithm software developed.
- 1992–1998: TD-Gammon (ANN-based backgammon), LSTM (recurrent neural networks), Deep Blue defeated Kasparov, MNIST dataset released.

**2000s:**

- 2000–2006: Neural probabilistic language models, Torch ML library, deep learning coined by Geoffrey Hinton, and Netflix Prize initiated.
- Fei-Fei Li started working on ImageNet; IBM Watson project began.

**2010s:**

- 2010–2012: Microsoft Kinect released; Kaggle founded; IBM Watson won Jeopardy!; CNNs triggered deep learning explosion (ImageNet 2012).
- 2013–2014: DeepMind developed deep reinforcement learning; word2vec and GANs introduced; DeepFace facial recognition system unveiled.
- 2016–2019: Uber's self-driving pilot; transformer architecture (Attention is All You Need); OpenAI's GPT released; major advances in medical AI.

**2020s:**

- 2021–2022: OpenAI introduced DALL-E; DeepMind launched AlphaTensor; ChatGPT (GPT-3.5) released.
- 2023–2024: OpenAI launched GPT-4; Nvidia surged as the top AI chipmaker; new compact AI chips and Microsoft's Aurora weather tool introduced.

## 1.2. Types of Machine Learning

There are so many different types of Machine Learning systems that it is useful to classify them in broad categories, based on the following criteria:

- ➢ Whether or not they are trained with human supervision (supervised, unsupervised, semi-supervised, and Reinforcement Learning)
- ➢ Whether or not they can learn incrementally on the fly (online versus batch learning)
- ➢ Whether they work by simply comparing new data points to known data points, or instead by detecting patterns in the training data and building a predictive model, much like scientists do (instance-based versus model-based learning)

Machine Learning systems can be classified according to the amount and type of supervision they get during training.

There are **four major categories**: supervised learning, unsupervised learning, semi-supervised learning, and Reinforcement Learning.

### 1.2.1. Supervised Learning

- In this approach, the algorithm is trained on a labeled dataset (the training set you feed to the algorithm includes the desired solutions). i.e. data comes with correct answers already provided.

*OR*

- Supervised learning is a machine learning model that uses labeled training data (structured data) to map a specific feature to a label. In supervised learning, the output is known (such as recognizing a picture of an apple) and the model is trained on data of the known output. In simple terms, to train the algorithm to recognize pictures of apples, feed it pictures labeled as apples.
- The machine learns to make predictions or decisions by comparing its output to the correct answers and adjusting accordingly.
- For example, supervised learning is used in email filtering systems to identify spam emails based on examples it has been trained on.

Imagine you're learning to play the guitar with a teacher by your side. They show you which notes to play, correct you when you're wrong, and gradually you get better. That's what supervised learning is like for machines.

- some of the most important supervised learning algorithms
  - k-Nearest Neighbors (KNN)
  - Linear Regression
  - Logistic Regression
  - Support Vector Machines (SVMs)
  - Decision Trees and Random Forests
  - Neural networks

### 1.2.2. Unsupervised Learning

- In this approach, the machine is given data without any labels or correct answers, and it has to figure out the patterns or groupings on its own.

*OR*

- Unsupervised learning is a machine learning model that uses unlabeled data (unstructured data) to learn patterns. Unlike supervised learning, the "correctness" of the output is not known ahead of time. Rather, the algorithm learns from the data without human input (and is thus, unsupervised) and categorizes it into groups based on attributes. For instance, if the algorithm is given pictures of apples and bananas, it will work by itself to categorize which picture is an apple and which is a banana.

- It is like the system tries to learn without a teacher.
- Unsupervised Learning is like a self-guided discovery process, where the model learns to make sense of the data without any labeled examples.
- some of the most important unsupervised learning algorithms are:
    - Clustering
        - K-Means
        - DBSCAN
        - Hierarchical Cluster Analysis (HCA)
    - Anomaly detection and novelty detection
        - One-class SVM
        - Isolation Forest
    - Visualization and dimensionality reduction
        - Principal Component Analysis (PCA)
        - Kernel PCA
        - Locally Linear Embedding (LLE)
        - t-Distributed Stochastic Neighbor embedding (t-SNE)
    - Association rule learning
        - Apriori
        - Eclat

### 1.2.3. Reinforcement Learning

- Reinforcement learning is a machine learning model that can be described as “learn by doing” through a series of trial-and-error experiments. An “agent” learns to perform a defined task through a feedback loop until its performance is within a desirable range. The agent receives positive reinforcement when it performs the task well and negative reinforcement when it performs poorly.

