Lecture 04: From Chatbots to Agents

Learning Objectives

By the end of this lecture, you should be able to:

- Differentiate between traditional chatbots and agentic AI systems.
- Identify the limitations of basic conversational agents.
- Understand the essential features that define autonomous agents.
- Recognize the architectural shift from reactive dialogue to proactive action.

Key Concepts

Chatbots vs. Agents

Chatbots:

- Designed for turn-based conversation.
- Reactive: respond to user input without long-term goals.
- Typically stateless or short-term memory based.
- No planning or action beyond replying with text.

Agents:

- Goal-driven and capable of initiating actions.
- Maintain memory, use tools, and perform multi-step reasoning.
- Operate over time to achieve complex tasks.
- Can perceive context and make decisions autonomously.

Key Agentic Features

- **Autonomy**: Operate without continuous human intervention.
- **Memory**: Store and retrieve past interactions and facts.
- **Tool Use**: Call external APIs, databases, or perform computations.
- **Planning**: Break down tasks into sequential or parallel steps.
- **Persistence**: Maintain a loop of observation, decision, and action.

Required Tools/Libraries

- LangChain (for exposure to agent architecture)
- OpenAI or Hugging Face models
- No setup required for conceptual understanding

Hands-on Exercise: Feature Comparison

Goal: Identify what distinguishes a chatbot from an agent by experimentation.

Task:

1. Interact with a basic chatbot (e.g., OpenAI's ChatGPT or Hugging Face's basic models).
2. Record its behavior in different scenarios:
    - Does it remember facts from earlier?
    - Can it initiate action or ask clarifying questions?
    - Is it goal-oriented?
3. Compare that with an open-source agent (e.g., AutoGPT or LangChain Agent).
4. Fill in the following comparison table:

Capability	Chatbot	Agentic System
Memory	❌	☑
Tool use	❌	☑
Planning	❌	☑
Multi-step tasks	❌	☑
Autonomy	❌	☑

Reflection:

- What was the biggest gap between the two systems?
- How does adding memory and tools transform the interaction?
