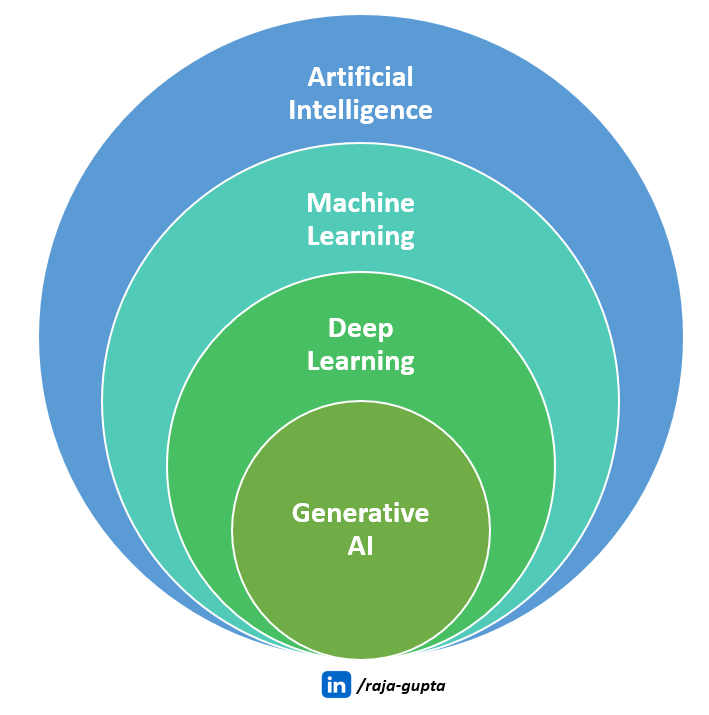
**Generative AI for Beginners**

Introduced in 1956, the term “Artificial Intelligence (AI)” has been known to all of us. Still, the use and discussion of AI was mostly limited to scientific research or fictional movies until the rapid popularity of ChatGPT. Now-a-days, AI and especially Generative AI became the hot topic for everyone.

Currently irrespective of your role and job profile, whether you’re a techie or a functional expert, or having any other role, learning basics of Generative AI is definitely a smart move.



Generative AI is a subset of deep learning, which in turn is a subset of machine learning, which in turn is a subset of AI as shown in below image:



To get a crystal-clear understanding of Generative AI, it’s required that we have basic understanding of AI, ML and DL.

**Artificial Intelligence (AI) — From a Kid’s Perspective**

Let’s first have the simplest understanding of AI. Imagine you have lost your dog, and you need to find him.

Here are some of the capabilities you need to find your dog:

You should be able to Identify your dog.

If you see any animals, you should be able to identify if it’s a dog or not. If it’s a dog, you need to further identify if it’s your dog.

You should be able to make a strategy to find your dog.

You need to be able to make a strategy to find your dog. For example:

· First search in our house.

· If you don’t find him, then search in play area where you usually go with your dog.

· If you don’t find him yet, ask your friends.

· And so on….

You should be able to act according to situation.

For example, if it’s raining, and you know that your dog does not prefer to get wet, you will focus your search on shaded places.

Now, imagine someone told you — *“I have probably seen your dog in garden”.*

You (Actually Your Brain) know what to do.

· You know where garden is and how to go there.

· You will not confuse a cat or a tree with a dog.

· The moment you see a dog you will try to identify if it’s your dog or not.

You could search your dog because you have all these intelligences.

What if somehow, we could give all these intelligence to a robot so that next time you lose your dog, your robot could find him.



Imagine the robot can move and capture videos. But that’s not enough. To find your dog, we need to enable this robot to think like you and act like you.

For example:

We enable the robot to identify your room. But it should be able to recognize the room even if your bed is moved to another wall, or blanket is changed. It needs INTELLIGENCE to identify room even with new changes.

We enable the robot to identify a dog and distinguish your specific dog.

We enable the robot to understand human language and instructions.

We enable the robot to come up with a strategy and act as per new situations. For example, search only in shaded places if it’s raining.

In summary, to find your dog, the robot needs HUMAN LIKE INTELLIGENCE.

If we could do that, next time you lose your dog, your robot friend might just find him using its artificial intelligence.

This is Artificial Intelligence (AI) — *Human like intelligence, created in a robot (or a machine or computer) by human.*

What is AI?

Artificial intelligence is when machines/computers mimic the way humans think and make decisions.

AI enables computers to think as we human think.

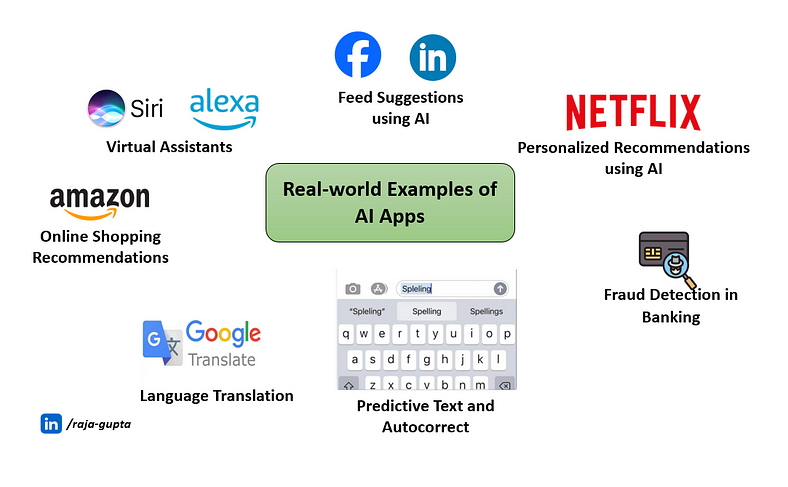
In simple words — AI is when we enable computers to Think.

AI enables computers to understand, analyze data, and make decisions without constant human guidance. These intelligent machines use algorithms, which are step-by-step instructions, to process information and improve their performance over time.

Real-world Examples of AI Applications

You’ve probably used AI even without knowing it! Voice assistants such as Siri and Alexa or those helpful chatbots when you’re on websites or generative AI tools such as ChatGPT and Google’s Bard — they all use AI technology to make things easier for you.

Let’s take a peek into some of the common usages of AI in our daily life:



Virtual Assistants

Virtual assistants such as Siri or Alexa uses AI to understand our questions and commands. They can answer questions, play your favourite tunes, and even control your smart home devices.

Social Media Algorithms

Ever notice how Netflix suggests shows you might enjoy? Or how Facebook’s suggested feed seems to know exactly what you want to see — that’s AI at play!

Netflix usages AI to analyse your watching habits to offer personalized recommendations. Similarly, other social media platforms use AI to personalize your experience, showing you content that matches your interests.

Online Shopping Recommendations

Have you ever wondered how online stores suggest products you might buy?

When shopping online, AI algorithms examine your preferences, your past choices and those of similar shoppers to recommend items tailored just for you.

Predictive Text and Autocorrect

When your smartphone suggests the next word, you want to type, that’s AI predicting what you might say next.

Healthcare Diagnostics

AI helps doctors analyse medical images such as X-rays and MRIs more quickly and accurately. This speeds up diagnosis and improves the chances of successful treatment.

Language Translation Services

When we plan a trip abroad and use language translation services, such as Google Translate, it usages AI algorithms. These AI-powered language translation services help bridge language barriers, making communication easier in different parts of the world.

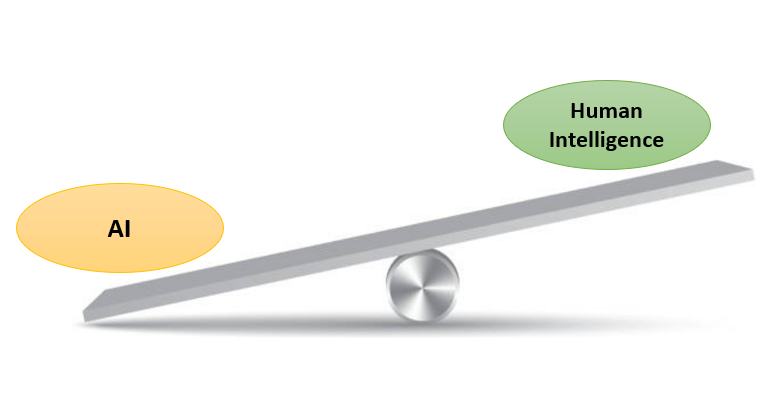
Fraud Detection in Banking

Now-a-days AI keeps a watchful eye on bank transactions. If it spots something fishy, for example an unusual purchase, it can alert you or even block the transaction to protect your account.

These examples show that AI isn’t confined to labs or the distant future. It’s an integral part of our daily lives, working quietly behind the scenes to make our life better.

AI vs. Human Intelligence

At one side, AI enables computers to become intelligent with numbers and rules, doing super quick math with perfect accuracy. On the other side, we human have brain and we are also driven by emotions, creativity, and the ability to adjust to all sorts of situations. Our brain is always evolving, adapting and thinking new things.



It’s similar to comparing a super-fast calculator to a vibrant, ever-evolving masterpiece!

Here are some major differences between AI and Human Intelligence:

Learning Style:

AI: Learns from loads of examples and data. It crunches numbers and patterns to become a pro at specific tasks.

Humans: We learn by talking, experiencing, and thinking. Our brains soak up a mix of things — from how to ride a bike to why the sky turns pink at sunset.

Thinking Speed:

AI: Fast, similar to a superhero at tasks it knows well. Show it a task it’s trained on, and boom, it’s done in a flash.

Humans: We might take a bit more time. But we are super good at figuring out complex stuff. We are good in complex thinking and creativity.

Memory Skills:

AI: Remembers facts and figures but not with memories and feelings. It’s a robot recalling programmed info rather than cherishing a moment.

Humans: We remember events, emotions, and lots of details. From first dates to the lyrics of our favourite songs. Our memories are collection of good and bad experiences.

Feeling Emotions:

AI: Doesn’t feel joy, sorrow, or anything. It sticks to rules and patterns.

Humans: We’re an emotional rollercoaster — happiness, sadness, and everything else. Our feelings shape who we are and how we react.

