**Introducing Machine Learning**

**What is machine learning?**

Machine learning is a branch of [artificial intelligence (AI)](https://www.ibm.com/in-en/topics/artificial-intelligence) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.

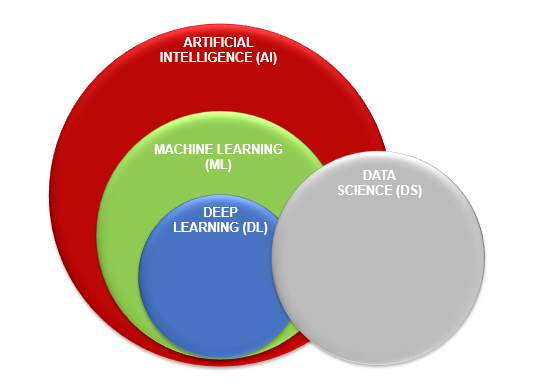
Over the last couple of decades, the technological advances in storage and processing power have enabled some innovative products based on machine learning, such as Netflix’s recommendation engine and self-driving cars.

Machine learning is an important component of the growing field of data science. Through the use of statistical methods, algorithms are trained to make classifications or predictions, and to uncover key insights in data mining projects. These insights subsequently drive decision making within applications and businesses, ideally impacting key growth metrics. As big data continues to expand and grow, the market demand for data scientists will increase. They will be required to help identify the most relevant business questions and the data to answer them.

Machine learning algorithms are typically created using frameworks that accelerate solution development, such as TensorFlow and PyTorch.

**Machine Learning vs. Deep Learning vs. Neural Networks**

Since deep learning and machine learning tend to be used interchangeably, it’s worth noting the nuances between the two. Machine learning, deep learning, and neural networks are all sub-fields of artificial intelligence. However, neural networks is actually a sub-field of machine learning, and deep learning is a sub-field of neural networks.



The way in which deep learning and machine learning differ is in how each algorithm learns. "Deep" machine learning can use labeled datasets, also known as supervised learning, to inform its algorithm, but it doesn’t necessarily require a labeled dataset. Deep learning can ingest unstructured data in its raw form (e.g., text or images), and it can automatically determine the set of features which distinguish different categories of data from one another. This eliminates some of the human intervention required and enables the use of larger data sets.

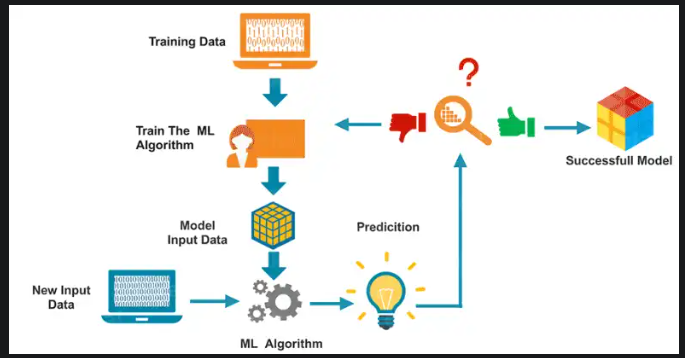
Classical, or "non-deep", machine learning is more dependent on human intervention to learn. Human experts determine the set of features to understand the differences between data inputs, usually requiring more structured data to learn.

Neural networks, or artificial neural networks (ANNs), are comprised of node layers, containing an input layer, one or more hidden layers, and an output layer. Each node, or artificial neuron, connects to another and has an associated weight and threshold. If the output of any individual node is above the specified threshold value, that node is activated, sending data to the next layer of the network. Otherwise, no data is passed along to the next layer of the network by that node. The “deep” in deep learning is just referring to the number of layers in a neural network. A neural network that consists of more than three layers—which would be inclusive of the input and the output—can be considered a deep learning algorithm or a deep neural network. A neural network that only has three layers is just a basic neural network.

Deep learning and neural networks are credited with accelerating progress in areas such as computer vision, natural language processing, and speech recognition.

**How machine learning works**

breaks out the learning system of a machine learning algorithm into three main parts.



