What is machine learning?

Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.

IBM has a rich history with machine learning. One of its own, Arthur Samuel, is credited for coining the term, “machine learning” with his research (link resides outside ibm.com) around the game of checkers. Robert Nealey, the self-proclaimed checkers master, played the game on an IBM 7094 computer in 1962, and he lost to the computer. Compared to what can be done today, this feat seems trivial, but it’s considered a major milestone in the field of artificial intelligence.

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 new 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 such as Python that accelerate solution development by using platforms like TensorFlow or 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. The deep learning process 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 large amounts of data. You can think of deep learning as "scalable machine learning" as Lex Fridman notes in this MIT lecture (link resides outside ibm.com).

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.
See the blog post “AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What’s the Difference?” for a closer look at how the different concepts relate.
Related content
Explore the watsonx.ai interactive demo
Download “Machine learning for Dummies”
- This link downloads a pdf
Explore Gen AI for developers
How does machine learning work?
UC Berkeley (link resides outside ibm.com) breaks out the learning system of a machine learning algorithm into three main parts.
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.
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.
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 iterative “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 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 or 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, also known as unsupervised machine learning, uses machine learning algorithms to analyze and cluster unlabeled datasets (subsets called clusters). 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.
For a deep dive into the differences between these approaches, check out "Supervised vs. Unsupervised Learning: What's the Difference?"

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.

The IBM Watson® system that won the Jeopardy! challenge in 2011 is a good example. The system used reinforcement learning to learn when to attempt an answer (or question, as it were), which square to select on the board, and how much to wager—especially on daily doubles.

Learn more about reinforcement learning

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.

Advantages and disadvantages of machine learning algorithms

Depending on your budget, need for speed and precision required, each algorithm type—supervised, unsupervised, semi-supervised, or reinforcement—has its own advantages and disadvantages. For example, decision tree algorithms are used for both predicting numerical values (regression problems) and classifying data into categories. Decision trees use a branching sequence of linked decisions that may be represented with a tree diagram. A prime advantage of decision trees is that they are easier to validate and audit than a neural network. The bad news is that they can be more unstable than other decision predictors.

Overall, there are many advantages to machine learning that businesses can leverage for new efficiencies. These include machine learning identifying patterns and trends in massive volumes of data that humans might not spot at all. And this analysis requires little human intervention: just feed in the dataset of interest and let the machine learning system assemble and refine its own algorithms—which will continually improve with more data input over time. Customers and users can enjoy a more personalized experience as the model learns more with every experience with that person.

On the downside, machine learning requires large training datasets that are accurate and unbiased. GIGO is the operative factor: garbage in / garbage out. Gathering sufficient data and having a system robust enough to run it might also be a drain on resources. Machine learning can also be prone to error, depending on the input. With too small a sample, the system could produce a perfectly logical algorithm that is completely wrong or misleading. To avoid wasting budget or displeasing customers,

organizations should act on the answers only when there is high confidence in the output.

Real-world machine learning use cases

Here are just a few examples of machine learning you might encounter every day:

Speech recognition: It is also known as automatic speech recognition (ASR), computer speech recognition, or speech-to-text, and it is a capability which uses natural language processing (NLP) to translate human speech into a written format. Many mobile devices incorporate speech recognition into their systems to conduct voice search—e.g. Siri—or improve accessibility for texting.

Customer service: Online chatbots are replacing human agents along the customer journey, changing the way we think about customer engagement across websites and social media platforms. Chatbots answer frequently asked questions (FAQs) about topics such as shipping, or provide personalized advice, cross-selling products or suggesting sizes for users. Examples include virtual agents on e-commerce sites; messaging bots, using Slack and Facebook Messenger; and tasks usually done by virtual assistants and voice assistants.

Computer vision: This AI technology enables computers to derive meaningful information from digital images, videos, and other visual inputs, and then take the appropriate action. Powered by convolutional neural networks, computer vision has applications in photo tagging on social media, radiology imaging in healthcare, and self-driving cars in the automotive industry.

Recommendation engines: Using past consumption behavior data, AI algorithms can help to discover data trends that can be used to develop more effective cross-selling strategies. Recommendation engines are used by online retailers to make relevant product recommendations to customers during the checkout process.

Robotic process automation (RPA): Also known as software robotics, RPA uses intelligent automation technologies to perform repetitive manual tasks.

Automated stock trading: Designed to optimize stock portfolios, AI-driven high-frequency trading platforms make thousands or even millions of trades per day without human intervention.

Fraud detection: Banks and other financial institutions can use machine learning to spot suspicious transactions. Supervised learning can train a model using information about known fraudulent transactions. Anomaly detection can identify transactions that look atypical and deserve further investigation.

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 (link resides outside ibm.com) 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 (link resides outside ibm.com) 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. However, at the moment, these only serve to guide. Some research (link resides outside ibm.com) shows that the combination of distributed responsibility and a lack of foresight into potential consequences aren't conducive to preventing harm to society.

Read more about IBM's position on AI Ethics

How to choose the right AI platform for machine learning

Selecting a platform can be a challenging process, as the wrong system can drive up costs, or limit the use of other valuable tools or technologies. When reviewing multiple vendors to select an AI platform, there is often a tendency to think that more features = a better system. Maybe so, but reviewers should start by thinking through what the AI platform will be doing for their organization. What machine learning capabilities need to be delivered and what features are important to accomplish them? One missing feature might doom the usefulness of an entire system. Here are some features to consider.

MLOps capabilities. Does the system have:

a unified interface for ease of management?

automated machine learning tools for faster model creation with low-code and no-code functionality?

decision optimization to streamline the selection and deployment of optimization models?

visual modeling to combine visual data science with open-source libraries and notebook-based interfaces on a unified data and AI studio?

automated development for beginners to get started quickly and more advanced data scientists to experiment?

synthetic data generator as an alternative or supplement to real-world data when real-world data is not readily available?

Generative AI capabilities. Does the system have:

a content generator that can generate text, images and other content based on the data it was trained on?

automated classification to read and classify written input, such as evaluating and sorting customer complaints or reviewing customer feedback sentiment?

a summary generator that can transform dense text into a high-quality summary, capture key points from financial reports, and generate meeting transcriptions?

a data extraction capability to sort through complex details and quickly pull the necessary information from large documents?