Building Modern Systems: Theory and Implementation (Computational Intelligence)

Hamas ur Rehman

Course Contents

- Module 1: Advanced AI Systems
- Module 2: Generative AI and Large Language Models (LLMs)
- Module 3: APIs – Theory and Practical Implementation
- Module 4: Building a Chatbot with LLMs
- Module 5: Logging in Applications
- Module 6: Environment Variables and Secrets Management
- Module 7: Storing Chats in MongoDB
- Module 8: Vector Databases and ChromaDB
- Module 9: Local Server Setup and Hosting APIs
- Module 10: Docker for Modern Applications
- Module 11: Version Control with Git
- Module 12: API Testing with PyTest and Postman
- Module 13: Cloud Deployment with Azure

Course Overview

- Purpose:
  - To understand the design and development of advanced computational systems.
  - Bridge the gap between theoretical concepts and practical applications.
- Key Topics:
  - Advanced AI Systems
  - Generative AI and Large Language Models
  - APIs and Their Implementation
  - Building Intelligent Applications
  - Modern Development Tools and Practices
- Outcome:
  - Equip students with the skills to build intelligent, scalable, and efficient systems.

Lecture Overview

- In this first lecture of Module 1: Advanced AI Systems, we will cover the fundamental theoretical concepts that form the backbone of modern artificial intelligence (AI) systems. This session focuses solely on theory, providing a solid foundation for understanding advanced AI technologies and their applications.

Learning Objectives

By the end of this lecture, students will be able to:

- Define and explain what constitutes an advanced AI system.
- Identify and describe various AI technologies and their applications.
- Understand the historical evolution of AI systems.
- Recognize current trends and anticipate future directions in AI.

What is Computational Intelligence?

What is Computational Intelligence?

Computational Intelligence (CI) is a subfield of artificial intelligence that focuses on the development of adaptive and intelligent computational systems. It encompasses techniques such as machine learning, neural networks, fuzzy systems, and evolutionary computation. CI aims to create systems that can learn from data, adapt to new situations, and make informed decisions, thereby enabling the creation of modern, intelligent systems.

Why "Building Modern Systems: Theory and Implementation"?

The course title emphasizes a comprehensive approach to system development. "Building Modern Systems" highlights the focus on creating advanced, scalable, and efficient computational systems. "Theory and Implementation" signifies the dual emphasis on understanding the foundational theoretical concepts and applying them through practical, hands-on projects. This combination ensures that students not only grasp the underlying principles of computational intelligence but also acquire the skills to implement these concepts in real-world applications.

Introduction to Advanced AI Systems

What are Advanced AI Systems

Advanced AI Systems refer to sophisticated artificial intelligence frameworks that exhibit higher levels of

1. Autonomy
2. Adaptability
3. Learning capabilities
4. Decision-making processes

Autonomy

Autonomy refers to the ability of AI systems to operate independently, without continuous human intervention or supervision. In the context of advanced AI systems, autonomy is the degree to which an AI can perform tasks, make decisions, and pursue goals on its own, while adapting to real-world complexities.

Levels of Autonomy

Low Autonomy: The system requires constant supervision and intervention.

Examples include basic automation tools like rule-based systems or early expert systems, where the AI follows pre-programmed rules.

Example: Medical Diagnosis System

Rules:

1. If **temperature** > 100°F and **coughing**, then **diagnosis** = "flu".
2. If **temperature** > 102°F and **rash**, then **diagnosis** = "measles".
3. If **headache** and **sensitivity to light**, then **diagnosis** = "migraine".
4. If **sore throat** and **coughing**, then **diagnosis** = "cold".

Input Data:

- Patient 1: Temperature = 101°F, Coughing = Yes
- Patient 2: Temperature = 103°F, Rash = Yes

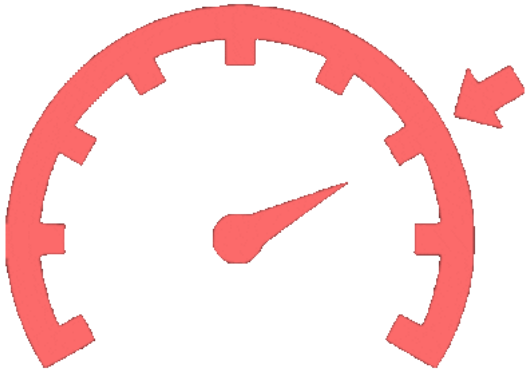
Output:

- Patient 1 is diagnosed with "flu" (based on rule 1).
- Patient 2 is diagnosed with "measles" (based on rule 2).

Levels of Autonomy - *Low*

Example: Basic Cruise Control in a Car

A **basic cruise control** system in a car is a classic example of **low autonomy**. The system can maintain a set speed chosen by the driver, but it requires constant human supervision and control for most other tasks.



Features:

- **Speed Maintenance**: The car keeps a constant speed but cannot adjust for traffic, road conditions, or obstacles.
- **Manual Intervention**: The driver must handle steering, braking, and acceleration when necessary, such as when approaching slower vehicles or changes in terrain.

Human Involvement:

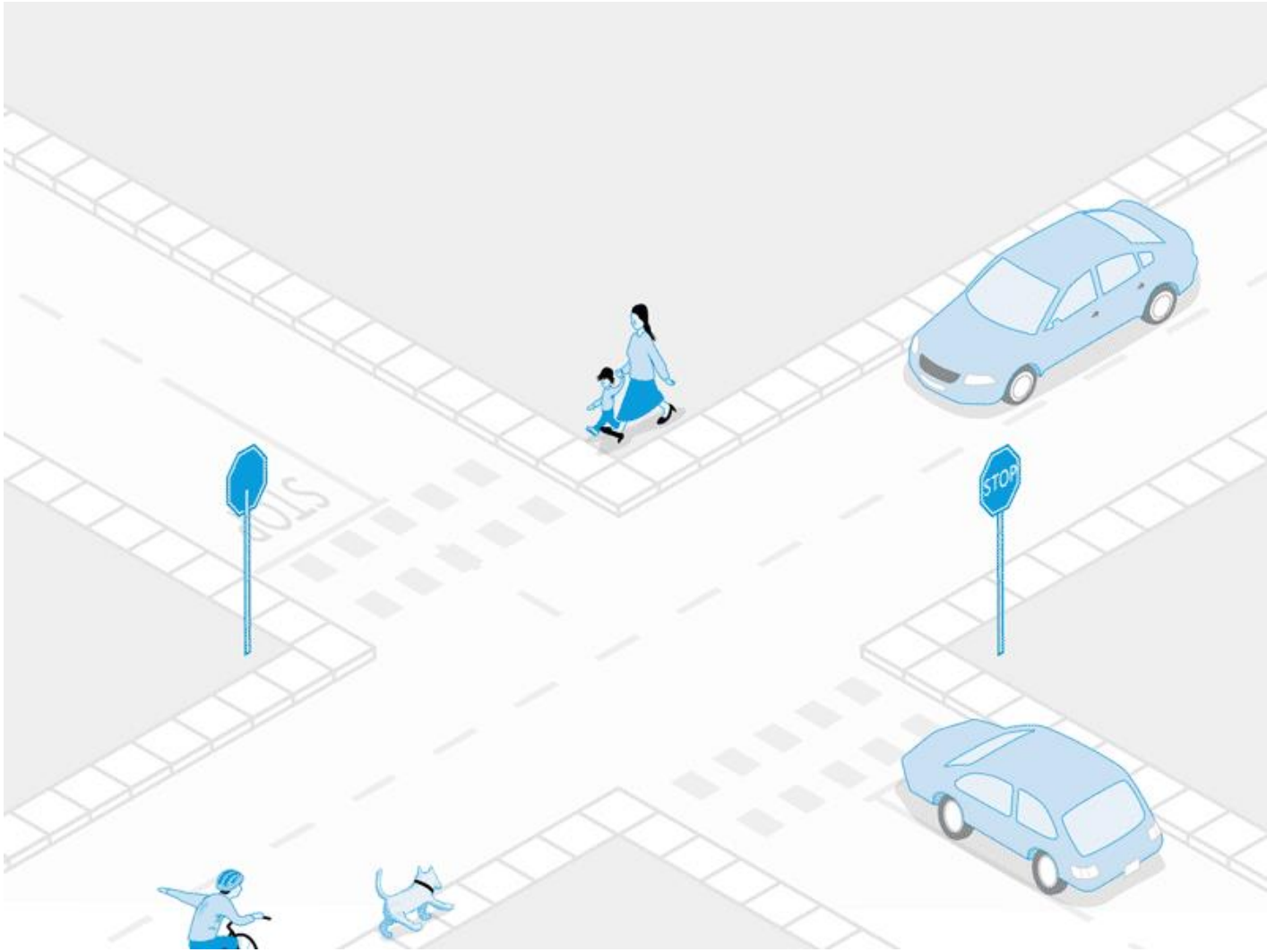
The driver is responsible for nearly all driving tasks beyond maintaining speed, making this a low-autonomy system.