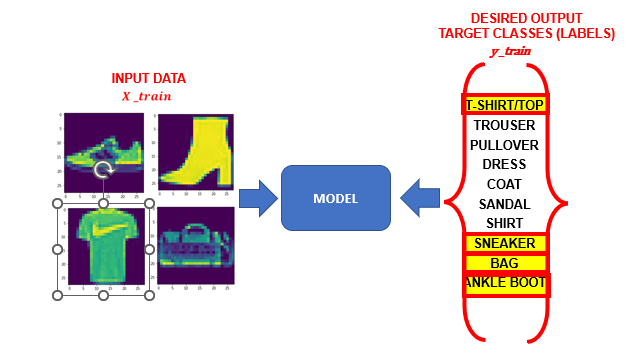
1. A Decision Process: In general, machine learning algorithms are used to make a prediction or classification. Based on some input data, which can be labeled or unlabeled, your algorithm will produce an estimate about a pattern in the data.
2. An Error Function: An error function evaluates the prediction of the model. If there are known examples, an error function can make a comparison to assess the accuracy of the model.
3. A Model Optimization Process: If the model can fit better to the data points in the training set, then weights are adjusted to reduce the discrepancy between the known example and the model estimate. The algorithm will repeat this “evaluate and optimize” process, updating weights autonomously until a threshold of accuracy has been met.

**Machine learning methods**

Machine learning models fall into three primary categories.

**Supervised machine learning**

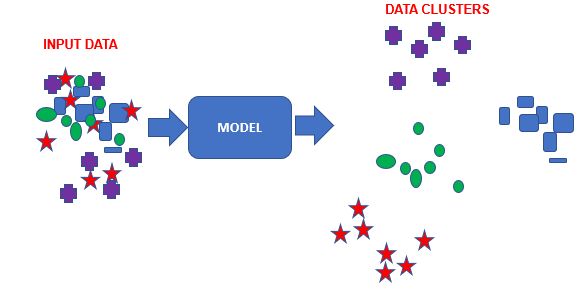
* **Supervised: used to train algorithms using labeled input and output data.**
* **Performance is assessed by comparing trained model prediction vs. real output**



[Supervised learning](https://www.ibm.com/in-en/topics/supervised-learning), also known as supervised machine learning, is defined by its use of labeled datasets to train algorithms to classify data or predict outcomes accurately. As input data is fed into the model, the model adjusts its weights until it has been fitted appropriately. This occurs as part of the cross validation process to ensure that the model avoids [overfitting](https://www.ibm.com/in-en/topics/overfitting) or [underfitting](https://www.ibm.com/in-en/topics/underfitting). Supervised learning helps organizations solve a variety of real-world problems at scale, such as classifying spam in a separate folder from your inbox. Some methods used in supervised learning include neural networks, naïve bayes, linear regression, logistic regression, random forest, and support vector machine (SVM).

**Unsupervised machine learning**

* **Unsupervised learning: provides the algorithm with no labeled data.**
* **The algorithm attempts at discovering hidden patterns within the training data.**
* **Unsupervised learning methods can analyze complex data that humans might find difficult to interpret.**



[Unsupervised learning](https://www.ibm.com/in-en/topics/unsupervised-learning), also known as unsupervised machine learning, uses machine learning algorithms to analyze and cluster unlabeled datasets. These algorithms discover hidden patterns or data groupings without the need for human intervention. This method’s ability to discover similarities and differences in information make it ideal for exploratory data analysis, cross-selling strategies, customer segmentation, and image and pattern recognition. It’s also used to reduce the number of features in a model through the process of dimensionality reduction. Principal component analysis (PCA) and singular value decomposition (SVD) are two common approaches for this. Other algorithms used in unsupervised learning include neural networks, k-means clustering, and probabilistic clustering methods.

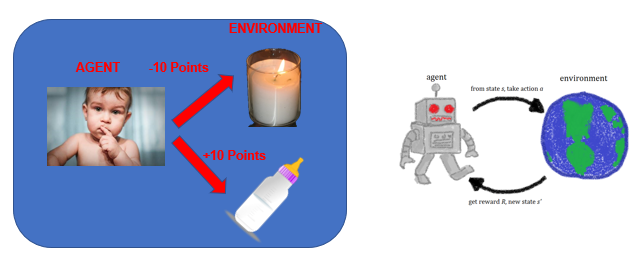
**Semi-supervised learning**

Semi-supervised learning offers a happy medium between supervised and unsupervised learning. During training, it uses a smaller labeled data set to guide classification and feature extraction from a larger, unlabeled data set. Semi-supervised learning can solve the problem of not having enough labeled data for a supervised learning algorithm. It also helps if it’s too costly to label enough data.