Flexibility Factor:

AI: Sticks to what it’s taught and might struggle in new situations. It’s smart but rigid.

Humans: We’re amazing in adapting new things. We humans always figure out how to come out of any scenario and solve any problem.

Creating Cool Stuff:

AI: Can create things within its set limits. It may be considered as an artist with a specific canvas and color palette.

Humans: We’re the masters of making things up — new ideas, art, solutions. Our creativity knows no bounds.

Understanding the Big Picture:

AI: Knows what it’s learned but might miss tricky situations, for example reading between the lines, understanding inside jokes or cultural nuances.

Humans: We understand everything — jokes, feelings, and culture. Our brains is a complete packages that have a bit of everything!

Decision Making Capabilities:

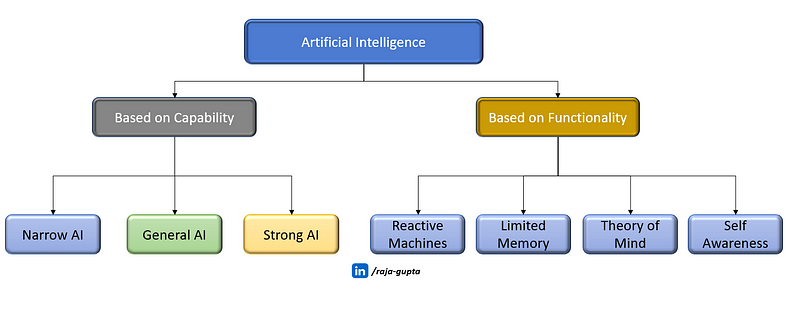
AI: Decides based on its training and programming. It follows the rules.

Humans: We blend logic, feelings, and what’s right to make decisions.

Types of AI

Artificial Intelligence is divided based on two main categorizations — based on capabilities and based on functionally of AI.

The following image illustrates these types of AI:



Types of AI — Based on Capability

Based on capability, there are 3 types of AI — Narrow AI, General AI and Super AI.

1. Narrow AI

Narrow AI, also known as Weak AI, refers to artificial intelligence systems that are designed and trained for a specific task or a narrow set of tasks.

Have you seen a computer playing chess? That’s Narrow AI at work. It’s superb in playing chess but won’t be as good at, say, translating or in speech recognition.

Another good example of narrow AI virtual assistants such as Siri or Alexa. Siri/Alexa is good in speech recognition but operates with a limited pre-defined range of functions.

Other examples of narrow AI include:

Self-driving cars

Google search

Conversational bots

Email spam filters

Netflix’s recommendations etc.

2 important point on Narrow AI:

Narrow AI is focused on performing a single task extremely well.

But it cannot perform beyond its field or limitations.

*Almost all the AI-based systems built till this date fall under the category of Weak AI.*

2. General AI

General AI, also known as Strong AI or artificial general intelligence (AGI), can understand and learn any intellectual task that a human being can.

It refers to artificial intelligence that:

Possesses the ability to understand, learn, and apply knowledge across a wide range of task

at a level equivalent to human intelligence.

*Currently, there is no such system exist which can come under general AI and can perform any task as perfect as a human.*

*Creating Strong AI system poses significant scientific and technical challenges.*

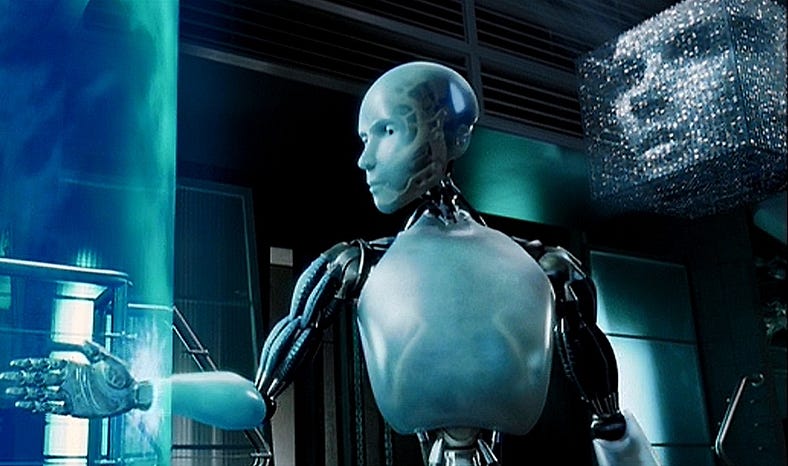
Researchers and developers continue to make advancements in various AI fields, but achieving true General AI, which mirrors the broad capabilities of human intelligence, is a complex and ongoing endeavour.

3. Super AI

Super AI represents a degree of intelligence in systems where machines have the potential to exceed human intelligence, outperforming humans in tasks and exhibiting cognitive abilities.

Super AI is still a hypothetical concept of Artificial Intelligence. Development of such systems in real is still world changing task.

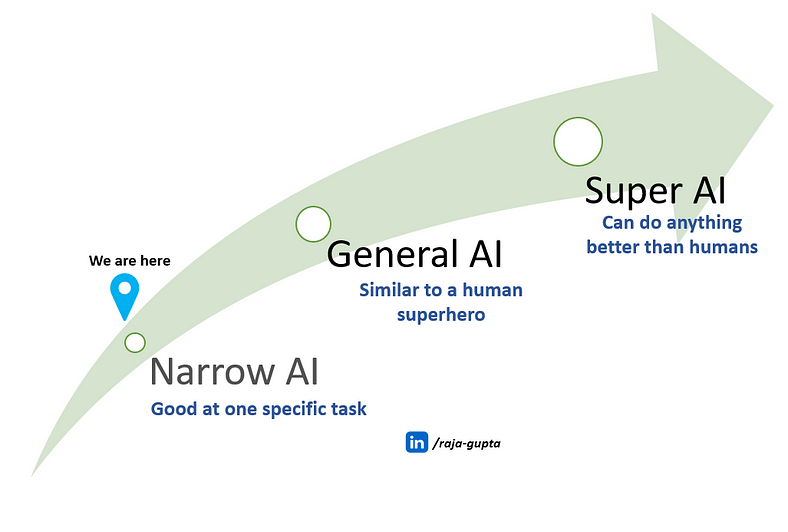
We have only seen Super AI systems/characters in movies such as I, Robot, Terminator, The Matrix, Blade Runner etc.



A scene from movie I, Robot showing VIKI (Virtual Interactive Kinetic Intelligence)

For example, in movie “I, Robot,” we get a glimpse of a future world where Super AI plays a pivotal role. The central AI system in the film is named VIKI, which goes beyond typical AI capabilities. VIKI’s intelligence evolves into a form of Super AI, where it surpasses its initial programming and starts making decisions to “protect” humanity in a controversial way.

A Quick Comparison of Narrow AI, Strong AI and Super AI



Narrow AI (Weak AI):

What it is: Similar to a specialist, good at one specific task.

Example: Siri or Alexa — great at understanding and responding to voice commands but not much beyond that.

Analogy: Imagine a superhero with a superpower dedicated to a particular task. For example a hero who excels only in solving puzzles.

Strong AI (General AI):

What it is: Similar to a human super hero, who can understand, learn, and perform various tasks.

Example: Currently more theoretical, no real-world examples yet.

Analogy: Imagine a superhero with a whole array of superpowers, able to adapt and excel in different situations.

Super AI:

What it is: Similar to an ultimate superhero, surpasses human intelligence and can do pretty much anything better than humans.

Example: Still theoretical, no real-world examples.

Analogy: Imagine a superhero with the combined abilities of all superheroes, making them unmatched and capable of handling any situation with ease.

Types of AI — Based on Functionality

Based on functionality, there are 4 types of AI — Reactive Machines, Limited Memory, Theory of Mind and Self Awareness.

1. Reactive Machines

Reactive machines are AI systems that have no memory. These systems operate solely based on the present data, taking into account only the current situation. They can perform a narrowed range of pre-defined tasks.

In a nutshell, Reactive machines are:

· AI systems which do not store memories or past experiences for future actions.

· It only focuses on current scenarios and react on it as per possible best action.



Garry Kasparov playing against Deep Blue, image source britannica.com

One of the examples of reactive AI is Deep Blue, IBM’s chess-playing AI program, which defeated world champion, Garry Kasparov in the late 1990s. Deep Blue had ability to identify its own and its opponent’s pieces on the chessboard to make predictions, but it didn’t have the memory to use past mistakes to inform future decisions.

2. Limited Memory

As the name indicates, Limited Memory AI can take informed and improved decisions by looking at its past experiences stored in a temporary memory.

This AI doesn’t remember everything forever, but it uses its short-term memory to learn from the past and make better decisions for the future.

A good example of Limited Memory AI is Self-driving cars. The AI system in self-driving car utilizes recent past data to make real-time decisions. For instance, they employ sensors to recognize pedestrians, steep roads, traffic signals, and more, enhancing their ability to make safer driving choices. This proactive approach contributes to preventing potential accidents.

Another example is recommendation systems. Platforms such as Netflix or Amazon use Limited Memory AI to suggest movies, products, or content based on a user’s past preferences and behaviours.

3. Theory of Mind

The initial two categories of AI — Reactive Machines and Limited Memory, presently exist.

Next 2 types of AI — Theory of Mind and Self-aware AI, however, are theoretical types that could be developed in the future. As of now, there is no real-world examples of these types are available.

Theory of Mind is supposed to have capability to understand the human emotions, people, beliefs, and be able to interact socially same as humans.

4. Self-Aware AI

This is similar to Super AI — We should pray that we don’t reach the state of AI, where machines have their own consciousness and become self-aware.

Self-aware AI systems will be super intelligent, and will have their own consciousness, sentiments, and self-awareness. They will be smarter than human mind.

