

# AI SUMMIT 2025

---

## AI AGENTS

ARUP DAS

# What is an AI Agent?

---

- An AI agent is an entity that can perceive (sense : **visual, auditory and physical inputs**) its environment and take actions to affect that environment.
- Given a situation (known as the **start state**), the agent's task is to make a series of decisions (**actions**) that move it toward a desired outcome (**goal state**). [**goal-oriented**]

# What is an LLM Agent?

A system that uses an LLM (think of it as the  of the AI Agent) to

- **reason** through a problem,
- **create a plan** to solve the problem,
- **execute** the plan with the help of a set of tools and
- **iterate** on the plan using feedback from tools and past interactions  
[**Non-deterministic**]

# What are LLM Agent so popular?

---

- Agents were around before LLMs took off.
- Used hard-coded rules or custom-trained models like BERT
- Rule-based systems could only respond based on predetermined paths.
- BERT has limited reasoning ability, understands text well, but it doesn't generate.
- LLMs are trained on massive datasets, generate coherent human like responses.

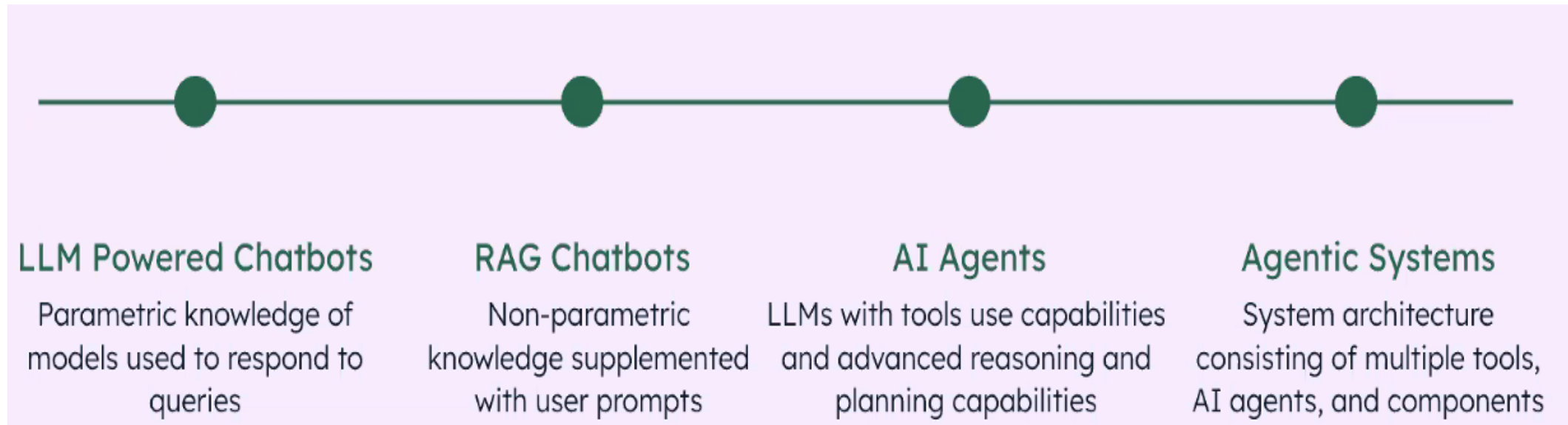
# Why not fine tune LLMs instead of using LLM Agents?

---

- Domain specific fine-tuning degrades generality.
- Fine-tuning adequately trained pretrained models rarely augments reasoning capability.
- LLMs are closed systems and cannot use external tools.

# Evolving Intelligent Interfaces

---



# When to use agents?

---

Who was the first Prime Minister of India?

# When to use agents?

---

Who was the first Prime Minister of India?

NO



# When to use agents?

---

What is the travel reimbursement policy for my company?

# When to use agents?

---

What is the travel reimbursement policy for my company?