"

**Reinforcement machine learning**

Reinforcement machine learning is a machine learning model that is similar to supervised learning, but the algorithm isn’t trained using sample data. This model learns as it goes by using trial and error. A sequence of successful outcomes will be reinforced to develop the best recommendation or policy for a given problem.



* Reinforcement learning allows machines take actions to maximize cumulative reward.
* Reinforcement algorithms learn by trial and error through reward and penalty.
* Two elements: environment and learning agent.
* The environment rewards the agent for correct actions.

Based on the reward or penalty, agent improves its environment knowledge to make better decision

**Common machine learning algorithms**

**A number of machine learning algorithms are commonly used. These include:**

* **Neural networks:** Neural networks simulate the way the human brain works, with a huge number of linked processing nodes. Neural networks are good at recognizing patterns and play an important role in applications including natural language translation, image recognition, speech recognition, and image creation.
* **Linear regression:** This algorithm is used to predict numerical values, based on a linear relationship between different values. For example, the technique could be used to predict house prices based on historical data for the area.
* **Logistic regression:** This supervised learning algorithm makes predictions for categorical response variables, such as“yes/no” answers to questions. It can be used for applications such as classifying spam and quality control on a production line.
* **Clustering:** Using unsupervised learning, clustering algorithms can identify patterns in data so that it can be grouped. Computers can help data scientists by identifying differences between data items that humans have overlooked.
* **Decision trees:** Decision trees can be used for both predicting numerical values (regression) and classifying data into categories. Decision trees use a branching sequence of linked decisions that can be represented with a tree diagram. One of the advantages of decision trees is that they are easy to validate and audit, unlike the black box of the neural network.
* **Random forests:** In a random forest, the machine learning algorithm predicts a value or category by combining the results from a number of decision trees.

**Importance of Machine Learning:**

* Machine learning helps businesses by driving growth, unlocking new revenue streams, and solving challenging problems.
* Data is the critical driving force behind business decision-making but traditionally, companies have used data from various sources, like customer feedback, employees, and finance.
* Machine learning research automates and optimizes this process. By using software that analyzes very large volumes of data at high speeds, businesses can achieve results.

**Machine Learning Applications**

**Manufcaturing**

* Machine learning can support predictive maintenance, quality control, and innovative research in the manufacturing sector. Machine learning technology also helps companies improve logistical solutions, including assets, supply chain, and inventory management.
* For example, manufacturing giant [3M](https://aws.amazon.com/machine-learning/customers/3m/) uses [AWS Machine Learning](https://aws.amazon.com/machine-learning/) to innovate sandpaper.
* Machine learning algorithms enable 3M researchers to analyze how slight changes in shape, size, and orientation improve abrasiveness and durability. Those suggestions inform the manufacturing process.

**Health Care and Life Sciences**

* The proliferation of wearable sensors and devices has generated a significant volume of health data. Machine learning programs can analyze this information and support doctors in real-time diagnosis and treatment.
* Machine learning researchers are developing solutions that detect cancerous tumors and diagnose eye diseases, significantly impacting human health outcomes.
* For example, [Cambia Health Solutions](https://aws.amazon.com/solutions/case-studies/cambia-health-solutions/) used AWS Machine Learning to support healthcare start-ups where they could automate and customize treatment for pregnant women.

**Financial Services**

* Financial machine learning projects improve risk analytics and regulation. Machine learning technology can allow investors to identify new opportunities by analyzing stock market movements, evaluating hedge funds, or calibrating financial portfolios.
* In addition, it can help identify high-risk loan clients and mitigate signs of fraud.
* Financial software leader [Intuit](https://aws.amazon.com/machine-learning/customers/intuit/) uses AWS Machine Learning system, [Amazon Textract](https://aws.amazon.com/textract/), to create more personalized financial management and help end users improve their financial health.

