Agentic AI with LLMs

Duration: 16 hours (2 days)

Pre-requisites

- Basic knowledge of Python programming
- Familiarity with LLMs like ChatGPT
- Basic understanding of APIs & JSON
- Optional: Experience with LangChain, Autogen, or similar libraries

---

Course Outcomes

By the end of this workshop, you will:

- Understand AgentAI fundamentals and LLM integration
- Build and deploy single and multi-agent systems
- Integrate tools, memory, and planning in agent workflows
- Design autonomous agents for real-world tasks

Day 1: Fundamentals & Building Simple Agents

1. **Introduction to AgentAI**
    - What is AgentAI?
    - Evolution from chatbots to intelligent agents
    - Agent vs. traditional automation
2. **LLMs in Agent Workflows**
    - Role of LLMs in reasoning and decision-making
    - Prompting basics for agents
3. **Types of Agents**
    - Reactive vs. Proactive
    - Planning vs. Tool-using
    - Autonomous vs. Human-in-the-loop
4. **LLM Agent Architecture**

- Components: Input, Planner, Memory, Executor, Tools
- Communication loop explained

5. **Building a Basic Agent**
    - Environment setup
    - Create a simple echo agent using LangChain / Autogen / CrewAI
    - Add a basic tool (e.g., calculator or API caller)
6. **Memory & Context Handling**
    - Short-term and long-term memory
    - Use of vector stores: FAISS, Chroma, Pinecone
7. **Hands-on Lab: Tool-Using Agent**
    - Build an agent that answers questions via a search tool

---

Day 2: Multi-Agent Collaboration & Deployment

8. **Multi-Agent Systems (MAS)**
    - Agent roles: Manager, Worker, Specialist
    - Collaboration vs. coordination
9. **Planning & Task Decomposition**
    - Using LLMs for breaking down goals
    - Auto-GPT & BabyAGI concepts
10. **Lab: Create a Multi-Agent Team**
    - Assign tasks to sub-agents (e.g., research, summarize, email)
11. **Advanced Tool Integration**
    - Calling APIs (e.g., Google, SQL, custom tools)
    - Chaining multiple tool outputs
12. **Agent Autonomy & Guardrails**
    - Human-in-the-loop design
    - Rate-limiting, safety, audit logging