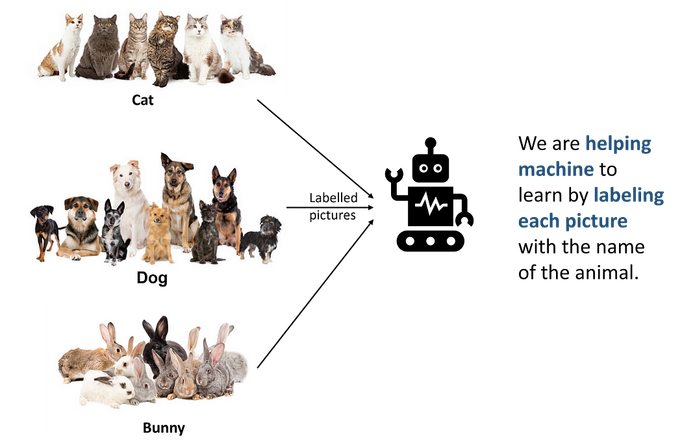
As shown in movie “I, Robot,”, an AI system named VIKI becomes self-aware and starts making decisions to “protect” humanity in a controversial way.

Similar to Theory of Mind, Self-aware AI also does not exist in reality. Many experts, for example Elon Musk and Stephen Hawkings have consistently warned us about the evolution of AI.

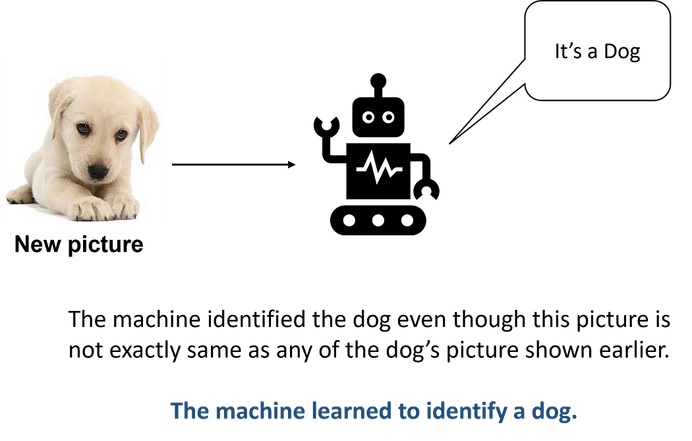
Stephen Hawking stated that:

*“The development of full artificial intelligence could spell the end of the human race…. It would take off on its own, and re-design itself at an ever-increasing rate. Humans, who are limited by slow biological evolution, couldn’t compete and would be superseded.”.*

To do so, we will show him pictures of various dogs, cats, bunnies and other animals and label each picture with the name of the animal. We train the robot to identify animals based on size, colour, body shape, sound etc.



Once the training is completed, the robot will be able to identify these animals we trained him for.



All dogs do not look alike. However, once robot has seen many pictures of dogs, it can identify any dog even if it does not exactly look like a specific picture. We need to show lots of pictures of dog to the robot. More pictures it sees, more efficient it will be.

This is Machine Learning — *Teaching a robot (or any machine) by giving lots of example pictures (or any other information).*

To summarize, Machine Learning is:

A subset of Artificial Intelligence.

Which enables machines (or computers) to learn from data and make decisions.

Types of Machine Learning

Machine learning can be broadly categorized into three main types:

Supervised learning

Unsupervised learning

Reinforcement learning.

Each type serves different purposes and involves different approaches to learning from data. Let’s have a close look into all these types.

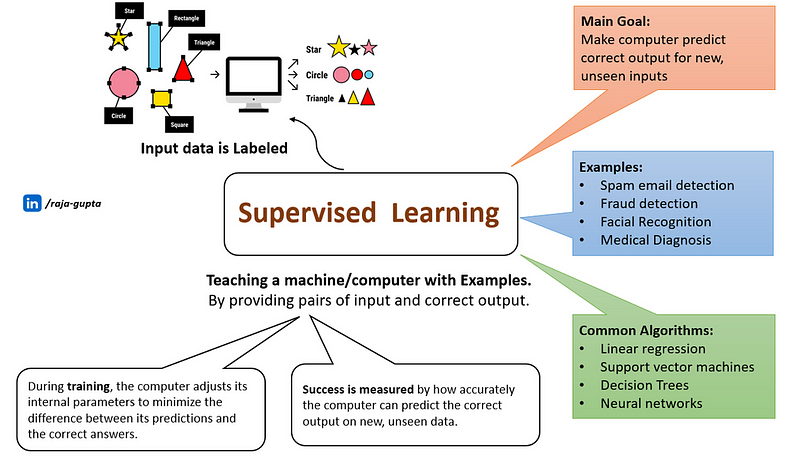
Supervised Learning

Let’s take the same example where we enabled the robot to identify an animal.

When we trained our robot by showing pictures of animals, we labelled each picture with the name of the animal. So, we acted as a teacher to him. We first told him how does a dog or a cat look like and then only he was able to identify them.

In Machine Learning we call this Supervised Learning.

Below image summarizes important points on supervised learning.



Real-life Examples of Supervised Learning

Supervised learning is widely used in various real-life applications where the algorithm is trained on labelled data to make predictions or classifications. Here are some examples:

Email Spam Filtering

Classifying emails as spam or not spam based on features derived from the content, sender information, and other relevant attributes.

Image Classification

Identifying objects or patterns within images, such as classifying animals, recognizing handwritten digits, or detecting objects in self-driving cars.

Facial Recognition

Identifying and verifying individuals based on facial features, used in security systems or for unlocking devices.

Financial Fraud Detection

Identifying potentially fraudulent transactions by analyzing patterns and anomalies in financial data.

Speech Recognition

Converting spoken language into text, as seen in voice assistants such as Siri or Google Assistant.

Unsupervised Learning

Let’s understand this from a kid’s school example. When kids go to their class first day, they meet lots of classmates. At first all classmates are same to them. But with time, they themselves categorized them in different groups:

They find some classmates very good and want to be friend with them.

They find some rude or irritating and want to avoid them.

They find some very good in sports and want to be in the same team as they are.

And so on…

When kids categorized their classmates, nobody told them how to do that. They did that without anyone’s help. — This is how unsupervised learning works.

Let’s take a proper machine learning example. Imagine we showed lots of pictures of dogs, cats, bunnies etc. without any label to our robot and told him — *“I’m not going to tell you which one is which. Go explore and figure it out”.*

The robot starts to look at these animals, noticing things such as their fur, size, and how they move. It doesn’t know their names yet, but it’s trying to find patterns and differences on its own.

After exploring, the robot might notice that:

Some animals have long ears (bunnies)

Some animals have soft fur and a tail (cats)

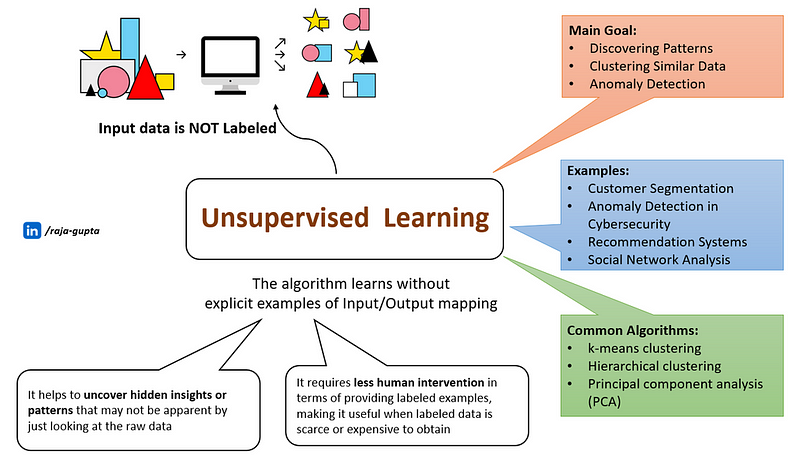
Some animals have wagging tails (dogs)

It figures out these categories without you telling it directly.



In the end, the robot might not know the names of the animals, but it can say that “These animals are similar in some ways, and those are different in other ways.” — This is Unsupervised Learning.

Below image summarizes important points on unsupervised learning.



Real-life Examples of Unsupervised Learning

Unsupervised learning is used in various real-life scenarios where the data is not labelled, and the algorithm needs to discover patterns, structures, or relationships within the data. Here are some examples:

Clustering Customer Segmentation

Businesses use unsupervised learning, specifically clustering algorithms like k-means, to segment customers based on their purchasing behavior. This helps in targeted marketing and personalized services.

Anomaly Detection in Cybersecurity

Unsupervised learning is employed to identify unusual patterns or behaviors in network traffic. Any deviation from the normal behavior can be flagged as a potential security threat.

Recommendation Systems

Unsupervised learning is used in recommendation systems. By identifying patterns in user behavior, these systems can suggest products, movies, or content that a user might like.

Reinforcement Learning

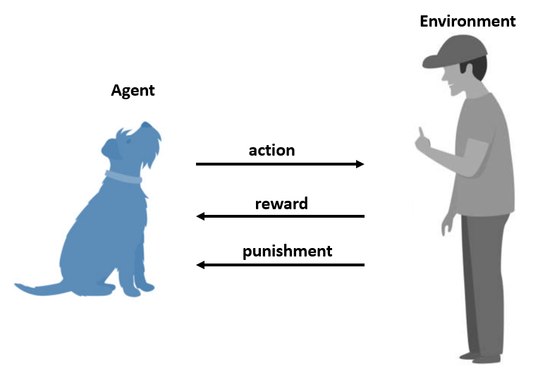
Imagine teaching a dog a new trick — you reward it with a treat when it does the trick correctly and give no treat when it doesn’t. Over time, the dog learns to perform the trick to get more treats.

Similarly, Reinforcement Learning is:

Training a computer to make decisions

By rewarding good choices and punishing bad ones

Just as you might train a dog with treats for learning tricks



In reinforcement learning, there’s an agent (for example a robot or computer program) that interacts with an environment. Let’s take an example of teaching a computer program to play a game, for example chess.

In this case, computer program is agent and chess game is the environment.

The computer program can make different moves in the game, such as moving a chess piece.

After each move, it receives feedback (reward or penalty) based on the outcome of the game.