*OR*

- Reinforcement Learning is a very different beast. The learning system, called an agent in this context, can observe the environment, select and perform actions, and get rewards in return (or penalties in the form of negative rewards)

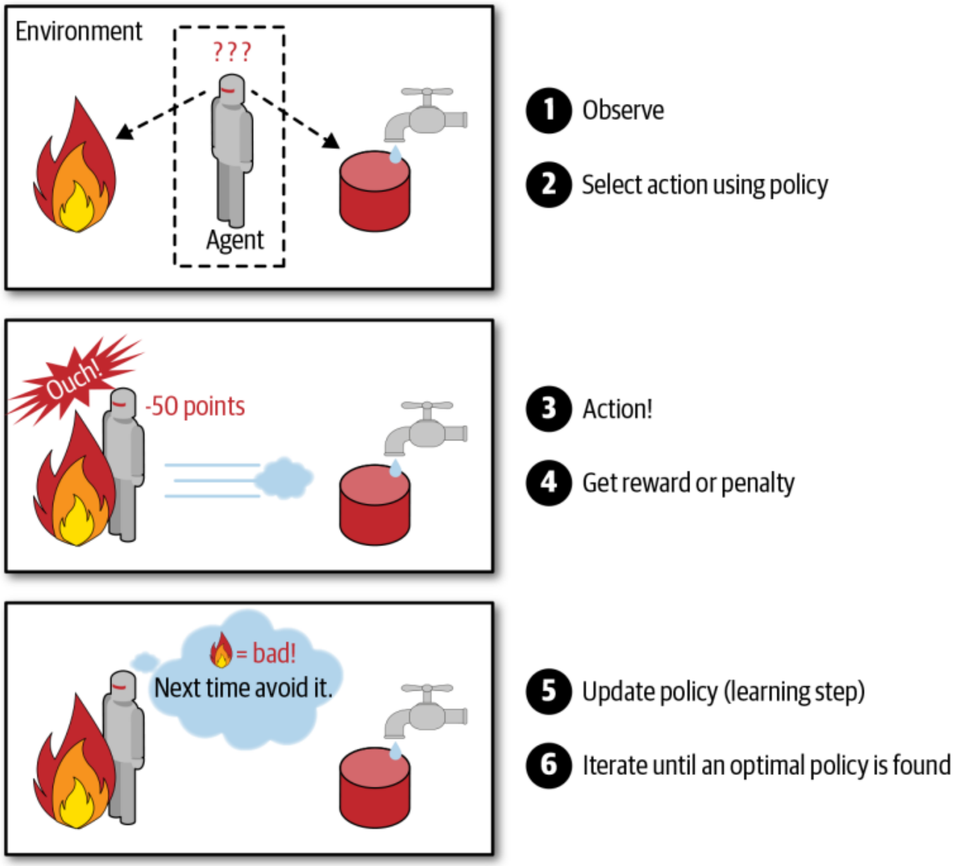
Environment
???
Agent
1 Observe
2 Select action using policy
Ouch!
-50 points
3 Action!
4 Get reward or penalty
= bad!
Next time avoid it.
5 Update policy (learning step)
6 Iterate until an optimal policy is found

Figure: Reinforcement Learning [Image Source: Aurélien Géron's Book]

### 1.2.4. Active Learning

- It is semi-supervised machine learning.
- A subset of machine learning works with very less labeled data and huge size of unlabeled data.
- It allows a learning algorithm to interactively query a user to label data with the desired outputs.
- The algorithm actively chooses from the pool of unlabeled data the subset of examples to be labelled next in active learning.
- The basic idea behind the active learner algorithm concept is that if a machine learning algorithm could select the data it wants to learn from, it might be able to achieve a higher degree of accuracy with fewer training labels.

