SUNG KYUN KWAN UNIVERSITY
SKK GSB

FMBA AI Workshop 3

Introduction to AI Agents

Dr. Yuan Tian

Overview

- AI Agents
- Agentic AI and Use Cases
- Lab: Market Research of AI Use

A brief history - Stage 1 (LLMs with simple prompts)

User Prompt

- **Direct instructions** provided by the **user**.
- Free-form natural-language content reflecting the user’s intention

Characteristics:

- The “entry point” for activating an LLM.
- User prompts are the primary driver of the model’s output.
- Despite being simple, user prompts alone **cannot support advanced multi-step automation workflows**.

A brief history - Stage 2 (LLMs with prompt engineering)

System Prompt

- High-level instructions used to define the AI model’s core behavior, persona, boundaries, and constraints. *E.g., “Act as a business manager…..”*

Objective

- Sets global behavioral rules and overall tone for the LLM.
- Helps the model stay within defined limits regardless of the user prompt.
- In custom solutions (e.g., Customized ChatGPT), system prompts can define special personas (e.g., “Act as an AI travel consultant.”)

A brief history - Stage 2 (LLMs with prompt engineering)

Limitations:

- System prompts **cannot independently support multi-step workflows**.
- They **only** control **model behavior, not tool invocation or autonomous actions.**

In short, it can tell you what to do, but you still have to carry out each step yourself.

But what if the LLM could generate actions and those actions could be executed automatically?

A brief history - Stage 3 (LLMs with AI Agents Tools)

What Is an AI Agent?

- Traditional LLMs can only provide responses when prompted; they cannot **initiate or execute autonomous workflows**.
- **AI Agent:**
  A system that can ***interpret***, ***plan***, **and *act***—capable of **multi-step** reasoning and autonomous tool-use.
- **ChatGPT (or other AI Tools) with Agent Mode/Feature**
  a. E.g., ChatGPT agent can "think" and "act" using its own virtual computer to conduct tasks such as *browsing the internet, using coding tools to run code or analyze data, breakdown a high-level goal to smaller steps.*

A brief history - Stage 3 (LLMs with AI Agents Tools)

Challenges in AI Agents

- AI may **generate incorrect plan steps**, causing chain reaction failures.
- Even with a correct plan, **a single step failure may halt the entire workflow**.
- When an agent relies on multiple tools, each tool's performance directly affects task success.

A brief history - Stage 4 (From AI Agents to Agentic AI)

What is Agentic AI system?

The core of agentic AI is the use of **AI agents** to perform automated tasks with limited human intervention.

- **Multi-agents (not single agent)**. Coordinate multiple system to handle different steps in a complex workflow.
- **Tool use**. Connect AI to various tools such as browser, databases, APIs, and external services to actually perform the task but not just generate text.
- **Divide and conquer**. Break a high-level tasks into smaller steps that can be executed.
- **Reasoning and reflection**.

A brief history - Stage 4 (From AI Agents to Agentic AI)

Agentic AI systems have all the following components to complete multi-step goals:

- LLM reasoning
- tool availability (via MCP)
- action execution (via function calling)

Concept	Analogy	Role
Function Calling	Buttons on a machine	Lets AI trigger specific actions
Model Context Protocol (MCP)	Wiring + APIs	Connects many machines in a standard way
Agentic AI	Operator	Decides which buttons to press and in what order