**NO**

# When to use agents?

---

How has the trend in average daily calorie intake among adults changed over the last decade in India, and what impact does this have on obesity rates? Also, provide a graphical representation of the trend in obesity rates over this period.

# When to use agents?

---

How has the trend in average daily calorie intake among adults changed over the last decade in India, and what impact does this have on obesity rates? Also, provide a graphical representation of the trend in obesity rates over this period.

YES

Multiple sub-tasks:

1. Data Aggregation
2. Visualization
3. Reasoning through results obtained from previous tasks

# When to use agents?

---

Build the personal GATE Chatbot that teach concepts by reviewing the syllabus for an exam. It reviews the student's performance in an AI generated mock test, identifies the key areas for improvement and sets clear goals.

# When to use agents?

---




**Weekly Goal Example:** *Master page replacement algorithms and recursion.*

## What the AI Agent Can Do?



- **Review Past Year Papers** – Understand question trends & patterns
- **Generate Mock Questions** – Tailored to topic, difficulty, and goal
- **Create Smart Study Plans** – Prioritize high-weightage topics dynamically
- **Assess Student Progress** – Adapts plan based on test scores & time left
- **Detect Exam Patterns** – Adjusts for institute-specific question styles
- **Recommend Resources** – Picks best-fit tutorials, sheets, and tests
- **Proactive Support** – Intervenes when the student struggles (e.g., with Deadlocks)

# When to use agents? - TLDR

---

- Complex multi-step tasks 
- Personalized and adaptive experiences 
- Multiple capabilities such as Q&A, task analysis and execution required. 

## Do not use Agents when

1. The task is simple, well-defined. E.g. language translation 
2. Where speed and predictable execution matters. E.g. medical devices like pacemakers. Here, we require a low-level firmware with deterministic execution. 

# Single vs Multi *Agent systems*

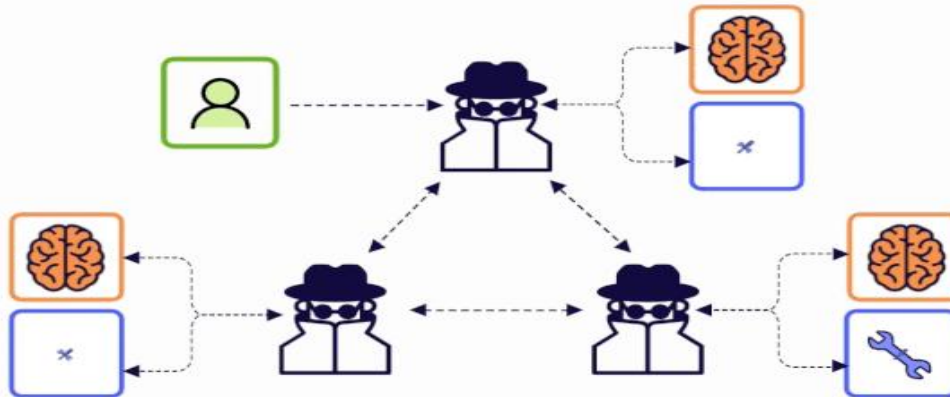
for retrieval-intensive applications



Single-agent architectures



Multi-agent architectures



## Single-Agent Systems:

- Centralised reasoning and task handling.
- Selects all knowledge sources independently.
- Entirely manages input to output workflow.
- Ideal for simple tasks with clear decision paths.
- Easy to implement and maintain.

## Multi-Agent Systems:

- Distributes tasks across multiple agents
- Master agent coordinates overall workflow.
- Each agent specialises in specific domain.
- Used for diverse knowledge needs
- Handles complex, multi-step processes.



