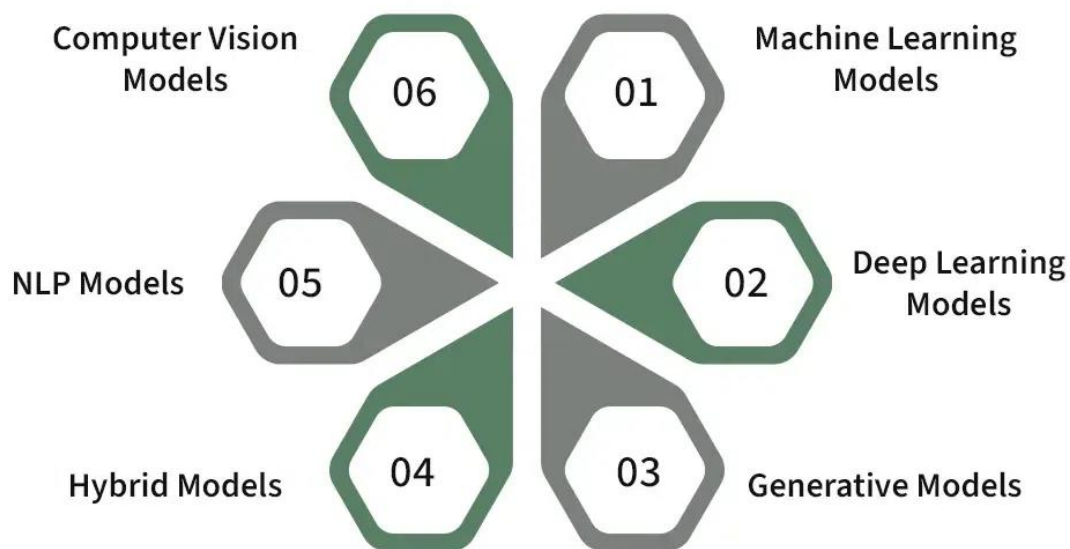


Common AI Models and When to use them?

Artificial intelligence (AI) models include a wide range of techniques and approaches designed to mimic human thought processes and perform tasks that would typically need human intervention. These models vary widely in their applications, complexity, and the specific tasks they are designed to perform, each suited to different aspects of professional and everyday life.



Types of AI Models



Common AI Models and When they are used?

In this article, we will explore various types of Artificial Intelligence Models, their characteristics, and their uses in the rapidly evolving area of modern technology.

What is AI Model?

An AI model is a computational representation or framework that is designed to perform specific tasks or functions by learning from data. In the context of artificial intelligence (AI) and machine learning (ML), an AI model is trained on a dataset to recognize patterns, make predictions, or take actions without being explicitly programmed to perform the task. The AI model is trained using algorithms and techniques to optimize its performance and achieve the desired outcomes.

Common Types of AI Models

There are two primary categories into which [AI](#) models may be classified: **traditional and contemporary**. Rule-based systems and expert systems are examples of old AI models, while [machine learning](#), [natural language processing](#) (NLP), and computer vision models are examples of contemporary AI models. Each category fulfills certain roles and offers unique skills that add to the many applications of AI across industries.

1. Machine Learning AI Models

Machine learning models are created to learn from data and improve performance on certain tasks. These models include a variety of techniques, such as [support vector machines](#), [random forests](#), [decision trees](#), and [linear regression](#). They are widely used in applications such as [reinforcement learning](#), [regression](#), [clustering](#), and [classification](#).

Common Algorithms:

- **Linear and Logistic Regression:** Basic yet powerful methods for prediction and classification.
- **Decision Trees and Random Forests:** Useful for handling complex datasets with high accuracy.
- **Support Vector Machines (SVM):** Excellent for classification tasks, especially in high-dimensional spaces.

When to Use:

- Ideal for predictive analytics in business, healthcare, finance, and more.
- When working with labeled datasets to perform classification or regression tasks.
- Using historical financial data to predict market trends and investment opportunities.
- Identifying patterns that indicate when a customer might leave a service.

Real-Life Application:

- **Real Estate Pricing:** Real estate companies use linear regression to predict home prices based on characteristics like size, location, and number of rooms, helping both buyers and sellers make informed decisions

2. Deep Learning AI Models

[Deep learning](#) models are advanced forms of machine learning that use neural networks with many layers. These models are particularly good at processing large volumes of unstructured data. They are extensively used in applications involving image recognition, natural language processing, and audio recognition.