**Retail**

* Retail can use machine learning to improve customer service, stock management, upselling and cross-channel marketing.
* For example, [Amazon Fulfillment (AFT)](https://aws.amazon.com/solutions/case-studies/amazon-fulfillment-technologies-case-study/) cut infrastructure costs by 40 percent using a machine learning model to identify misplaced inventory.
* This helps them deliver on Amazon’s promise that an item will be readily available to customers and arrive on time, despite processing millions of global shipments annually.

**Media and Entertainment**

* Entertainment companies turn to machine learning to better understand their target audiences and deliver immersive, personalized, and on-demand content.
* Machine learning algorithms are deployed to help design trailers and other advertisements, provide consumers with personalized content recommendations, and even streamline production.
* For example, [Disney](https://aws.amazon.com/machine-learning/customers/innovators/disney/) is using [AWS Deep Learning](https://aws.amazon.com/deep-learning/) to archive their media library.
* AWS machine learning tools automatically tag, describe, and sort media content, enabling Disney writers and animators to search for and familiarize themselves with Disney characters quickly.

**Advantages of machine learning models:**

Can identify data trends and patterns that humans might miss.

Can work without human intervention after set up. For example, machine learning in cybersecurity software can continuously monitor and identify irregularities in network traffic without administrator input.

Results can become more accurate over time.

Can handle a variety of data formats in dynamic, high volume, and complex data environments.

**Disadvantages of machine learning models:**

Initial training is a costly and time-consuming process. It may be hard to implement if sufficient data is not available.

It is a compute-intensive process requiring heavy initial investment

**Challenges of machine learning**

As machine learning technology has developed, it has certainly made our lives easier. However, implementing machine learning in businesses has also raised a number of ethical concerns about AI technologies. Some of these include:

**Technological singularity**

While this topic garners a lot of public attention, many researchers are not concerned with the idea of AI surpassing human intelligence in the near future. Technological singularity is also referred to as strong AI or superintelligence. Philosopher Nick Bostrum defines superintelligence as “any intellect that vastly outperforms the best human brains in practically every field, including scientific creativity, general wisdom, and social skills.” Despite the fact that superintelligence is not imminent in society, the idea of it raises some interesting questions as we consider the use of autonomous systems, like self-driving cars. It’s unrealistic to think that a driverless car would never have an accident, but who is responsible and liable under those circumstances? Should we still develop autonomous vehicles, or do we limit this technology to semi-autonomous vehicles which help people drive safely? The jury is still out on this, but these are the types of ethical debates that are occurring as new, innovative AI technology develops.

**AI impact on jobs**

While a lot of public perception of artificial intelligence centers around job losses, this concern should probably be reframed. With every disruptive, new technology, we see that the market demand for specific job roles shifts. For example, when we look at the automotive industry, many manufacturers, like GM, are shifting to focus on electric vehicle production to align with green initiatives. The energy industry isn’t going away, but the source of energy is shifting from a fuel economy to an electric one.

In a similar way, artificial intelligence will shift the demand for jobs to other areas. There will need to be individuals to help manage AI systems. There will still need to be people to address more complex problems within the industries that are most likely to be affected by job demand shifts, such as customer service. The biggest challenge with artificial intelligence and its effect on the job market will be helping people to transition to new roles that are in demand.

**Privacy**

Privacy tends to be discussed in the context of data privacy, data protection, and data security. These concerns have allowed policymakers to make more strides in recent years. For example, in 2016, GDPR legislation was created to protect the personal data of people in the European Union and European Economic Area, giving individuals more control of their data. In the United States, individual states are developing policies, such as the California Consumer Privacy Act (CCPA), which was introduced in 2018 and requires businesses to inform consumers about the collection of their data. Legislation such as this has forced companies to rethink how they store and use personally identifiable information (PII). As a result, investments in security have become an increasing priority for businesses as they seek to eliminate any vulnerabilities and opportunities for surveillance, hacking, and cyberattacks.