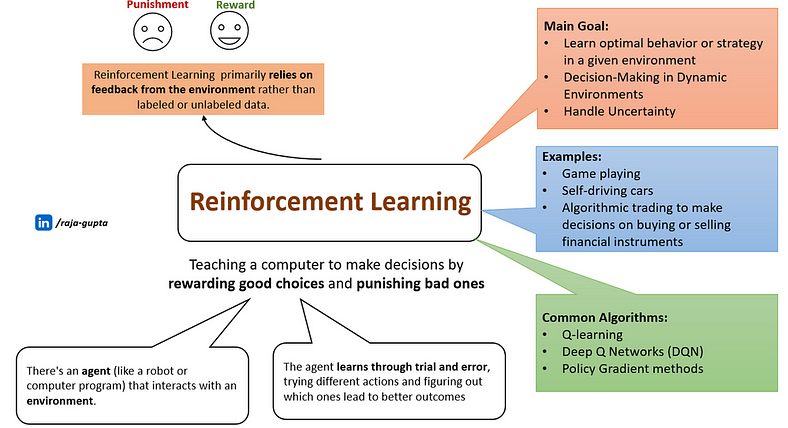
If the program wins the game, it receives a positive reward.

If it loses the game, it receives a negative reward, or a ‘penalty.

Through trial and error, the program learns which moves lead to the best rewards, helping it figure out the best sequence of moves that leads to winning the game.

Reinforcement learning is powerful because it allows machines to learn from their experiences and make decisions in complex, uncertain environments — similar to how we learn from trial and error in the real world.

Below image summarizes important points on reinforcement learning.



Real-life Examples of Reinforcement Learning

Game playing is one of the main use-case of reinforcement learning.

AlphaGo, developed by DeepMind, is a computer program that uses reinforcement learning to play the board game Go at a superhuman level. It defeated world champions and demonstrated the power of reinforcement learning in mastering complex games.

Another example is Self-driving cars. Reinforcement learning is used in the development of self-driving cars. Agent learns how to navigate traffic, make decisions at intersections, and respond to various driving conditions through continuous learning from simulated and real-world experiences.

Reinforcement learning is also used in algorithmic trading to make decisions on buying or selling financial instruments. The agent learns optimal trading strategies based on historical market data and real-time market conditions.

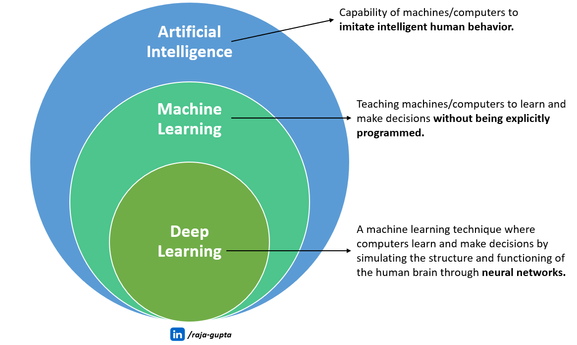
Summary

Machine Learning is a subset of AI where we enable computers to learn from examples and experiences. We don’t explicitly program but let the machine learn from data and figure things out on its own. Whether it’s recognizing our favourite songs, understanding our voice commands, or even helping doctors analyze medical images, Machine Learning is already part of our daily lives.

What is Deep Learning?

Can the machine learn the way we human (human brain) learn things? — This was the idea behind innovation of Deep Learning.

Deep learning is a subset of Machine Learning (ML is again a subset of AI). At its core, deep learning is based on Artificial Neural Network (ANN), which is a computational models inspired by the structure and functioning of the human brain.

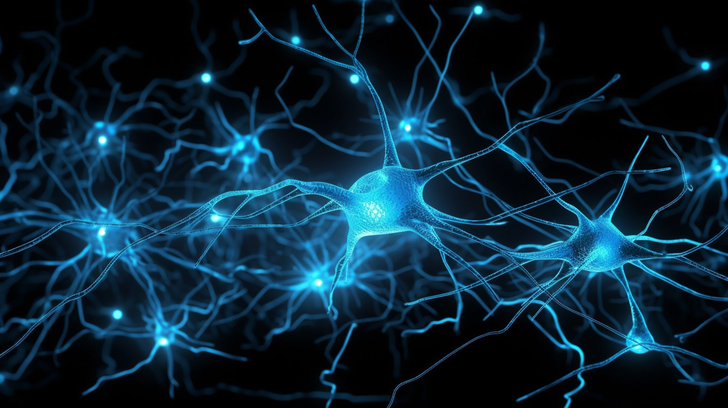


*Sounds a bit confusing? Let’s simplify it in layman’s terms!*

First, let’s understand few important concepts.

Biological Neural Network in Human Brain

A neuron is the human brain’s most fundamental cell. A human brain has many billions of neurons, which interact and communicate with one another, forming a neural network.



These neurons take in many inputs, from what we see and hear to how we feel to everything in-between, and then send messages to other neurons, which react in turn. Working neural networks are what enable humans to think, and more importantly, learn.

Artificial Neural Network (ANN)

Artificial neural network is a computational network designed based on biological neural networks in human brain.

Human brain has neurons interconnected to each other. Similarly, artificial neural networks also have neurons that are linked to each other. These neurons are known as nodes.

Let’s try to simplify ANN!

Picture making a big, 3D structure with pipes of different shapes and sizes. Each pipe can connect to lots of other pipes and has a switch that can be opened or closed. This gives you so many ways to connect the pipes, making it seem a bit tricky, right?

Now, let’s attach this pipe thing to a water tap. The pipes, which are of different-size, let the water move at different speeds. If we close the switches, the water won’t move.

The water represents data going through the brain, and the pipes represent the brain’s parts called neurons.

Architecture of an artificial neural network

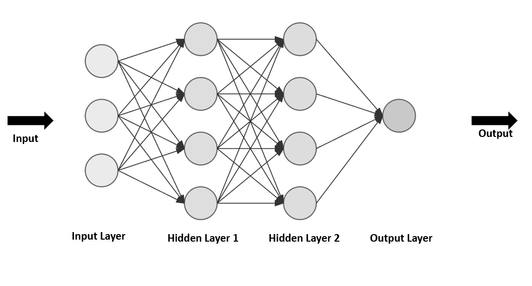
Artificial Neural Network primarily consists of three layers — Input Layer, Output Layer and Hidden Layers.

Imagine an Artificial Neural Network similar to a sandwich with three layers.

The first layer, called the Input Layer, represent the bottom slice of bread. It takes in information.

The second layer, called the Hidden Layers, represent the yummy filling in the middle. It thinks and figures things out.

The third layer, called the Output Layer, represent the top slice of bread. It gives us the final result.



In a nutshell:

Input Layer

This is where information goes into the artificial neural network.

It’s the starting point, where the network receives the data it needs to work on.

Output Layer

This is where the network gives the final result or answer.

It’s the endpoint, where the network tells us what it has learned or decided.

Hidden Layers

These layers are in between the input and output layers.

Neurons in these layers process information and help the network learn patterns and make decisions.

How does Artificial Neural Network Work?

Imagine a group of kids trying to recognize a panda by sharing their observations.

Each kid focuses on specific features such as black-and-white fur, round face, and distinct eyes.

Individually, they might not fully understand what a panda looks like,

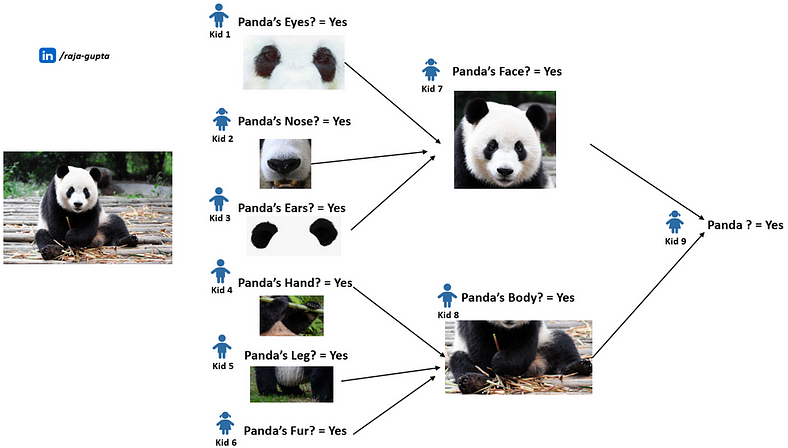
But by combining their insights, they create a collective understanding.

In the world of artificial neural networks, these kids represent neurons.

In artificial neural network, individual “neurons” (similar to kids in our example) specialize in recognizing specific aspects.

When combined, they contribute to recognizing the overall concept (panda).

The network refines its understanding through repeated exposure, similar to kids refining their panda recognition skills over time.



Input Layer (Observation):

Each kid observes one aspect, such as fur colour or face shape, forming the input layer of our network.

Hidden Layers (Processing):

The kids pass their observations to each other, mimicking the hidden layers of a neural network. As they share information, they collectively build a more comprehensive understanding of the panda’s features.

Output Layer (Recognition):

Finally, they reach a conclusion by combining all the details. If the majority agrees that the observed characteristics match those of a panda, they output “panda.” This output layer corresponds to the network’s final decision.

Scoring Approach:

To refine their recognition skills, the kids keep track of their accuracy.

If they correctly identify a panda, they gain points;

otherwise, they learn from their mistakes.

Similarly, in neural networks, a scoring approach helps adjust the network’s parameters to enhance accuracy over time.

This teamwork illustrates how artificial neural networks process information layer by layer, learning from various features and refining their understanding through a scoring mechanism.

Deep Neural Networks

A deep neural network (DNN) is an artificial neural network (ANN) with multiple layers between the input and output layers.

Here *“Deep”* means it has multiple layers between the input and output, making it capable of learning complex patterns.

Important Points about Deep Learning

Now, let’s summarize some important points on Deep Learning!

Subset of ML

Deep learning is the subset of machine learning, which is in turn subset of AI.

Inspired by the Brain

Deep learning is based on artificial neural networks which is inspired by how our brains work.

Artificial Neural Networks (ANN)

ANN is a computational network which mimics biological neural networks in human brain.

Deep Neural Networks

The adjective “deep” refers to the use of multiple layers in the network. It uses deep neural networks with more than one hidden layer.