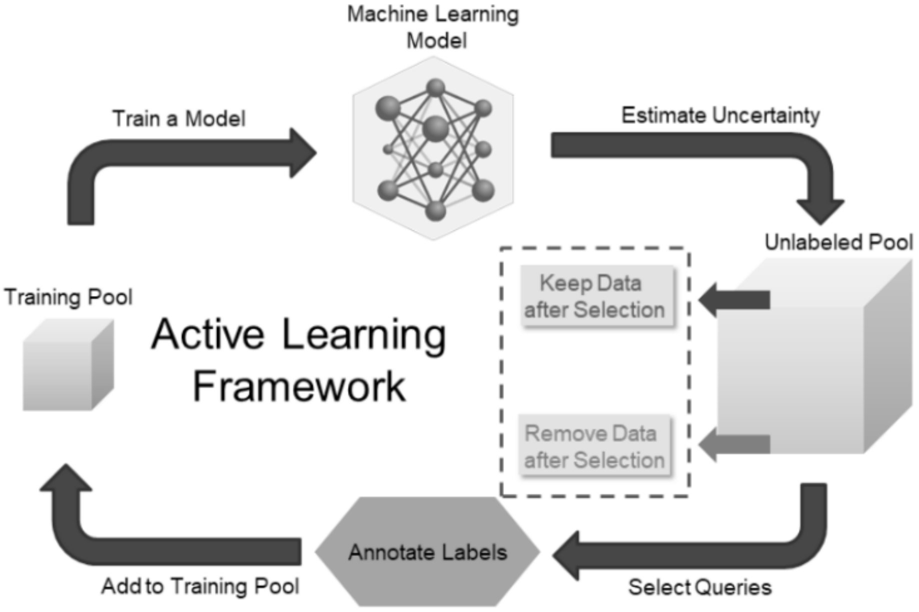

Figure: Active Learning Cycle [IS: Viso.ai]

## 1.3. Machine Learning Workflow

A machine learning workflow is the systematic process of developing, training, evaluating, and deploying machine learning models. It encompasses a series of steps that guide practitioners through the entire lifecycle of a machine learning project, from problem definition to solution deployment.

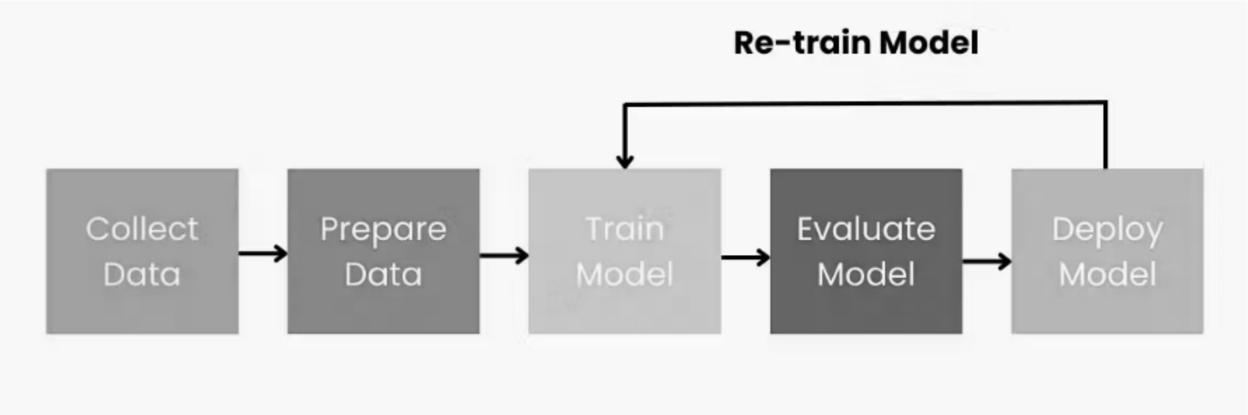

Figure: General machine learning workflow

### 1.3.1. Problem Definition

- **In** Problem definition, you have to clearly define the problem to be solved and establish the project goals.

- This step involves understanding the business context, identifying relevant data sources, and defining key performance metrics.
- Before you start thinking about how to solve a problem with ML, take some time to think about the problem you are trying to solve. Ask yourself the following questions
  - Do you have a well-defined problem to solve?
  - Is ML the best solution for the problem?
  - How can you measure the model's success?

### 1.3.2. Data Collection and Preprocessing

***Data Collection:***

- The process of data collection depends on the type of project we desire to make
- If we want to make an ML project that uses real-time data, then we can build an IoT system that using different sensors data.
- The data set can be collected from various sources such as a file, database, sensor and many other such sources.
- Kaggle and UCI Machine Learning Repository are the source example where the free data present on the internet.

***Preprocessing:***

- Collected data cannot be used directly for performing the analysis process as there might be a lot of missing data, extremely large values, unorganized text data or noisy data. Therefore, to solve this problem Data Preparation is done.
- Data pre-processing is one of the most important steps in machine learning that helps in building machine learning models more accurate.
- In machine learning, there is an 80/20 rule. Every data scientist should spend 80% time for data pre-processing and 20% time to actually perform the analysis.