Common Algorithms:

- **Convolutional Neural Networks (CNNs):** Dominant in processing images, video, and other 2D data.
- **Recurrent Neural Networks (RNNs):** Effective for sequential data such as time series or natural language.
- **Long Short-Term Memory Networks (LSTMs):** A special kind of RNN, capable of learning long sequences of information.

When to Use:

- Ideal for tasks involving big data and complex pattern recognition like voice recognition systems, image classification, and time series forecasting.
- When handling unstructured data such as texts, images, and sounds.
- Using LSTMs to understand and generate human speech for applications like Siri and Google Assistant.
- Employing CNNs to identify individuals in security systems and smartphones.

Real-Life Application:

- **Medical Diagnosis:** Hospitals use CNNs to analyze medical images such as X-rays and MRIs to diagnose diseases and suggest treatments, improving accuracy and speed in medical diagnostics.

3. **Generative AI Models**

Generative models are designed to generate new data instances that resemble your training data, enabling machines to learn the distribution of data points and generate similar items. They're crucial in fields requiring new content generation or feature enhancement.

Common Algorithms:

- **Generative Adversarial Networks (GANs):** Use a dual-network architecture of generators and discriminators to improve each other.
- **Variational Autoencoders (VAEs):** Provide a probabilistic way to describe an observation in latent space.

When to Use:

- When you need to enhance, increase, or generate new data samples from existing data.

- Suitable for tasks like data augmentation, synthetic data generation for training models, and creative content generation.
- Using GANs to create realistic and infinite new environments for video game development.
- Utilizing VAEs to generate new clothing items based on current fashion trends.

Real-Life Application:

- **Film and Video:** Film companies use GANs to enhance the resolution of old movies or generate realistic special effects for new productions without the need for expensive practical effects.

4. Hybrid AI Models

Hybrid models combine multiple different AI techniques to leverage their strengths and mitigate weaknesses. These models are especially useful in complex scenarios where a single model type is insufficient.

Common Algorithms:

- **Integrated Neural Networks:** Combining CNNs and RNNs to handle tasks that involve both visual and sequential data processing.
- **Ensemble Methods:** Using a combination of various models like decision trees and regression models to improve predictions.

When to Use:

- In complex decision-making environments where diverse data types must be processed simultaneously.
- When the problem requires robustness and accuracy beyond what can be achieved by a single model.
- Integrating computer vision for navigation with NLP for voice commands and control.
- Combining multiple classifiers to detect patterns of fraudulent transactions with higher accuracy.

Real-Life Application:

- **Smart Home Systems:** Hybrid models in IoT devices can process environmental data to automate home systems efficiently, like adjusting lighting based on time of day and occupancy detected through cameras and sensors.

5. NLP AI Models

Natural Language Processing (NLP) models are specialized to process and understand human language, making them essential for applications involving text data.

Common Algorithms:

- **BERT (Bidirectional Encoder Representations from Transformers):** Improves the understanding of the context within the text.
- **GPT (Generative Pre-trained Transformer):** Excels in generating coherent and contextually appropriate text.

When to Use:

- When dealing with tasks that involve human language, such as translating languages, generating text, or extracting information.
- For applications like chatbots, sentiment analysis, and automated content generation.
- Using GPT to write articles, compose poetry, or generate code.
- Employing BERT to analyze customer reviews and determine the sentiment expressed in social media posts.

Real-Life Application:

- **Customer Support Automation:** Companies use [NLP](#) models to power chatbots on their websites, providing instant responses to customer inquiries, which improves customer experience and operational efficiency.

6. Computer Vision AI Models

[Computer vision](#) models are tasked with interpreting and understanding visual information from the world, converting it into a digital format.

Common Algorithms:

- **CNNs:** Standard for image classification and recognition tasks.
- **Capsule Networks:** Designed to understand spatial hierarchies between features, potentially overcoming some of CNNs' limitations.

When to Use:

- When tasks require the interpretation of visual data, such as identifying objects, classifying images, or analyzing video content.
- In applications like surveillance, quality control in manufacturing, and interactive gaming.
- Using [CNNs](#) to detect defects in manufacturing products on assembly lines.

- Employing capsule networks to improve the interaction of AI characters with environments in complex video games.

Real-Life Application:

- **Retail:** Stores use computer vision to analyze customer behavior, optimize store layouts, and even to check out customers without the need for traditional cashiers, enhancing the shopping experience and reducing wait times.

Conclusion

By leveraging the strengths of each AI model, organizations can unlock new opportunities, optimize performance, and anticipate future trends, all while delivering unprecedented value to customers and stakeholders.

