

Introduction to Agentic AI

Overview

This course – Introduction to Agentic AI provides a complete journey into designing, building, and deploying Agentic AI Systems. Learners begin by understanding how Agentic AI differs from GenAI and RAG, exploring key components like reasoning, action, and memory, as well as the foundational ReAct pattern.

The course covers agent types—and their practical applications in domains like healthcare. Learners will build tool-using agents via frameworks like LangChain and LangGraph. Advanced modules dive into planning, reflection, memory handling, and both single and multi-agent workflows.

Key topics also include securing GenAI applications, ensuring fairness and compliance, and evaluating agents through various techniques. This course empowers learners to build scalable, ethical, and human-centric AI agents for real-world use.

Course Structure

Item	Description
Concept Video	Lecture video mostly 4-7 mins
Screen Recording Demo Video	Demonstration videos of various concepts done in real life.
Reading Materials	PDFs, presentations, or on-screen texts
Downloadable	PDFs
Hands-on Assignments/Exercise	Instructions to practice some concepts to be added wherever they are applicable and best fit for learning
Case Studies/Examples	Examples of similar applications across the domain to be added wherever they are applicable and best fit for learning
Practice Quiz	Set up questions as practice for learners to master the concept/s to be added a logical interval

Course Outcomes

CO Code	Course Outcome	Description
CO1	Define key concepts and terminology related to Agentic AI, including types of agents, core components, and standard architectural patterns.	Explain foundational elements of Agentic AI such as reasoning, action, memory, ReAct pattern, and classify agents.
CO2	Differentiate between traditional GenAI, RAG systems, and Agentic AI by identifying their roles, capabilities, and design principles in solving business problems.	Contrast system types based on autonomy, context-awareness, tool-use, and reasoning, highlighting where and why Agentic AI is more suitable for complex tasks.
CO3	Implement basic and advanced Agentic AI systems using various frameworks, incorporating tool calling, memory, and planning components.	Use platforms like LangChain, and LangGraph to build agentic systems that perform tool calls, use memory, and apply planning and reflection techniques.
CO4	Analyze real-world use cases to determine appropriate agent types, workflows, and architecture patterns.	Examine business scenarios (e.g., healthcare research assistants) to select and map suitable agent types, components, and patterns for implementation.
CO5	Evaluate fairness, transparency, security, and regulatory compliance of Agentic AI systems using best practices and agent evaluation techniques.	Apply frameworks like HIPAA, fairness audits, and evaluation methods (LLM-as-judge, tool-call accuracy) to assess the ethical deployment of agents.
CO6	Design and orchestrate scalable, human-centric Agentic AI workflows to automate business processes and enhance collaboration between agents and users.	Create complex single or multi-agent workflows leveraging standard design patterns (e.g., planning, reflection, hierarchy) with an emphasis on usability and trust.

Module Details

Module Name	Module Outcome	Course Outcomes (COs) Mapped
Module 1: What is Agentic AI	<ul style="list-style-type: none"> Define the characteristics and components of Agentic AI Systems, including reasoning and action patterns. Differentiate between GenAI, RAG, and Agentic AI through analysis of real-world use cases and architectural evolution. 	CO1, CO2, CO4
Module 2: Building Agentic Ai Systems	<ul style="list-style-type: none"> Explain the roles of tools, memory, reasoning, and LLMs in Agentic AI systems, and explain how frameworks like LangChain/LangGraph simplify their integration. Build agents that invoke external APIs and services using LangChain, demonstrating how tool calling enables autonomous action. Architect single-agent workflows (e.g., research assistants) that leverage stateful memory and planning to solve multi-step problems. Audit Agentic AI systems for security, bias, and compliance risks, applying protocols like MCP to standardize tool interactions. Explain agent evaluation techniques (e.g., LLM-as-judge, step trajectory analysis, goal accuracy) to assess performance and safety. 	CO1, CO2, CO3, CO4, CO3, CO5, CO6
Module 3: The Future of Agentic AI Systems with Responsible Design, and Governance	<ul style="list-style-type: none"> Apply fairness, transparency, and accountability principles in the design of Agentic AI systems. Evaluate ethical risks, misinformation challenges, and compliance requirements for deploying Agentic AI in regulated environments. Design governance strategies to mitigate risk and align AI behavior with human values and legal standards. 	CO4, CO5, CO6

Module Description

Module 1: What is Agentic AI



This module provides a foundational introduction to Agentic AI Systems, tracing their evolution from traditional Generative AI and Retrieval-Augmented Generation (RAG) systems to more autonomous, goal-driven architectures. Learners will examine the core components of Agentic AI—including reasoning, action, and autonomy—and explore the influential ReAct (Reasoning + Acting) pattern that underpins agentic workflows. The module introduces the four major types of agents: Reactive, Deliberative, Hybrid, and Learning Agents, highlighting their differences in decision-making and adaptability. Real-world use cases, especially in healthcare, illustrate practical relevance. This module lays the groundwork for more technical exploration in future sessions, bridging theory and applied agentic design.

Module 2: Building Agentic AI Systems

This module dives deep into the architectural and technical foundations of building Agentic AI Systems, with a strong focus on tool calling, frameworks, and design patterns. Learners will explore how reasoning, action, memory, and tool-use interact to form intelligent, goal-driven agents. The module introduces key frameworks—LangChain and LangGraph—and demonstrates how to build tool-using agents through and code-based implementations. Students will learn how to implement and standardize tool calling using Model Context Protocol (MCP) and incorporate components such as planning, memory, and reflection for more advanced capabilities. Through live demos and labs, learners will gain hands-on experience in building both single-agent and multi-agent systems, with a focus on observability, modularity, and scalability. The module concludes with best practices for securing GenAI applications, ensuring robustness against common vulnerabilities like prompt injection and PII exposure. The module also introduces the fundamentals of Agent Evaluation, including why it is critical and how it can be implemented through various methods like LLM-as-judge, router evaluation, and tool-call accuracy. By the end of this module, learners will be equipped to develop AI systems that are both technically sound and socially responsible.

Module 3: The Future of Agentic AI Systems with Responsible Design, and Governance

This module focuses on the ethical, regulatory, and governance aspects of developing and deploying Agentic AI Systems. Learners will explore how to embed fairness, transparency, and accountability into AI agents, while also addressing challenges like misinformation, bias, and ethical risk. The module provides guidance on applying governance frameworks and compliance strategies, including key regulatory standards such as HIPAA and the EU AI Act. Learners will also study the evolution of AI agents toward greater autonomy and multi-agent collaboration and examine how agents can be responsibly used for automating business processes.



Course Completion Criteria

To successfully complete this course, you must fulfill the following requirements:

Completion of Learning Modules: Complete all learning modules, including watching all lecture videos, Screen demo recordings, reviewing all provided reading materials, and accessing any external links shared in the course.

End of Course Assessment: Complete the MCQ assessments at the end of the course, and it is mandatory for overall course completion. A passing score or higher is required to mark the course as complete.

End of Module/Lesson Practice Assessment: After each module, you should complete the practice assessment associated with that module.

Hands-On Exercises/Labs (Practice): Hands-on exercises are provided to help you apply the concepts demonstrated in the demo videos. The corresponding code files and datasets are provided to help you apply the concepts demonstrated in the demo videos. Login to the UAIS environment to access the files, and follow the instructions to complete/practice the hands-on practice exercises.