Low-autonomy systems assist with a specific function but rely heavily on human control for complex decisions and changes in the environment.

Levels of Autonomy

Medium Autonomy: The system can perform tasks independently for a period but requires occasional human oversight.

For example, self-driving cars may operate independently in good conditions but need human intervention in certain complex or unusual scenarios.



Levels of Autonomy - *Medium*

Example: Semi-Autonomous Vehicle (Level 3 Autonomy)

In a **Level 3 autonomous vehicle**, the car can handle most driving tasks such as steering, braking, and acceleration under specific conditions (e.g., highway driving, good weather). However, the system may request human intervention when it encounters more complex scenarios, such as:

Scenario:

- The car can autonomously drive on the highway, maintain speed, change lanes, and follow traffic. But when road conditions change (e.g., construction zones, poor weather, or complex city driving), the system alerts the driver to take control.

Medium Autonomy Features:

- **Cruise Control**: The car adjusts its speed automatically based on the distance to the car ahead.
- **Lane Keeping Assistance**: The car can stay within a lane but might need the driver to take over in sharp turns or ambiguous lane markings.
- **Traffic Jam Assist**: In slow-moving traffic, the car can stop and start autonomously but will prompt the driver to take control when traffic clears or becomes unpredictable.

What is Level 3 Autonomy?

Defined by the **SAE (Society of Automotive Engineers)**, Level 3 autonomy allows a vehicle to handle most driving tasks independently but requires human intervention in complex situations. For instance, a Level 3 car can navigate highways but asks the driver to take over in road construction or bad weather. It's the middle ground between driver assistance and full automation!

Hamas ur Rehman

Levels of Autonomy - *Medium*

Human Intervention:

When the system reaches a limit of its autonomy, such as when facing a construction zone, severe weather, or navigating complex urban intersections, it requests human intervention, and the driver must take over.

This level of autonomy gives the system the ability to perform a significant number of tasks autonomously, but not all tasks, especially in situations that are less structured or predictable.

Medium-autonomy systems are commonly used in other domains like:

- **Drones**: Capable of flying autonomously but may require a human pilot for landing or during emergencies.
- **Robotic Surgery**: Robots can perform precise, repetitive tasks during surgery but rely on a surgeon for decision-making and complex interventions.

Levels of Autonomy

High Autonomy: The system can function entirely independently and handle unforeseen situations.

Examples include certain advanced military drones or autonomous trading algorithms that operate 24/7 without human involvement.

Levels of Autonomy - *High*

Example: Fully Autonomous Delivery Drone

A fully autonomous delivery drone can manage the entire delivery process with minimal human intervention.

Features:

- **Route Planning**: It calculates and navigates an optimal route, adjusting dynamically to obstacles (e.g., buildings, weather).
- **Obstacle Avoidance**: Uses sensors (LIDAR, cameras) to detect and avoid objects in real time.
- **Decision-Making**: Handles unexpected issues, such as rerouting due to no-fly zones or power issues.
- **Autonomous Delivery**: Identifies safe landing spots and delivers packages without human input.

Human Oversight:

Humans monitor only for emergencies or regulatory needs, but day-to-day operations are fully autonomous.

Levels of Autonomy - *High*

Other Examples of High Autonomy Systems:

- **Mars Rover (Curiosity, Perseverance)**: The rover can autonomously navigate the Martian surface, collect samples, and avoid hazards, while scientists on Earth provide only high-level goals and commands.
- **Autonomous Factories**: Industrial robots in smart factories can manage production lines, perform quality checks, and optimize operations with minimal human oversight.
- **Self-Driving Cars (Level 5 Autonomy)**: A fully autonomous vehicle (Level 5) would drive in any conditions and handle any situation without human intervention, making all driving decisions autonomously.

Challenges of Autonomy

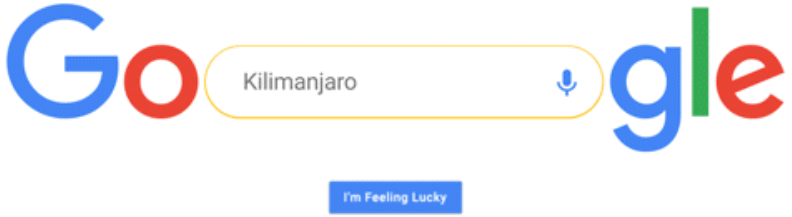
- Trust and Safety: Ensuring the system makes safe decisions in unpredictable environments.
- Ethics: Autonomous systems must be programmed with ethical considerations, particularly in life-and-death situations (e.g., autonomous vehicles).
- Legal Frameworks: There are often legal and regulatory challenges in allowing highly autonomous systems to operate, particularly when accountability becomes ambiguous.

Adaptability

Adaptability is the ability of an AI system to modify its behavior based on changes in its environment, goals, or feedback. Unlike traditional AI systems that follow static instructions, adaptable systems dynamically adjust to new data, environments, or objectives.

Types of Adaptability

Reactive Adaptability: The AI adapts based on immediate feedback. For instance, a trading algorithm might change its investment strategy in response to market fluctuations.



Example: Google Search Algorithm (SEO) Updates

Google's search algorithm is a good example of reactive adaptability. It adapts in real-time to users' search behavior. For example, when there is a sudden surge in searches for a breaking news event, the algorithm dynamically adjusts to display relevant, up-to-date content. This reaction happens immediately as it analyzes user interactions and content relevance to ensure better search results.