**Bias and discrimination**

Instances of bias and discrimination across a number of machine learning systems have raised many ethical questions regarding the use of artificial intelligence. How can we safeguard against bias and discrimination when the training data itself may be generated by biased human processes? While companies typically have good intentions for their automation efforts, [Reuters](https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G) (link resides outside IBM) ) highlights some of the unforeseen consequences of incorporating AI into hiring practices. In their effort to automate and simplify a process, Amazon unintentionally discriminated against job candidates by gender for technical roles, and the company ultimately had to scrap the project. [Harvard Business Review](https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring) (link resides outside IBM) has raised other pointed questions about the use of AI in hiring practices, such as what data you should be able to use when evaluating a candidate for a role.

Bias and discrimination aren’t limited to the human resources function either; they can be found in a number of applications from facial recognition software to social media algorithms.

As businesses become more aware of the risks with AI, they’ve also become more active in this discussion around AI ethics and values. For example, IBM has sunset its general purpose facial recognition and analysis products. IBM CEO Arvind Krishna wrote: “IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency.”

**Accountability**

Since there isn’t significant legislation to regulate AI practices, there is no real enforcement mechanism to ensure that ethical AI is practiced. The current incentives for companies to be ethical are the negative repercussions of an unethical AI system on the bottom line. To fill the gap, ethical frameworks have emerged as part of a collaboration between ethicists and researchers to govern the construction and distribution of AI models within society..

**Evaluation of machine learning algorithm**

Evaluating your machine learning algorithm is an essential part of any project. Your model may give you satisfying results when evaluated using a metric say accuracy\_score but may give poor results when evaluated against other metrics such as logarithmic\_loss or any other such metric. Most of the times we use classification accuracy to measure the performance of our model, however it is not enough to truly judge our model. In this post, we will cover different types of evaluation metrics available.

***Classification Accuracy***

***Logarithmic Loss***

***Confusion Matrix***

***Area under Curve***

***F1 Score***

***Mean Absolute Error***

***Mean Squared Error***

**Classification Accuracy**

Classification Accuracy is what we usually mean, when we use the term accuracy. It is the ratio of number of correct predictions to the total number of input samples.

It works well only if there are equal number of samples belonging to each class.For example, consider that there are 98% samples of class A and 2% samples of class B in our training set. Then our model can easily get **98% training accuracy** by simply predicting every training sample belonging to class A.When the same model is tested on a test set with 60% samples of class A and 40% samples of class B, then the **test accuracy would drop down to 60%.**Classification Accuracy is great, but gives us the false sense of achieving high accuracy.The real problem arises, when the cost of misclassification of the minor class samples are very high. If we deal with a rare but fatal disease, the cost of failing to diagnose the disease of a sick person is much higher than the cost of sending a healthy person to more tests.

**Logarithmic Loss**

Logarithmic Loss or Log Loss, works by penalising the false classifications. It works well for multi-class classification. When working with Log Loss, the classifier must assign probability to each class for all the samples. Suppose, there are N samples belonging to M classes, then the Log Loss is calculated as below :



where,

y\_ij, indicates whether sample i belongs to class j or not

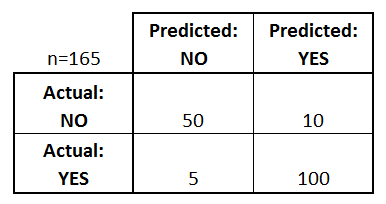
p\_ij, indicates the probability of sample i belonging to class j

Log Loss has no upper bound and it exists on the range [0, ∞). Log Loss nearer to 0 indicates higher accuracy, whereas if the Log Loss is away from 0 then it indicates lower accuracy.

In general, minimising Log Loss gives greater accuracy for the classifier.

**Confusion Matrix**

Confusion Matrix as the name suggests gives us a matrix as output and describes the complete performance of the model.Lets assume we have a binary classification problem. We have some samples belonging to two classes : YES or NO. Also, we have our own classifier which predicts a class for a given input sample. On testing our model on 165 samples ,we get the following result.



Confusion Matrix

There are 4 important terms :

* **True Positives** : The cases in which we predicted YES and the actual output was also YES.
* **True Negatives** : The cases in which we predicted NO and the actual output was NO.
* **False Positives** : The cases in which we predicted YES and the actual output was NO.
* **False Negatives** : The cases in which we predicted NO and the actual output was YES.