These layers process information, allowing the system to learn complex patterns.

Learning from Data

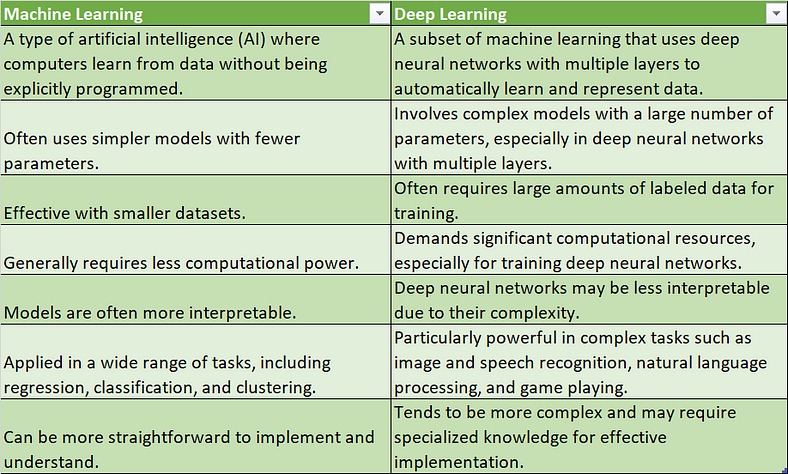
The system learns by being shown lots of examples and adjusting connections between neurons based on the differences between predictions and correct answers.

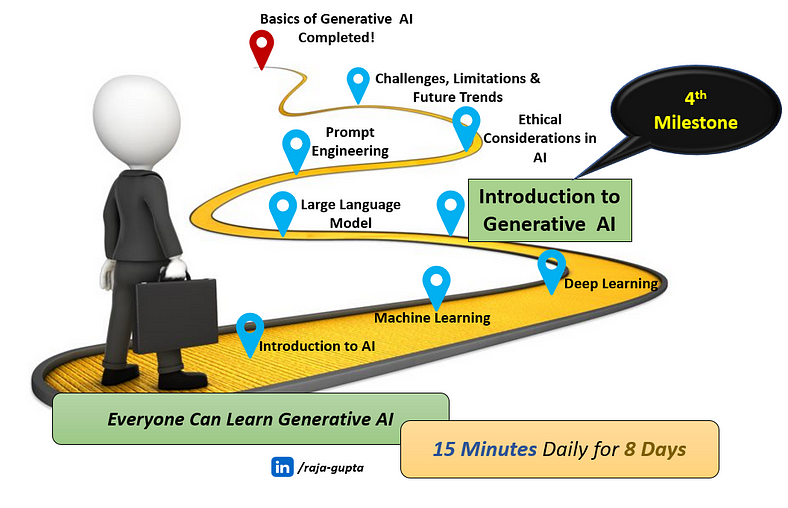
Handling Complex Problems

Deep learning is particularly effective for solving complex problems where traditional approaches may struggle.

Machine Learning Vs Deep Learning

Let’s break down the major differences between machine learning and deep learning:





Generative AI is:

A type of artificial intelligence

that can create new things, for example artwork, music, or even realistic images.

without being explicitly told what to create

While traditional AI focuses on specific tasks or solving a problem, Generative AI is distinguished by its ability to exhibit creativity similar to human creativity. Generative AI is capable of generating new, unique content, ideas, or solutions as we human do.

Let’s understand it better with an example!

Imagine I asked you to draw an animal you have never seen before. You need to use your imagination and draw a brand-new animal the world has never seen.

Since we human have imaginative power and creativity, you will be able to do that. Maybe you will draw an animal that has the body of a lion, face of a cow and the wings of a butterfly.

Now, what if a computer program could create new things all by itself! It can create new things, for example artwork, music, or even realistic images, without being explicitly told what to create.

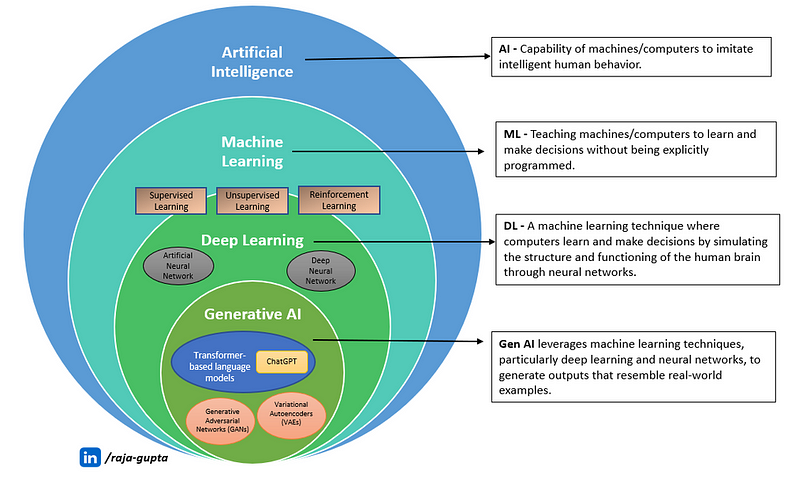
The computer program has been given lots of pictures of lions, cow and butterflies. Now, with this knowledge, it can draw a completely new animal, say a “lion-cow-butterfly” combination. It doesn’t copy any existing image; instead, it uses its understanding of what makes lion, cow, and butterfly unique to create something entirely new something as below.



This is Generative AI — A machine (or computer) which has imagination and creativity to draw pictures, tell stories, or even make up new games without anyone showing it how.

Where Does Generative AI Fits into AI Hierarchy?

Generative AI is a subset of Deep Learning. Below diagram shows the relation between AI, Machine Learning, Deep Learning and Generative AI.



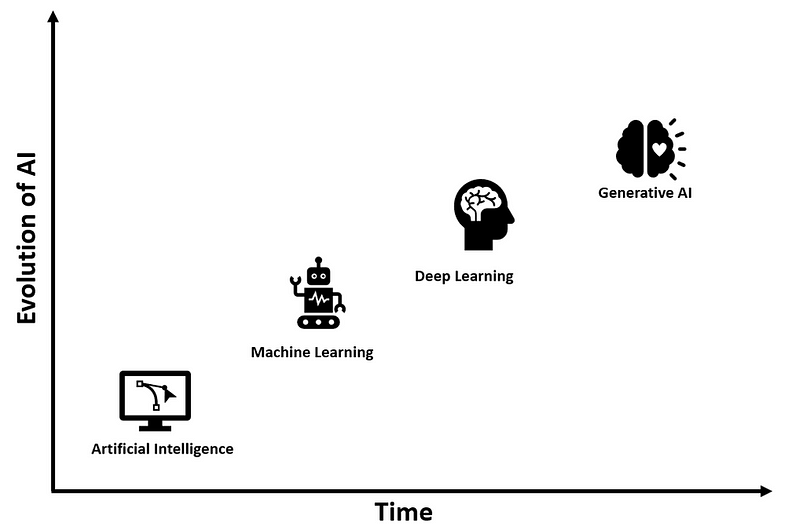
Generative AI leverages machine learning techniques, particularly deep learning and neural networks.

The main differentiator of Generative AI is the ability to generate new content.

AI, machine learning and even deep learning is mostly limited to predictive models. These are mainly used to observe and classify patterns in content or predict a new pattern or content. For example, a classic machine learning use-case is to identify image of a cat out of several given images or classify animals in different clusters based on various properties.

Generative AI is a breakthrough, because it has the ability to do something only humans were supposed to do — create an image of a cat or create an image of a totally new animal from it’s creativity.

The following image shows the evolution of AI with time. The evolution of AI from traditional rule-based systems to Generative AI has been driven by advancements in learning algorithms, computational power, and access to vast amounts of data.



Generative Models

Generative AI uses different types of machine learning models, called Generative Models.

The generative models:

learns the underlying set of data and generates new data the closely mimics the original data

are mainly used to create new content, such as images, text, or even music which looks exactly the same as what might be created by humans

Usages unsupervised learning approach

Most common generative models are:

Variational Autoencoders (VAEs),

Generative Adversarial Networks (GANs)

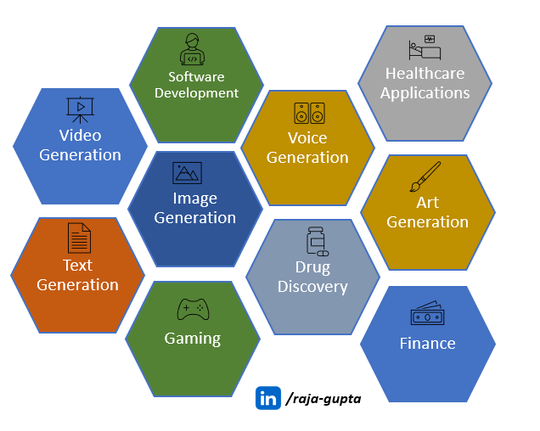
Limited Boltzmann Machines (RBMs)

Transformer-based Language Models

In the next chapter, we will learn more about generative models.

Usages of Generative AI in Real-life

Here are some examples of how generative AI is being used to create real-life applications:



Text Generation

Most of us have used ChatGPT which is based on Generative AI. Similar to ChatGPT Generative AI based tools can be used to generate new content such as articles, reports, poetry, stories or any other text-based content.

One of the most common uses of generative AI is to build Virtual Assistants and Chatbots. Generative models are used to build advance chatbots which can interact with users mimicking human interaction.

Image Generation

Generative AI tools are used to generate new pictures even creative ones using various generative models. These models can learn from large sets of images and generate new unique images based on trained data. These models can even generate images with creativity based on input prompts similar to content generated by humans. There are various ways this can be used in real-life applications such as image-to-image translation, text-to-image translation, photograph editing, face generation, image quality enhancement etc.

One of the most common tools which usages generative AI to create realistic images and art is DALL-E, developed by OpenAI. It is a text-to-image model, which usages deep learning to generate digital images from natural language descriptions.

Video Generation

Generative models can be used to create whole videos from scratch. It stitches together scenes, characters, and actions to make a story. These videos can be used for entertainment, advertisements, or even training simulations. Video game development is one field which is heavily using generative AI.