Types of Adaptability

Proactive Adaptability: The AI anticipates future changes or challenges and adapts in advance. For example, a self-driving car may anticipate a traffic jam and choose an alternate route before the jam occurs.

Example: Tesla's Autopilot (Self-Driving Car)

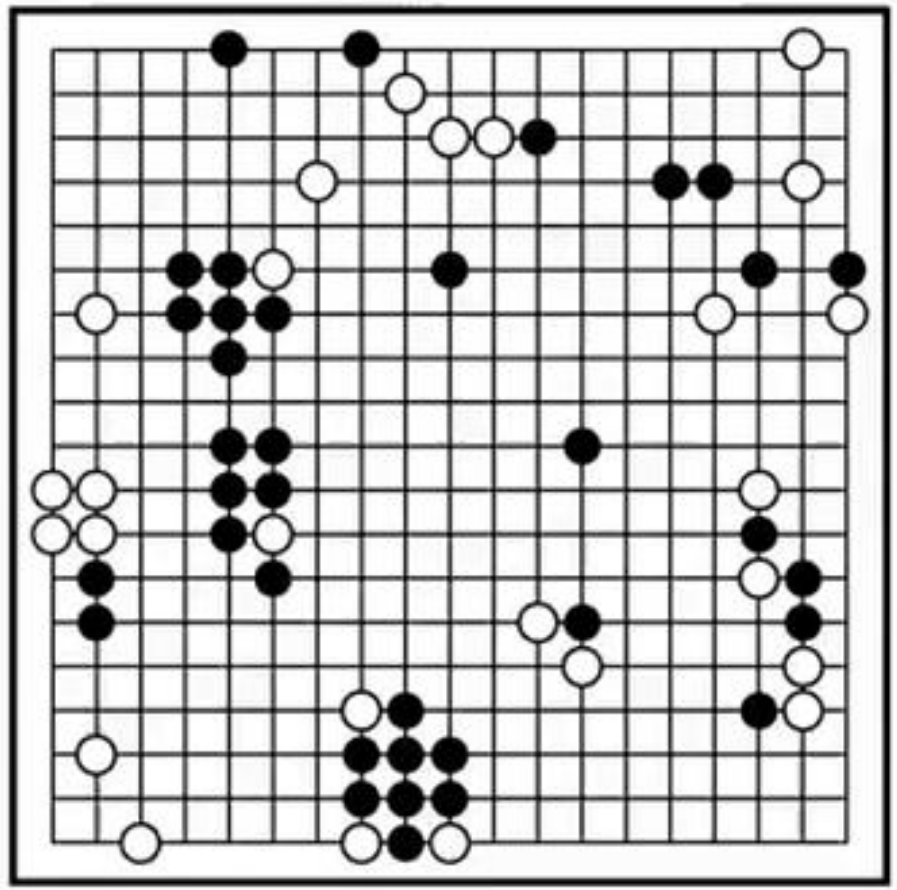
Tesla's Autopilot system anticipates traffic conditions and proactively adapts its route or driving behavior. For example, if the car's navigation system predicts a traffic jam ahead, it proactively reroutes the car to avoid the delay, based on real-time traffic data and forecasting. This avoids congestion and optimizes travel time before the situation impacts the vehicle.

Types of Adaptability

Self-Optimization: Advanced systems can also optimize their own parameters without external guidance. This could involve tuning hyperparameters in machine learning models based on performance feedback.

Example: AlphaGo Zero by DeepMind

AlphaGo Zero, the AI system that mastered the game of Go, is an example of self-optimization. It started with no prior knowledge and optimized its strategy by playing games against itself, adjusting its parameters as it learned from wins and losses. Over time, it developed a stronger game strategy through self-driven improvement without external guidance, ultimately outperforming previous versions and human champions.



Challenges of Adaptability

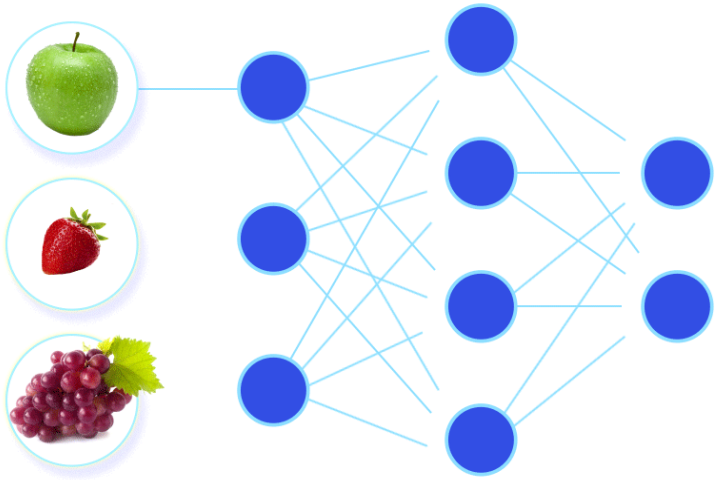
- Environment Complexity: Real-world environments are often highly dynamic and unpredictable, making adaptability a difficult challenge.
- Generalization: AI systems must not only adapt to the specific situation but generalize their learning to broader circumstances.
- Overfitting vs. Underfitting: While adapting to new environments, AI systems must avoid overfitting to specific scenarios at the cost of broader applicability.

Learning Capabilities

Learning capabilities refer to an AI system's ability to improve its performance over time by learning from data, experiences, and interactions. These capabilities allow systems to go beyond static rule-based behaviors and continuously evolve based on exposure to new data or feedback.

Types of Learning

Supervised Learning: The AI learns from labeled data where the desired output is provided. This form of learning requires significant human intervention for labeling but provides high accuracy.

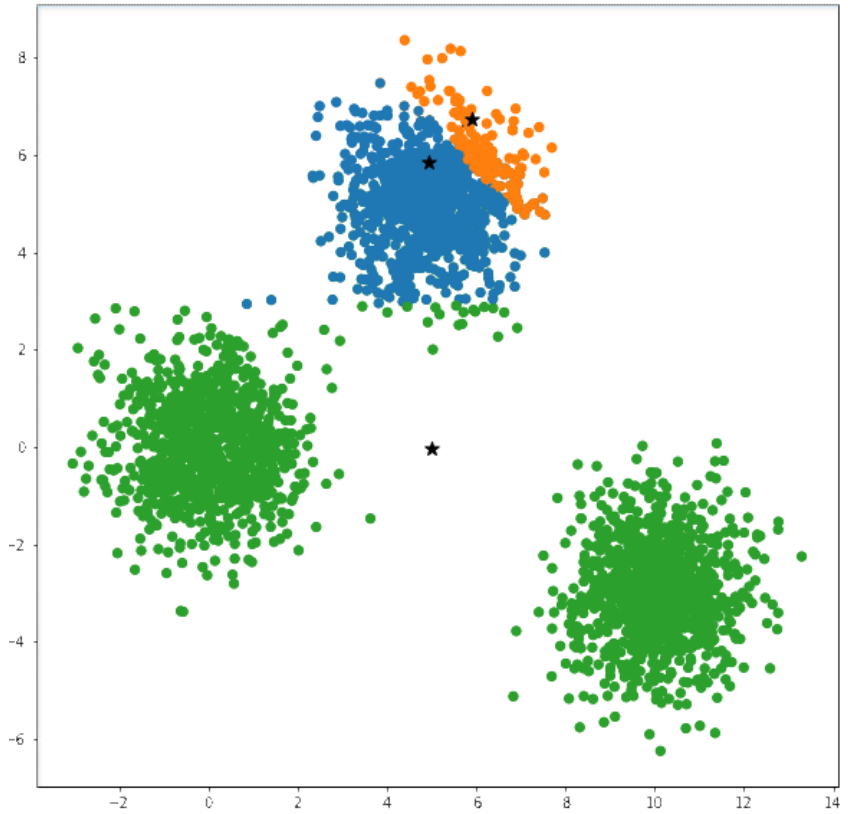


Real-World Example: Image Recognition in Healthcare (AI for Diagnosing Diseases)