How Agentic AI System works? An example

Automated Task Workflow with Agentic AI System

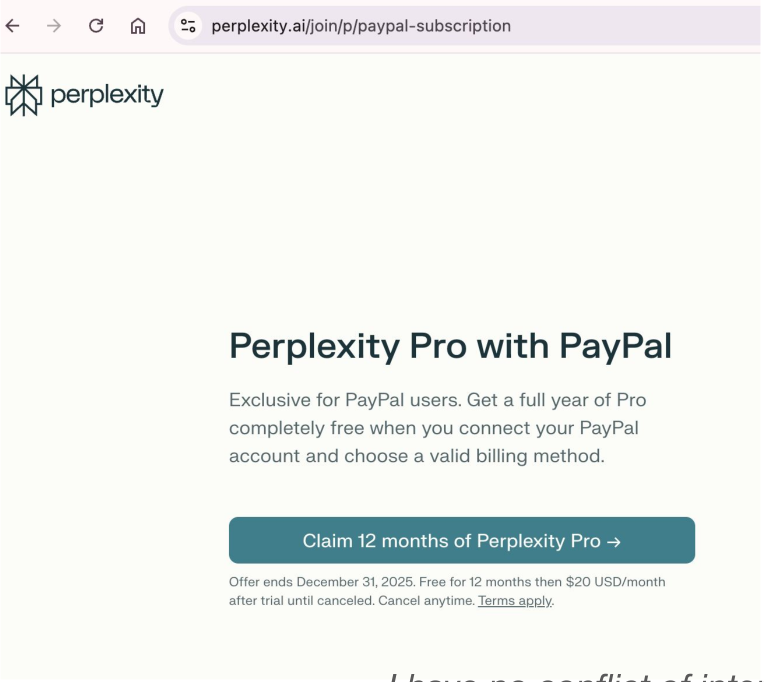
1. **User Input:**
   User provides a request via an MCP client (e.g., “Help me book a flight from seoul to tokyo next week.”)

2. **Agent Interprets (LLM):**
   The agent extracts the intent and plans next steps.
3. **Tool Discovery (Planning):**
   Agent checks available tools.
4. **Function Calling (Tool or API Use):**
   Agent invokes tools through MCP servers using function calls.
5. **Data Retrieval (Tool or API Use):**
   Tool returns execution results to the agent.
6. **Reasoning (LLM):**
   Agent processes results and decides next steps.
7. **Final Output:**
   Agent generates the final answer for the user.

How Agentic AI System works? An example

Demonstration (ChatGPT, Gemini, and Comet):

- Comet Browser: a Personal AI Assistant
- https://www.perplexity.ai/comet
- 12 month pro plan free for paypal users.



perplexity.ai/join/p/paypal-subscription
perplexity

Perplexity Pro with PayPal

Exclusive for PayPal users. Get a full year of Pro completely free when you connect your PayPal account and choose a valid billing method.

Claim 12 months of Perplexity Pro →

Offer ends December 31, 2025. Free for 12 months then $20 USD/month after trial until canceled. Cancel anytime. Terms apply.

If you claim it, don't forget to cancel after 12 months, otherwise, you will be charged 20 dollars per month.

I have no conflict of interests

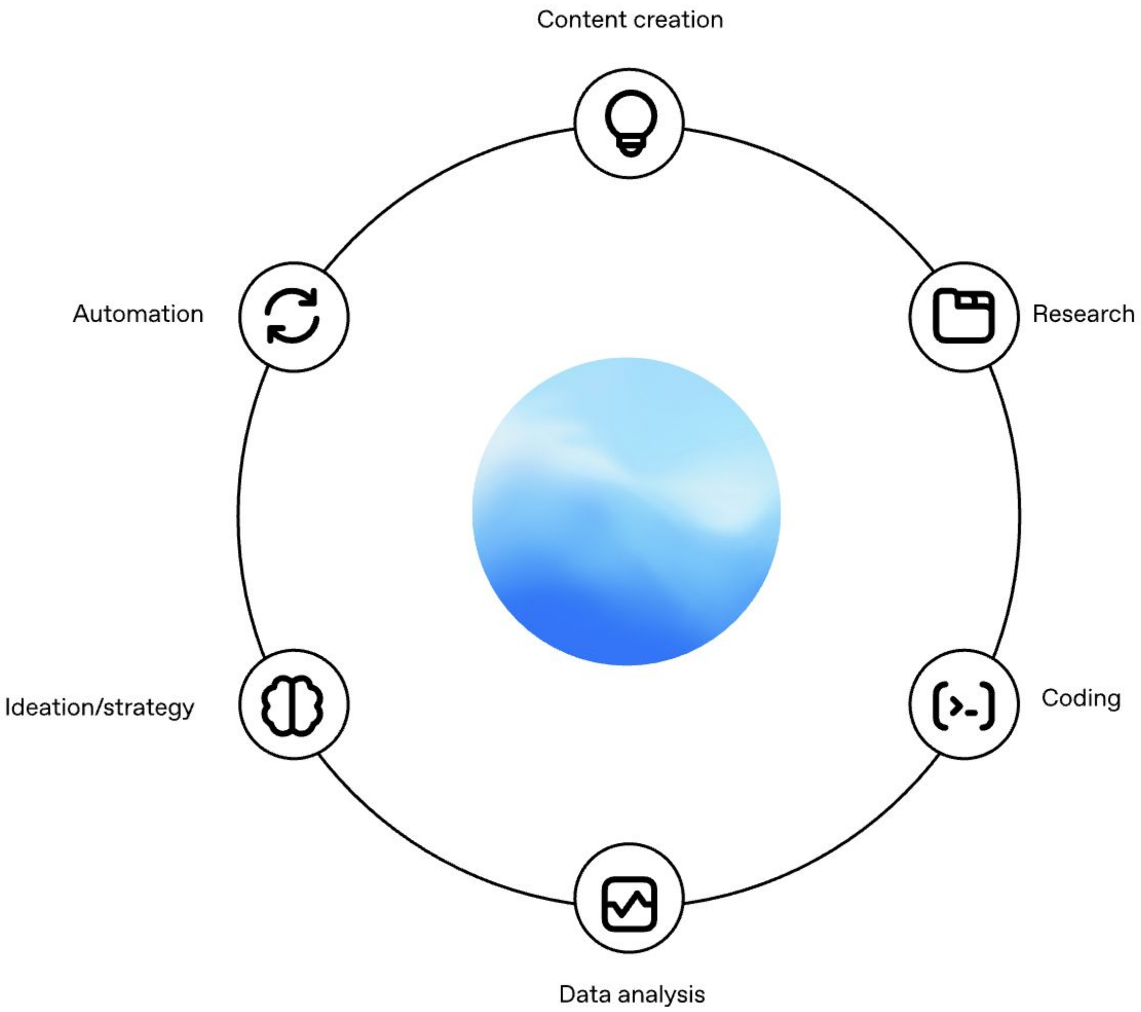
Questions?