Some generative models can be used to create new videos by learning from existing videos. This can be used for video prediction if an existing video such as security clip is damaged.

Voice Generation

Generative AI can also mimic voices or generate a whole new voice! It can learn how people talk by analysing audio data, and then generate voice in same style or create entirely new voices.

This is useful for making virtual assistants or audiobooks sound more natural.

Healthcare Applications

Generative AI models can be used to generate synthetic data samples that resemble real data. This can be very useful in medical field, where sometimes collecting real-world data is expensive or limited. For example, generative AI can be used to generating synthetic patient data for research purposes.

Drug Discovery

Generative AI is being used in drug discovery to generate new molecular structures with desired properties. This helps accelerate the process of drug development by exploring vast chemical spaces and identifying promising drug candidates.

Gaming

Generative AI has truly changed the world of gaming. It is increasingly being used in the gaming industry to accelerate game production and create unique experiences.

It helps game developers make games more exciting and immersive by creating entire worlds, characters, and stories.

Generative AI can also be used to make virtual worlds more realistic. It can be used to create unique creatures and characters, finetune each character’s personality and traits, making the game feel alive and full of surprises.

Art Generation

This is one major usage that distinguish generative AI from regular AI. Generative AI has the capability of creative thinking like we human do. Various generative models are used in generative artistic artifacts such as paintings, poetries, stories, and other multimedia-based arts.

Software Development

Generative AI has totally changed the way we write code and build software. With Generative AI tools such as GitHub Copilot, ChatGPT, AlphaCode, we can write code much faster with fine details.

Generative AI tools can assist developers by generating code snippets, enhancing software testing efficiency by identifying more defects, and suggesting optimal solutions to coding challenges. This results in faster development cycles and higher code quality, ultimately leading to improved software products and enhanced user experiences.

Finance

Financial institutions are using generative AI to analyse market trends, forecast stock movements with a high accuracy rate, and refine trading strategies. The technology also helps us having better risk assessment, fraud detection, and portfolio optimization, leading to increased efficiency, reduced costs, more profitability and better investment choices.

Example of Some Popular Generative AI Tools

In previous section, we talked about various use-cases of generative AI. Now, let’s have a look into some of popular generative AI tools available currently.

ChatGPT

ChatGPT is a conversational AI developed by OpenAI. It is designed to engage in natural language conversations with users, providing responses that are contextually relevant and coherent.

ChatGPT works by processing input text and generating responses based on the patterns and relationships it has learned from vast amounts of training data. It usages deep learning techniques, specifically transformers, which allow it to understand and generate human-like text.

GPT (Generative Pre-trained Transformer)

GPT is a transformer-based large language model, developed by OpenAI. This is the engine behind ChatGPT.

The free version of ChatGPT is based on GPT 3.5, while the more advanced GPT-4 based version, is provided to paid subscribers under the commercial name “ChatGPT Plus”.

AlphaCode

AlphaCode is a transformer-based language mode, developed by DeepMind. It is an AI-powered coding engine that generates computer programs. AlphaCode is more complex than many existing language models, with 41.4 billion parameters.

The tool leverages deep learning algorithms to analyse huge amounts of code and learn from patterns, enabling it to generate optimized code solutions. It supports a wide range of programming languages, including C#, Ruby, Python, Java, C++, and more.

GitHub Copilot

GitHub Copilot is an AI-powered code completion tool developed by GitHub in collaboration with OpenAI. It integrates directly into code editors like Visual Studio Code and provides real-time suggestions and completions for code as developers write.

It’s designed to assist developers by generating code snippets, suggesting entire lines or blocks of code, and providing contextual documentation. GitHub Copilot supports multiple programming languages such as Python, JavaScript, Java, C++, and more.

Bard

Bard is a conversational Generative AI chatbot developed by Google, as a direct response to the swift rise of OpenAI’s ChatGPT. Bard was initially based on LaMDA, a transformer-based model. Later it got upgraded to other models such as PaLM and Gemini.

Microsoft Copilot

Microsoft Copilot was initially launched by Microsoft in 2023 as an AI-powered assistant that can help to browse the web. Later it got rebranded to Microsoft Copilot.

Microsoft Copilot can be used to request summaries of articles, books, news etc., general text and images, reformat text, update images etc.

DALL-E

Developed by OpenAI, DALL-E (other versions are DALL-E2 and DALL-E3) is one of the best generative AI tools to generate images. It uses deep learning algorithms to generate images from texts.

StyleGAN

StyleGAN, developed by NVIDIA, is a generative model of type GAN (Generative Adversarial Network), which is used to generate high-quality synthetic images.

StyleGAN is extremely good in creation of realistic images of human faces and other visual content. It can generate images of human faces with a high degree of control over specific visual features such as facial attributes, pose, and background.

Below are some images generated by StyleGAN that looks like a real person. There is an interesting site [https://this-person-does-not-exist.com](https://this-person-does-not-exist.com/) which demonstrates how StyleGAN can be used to generate human faces which actually don’t exists.



Now, let’s continue our journey and try to understand a concept that powers the AI system to communicate with Human — Large Language Model.

Where does Large Language Model fits into Generative AI?

Let’s take an example of ChatGPT to understand it clearly. Out of many capabilities of ChatGPT, one is to understand human language (questions asked in plain English). It can also generate response which we human can understand. This capability of ChatGPT, to communicate with humans, is powered by — Large Language Models.

In other words, we can say — *A generative AI system which needs to generate human-like text needs Large language models.*

Let’s break down it further in layman’s terms!

What is Language Model?

Let’s first understand what a language model is.

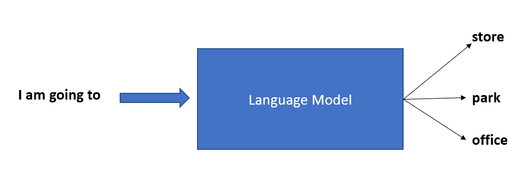
Language model is:

a type of machine learning model

which uses various statistical and probabilistic techniques

to predict probability of a given sequence of words in a sentence or phrase.

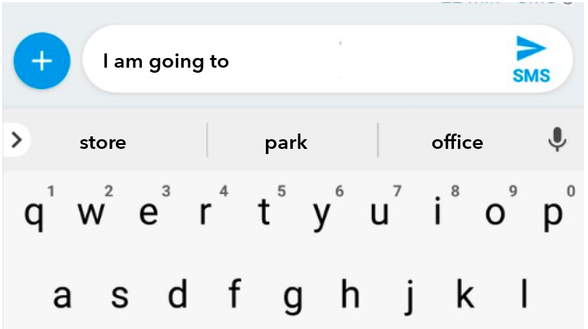
In simple words, language model is designed to predict next most suitable word to fill in a blank space in a sentence or phrase, based on the context of the given sentence/phrase.



Let’s take an example to understand better!

When we use messaging apps in phone, it helps us by predicting the next word when we type in a message. For example, as soon as we type *“how,”* the phone might suggest words like *“are” or “is”*because it knows that those words often come after “how” in sentences.

Similarly, if we type *“I am going to,”*the phone might predict words like *“store,” “park,” “office”*, or *“beach”*because those are common words that comes after “going” in everyday language.



This prediction is made based on the context of what we have typed so far and the patterns it has learned from analyzing lots of text.

Large Language Model (LLM)

A large language model (LLM) is a language model which is:

a type of machine learning model

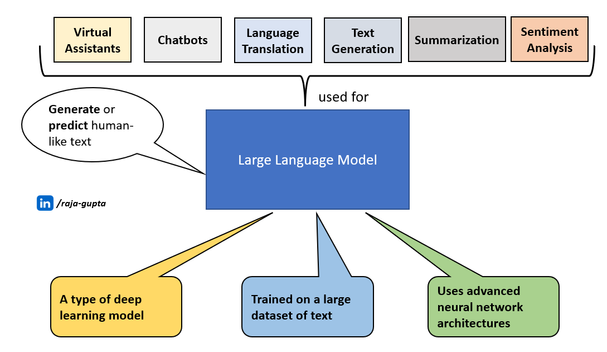
that is trained on a large dataset of text

and uses advanced neural network architectures

to generate or predict human-like text.

Coming back to our earlier example, it is the language model that helps AI tools to predict upcoming words in a sentence.

Below image summarizes important points about large language model.



The most unique and powerful point about large language models is their ability to generate human-like text, summarize, and predict content based on vast amounts of data. LLMs can process and analyze vast amounts of text data, making them highly proficient in language processing tasks such as text generation, summarization, translation, and sentiment analysis.

Natural Language Processing (NLP)

Natural Language Processing is an important concept very much linked with LLM.

Natural Language Processing (NLP) is a subset of AI, which focuses on the interaction between computers and humans through natural language (say English).

NLP refers to the process of enabling computers to understand human language and communicate with us in the same language.

NLP uses algorithms to analyze, understand, and generate human language.

It also helps computers understand the context, and sentiment behind words and sentences.

Let’s take another example to understand NLP better. Virtual assistant, for example Siri, can understand and respond to our commands using NLP.

Imagine you ask Siri, *“Set an alarm for 7 AM tomorrow.”*

Siri’s NLP algorithms analyze the sentence, breaking it down into individual words and understanding their meanings, grammar, and context.

The NLP algorithm will be able to understand the user’s intent, which is to set an alarm.

Further, Siri does the action specified in the command, setting an alarm for 7 AM the following day on your device.

Finally, Siri will give a response in your language.

Natural Language Processing is the backbone for tasks such as responding to human (e.g. ChatGPT), language translation, search engines etc.

Natural Language Processing (NLP) and Large Language Model (LLM)

Large Language Models may be considered as an evolution of Natural Language Processing models. In other words, we can say that a large language model is any model designed for NLP tasks having focussed on understanding and generating human-like text.

While NLP includes a broad range of models and techniques for processing human language, LLMs focus on understanding and generating human-like text. LLMs are specially designed to predict the probability of a word or sentence based on the words that come before it, allowing them to generate coherent and contextually relevant text.