In medical imaging, AI systems like Google's DeepMind are trained using **supervised learning** on labeled data, such as MRI or X-ray scans. Doctors provide labeled examples of healthy and diseased tissues, and the AI learns to distinguish between them. Over time, it can accurately predict the presence of conditions like cancer or fractures by analyzing new scans, thanks to the labeled data used during training.

Types of Learning

Unsupervised Learning: The AI system discovers patterns and structures in unlabeled data without human intervention, such as clustering algorithms or generative models.

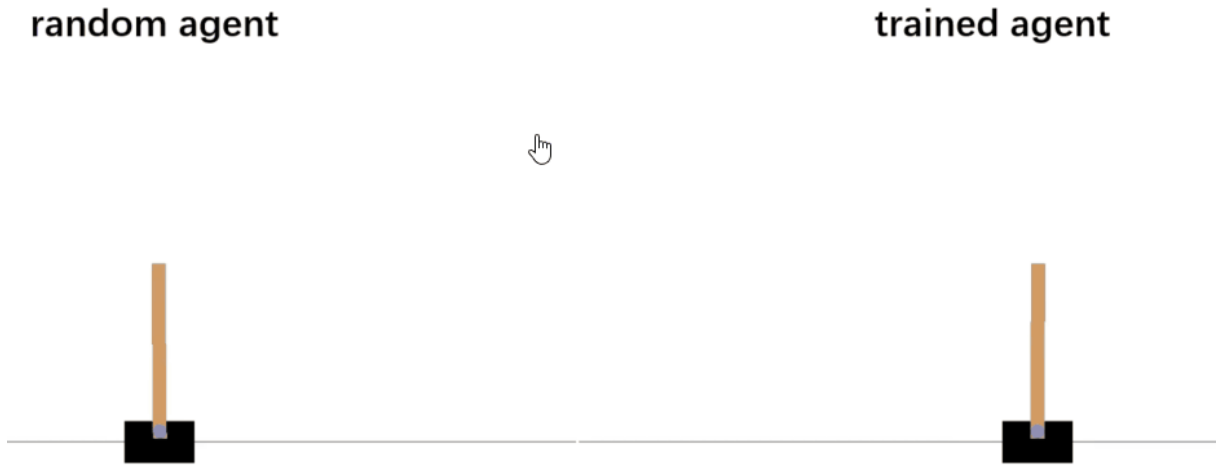


Real-World Example: Customer Segmentation in Marketing

Companies like Amazon and Netflix use **unsupervised learning** algorithms to analyze vast amounts of customer data and identify patterns without human labeling. For example, they use clustering algorithms to segment customers into different groups based on buying behavior or viewing preferences, enabling more targeted marketing strategies. These clusters are formed without predefined labels, allowing the AI to discover natural groupings within the data.

Types of Learning

Reinforcement Learning: The AI learns by trial and error, receiving rewards or penalties for actions taken in an environment. Over time, it optimizes its behavior to maximize cumulative reward.

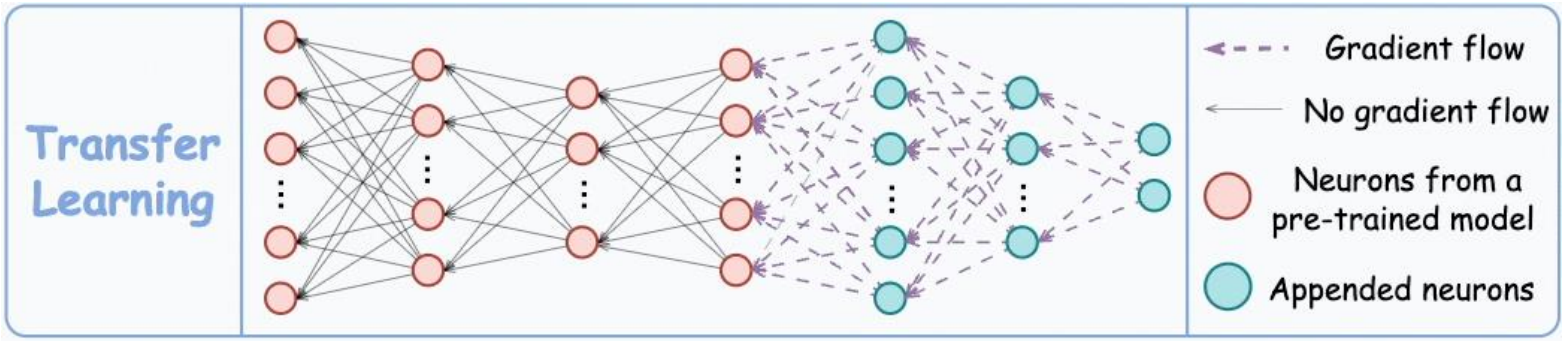


Real-World Example: Robotics and Autonomous Systems (Boston Dynamics)

Boston Dynamics' robots use **reinforcement learning** to improve their ability to navigate through complex environments. These robots learn by trial and error, receiving positive rewards when they successfully complete tasks like walking, jumping, or recovering from a fall. Over time, the robots refine their movements to optimize their behavior for stability and efficiency in challenging terrains.

Types of Learning

Transfer Learning: The system applies knowledge gained from one domain to a different, but related, domain, enabling it to solve new problems more quickly.



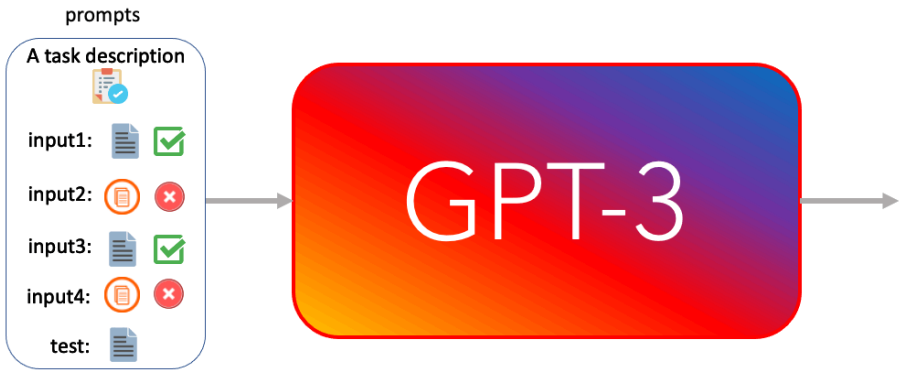
Real-World Example: NLP Models like GPT-3

OpenAI's **GPT-3** (and similar large language models) use **transfer learning** to apply knowledge learned from one domain to other tasks. GPT-3 is initially trained on a massive dataset from the internet and then fine-tuned for specific tasks like answering questions, translation, or summarization. The model uses general linguistic knowledge gained during pretraining to perform well on new tasks, even without task-specific data.

