Research task

Basics of Agentic Ai

Ai agents is a type of ai which not only gives an answer but also makes decision , complete the task and goal by following steps it is like a helper robot which does a lot of work like searching something from the internet , sending emails and complete any type of task

Example:

Imagine we're building an Agentic AI that helps you plan trips.

Let's say your goal is: to book the cheapest flight and hotel from Karachi to Islamabad.

Here are the steps the Agentic AI might take on its own:

Understanding: The AI first gets what you want: 'cheapest flight and hotel from Karachi to Islamabad'.

Planning: It then figures out how to make that happen. It might think of these steps:

- Check different flight booking websites.
- Check different hotel booking websites.
- Compare the prices of flights and hotels.
- Pick the cheapest options.
- Tell you the booking details.

Action: Now the AI starts doing the actual work:

- It uses a web browser to go to flight and hotel booking sites. (This is it using a 'tool' by itself).
- It enters the dates and city information.
- It looks at the results and compares the prices.

Observation: The AI sees what each website shows. If a site has an error or doesn't have the info, it takes note of that.

Decision Making:

- When it finds the cheapest flight and hotel, it decides that's the best choice.
- If it runs into a problem (like not finding a cheap hotel), it might change its plan. Maybe it would ask you if you're okay with spending a bit more or looking at hotels in a different area.

Output: Finally, it tells you what it found: 'I found the cheapest flight and this hotel for your trip from Karachi to Islamabad.' It might also give you the booking details."

LLM(Large Language Model):

So, an LLM, which stands for Large Language Model, is basically a type of AI that's been trained on a massive amount of text data. Think of things like:

- Books
- Articles
- Text you find all over the internet

Its job is to write and respond in a way that sounds like a human would.

A good example of an LLM is ChatGPT. It understands your questions and answers you using natural language."

How LLM works?

So, how do these Large Language Models (LLMs) actually work? Well, they're basically AI that have been trained on a ton of text like millions of books, articles, and websites. This massive training helps them learn to understand and respond to human language.

It kind of happens in three main steps:

1. Training (Learning): The LLM gets fed this huge ocean of text data.

Think of things like:

- Wikipedia
- News articles
- Stories
- Conversations

The model reads all of this stuff and learns things like:

- What words usually come after other words.
- How sentences are structured.
- How questions and answers work.

For example:

If the model reads "The sky is..." a million times, it learns that "blue" often comes next.

2. Understanding: When you ask it something, the LLM:

- Looks at your words.
- Figures out what you're trying to say.
- Remembers similar things it learned during its training.

For example:

If you ask: 'What's the capital of France?' The LLM will recognize this as a general knowledge question, and it would have learned during training that:

'The capital of France = Paris'

3. Generating the Answer: Now, the LLM tries to guess the best way to respond.

It writes the answer word by word, like: 'The capital of France is Paris.'

This whole process happens super fast, which is why it feels like the AI is responding instantly.

Fun Fact: LLMs don't really 'think' in the way humans do. They just work based on patterns and the data they were trained on.

It's almost like a really smart parrot that can say incredibly relevant things when you talk to it – but it doesn't have its own thoughts.

A Simple Example: If you write:

'Once upon a time...' The LLM might predict:

'there was a king.' 'who lived in a castle.' 'he had a beautiful daughter...'

Basically, it understands the flow of language and guesses the next word that makes sense."

Generative Ai:

so Generative AI is basically the kind of AI that can create new stuff.

Think of it like this:

- It can write text for you.
- It can make images.
- It can even create audio and videos.

If you tell the AI, "Hey, write me a story," and it actually writes one, that's Generative AI in action.

Difference between Generative AI and Agentic ai

Aspect	Generative AI	Agentic AI
Purpose	Generate content (text, images)	Take autonomous actions & decisions
Interaction	Responds to user prompts	Acts independently in environment
Examples	ChatGPT, DALL·E	Autonomous robots, smart agents
Autonomy level	Low to moderate (prompt-driven)	High (self-directed agency)
Typical Use Case	Content creation, text/image generation	Task automation, complex problem solving

Open AI Agent SDK:

the OpenAI Agents SDK is basically a set of tools from OpenAI that helps us build AI "agents." Think of these agents as smart programs that can do things on their own by using other tools, like different apps or websites.

Instead of just having AI that spits out text or answers simple questions, this SDK lets us create AI that can think through tasks step-by-step, take actions, and automatically work with other systems.

It takes care of the tricky part of managing how the AI figures things out, plans what to do, uses those external tools, and then gives you the result. So, it's a way to build AI that's not just talking, but actually *doing* things intelligently.

Why are we using it?

- **To make smarter AI:** We can build AI that doesn't just chat, but can actually perform tasks and interact with other things automatically.
- **To make complicated stuff easier:** It helps us handle complex sequences of thinking, deciding, and using tools without having to code every single step ourselves.
- **It's flexible:** We can easily add different tools and make the AI act how we want it to.
- **It saves us time:** OpenAI has already built a lot of the basic pieces we need, so we don't have to start from scratch.
- **It uses really good AI:** It works with OpenAI's powerful language models, so the agents can understand what we're saying, generate text, and reason pretty well.

What's good about using it?

Benefit	Explanation
Autonomy	The AI can make its own decisions and do multiple things without us telling it every single step.
Multi-step reasoning	It can handle tasks that need several steps of thinking and action.
Tool integration	It's easy to connect the AI with other things like websites, databases, and search engines.
Better accuracy	By using its "brain" along with outside tools, the AI can give more accurate and helpful answers.
Scalability	The way it's built lets us create a lot of these agents and make them do more stuff.
Customization	We can tell the AI what its goals are, what rules it needs to follow, what tools it can use, and how it should behave for different situations.

Better user experience	The AI can be more helpful, know what you need, and interact with you in a more natural way.
Rapid prototyping	We can quickly build and test these smart agents using the pieces that are already there.
OpenAI ecosystem	It works smoothly with OpenAI's other AI stuff, and we get their updates and support.

Export to Sheets

What can we use it for?

- **Customer support bots:** AI that can answer questions, look up info, and even create support tickets.
- **Personal assistants:** AI that can help with your schedule, set reminders, and draft emails by talking to your calendar and email.
- **Research assistants:** AI that can find information by searching databases, summarize documents, and answer tricky questions.
- **E-commerce bots:** AI that can help you find products, check if they're in stock, and place orders by connecting to shopping websites.