Lab: Market Research of AI Use

Goal:

- Explore and analyze how Generative AI (Gen AI) and Agentic AI are being adopted across industries and time.

Six Major AI Use Cases



Real-world AI Use Case - Content Creation

Klarna, the fintech company, used generative AI (tools like DALL·E, Midjourney, Adobe Firefly) to generate **marketing images**. They reported savings of about USD 6 million by **cutting traditional image production costs.**

- **Increased Efficiency and Creativity:** Generated over 1,000 images in the first three months of 2024 using genAI, reducing the image development cycle from 6 weeks to just 7 days. This acceleration includes checks for brand consistency, image quality, and legal compliance.
- **GenAI is also driving savings in writing marketing copy.** Klarna has built an AI-powered copywriting tool, Copy Assistant, which allows the company to use AI for 80% of all copywriting.

- https://www.klarna.com/international/press/ai-helps-klarna-cut-marketing-agency-spend-by-25-and-run-more-campaigns/
- https://www.marketingdive.com/news/klarna-gen-ai-openai-cut-marketing-spend-efficiency/717332/

Real-world AI Use Case - Content Creation

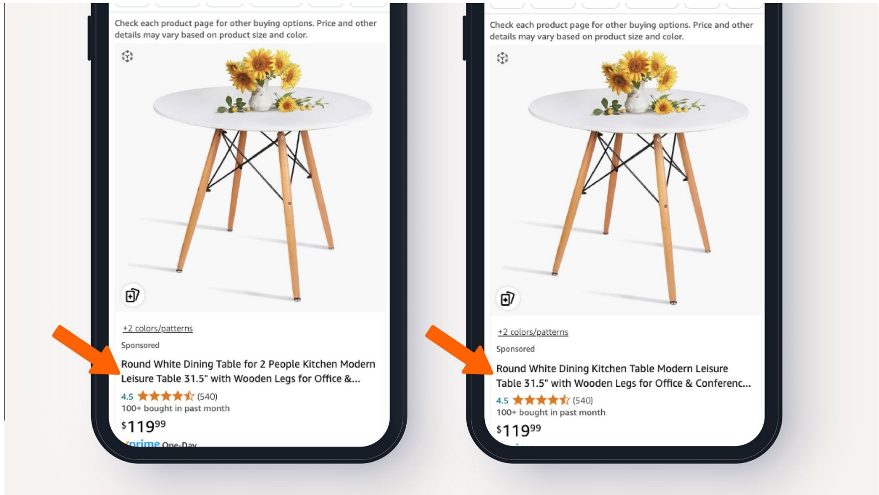
European online fashion retailer **Zalando** is using generative artificial intelligence to **produce imagery faster for its app and website**.