Types of Learning

Few-Shot Learning/Zero-Shot Learning: Advanced models can generalize from very few examples or even solve tasks without specific training on those tasks, mimicking human learning efficiency.

Prompt-base Few-shot Learning



Real-World Example: AI Assistants (Virtual Assistants like Siri or Alexa)

Modern AI assistants like **Siri** or **Alexa** utilize **few-shot learning** and **zero-shot learning** capabilities. These systems can understand and respond to tasks they haven't been explicitly trained for. For example, they can understand a new command or question with very few or even no prior examples, generalizing from existing language data. This mirrors human-like learning efficiency, allowing them to perform novel tasks without extensive retraining.

Challenges of Learning

- Data Quality and Availability: Learning systems require vast amounts of high-quality data, which may not always be available.
- Bias in Learning: AI systems can inherit biases from their training data, which may result in unfair or unethical outcomes.
- Catastrophic Forgetting: When retraining on new data, some AI systems lose the knowledge they previously acquired, which poses a problem in continually learning environments.

Decision-Making Processes

Decision-making in AI refers to the process by which systems choose the most appropriate actions or solutions based on available information, predicted outcomes, and a set of objectives. In advanced AI systems, decision-making is often probabilistic, multi-faceted, and involves high levels of complexity.

Types of Decision-Making Models

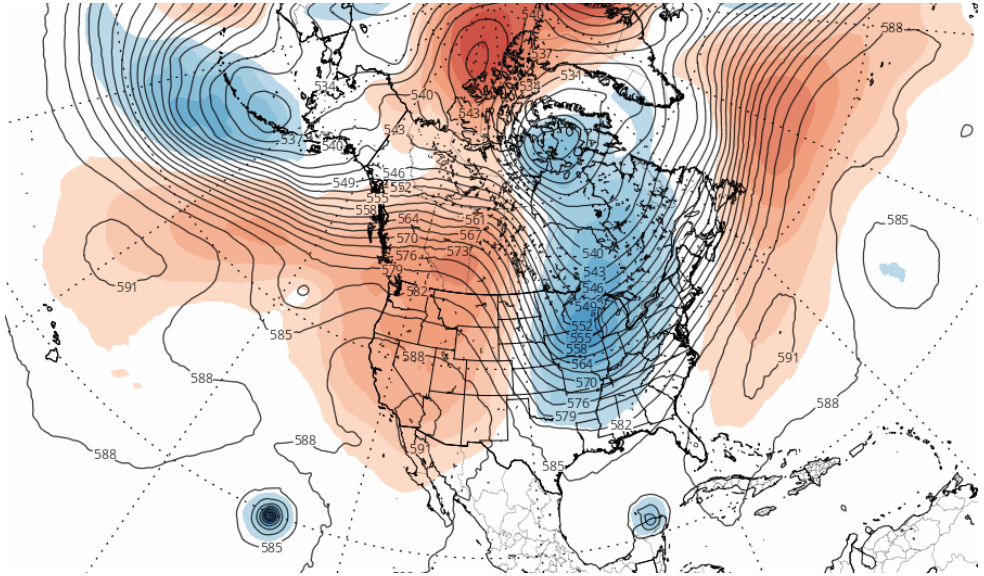
Deterministic Models: These models follow a fixed set of rules or algorithms, which are ideal for situations where all variables are known, and the system only needs to follow pre-established protocols.

Real-World Example: Automated Manufacturing Systems

In **automated manufacturing**, robotic arms follow **deterministic models** to assemble parts. These robots are programmed to execute precise sequences of actions based on fixed rules. Since all variables (e.g., part positions, dimensions) are known in advance, the system follows pre-established protocols without any uncertainty, ensuring consistent and repeatable results in assembling products like cars or electronics.

Types of Decision-Making Models

Probabilistic Models: In scenarios with uncertainty, probabilistic models (like Bayesian networks or Markov Decision Processes) are used to make decisions based on the likelihood of various outcomes.



Real-World Example: Weather Forecasting

Weather prediction models use **probabilistic decision-making** to predict weather conditions. For example, meteorologists rely on **Bayesian networks** or **Markov Decision Processes** to account for uncertainty in data (e.g., temperature, pressure). The system outputs probabilities for various weather events (e.g., a 70% chance of rain), allowing people to make informed decisions based on these likelihoods.

Types of Decision-Making Models

Multi-Objective Decision Making: Many advanced systems must make trade-offs between competing objectives. For instance, in a self-driving car, the system must balance safety, efficiency, and passenger comfort.

Real-World Example: Self-Driving Cars (Tesla Autopilot)

Self-driving cars like those from Tesla use **multi-objective decision-making** to balance safety, efficiency, and passenger comfort. For example, while driving, the system continuously decides between multiple objectives: maintaining a safe distance from other vehicles (safety), choosing the fastest route (efficiency), and avoiding sudden acceleration or harsh braking (comfort). These trade-offs are optimized to provide the best overall driving experience.

Types of Decision-Making Models

Real-Time Decision Making: Some AI systems must make decisions in real-time, often in life-critical applications. Examples include autonomous drones in military applications or AI-driven medical devices in surgery.

Real-World Example: High-Frequency Trading Systems

In **high-frequency trading (HFT)**, AI systems make **real-time decisions** in financial markets. These systems analyze massive streams of market data and execute thousands of trades in milliseconds, responding to fluctuations in stock prices, currency exchange rates, or other financial indicators. The AI must make split-second decisions to capitalize on tiny market changes, optimizing for profit while minimizing risk, all in a highly dynamic environment where every millisecond counts.

Challenges of Decision-Making

- Computational Complexity: Making decisions in real-time, especially in complex environments with many variables, can be computationally expensive.
- Ambiguity and Uncertainty: Many real-world environments are fraught with incomplete or ambiguous data, making it difficult for AI to make optimal decisions.
- Ethical Decision Making: AI systems need to incorporate ethical considerations, particularly in situations like medical decisions or autonomous driving, where decisions can affect human lives.