Accuracy for the matrix can be calculated by taking average of the values lying across the**“main diagonal”**i.e





Confusion Matrix forms the basis for the other types of metrics.

**Area Under Curve**

*Area Under Curve(AUC)* is one of the most widely used metrics for evaluation. It is used for binary classification problem. *AUC* of a classifier is equal to the probability that the classifier will rank a randomly chosen positive example higher than a randomly chosen negative example. Before defining *AUC*, let us understand two basic terms :

**True Positive Rate (Sensitivity) : True Positive Rate is defined as TP/ (FN+TP). True Positive Rate corresponds to the proportion of positive data points that are correctly considered as positive, with respect to all positive data points.**



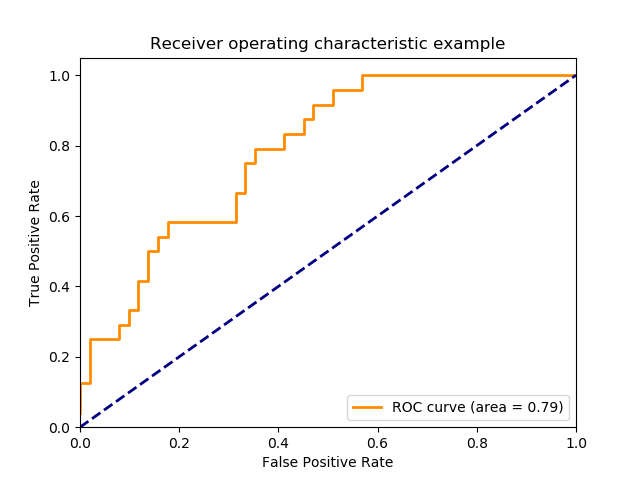
True Negative Rate (Specificity)**: True Negative Rate is defined as *TN / (FP+TN)*. False Positive Rate corresponds to the proportion of negative data points that are correctly considered as negative, with respect to all negative data points.**



**False Positive Rate**: False Positive Rate is defined as *FP / (FP+TN)*. False Positive Rate corresponds to the proportion of negative data points that are mistakenly considered as positive, with respect to all negative data points.



***False Positive Rate* and *True Positive Rate* both have values in the range**[0, 1]**. *FPR* and *TPR* both are computed at varying threshold values such as (0.00, 0.02, 0.04, …., 1.00) and a graph is drawn. *AUC* is the area under the curve of plot *False Positive Rate vs True Positive Rate* at different points in**[0, 1]**.**



*As evident,*AUC*has a range of [0, 1]. The greater the value, the better is the performance of our model.*

**F1 Score**

*F1 Score is used to measure a test’s accuracy*

*F1 Score is the Harmonic Mean between precision and recall. The range for F1 Score is [0, 1]. It tells you how precise your classifier is (how many instances it classifies correctly), as well as how robust it is (it does not miss a significant number of instances).*

*High precision but lower recall, gives you an extremely accurate, but it then misses a large number of instances that are difficult to classify. The greater the F1 Score, the better is the performance of our model. Mathematically, it can be expressed as :*



**F1 Score**

*F1 Score tries to find the balance between precision and recall.*

***Precision :****It is the number of correct positive results divided by the number of positive results predicted by the classifier.*

**

*Precision*

***Recall :****It is the number of correct positive results divided by the number of*all *relevant samples (all samples that should have been identified as positive).*

**

*Recall*

***Mean Absolute Error***

*Mean Absolute Error is the average of the difference between the Original Values and the Predicted Values. It gives us the measure of how far the predictions were from the actual output. However, they don’t gives us any idea of the direction of the error i.e. whether we are under predicting the data or over predicting the data. Mathematically, it is represented as :*

**

***Mean Squared Error***

*Mean Squared Error(MSE) is quite similar to Mean Absolute Error, the only difference being that MSE takes the average of the****square****of the difference between the original values and the predicted values. The advantage of MSE being that it is easier to compute the gradient, whereas Mean Absolute Error requires complicated linear programming tools to compute the gradient. As, we take square of the error, the effect of larger errors become more pronounced then smaller error, hence the model can now focus more on the larger errors.*

**

*Mean Squared Error*