- Using generative AI **cuts the time needed** to produce imagery to around three to four days from six to eight weeks, and **reduces costs by 90%,** Haase said, adding the AI-generated content drives greater engagement from customers.

- https://www.reuters.com/business/media-telecom/zalando-uses-ai-speed-up-marketing-campaigns-cut-costs-2025-05-07/

Real-world AI Use Case - Content Creation

Amazon is using generative AI to improve product recommendations and product descriptions so they are more relevant for customers.



Check each product page for other buying options. Price and other details may vary based on product size and color.

+2 colors/patterns

Sponsored

Round White Dining Table for 2 People Kitchen Modern Leisure Table 31.5" with Wooden Legs for Office &...

4.5 ★★★★☆ (540)

100+ bought in past month

$119.99

prime One-Day

Check each product page for other buying options. Price and other details may vary based on product size and color.

+2 colors/patterns

Sponsored

Round White Dining Kitchen Table Modern Leisure Table 31.5" with Wooden Legs for Office & Conferenc...

4.5 ★★★★☆ (540)

100+ bought in past month

$119.99

When you search "table for two"

- https://www.aboutamazon.com/news/retail/amazon-generative-ai-product-search-results-and-descriptions

Beware of Reporting Bias in AI “Success Stories”

The Hidden Side

- Many AI projects fail quietly — they don’t make it into case studies or press releases.
- **Reporting bias:** Only successful implementations are shared (similar to how positive research results get published more often).
- **Negative or neutral outcomes are underreported** — creating a false sense of universal success.

Beware of Reporting Bias in AI “Success Stories”

Why the Bias Exists

- Companies may use “AI success” stories for **marketing.**
- Startups want to attract investors — showing positive ROI helps **raise funding.**
- Internal teams highlight wins to secure more budget or visibility.

Think Critically

- Who is sharing this story, and **why**?
- Is this result **independently verified** or **self-reported**?
- What’s Hidden” (failed projects, unmet ROI, shelved pilots)?

Lab: Market Research of AI Use

Goal:

- Explore and analyze how Generative AI (Gen AI) and Agentic AI are being adopted across industries and time.

Task:

- Use **AI tools (workshop 1)** and **effective prompts (workshop 2)** to ***research AI use, adoption, impacts, risks and challenges***.
    - Conduct a market-level scan by reviewing recent reports, articles, and studies on how organizations are adopting Generative AI and Agentic AI.
    - Summarize your learning and takeaways in a proper format.

Lab: Market Research of AI Use

Starting References for AI Market Research

- Gen AI’s Early Years – AI Adoption 23-24
- The GenAI Divide: State of AI in Business 2025
- *You should add more sources as you discover them*

Responsible Use of AI (Important for This Lab)

- **Verify information**. AI-generated summaries or claims must be checked against real sources.
- **Avoid hallucinations**. Always cross-reference facts with credible literature.
- **Maintain critical thinking**. AI can assist research, but you evaluate accuracy, relevance, and bias.

Hallucination of LLMs

AI “hallucination” = when a model gives false or made-up information.

Why it happens:

- Trained to predict words, not facts.
- Missing or biased data.
- No real-world verification.

Examples:

- Fake citations or events.
- Incorrect facts stated confidently.

Responsible Use of AI

- **Data Privacy & Confidentiality – Never share sensitive or personal data (e.g., customer, patient, or financial info).**
- **Compliance Awareness – Follow company policies and laws (GDPR, CCPA, HIPAA).**
- **Appropriate Use – Use AI for productivity, not to bypass rules, security, or ethics.**
- **Accuracy & Verification – Always fact-check AI outputs before using or sharing.**
- **Security Practices – Avoid entering confidential info into public AI tools.**

Responsible Use of AI: Samsung's AI Data Leak

What Happened

- Samsung engineers accidentally uploaded **sensitive source code and meeting notes into ChatGPT** (Mar 2023).
- The data became part of ChatGPT's input history, raising concerns over **confidentiality and data governance**.

Company Response

- Samsung **banned** employee use of ChatGPT and other public AI tools, and Introduced stricter AI usage policies and limits on data sharing.

Source:
https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

Responsible Use of AI

AI make mistakes!

Lab: Market Research of AI Use

- We will use the last 20 minutes to discuss your findings.

Reminder: please set up your Github account and complete the lab on Github before the next session in Jan 2026.

Lab Time