Assignment

Distinguish Advanced AI from Basic AI Systems

Hamas ur Rehman

Overview of AI Technologies and Applications

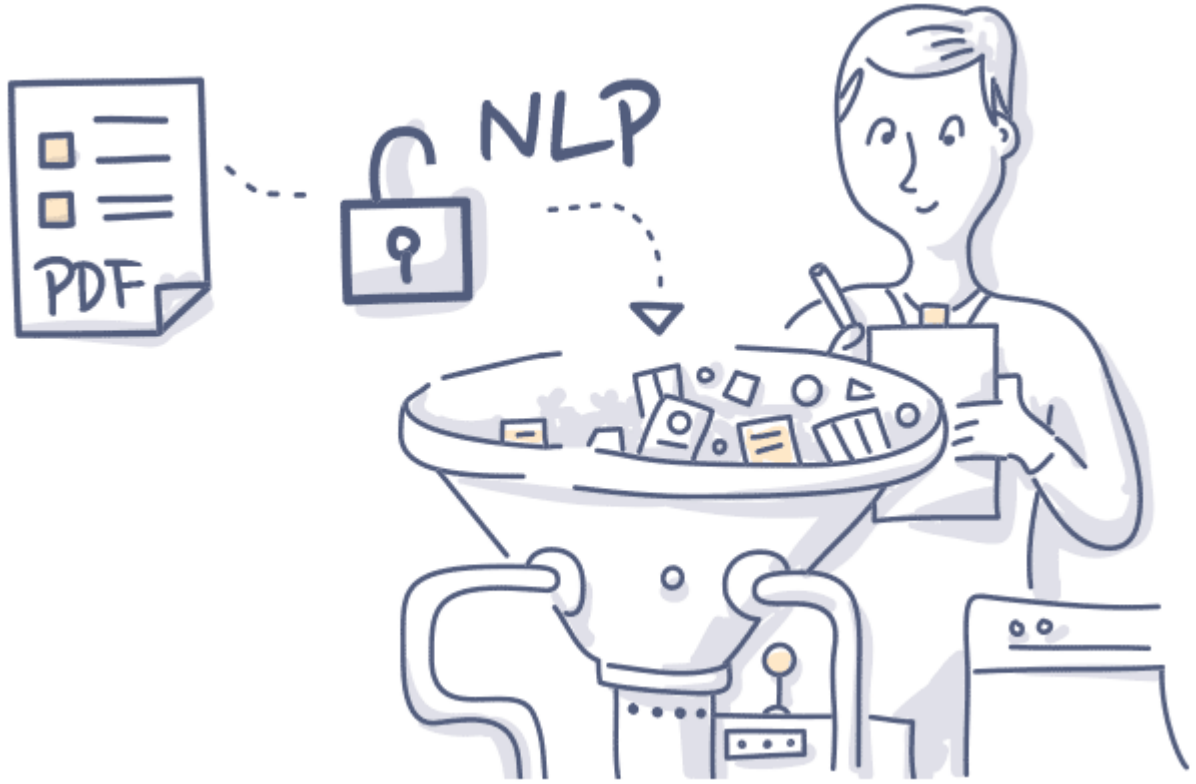
Hamas ur Rehman

Core AI Technologies

- Machine Learning (ML)
- Neural Networks and Deep Learning
- Natural Language Processing (NLP)
- Computer vision
- Robotics

Natural Language Processing (NLP)

A field of AI that focuses on the interaction between computers and humans through natural language.



Components:

- Text Processing: Tokenization, stemming, lemmatization.
- Language Understanding: Parsing, sentiment analysis, entity recognition.
- Language Generation: Text generation, machine translation, summarization.

Use Case Examples:

- Chatbots and Virtual Assistants, Language Translation, Sentiment Analysis

Modern NLP

Modern NLP has been revolutionized by transformer models, such as GPT and BERT, which excel in understanding context and generating human-like text. These models use self-attention mechanisms to process language more efficiently than previous architectures. Beyond transformers, research is exploring even more efficient models for better language understanding and generation.

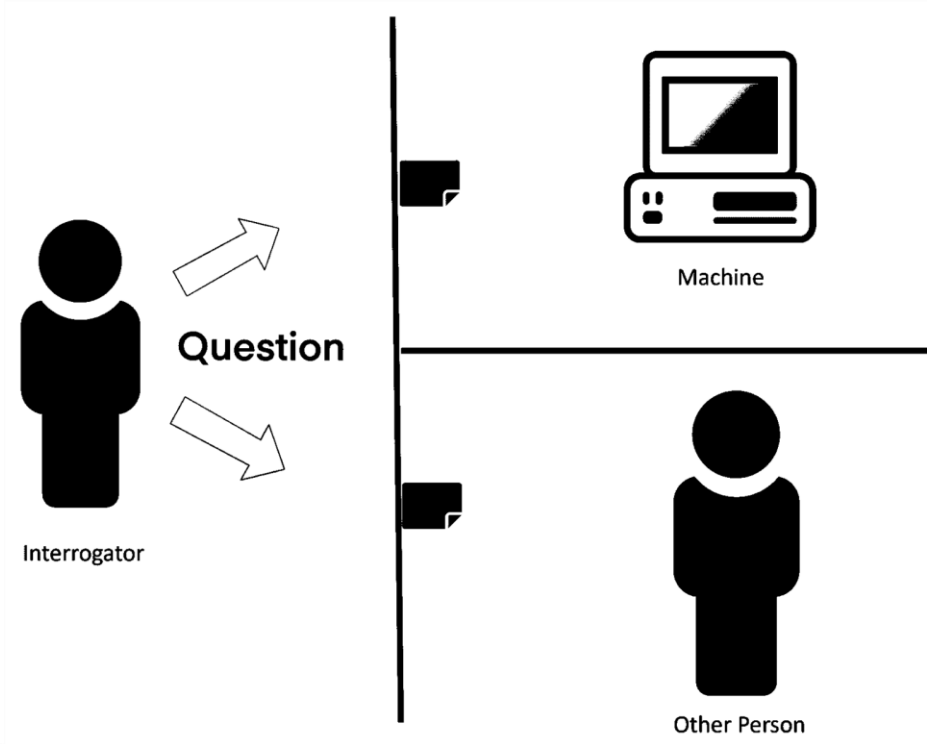
Transformers , BERT, GPT, RoBERTa, T5, XLNet

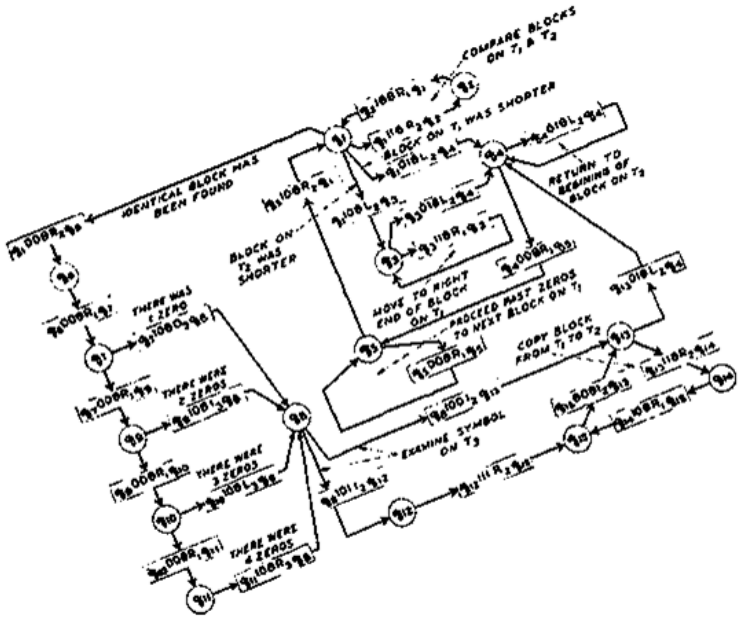
Evolution of AI Systems

Historical Milestones - Foundational Theories

Alan Turing

Proposed the concept of a universal machine (Turing Machine) capable of performing any computation. Introduced the Turing Test as a measure of machine intelligence.