Network:

Types of Network Protocols and Their Uses

Last Updated : 7 Jan, 2026

-
-
-

A network protocol is a collection of rules that governs how data is transmitted, received, and interpreted between devices on a network, regardless of their internal structure or design.

- Defines what, how, and when data is communicated.
- Enables communication between heterogeneous devices.
- Ensures reliable and standardized data exchange.
- Prevents data loss, duplication, and misinterpretation.

How Do Network Protocols Work?

Network protocols work by dividing communication tasks into layers, where each layer performs a specific function to ensure successful data transmission.

- Communication is based on the [OSI model](#), which consists of 7 layers.
- Each OSI layer uses specific protocols to perform its task.
- Data moves layer by layer from sender to receiver.

- Example: Internet Protocol (IP) operates at the Network Layer and handles routing using source and destination addresses.
- Layered communication improves reliability, scalability, and troubleshooting.

Types of Network Protocols

In most cases, communication across a network like the [Internet](#) uses the [OSI model](#). The OSI model has a total of seven layers. Secured connections, network management, and [network communication](#) are the three main tasks that the [network protocol](#) performs. The purpose of protocols is to link different devices.

The protocols can be broadly classified into three major categories:

- Network Communication
- Network Management
- Network Security

1. Network Communication

Communication protocols are really important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication. Below mentioned are some network communication protocol:

Hypertext Transfer Protocol(HTTP)

Hypertext Transfer Protocol ([HTTP](#)) is an application layer (Layer 7) protocol used for transferring hypertext data between systems on the World Wide Web.

- Works on a [client-server model](#).
- Used for loading web pages in browsers.
- Stateless protocol (does not store session information).
- Most data exchange on the web uses HTTP.
- Less secure unless used with HTTPS.

Transmission Control Protocol(TCP)

Transmission Control Protocol ([TCP](#)) is a [connection-oriented](#) transport layer protocol that provides reliable and ordered data delivery.

- Establishes a connection before data transmission.
- Uses sequenced acknowledgments to ensure reliability.

- Provides error detection and flow control.
- Guarantees data delivery in the correct order.
- Used in email, [FTP](#), web browsing, and streaming services.

User Datagram Protocol(UDP)

User Datagram Protocol ([UDP](#)) is a connectionless transport layer protocol that provides fast but unreliable [data transmission](#).

- Does not establish a connection before sending data.
- No error recovery, [flow control](#), or reliability mechanisms.
- Faster than TCP due to minimal overhead.
- Suitable where speed is more important than accuracy.
- Used in video streaming, online gaming, [multicasting](#), and broadcasting.

Border Gateway Protocol(BGP)

Border Gateway Protocol ([BGP](#)) is a routing protocol used to exchange routing information between autonomous systems on the Internet.

- Controls how data packets travel across multiple networks.
- Used between large networks operated by different organizations.
- Connects [LANs](#) to other LANs across the Internet.
- Ensures efficient and scalable Internet routing.
- Plays a critical role in global Internet connectivity.

Address Resolution Protocol(ARP)

Address Resolution Protocol ([ARP](#)) maps logical IP addresses to physical MAC addresses within a local network.

- Used in local area networks (LANs).
- Maintains an ARP cache for IP-to-MAC mappings.
- Helps devices identify each other on a network.
- Essential for packet delivery within a LAN.
- Operates between the Network and Data Link layers.

Internet Protocol(IP)

Internet Protocol (IP) is a network layer protocol responsible for addressing and routing data packets across networks.

- Sends data from source host to destination host.
- Uses IP addresses for device identification.
- Supports packet routing across different networks.
- Connectionless and best-effort delivery protocol.
- Forms the foundation of the Internet.

Dynamic Host Configuration Protocol(DHCP)

Dynamic Host Configuration Protocol ([DHCP](#)) is a network management protocol used to automatically configure devices on IP networks.

- Automatically assigns IP addresses to devices.
- Provides configuration details such as subnet mask, gateway, and DNS.
- Reduces manual network configuration errors.
- Enables devices to access services like [DNS](#) and [NTP](#).
- Simplifies network administration and management.

2. Network Management

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for [troubleshooting](#) connections between a host and a client.

Internet Control Message Protocol(ICMP)

Internet Control Message Protocol ([ICMP](#)) is a network layer (Layer 3) protocol used by network devices to send error messages and operational information.

- Reports network errors and congestion issues.
- Used for diagnostic purposes such as ping and traceroute.
- Helps detect unreachable hosts and timeouts.
- Does not transfer user data directly.
- Essential for network troubleshooting.