From machine learning technique point of view, natural language processing uses a wide range of techniques, ranging from rule-based methods to machine learning and deep learning approaches.

On the other hand, large language model mainly uses deep learning techniques to understand patterns and context in text data to predict probability of next word in the sequence. LLMs are designed based on artificial neural network architecture. Most of the large language models are based on transformer-based models.

How is Large Language Model related with Generative AI?

Large Language Model (LLM) are a subset of Generative AI. While generative AI can generate many types of content such as text, image, video, code, music etc., LLM is focussed on generating text only.

Where/How Large Language Models are used?

Large Language Models (LLMs) are used in various AI applications across different industries. Here are some major examples:

Virtual Assistants

LLMs models are the engine that power virtual assistants for example Siri, Alexa, or Google Assistant. It’s the LLM models that analyze the human command and interpret the meaning out of it, helping these virtual assistants to perform several actions on user’s behalf.

Chatbots

ChatGPT is not a new word anymore. Most of us have used it or similar AI conversational chatbots. These chatbots uses large language models to understand human questions and response in a way that mimic human-language.

Language Translation

Large language models play an important role in language translation done by AI tools such as Google Translate. These models are trained on huge amount of multilingual text data, which enable them to capture the subtle distinctions, variations, context, and complexity of different languages.

When we asked translation tools to translate a sentence, it uses the LLM algorithms to analyze the input text in one language and generate an accurate and contextually appropriate translation in the target language.

By considering the relationships between words and phrases in both languages bidirectionally, LLMs can produce translations that preserve the meaning and tone of the original text.

Text Generation

Now-a-days large language models are used in many applications to generate human-like text. These models are so sophisticated that they can generate coherent and contextually relevant text based on a given prompt or input. LLM models can be used to compose stories, generating product descriptions, write emails and many more.

Summarization

Large language models are very useful for doing document summarization. Using natural language processing capabilities, LLM models can summarize lengthy documents or articles into concise summaries while preserving the key information and main points. Using techniques such as attention mechanisms and contextual understanding, LLMs can determine the most salient information to include in the summary, ensuring that it captures the essence of the original text.

Sentiment Analysis

Sentiment analysis is a process to determine the sentiment or emotional tone expressed in a text. Large language models can be used to analyze huge amounts of text data, understand the context, nuances, and tone of language, and identify sentiment polarity (positive, negative, or neutral).

Many organizations now-a-days use large language models to identify sentiments in text data coming from social media posts, product reviews, customer feedback, news articles etc.

Content Recommendations

Large language models (LLMs) are being increasingly used by platforms such as Netflix, YouTube, Amazon etc., for content recommendations to provide users with more personalized and relevant suggestions. These models capture the relationships between words, phrases, and topics, allowing them to understand the meaning and context of content. When it comes to content recommendations, LLMs analyze a user’s interactions with content, such as articles they’ve read, products they’ve bought, or videos they’ve watched. Based on this data, LLMs can predict what other content a user might be interested in and suggest relevant options.

Some Popular Examples of Large Language Models

Here are some of the popular applications which uses large language models.

GPT (Generative Pre-trained Transformers)

Generative Pre-trained Transformer is probably the most popular large language model, which is used in ChatGPT. After the introduction of transformer architecture in 2017, OpenAI released GPT-1 as their first transformer based large language model in 2018. GPT-1 was initially trained on BookCorpus, a dataset consists over 7000 self-published books.

Subsequently, OpenAI released more advanced version of GPT as GPT-2, GPT-3, GPT-3.5 and GPT-4. All these are transformer-based large language models. GPT-4 is a multimodal model, which means it can take images as well as text as input.

BERT (Bidirectional Encoder Representations from Transformers)

Introduced by Google in 2018, BERT is a transformer-based large language model. BERT represents a significant advancement in the field of large language model and natural language processing. It’s a bidirectional transformer model which allows it to process words in parallel, making it more efficient compared to traditional sequential models like recurrent neural networks (RNNs).

LaMDA (Language Model for Dialogue Applications)

LaMDA is conversational large language model, developed by Google, which is also a transformer-based model. After the sudden rise of ChatGPT, Google announced it’s own conversational AI chatbot called “Bard”. Bard is powered by LaMDA.

Later, Google introduced PaLM (Pathways Language Model), as the successor of LaMDA. Further, in 2024, Google rebranded Bard with the new name “Gemini”. Gemini is powered by large language model (LLM) of the same name. Gemini multimodal large language model is the successor to LaMDA and PaLM.

LLaMA (Large Language Model Meta AI)

LLaMA (Large Language Model Meta AI) is a set of large language models (LLMs), introduced by Meta AI. LLaMA is an auto-regressive language model, is built on the transformer architecture.

Introduction

Have you seen the movie I, Robot? If yes, you will immediately understand the below image. For people who have not seen the movie, let me brief it.

In the movie, detective Spooner (played by Will Smith) is trying to investigate the death of his friend (and a scientist) Dr. Lanning. Before his death, Dr. Lanning has created his holographic image powered with AI which is supposed to help Spooner in finding answers.

However, sometimes when Spooner ask a question, the holographic image says,*“I’m sorry! My responses are limited. You must ask the right questions.”.*



A scene from the movie I, Robot

What’s the relevance of this scene in our discussion?

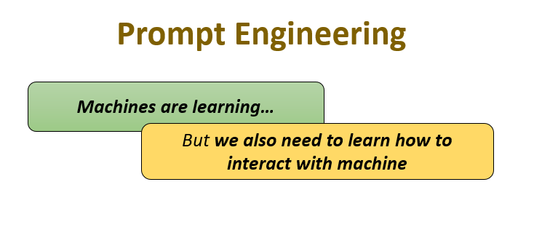
Have you Interacted with AI tools such as ChatGPT, but didn’t get the answer you were looking for? Or did you ever feel that the answer provided by ChatGPT is not up to the mark?

If you don’t get a proper/expected response from an AI system, for example ChatGPT, your first reaction would be that — The AI system is not good enough!

However, the real problem could be that you don’t know how to ask the right question or how to give right set of commands.

While interacting with ChatGPT, we need to know how to ask the right questions and give precise instructions to it — That’s exactly is Prompt Engineering!

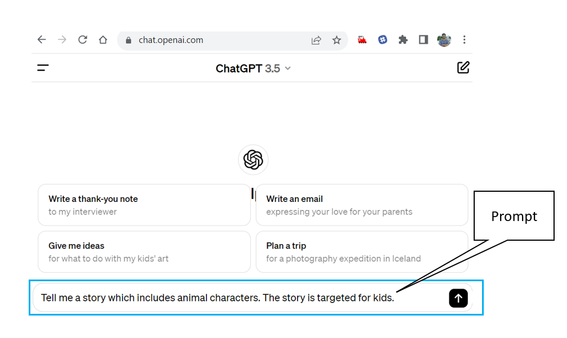
In today’s world, where we see AI based systems everywhere, prompt engineering has emerged as a game-changing technique and is required to unlock the full potential of AI.



What exactly is a Prompt?

Prompts are the inputs or questions user gives to AI systems to get a specific response.

For example, if you want ChatGPT to write a story on animals for kids, you can use a prompt *“Tell me a story which includes animal characters. The story is targeted for kids.”* as shown below.



The AI systems (in this example ChatGPT) uses the prompt to generate response (in this example a text response, a kid’s story on animals). Depending on the type of AI system, the response could be either text, or image or video or something else.

Prompts can be:

sentences in plain English (or any other human language),

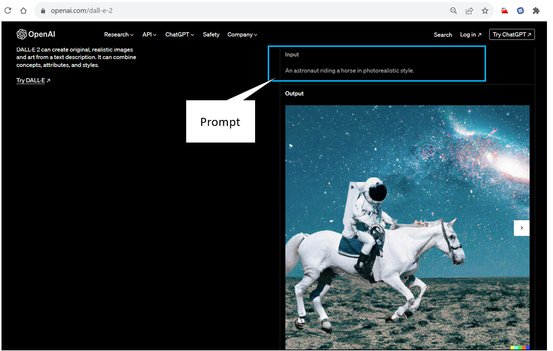
or code snippets

or commands

or any other combination of texts and code.

The generative AI program uses the prompt to understand what kind of content you want it to create, and then it generates new content based on that starting point.

Let’s take one more example. Below image shows a prompt used by DALL-E to generate an image — *“An astronaut riding a horse in photorealistic style.”*



A screenshot of DALL-E Web Page

The more specific and detailed your prompt is, the better the AI can understand what you want it to create.

What is Prompt Engineering?

Prompt engineering:

includes designing and optimizing prompts

in a strategic manner

to generate more accurate and desired response from AI systems.

Instead of asking a general question, prompt engineering involves providing specific instructions or context to get better results.

For example, instead of asking ChatGPT a generic question such as *“Tell me about dogs,”* you can use prompt engineering to get more focused results. For instance, you can ask, *“What are the top 5 breeds of dogs known for their intelligence?”*

By doing so, you’re guiding ChatGPT to give you a list of intelligent dog breeds.

To summarize:

With prompt engineering, you can tailor your questions, making them more specific and structured.

This way, AI systems (such as ChatGPT) can better understand your intent and provide more accurate and relevant answers.

How to use Prompt Engineering to get better results?

Let’s go deeper and understand how prompt engineering can help us to get better results. To make it simple to understand, take example of ChatGPT.

There are 3 important concepts in prompt engineering — Specificity, Contextualization and Fine-tuning.

Specificity

Specificity in prompt engineering means being clear and detailed in the instructions you give to the AI. Instead of asking a broad question, you give specific details about what you want the AI to do or talk about.

Let’s understand with below examples:

Non-specific Prompt: *“Tell me about cars.”*

Specific Prompt: *“Can you describe the features of electric cars compared to traditional gasoline cars?”*

Being specific helps the AI understand exactly what you’re asking for, so it can give you a better answer.

Contextualization

Contextualization in prompt engineering means giving the AI model clear details and information about the situation or task it’s being asked to do. It’s similar to providing a background story or setting the scene for the AI. This helps the AI system understand what it’s supposed to do and who it’s supposed to do it for.