Historical Milestones - Foundational Theories

John McCarthy

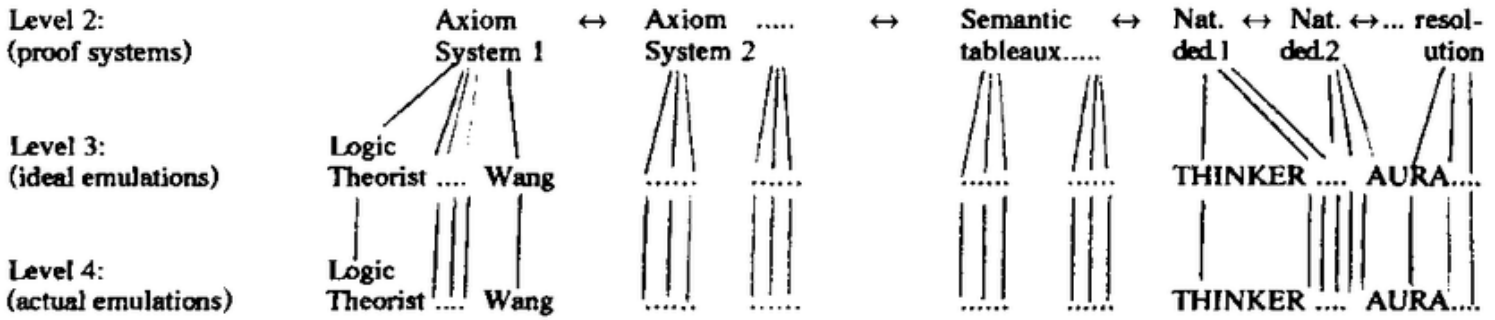
Coined the term "*Artificial Intelligence*" in 1956.Organized the Dartmouth Conference, the first AI conference, which laid the groundwork for AI research.

Will AI think like humans?

Historical Milestones - Pioneering Projects

Logic Theorist (1956)

Developed by Allen Newell and Herbert A. Simon. Considered the first AI program, capable of proving mathematical theorems.



ELIZA (1966)

Created by Joseph Weizenbaum. Early natural language processing program that simulated conversation.

Recent Advancements - Impact of Big Data and Improved Algorithms

Deep Learning Evolution

- Early Models:

  Simple feedforward neural networks with limited depth.

- Modern Architectures:

  Convolutional Neural Networks (CNNs)

  Specialized for processing grid-like data such as images. Image and video recognition, object detection.

  Recurrent Neural Networks (RNNs) and LSTMs

  Designed for sequential data processing. Language modeling, speech recognition, time-series prediction.

  Transformers

  Utilizes self-attention mechanisms for parallel processing. Machine translation, text generation, and more.

Notable Breakthroughs

ResNet (2015)

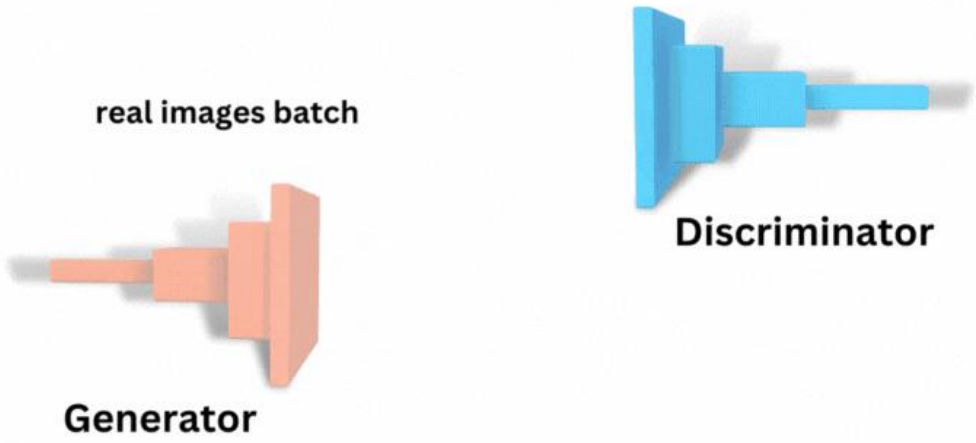
Introduced residual connections to enable training of very deep networks. Achieved state-of-the-art performance in image recognition tasks.

Generative Adversarial Networks (GANs):

Framework involving two networks (generator and discriminator) competing against each other. Applications: Image generation, style transfer, data augmentation.

Attention Mechanisms:

Enhanced the ability of models to focus on relevant parts of the input data. Key to the success of Transformer-based models like BERT and GPT.



Current Trends and Future Directions

Explainable AI (XAI)

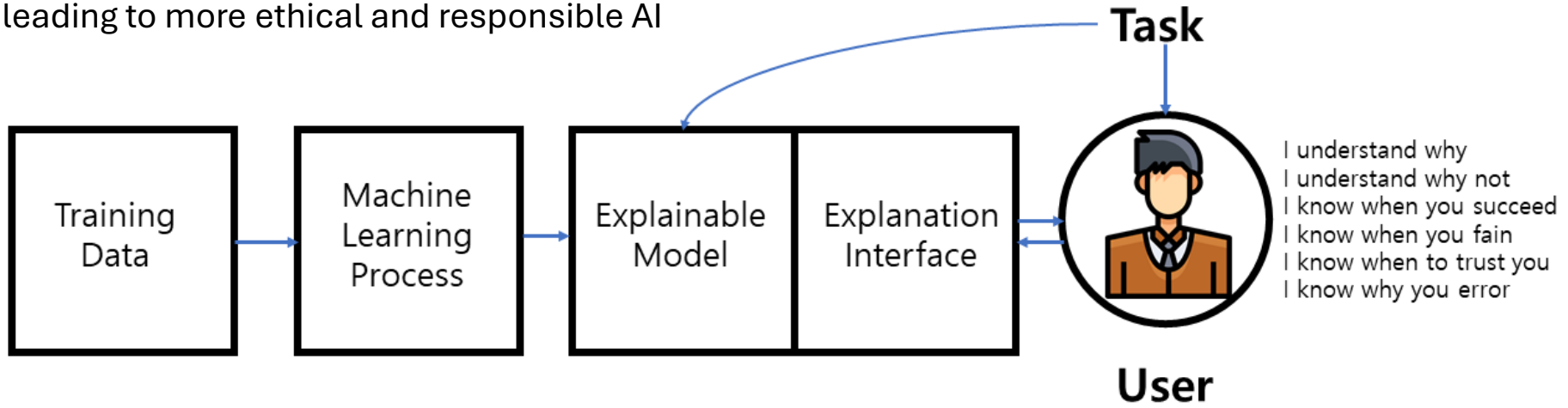
Explainable AI (XAI) focuses on making AI decision-making processes transparent and understandable to users.