# Components of AI Agents

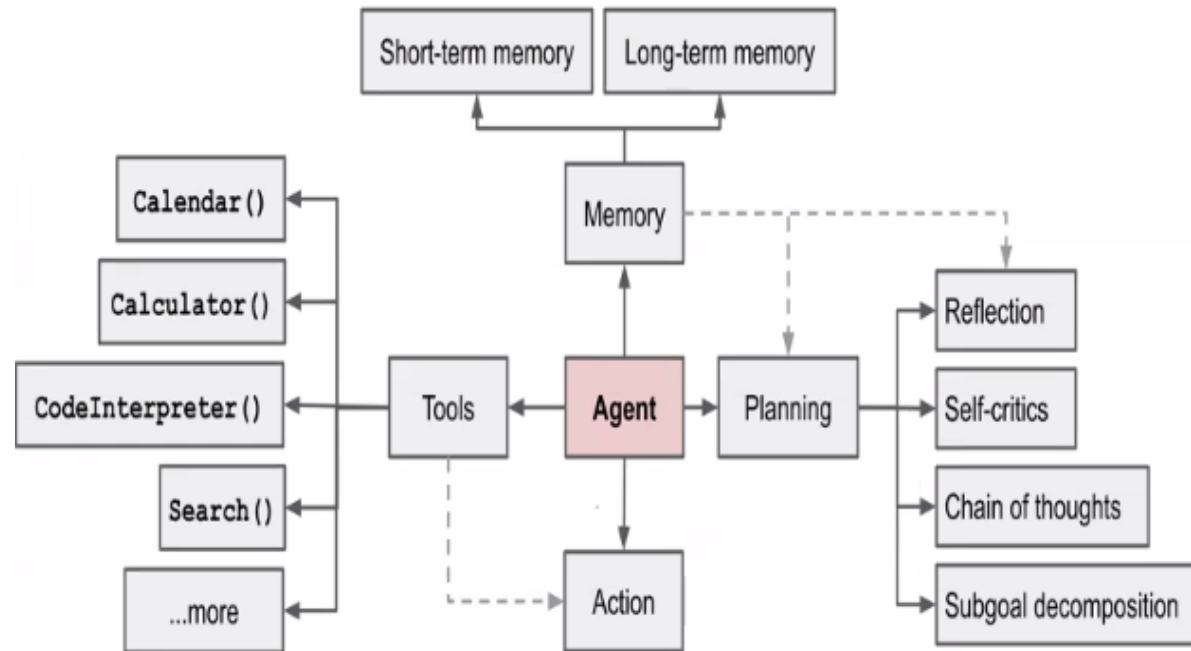
Agent/Brain

Planning

Action

Tool

Memory



# Memory

---

- Short-term
- Long-term
- Procedural
- Semantic
- Episodic

# Use Cases

---

- Simple Weather API using smolagents: <https://github.com/DocketAI/DocketTalks/blob/main/why-agents/Weather%20App%20-%20Agents%20Demo.ipynb>
- Customer Support Agent using arize ai pheonix: <https://github.com/Arize-ai/phoenix/blob/main/tutorials/experiments/agents-cookbook.ipynb>
- Build your own voice AI agent with no code: <https://www.youtube.com/playlist?list=PLWYu7XaUG3XP3o7Fy5G155SQU3Pt57WM>
- Virtual Primary Care Assistant for Medical Pharmacy: [https://github.com/mongodb-developer/GenAI-Showcase/blob/main/notebooks/agents/zero\\_to\\_hero\\_with\\_genai\\_with\\_mongodb\\_openai.ipynb](https://github.com/mongodb-developer/GenAI-Showcase/blob/main/notebooks/agents/zero_to_hero_with_genai_with_mongodb_openai.ipynb)

# Challenges

---

- 1. Limited Context:** LLMs can forget earlier conversation details; vector stores help but aren't perfect.
- 2. Long-Term Planning:** Struggle with extended tasks and adapting to unexpected changes.
- 3. Role Adaptation:** Hard to fine-tune for niche roles or align with complex human values.
- 4. Prompt Dependence:** Small prompt changes = major errors; crafting prompts is critical.
- 5. Cost & Efficiency**  
High compute needs = expensive and sometimes slow performance.