### 1.3.3. Model Selection

- Most important step of machine learning workflow where you choose appropriate machine learning algorithms and techniques based on the problem requirements and data characteristics.

- Then, train the selected models using the prepared data, and evaluate their performance using suitable evaluation metrics.

### 1.3.4. Model Evaluation and Validation

- Model Evaluation is an integral part of the model development process. It helps to find the best model that represents our data and how well the chosen model will work in the future.
- There are two methods of evaluating models in data science, Hold-Out (mostly large dataset is randomly divided to three subsets: Training, Validation and Test) and Cross-Validation (*k*-fold cross-validation).
- model validation is the task of confirming that the outputs of a model have enough fidelity to the outputs of the data-generating process that the objectives can be achieved.

### 1.3.5. Model Deployment

- In model deployment and monitoring, you have to deploy the trained model into the production environment, integrate it into the existing systems, monitor the model performance in real-world scenarios, and update it as needed to ensure continued effectiveness.

## 1.4. Challenges in Machine Learning

Machine learning is a rapidly growing field with many promising applications. However, there are also several challenges and issues that must be addressed to fully realize the potential of machine learning.

### 1.4.1. Data Quality Issues

- Data plays a significant role in the machine learning process.
- One of the significant issues that machine learning professionals face is the absence of good quality data.
- Unclean and noisy data can make the whole process extremely exhausting. We don’t want our algorithm to make inaccurate or faulty predictions. Hence the quality of data is essential to enhance the output.
- Data quality is a recurring issue, with noisy, incomplete, and inaccurate data undermining the accuracy of classification and overall results.

- Achieving high-quality data is essential for the success of ML models therefore we need data preprocessing mechanism.
- If the training data is full of errors, outliers, and noise (e.g., due to poor quality measurements), it will make it harder for the system to detect the underlying patterns, so ML model is less likely to perform well.
- Most data scientists spend a significant part of their time doing just that.

### 1.4.2. Computational Complexity

- Computational Complexity refers to the number of resources (like time, storage, and computational power) needed to train and run a machine learning model.
- The machine learning industry is evolving and is continuously changing.
- Rapid hit and trial experiments are being carried on.
- The process is transforming, and hence there are high chances of error which makes the learning complex. It includes analyzing the data, removing data bias, training data, applying complex mathematical calculations, and a lot more.
- Computational complexity affects scalability, speed, cost and feasibility. Hence it is complicated process which is another big challenge for Machine learning professionals. But these kinds of challenges can be addressed by using efficient algorithms, distributed computing, model pruning, dimensionality reduction.

### 1.4.3. Interpretability and Explainability

- **Interpretability**: How easily can a human understand the internal logic of a model?
- **Explainability**: How clearly can a model explain why it made a particular decision or prediction?
- Advanced models like deep neural networks, ensemble methods (e.g., random forests, XGBoost), and transformers are often hard to understand. We know they work—but how they make decisions isn't always clear.
- In sensitive areas like healthcare, finance, or law, people need to trust the system. If a model can't justify its decision, it's hard to trust or adopt.
- If you can’t interpret a model, it’s hard to debug, find bias, or improve it.
- If a model favors or discriminates against certain groups, interpretability helps expose such hidden biases.

### 1.4.4. Ethical Considerations

- Ethical considerations refer to the moral responsibilities and impacts of using machine learning on individuals and society.
- Due to various reason, it is challenging.
- ML models learn from historical data, which may carry social biases (e.g., gender, caste, race) and may results in Discriminatory decisions in hiring, lending, law enforcement, etc.
- ML often uses personal data (like location, health, or online behavior), if these kinds of data are not handled carefully, it can invade users' privacy or lead to data leaks
- Sometimes data is collected or used without users' informed consent which Violates privacy rights and ethical norms.
- Automation through ML can replace human workers, especially in routine jobs which may raises questions about unemployment and economic inequality
- When an ML model makes a harmful decision, who is responsible? developer? organization? algorithm itself?
- ML can be used in military and surveillance systems, raising concerns about human rights and misuse.

To address these challenges:

- Build fair and unbiased datasets
- Ensure transparency and accountability
- Follow data protection laws
- Establish ethical review boards for AI / ML projects
- Encourage inclusive and responsible AI development

****End of Chapter****