Importance of Transparency

Building Trust: When users can understand how AI makes decisions, they are more likely to trust and adopt AI solutions.

Accountability & Compliance: Transparent AI ensures that systems meet legal and ethical standards, making it easier to hold entities accountable for AI-driven outcomes.

Reliability & Ethics: Explainability improves the reliability of AI by identifying biases or errors, leading to more ethical and responsible AI deployment.



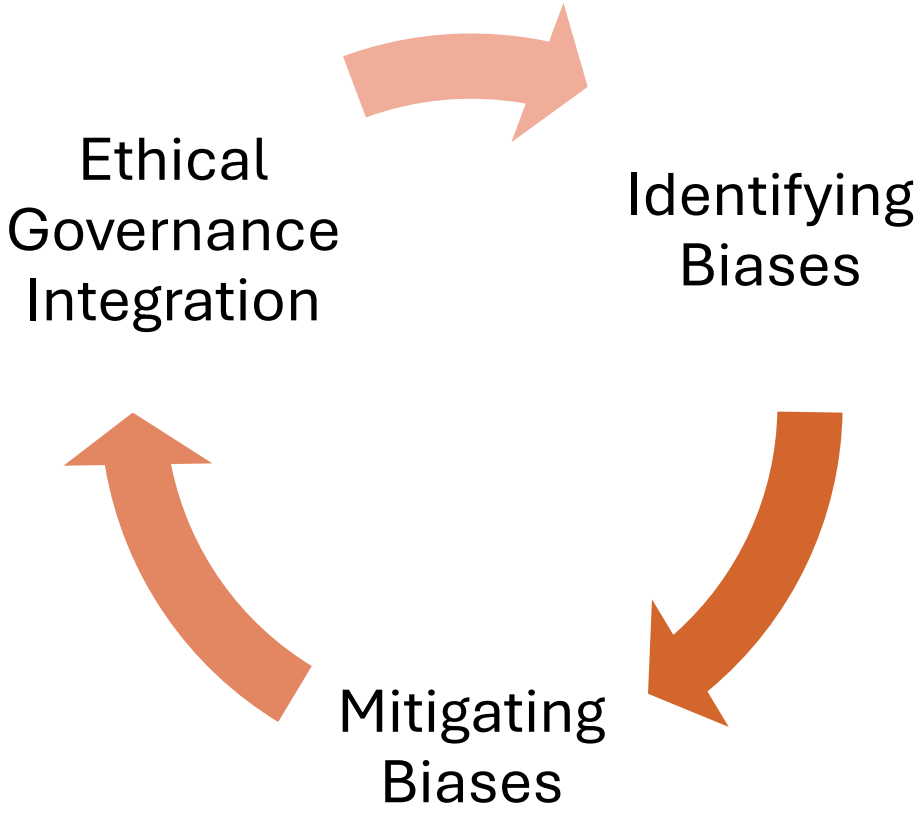
AI Ethics and Governance

Addressing Biases in AI Systems

Identifying and Mitigating Biases: Detecting biases in data and algorithms to promote fairness and reduce discrimination in AI outcomes.

Implementing Ethical Guidelines: Establishing clear ethical standards to ensure AI is used responsibly and in alignment with societal values.

Governance Frameworks: Developing structures to monitor and regulate AI practices, ensuring accountability and compliance with ethical principles.



Integration with Emerging Technologies

Internet of Things (IoT): Enhancing Connectivity and Data Collection

- Real-Time Data Acquisition: Gathers data from interconnected devices in real time.
- Smarter AI Applications: Utilizes continuous data streams to enhance AI capabilities.
- Automation & Efficiency: Improves automation across industries with enriched data.

Edge Computing: Processing Data Closer to the Source for Faster Decision-Making

- Reduced Latency: Processes data locally, reducing delays compared to centralized cloud servers.
- Enhanced Privacy: Maintains data security by processing sensitive information on local devices.
- Real-Time Applications: Supports AI systems that need immediate decision-making responses.

Future Directions in AI Systems

AI-Driven Personalization and Customization:

- Tailoring AI systems to individual user preferences and behaviors.
- Enhancing user experiences through customized interactions and services.
- Driving efficiency and satisfaction with personalized solutions.

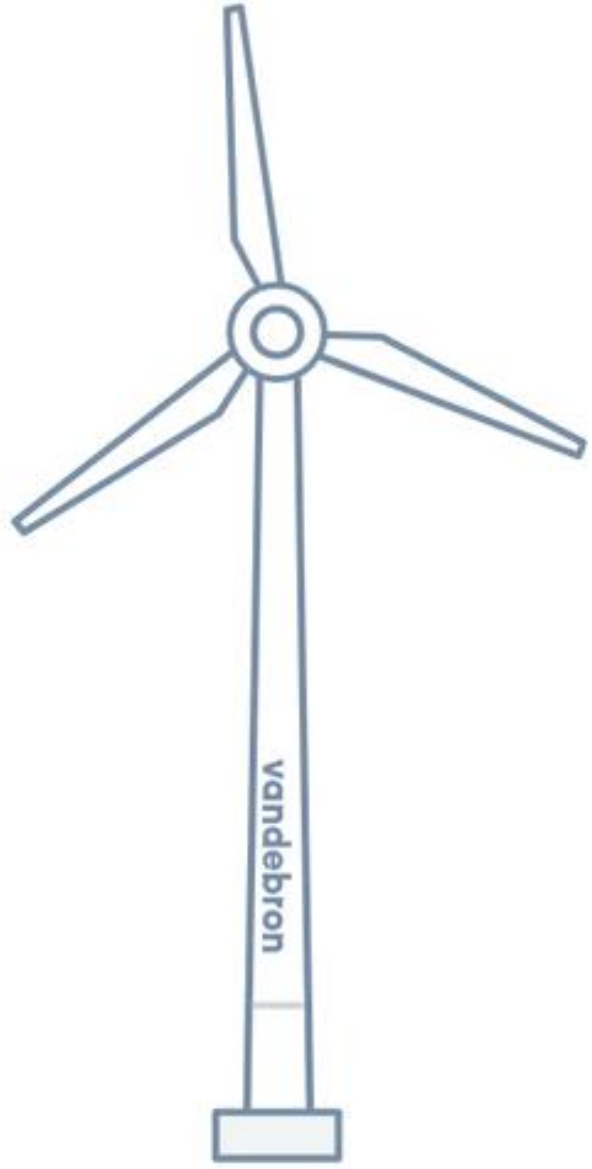
Advances in General AI and Autonomous Systems:

- Moving towards Artificial General Intelligence (AGI) with versatile cognitive abilities.
- Developing autonomous systems capable of independent decision-making.
- Addressing challenges in complexity, ethics, and safety for reliable AI operations.

Future Directions in AI Systems

Sustainable and Energy-Efficient AI Solutions:

- Reducing the environmental impact of large-scale AI models.
- Implementing green computing practices and optimizing algorithms for efficiency.
- Promoting sustainable AI development to ensure long-term viability.



What’s Next?

Generative AI and Large Language Models (LLMs)


THANK YOU!