Building Agentic AI Systems with Generative AI Models

Duration: 48 hours (06 days)

Course Outcomes

By the end of this course, participants will be able to:

1. Understand the fundamentals of Agentic AI and its practical applications.
2. Leverage open-source models (e.g., Llama 2, Bloom, AutoGPT) to build autonomous AI systems.
3. Create decision-making AI agents for text, vision, and multi-modal tasks.
4. Evaluate, monitor, and optimize Agentic AI systems using MLflow.
5. Build conversational AI chatbots using open-source tools for practical use cases.

Course Pre-requisites

- Foundational understanding of AI or software development.
- Basic Python programming knowledge along with experience in working with notebooks (Jupyter/Colab) and using common machine learning frameworks such as PyTorch or TensorFlow at an introductory level.
- A general understanding of APIs, JSON, and simple command-line operations will be helpful for building and deploying agents.
- Prior exposure to concepts like embeddings, vector databases, or LLMs is beneficial but not mandatory.

Table of Contents (TOC)

- Benefits of Using Open-Source Models for Agentic AI
- Popular Frameworks and Libraries

Module 3: Language Models for Agentic AI

- Hugging Face Transformers: Overview of GPT models viz., Bloom, Falcon, etc.
- Llama 2: Open-source alternative to proprietary models
- LangChain: Framework for autonomous AI applications

Module 4: Vision Models for Agentic AI

- OpenCV and Mediapipe: Processing visual data
- CLIP: Multi-modal understanding of text and images

Module 5: Multi-Modal Models

- OpenAI Whisper: Speech-to-text model (open-source)
- DALL-E Mini: Image generation and understanding (open-source alternative)
- DeepMind Perceiver: Multi-modal task processing

Module 6: RAG Pipelines Indexing PDFs, Docs, APIs into VectorDB and querying

- Introduction to Retrieval Augmented Generation (RAG)
- Document, PDFs, CSV, indexing
- Introduction to VectorDB
- Working with Weaviate
- Concept of Embedding, Retrieval, Chain and Agents using LangChain
- Lab: Build a Retrieval Augmented Generation (RAG) Application using LangChain
- Lab: Build an SQL database Agent
- Hands-On RAG Agent Build (Agentic RAG)

Module 7: Open-Source Tools for Creating Agentic AI Systems

- LangChain: Building complex agent workflows
- Gradio: Creating interactive user interfaces
- Streamlit: Lightweight UIs for Agentic AI applications
- Docker: Scaling and deploying open-source AI agents

Module 8: Building Chatbots with Agentic AI

- Using Llama 2 and Open-Assistant for Conversational Agents
- LangChain for Multi-Turn Conversations and Workflow Automation
- Integrating Gradio or Streamlit for Chatbot UIs
- Hands-On: Building a Task-Specific Chatbot

Module 9: Evaluation and Optimization Using MLflow

- Introduction to MLflow for Model Tracking and Experimentation
- Logging Metrics, Parameters, and Artifacts for Agentic AI Models
- Model Versioning and Deployment with MLflow
- Fine-Tuning and Re-Evaluating Open-Source Models Using MLflow

Module 10: Training and Fine-Tuning Open-Source Models

- Customizing Models for Specific Agentic Tasks
- Tools for Model Fine-Tuning (**Hugging Face Trainer**, **PEFT**)
- Dataset Preparation for Agentic AI

Module 11: Deployment Process on Azure Cloud (No Labs)

- Deploying Open-Source Models in Production
- Integrating Models with Azure Cloud Services

Module 12: Ethical and Responsible Use of Agentic AI

- Bias Detection and Mitigation in Open-Source Models
- Transparency in Decision-Making Processes
- Safeguards Against Unintended Outcomes

Module 13: Hands-On Projects

- Building a Text-Based Autonomous Customer Support Agent
- Creating a Multi-Modal Autonomous Data Entry Assistant
- Developing a Vision-Based Inventory Management Agent
- Case Study: Building a Task Automation Pipeline with AutoGPT

Module 14: Future Trends in Agentic AI

- Advances in Agent Architectures
- Evolution of Open-Source Model Ecosystems
- Cross-Domain Collaboration in Agentic AI