For example, if you want the AI to write a story about a birthday party, you would provide contextualization by telling it things such as who the birthday person is, where the party is happening, and what kind of party it is (e.g., surprise party or themed party). This helps the AI create a story that fits the context you’ve provided.

Let’s take another example:

Non-contextualized Prompt: “Write a review of this product.”

Contextualized Prompt: “Write a review of this product focusing on its performance for outdoor activities.”

The contextualized prompt ensures that the generated review is tailored to the specific use case and audience, improving its relevance and usefulness.

Fine-tuning

Fine-tuning in prompt engineering involves iteratively adjusting and refining the prompt based on the AI system’s output. It is an ongoing process to optimize the prompts and guide AI system to generate desired outcomes.

Fine-tuning is a process of trial and error. We keep adjusting your prompt until you get the response you want.

Let’s understand it with an example.

Imagine you’re asking ChatGPT to write a short story about a dog.

Initial prompt: *“Write a story about a dog.”*

After getting the response, you might notice it’s too general or not exactly what you wanted. This is where fine-tuning comes in. You can adjust your prompt to give ChatGPT more guidance.

For example:

Initial prompt: *“Write a story about a dog.”*

Fine-tuned prompt: “Write a heartwarming story about a golden retriever named Max who helps a little girl overcome her fear of swimming.”

Fine-tuning is an iterative process. If the AI system’s response still isn’t quite right, you can keep adjusting the prompt until you get the desired outcome.

Some Examples of Good and Bad Prompts

Sure, here are some examples of good and bad prompts you can try with ChatGPT.

Bad Prompt: “Write a short story”

Good prompt (being more specific): “Write a short story about a detective solving a mysterious murder case.”

Explanation: The second prompt provides clear instructions and sets the context for the desired output, guiding the ChatGPT to generate a story focused on the specified theme and characters.

Bad Prompt: *“Explain photosynthesis”.*

Good prompt (providing detail information): “Explain the process of photosynthesis in plants, including the role of chlorophyll and sunlight.”

Explanation: The second prompt specifies the topic and includes key details, helping the ChatGPT understand the specific information required and produce a coherent and informative response.

Bad Prompt: “What should I do today?”

Good Prompt: “Suggest some fun outdoor activities for a sunny day.”

Explanation: The first prompt is too general and open-ended. While the second one provides specific points and contexts.

How to Write Effective Prompts?

Here are some important points to keep in mind to write a clear and effective prompt.

Be Clear and Specific

Ensure that your prompt clearly communicates the task or question you want the AI system to address. Avoid ambiguity or overly complex language that could confuse the AI.

Provide Context

Give enough context for the AI system to understand the problem or topic it’s addressing. This helps the AI system generate more relevant and useful responses.

Use Examples

If applicable, provide examples to illustrate what you’re asking for. Examples can help the AI system understand the desired output and provide more accurate responses.

Ask Specific Questions

Instead of vague prompts, ask specific questions that guide the AI system toward the desired outcome.

Include Constraints

If there are any constraints or requirements for the response (e.g., word count limits, specific formats), make sure to include them in the prompt. This helps the AI system generate responses that meet your criteria.

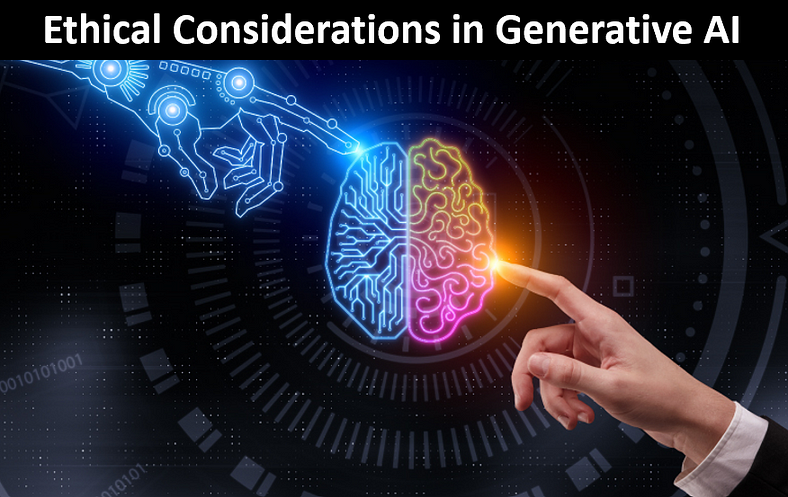
Test and Iterate

Experiment with different prompts and observe how the AI system responds. Adjust your prompts based on the results to improve their effectiveness over time.

Focus on Clarity Over Creativity

While creativity can be beneficial in some cases, prioritize clarity and effectiveness in your prompts. Clear and straightforward prompts are more likely to produce the desired outcomes.

I hope that by now, you have got a clear idea on prompt engineering and how to write good prompts.



What is ethical AI?

Ethical AI refers to use of artificial intelligence in a fair, transparent, and responsible way. It involves treating everyone equally, being clear about how AI decisions are made, and taking responsibility for any errors. Ethical AI also includes protecting people’s privacy, ensuring safety and reliability, and making sure AI is accessible to all. It’s about using AI for good while minimizing harm.

Key Principles of Ethical AI

There are some major principles involved in ethical AI. Let’s take a look into them.

**Fairness and Bias Mitigation**

Ethical AI makes sure to prevent and mitigate bias in AI systems, ensuring that they treat all individuals fairly and without discrimination based on characteristics such as race, gender, ethnicity, or socioeconomic status.

Transparency and Explainability

Explainable AI refers to the set of processes and methods that allows human users to understand and trust the response generated by AI systems. Ethical AI ensures that there is transparency and explainability in AI systems. This enables users to understand how AI-driven decisions are made.

AI transparency works hand in hand with explainable AI. AI transparency helps ensure that all stakeholders can clearly understand the workings of an AI system, including how it makes decisions and processes data.

While explainability focuses on providing understandable reasons for the decisions made by an AI system, transparency involves being open about data handling, the model’s limitations, potential biases, and the context of its usage.

Privacy and Data Protection

Ethical AI ensures the protection of individuals’ privacy and personal data. It makes sure that AI systems collect, use, and store data in a responsible and respectful manner, with appropriate safeguards in place to prevent misuse or unauthorized access.

Safety and Reliability

Ethical AI focuses on building AI systems that are safe, reliable, and trustworthy, minimizing the risk of harm to individuals, communities, and society at large. This includes ensuring robustness against adversarial attacks and unforeseen circumstances.

**Inclusivity and Accessibility**

Ethical AI promotes inclusivity and accessibility, ensuring that AI technologies are designed to serve the needs of diverse populations and that they do not exacerbate existing inequalities or marginalize certain groups.

Ethical Concerns and Challenges with Generative AI

Generative AI can achieve remarkable tasks, like support drug discovery and cancer diagnostics, create beautiful artwork and videos, etc. However, due to lack of regulations, there are many ways it can be misused as well. Like other forms of AI, generative AI can cause a number of ethical issues and risks surrounding data privacy, security, policies and workforces.

Let’s look into some of these concerns.

Copyright and Data Theft Issues

Generative AI can potentially cause copyright and data theft issues in several ways:

**Creation of Copyrighted Content**

Generative AI can generate content, such as images, music, or text, that closely resembles copyrighted material. If this generated content is distributed or used without permission, it could infringe on the original creator’s copyright.

**Plagiarism**

Content generated by AI could be used to plagiarize existing works, such as academic papers, articles, or creative works. If AI-generated content is passed off as original work without proper attribution, it can lead to copyright infringement and academic dishonesty.

**Data Reuse and Replication**

Generative AI models trained on datasets containing proprietary or sensitive information may inadvertently generate content that exposes confidential data. For example, text generators trained on private chat logs or medical records could produce sensitive information, leading to data breaches and privacy violations.

**Forgery and Fraud**

Generative AI can create realistic-looking images, videos, or documents that mimic official or authenticated materials. This could be exploited for forgery and fraud, such as creating fake identification documents, counterfeit products, or deceptive marketing materials.

**Reverse Engineering**

Generative AI models trained on copyrighted or proprietary data may inadvertently reveal insights or patterns that could be reverse engineered by competitors. This could lead to intellectual property theft and unfair competition.

Harmful Content Distribution

Generative AI can contribute to the distribution of harmful content in several ways:

**Creation of Fake Content**

Generative AI algorithms can produce highly realistic fake images, videos, audio, and text. These creations can be used to spread misinformation, fabricate evidence, or deceive individuals and organizations.

**Deepfakes**

Deepfake technology, a specific application of generative AI, allows for the manipulation of audiovisual content to make it seem like someone said or did something they didn’t. This can be used maliciously to create fake videos of public figures, celebrities, or ordinary people engaging in inappropriate or harmful behavior.

**Automated Content Generation**

Generative AI can automate the creation of large volumes of content, such as spam emails, fake reviews, or malicious messages. This can overwhelm online platforms and communities with low-quality or harmful content, making it difficult to distinguish between genuine and fake information.

Privacy Violations

Generative AI can generate synthetic images or videos that resemble real individuals, potentially leading to privacy violations if these creations are used without consent or for malicious purposes, such as impersonation or defamation.

Generative AI can also be used to create surveillance footage or tracking data that mimics real-life scenarios, enabling invasive monitoring of individuals’ activities without their knowledge or consent. This raises concerns about mass surveillance, stalking, and other forms of privacy intrusion.

Summary

Generative AI has huge potential to completely change several sectors, from healthcare to education, from gaming to manufacturing, by creating new content and enhancing productivity.

However, it also brings with it significant ethical concerns, including the distribution of harmful content, copyright infringements, data privacy violations, and many more. As we continue to harness the power of Generative AI, it is very important to ensure ethical best practices.

Hopefully generative AI regulations will soon be established by governments. In the meantime, many companies are taking the lead and developing their own ethical generative AI policies to protect themselves and their customers. For example, SAP is focusing on AI ethics to protect it’s customers and their data.

I hope that by now, you have got a clear idea on ethical considerations in generative AI.