Simple Network Management Protocol(SNMP)

Simple Network Management Protocol ([SNMP](#)) is an application layer (Layer 7) protocol used to manage and monitor network devices on an IP network.

- Used for network monitoring and management.
- Consists of three main components: SNMP Manager, SNMP Agent, Managed Device.
- SNMP agents collect and send network information to the manager.
- Helps monitor performance, detect faults, and troubleshoot issues.
- Widely used in enterprise networks.

Gopher

Gopher is a file retrieval protocol used to search, retrieve, and manage files stored on remote systems.

- Organizes files in a hierarchical (menu-based) structure.
- Provides descriptive information for easy file retrieval.
- One of the earliest Internet protocols.
- Largely obsolete and replaced by HTTP and FTP.

File Transfer Protocol(FTP)

File Transfer Protocol ([FTP](#)) is a client-server protocol used to transfer files between a local system and a remote host.

- Allows uploading and downloading of files.
- Operates over TCP/IP.
- Commonly used for file sharing and website management.
- Supports authentication using username and password.
- Less secure unless used with encryption.

Post Office Protocol(POP3)

Post Office Protocol version 3 ([POP3](#)) is an email protocol used by mail clients to retrieve emails from a mail server.

- Downloads emails from the server to the local device.
- Emails are usually deleted from the server after download.
- Uses TCP/IP for communication.

- Suitable for single-device email access.
- Simple but less flexible than IMAP.

Telnet

[Telnet](#) is a remote access protocol that allows users to connect to and control a remote system.

- Enables remote command execution.
- Operates in a client-server model.
- Transmits data in plain text (not secure).
- Mostly replaced by **SSH** due to security concerns.
- Used mainly for testing and legacy systems.

3. Network Security

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Secure Socket Layer(SSL)

Secure Socket Layer ([SSL](#)) is a network security protocol used to protect sensitive data and secure communication over the Internet.

- Encrypts data transferred between communicating systems.
- Supports both client-to-server and server-to-server communication.
- Prevents unauthorized access and data interception.
- Ensures confidentiality of sensitive information.
- Forms the foundation for secure web communication.

Hypertext Transfer Protocol(HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP that ensures encrypted communication between a web browser and a web server.

- Uses SSL/TLS to secure data transmission.
- Protects user data from interception and tampering.
- Commonly used for secure web browsing.

- Ensures data confidentiality and integrity.
- Indicated by a padlock icon in web browsers.

Transport Layer Security(TLS)

Transport Layer Security (TLS) is a security protocol designed to provide privacy, data integrity, and authentication over the Internet.

- Encrypts data during transmission.
- Verifies data integrity to detect tampering.
- Authenticates communicating parties.
- Widely used in web applications, email services, and [VoIP](#).
- Successor and more secure version of SSL.

Some Other Protocols

Internet Message Access Protocol (IMAP)

Internet Message Access Protocol (IMAP) is an email protocol used to retrieve and manage emails directly from a mail server.

- Allows users to view and manage emails without downloading them permanently.
- Emails remain stored on the mail server.
- Enables access to the same mailbox from multiple devices.
- Supports folder organization and synchronization.
- More flexible than POP3.

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is a signaling protocol used to initiate, manage, and terminate real-time communication sessions.

- Used in voice, video, and messaging applications.
- Establishes communication sessions between users.
- Manages session setup, modification, and termination.
- Commonly used in VoIP and video conferencing.
- Works with RTP to transmit media data.

Real-Time Transport Protocol (RTP)

Real-Time Transport Protocol (RTP) is used to transmit audio and video data over IP networks in real time.

- Supports real-time multimedia communication.
- Used along with SIP for audio and video transmission.
- Provides sequence numbering and timestamping.
- Ensures timely delivery of streaming media.
- Widely used in video calls and live streaming.

Point To Point Tunnelling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is a protocol used to implement Virtual Private Networks (VPNs).

- Encapsulates PPP frames inside IP datagrams.
- Enables secure data transmission over public networks.
- Used for remote access VPN connections.
- Simple to configure but less secure than modern VPN protocols.

Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol (TFTP) is a lightweight and simplified version of FTP used for basic file transfer.

- Uses UDP instead of TCP.
- Provides minimal functionality and no authentication.
- Commonly used for boot files and firmware updates.
- Faster but less secure than FTP.

Resource Location Protocol (RLP)

Resource Location Protocol (RLP) is used to locate and assign network resources to users.

- Helps locate resources such as printers, servers, and devices.
- Uses broadcast queries to find available resources.
- Supports efficient resource discovery on a network.
- Useful in distributed network environments.