

# Giải Mã Các Khái Niệm Về AI Cho Dân Non-Tech | Bài 1

Hiểu đúng - Dùng đúng - Không bị "hype" cuốn

**Bruce Tran (Trần Lâm Huân)**

*AI Enthusiast | Chia sẻ nội bộ cho anh em thân thiết*

# Mục Đích Của Series Này

Không chỉ hướng dẫn cách dùng — mà là HIỂU BẢN CHẤT

**AI đang tiến hóa như vũ bão.**

**Nếu chỉ học cách DÙNG → sẽ luôn chạy theo sau.**

**Nếu HIỂU bản chất → AI advance đến đâu, mình advance với nó đến đó!**

## Series này **KHÔNG** phải:

- Hướng dẫn bấm nút nào
- Review sản phẩm AI
- Dạy trick/hack ngắn hạn
- Theo trend rồi quên

## Mà LÀ:

- Hiểu bản chất công nghệ
- Xây nền tảng tư duy về AI
- Tự tin thích ứng mọi thay đổi
- Cùng tiến hóa với AI dài hạn

**Triết lý: Hiểu gốc → Thích ứng nhanh → Tiến hóa cùng AI**

Công cụ sẽ thay đổi liên tục. Nền tảng hiểu biết thì không bao giờ lỗi thời.

# Agenda

1. AI là gì? Tại sao bây giờ ai cũng nói về nó?
2. AI quanh ta — Bạn đang dùng AI mà không biết!
3. Machine Learning — Máy tự học kiểu gì?
4. Discriminative vs Generative — Phân biệt vs Tạo sinh
5. Deep Learning & Neural Networks
6. Bản đồ AI: AI > ML > DL > GenAI
7. Generative AI — AI biết sáng tạo
8. LLM — Bộ não đằng sau ChatGPT, Claude, Gemini
9. So sánh ChatGPT vs Claude vs Gemini vs DeepSeek
10. Vì sao AI hay "ảo giác"? (Phần 1)
11. Vì sao AI không ngừng bịa? (Phần 2)
12. Tầm quan trọng của Prompt
13. Tổng kết & Q&A

# AI Là Gì?

Artificial Intelligence — Trí tuệ nhân tạo

**AI = Bất kỳ hệ thống nào có khả năng thực hiện nhiệm vụ thường cần "trí thông minh" của con người**

## Rule-Based AI

- Hoạt động theo luật cứng
- IF... THEN... (Nếu... Thì...)
- VD: Chatbot cũ, bộ lọc spam đời đầu
- Không tự học được

## Machine Learning AI

- Tự học từ dữ liệu
- Càng nhiều data = càng giỏi
- VD: Gợi ý Netflix, Face ID
- Đây là AI thời đại mới!

**AI không phải "robot thông minh" trong phim. Nó đã ở quanh ta từ lâu!**

Gợi ý gõ chữ, lọc ảnh, nhận diện giọng nói... tất cả đều là AI.

# AI Quanh Ta

Bạn đang dùng AI mỗi ngày mà không biết!

**Smartphone** Nhận diện khuôn mặt (Face ID), gợi ý gõ chữ, trợ lý ảo Siri/Google Assistant

**Mạng xã hội** Facebook/TikTok chọn bài đăng hiển thị, lọc nội dung xấu, gợi ý kết bạn

**Mua sắm online** "Khách mua sản phẩm này cũng mua..." — Shopee, Lazada, Amazon

**Email** Lọc spam, Smart Reply ("Cảm ơn!", "OK!"), phân loại email

**Ngân hàng** Phát hiện giao dịch bất thường, chấm điểm tín dụng tự động

**Đi lại** Google Maps dự đoán kẹt xe, Grab tính giá theo nhu cầu

**Giải trí** Netflix/Spotify gợi ý phim/nhạc bạn sẽ thích

>> AI không mới. Cái mới là GenAI (ChatGPT...) — AI biết "nói chuyện" với bạn!

# Machine Learning — Máy Tự Học

Nhánh quan trọng nhất của AI hiện nay

## Ví dụ dễ hiểu:

Thay vì dạy con: "Chó có 4 chân, đuôi, lông..." (rule-based)

→ Cho con xem 10,000 ảnh chó. Con tự nhận ra pattern. Đó là Machine Learning!

## Quy trình Machine Learning:

- [1] Thu thập dữ liệu (hàng triệu ví dụ)
- [2] Đưa vào mô hình → máy tự tìm pattern
- [3] Kiểm tra độ chính xác → điều chỉnh
- [4] Đưa vào sử dụng thực tế

**Điểm mấu chốt: ML cần RẤT NHIỀU dữ liệu. Càng nhiều data = càng chính xác.**

GPT-4 được train trên hàng tỷ trang web, sách, code, Wikipedia...

# Discriminative vs Generative

Hai hướng tiếp cận của Machine Learning

## Discriminative

(Phân biệt / Phân loại)

- Trả lời: "Đây là cái gì?"
- Phân loại chó vs mèo
- Email spam hay không?
- Giao dịch gian lận hay hợp lệ?
- Vẽ đường ranh giới giữa các nhóm

## Generative

(Tạo sinh / Sáng tạo)

- Trả lời: "Tạo cho tôi cái mới!"
- Vẽ 1 con chó chưa ai vẽ
- Viết bài thơ mới
- Tạo nhạc, video, code
- Học pattern → tạo ra cái mới

## Dễ nhớ:

Discriminative = Giám khảo thi hoa hậu: "Cô này đẹp hơn cô kia"

Generative = Họa sĩ: "Tôi sẽ vẽ ra người đẹp mới!"

# Deep Learning — Neural Networks

Bắt chước cách não người xử lý thông tin

## Deep Learning là gì?

- ML nhưng dùng mạng neuron nhiều tầng
- Càng nhiều tầng (deep) → càng hiểu được pattern phức tạp
- Nền tảng của mọi AI "xịn" hiện nay

## Ứng dụng thực tế:

- Nhận diện khuôn mặt
- Xe tự lái
- Dịch ngôn ngữ
- Chẩn đoán y khoa

## Ví dụ: Nhận diện ảnh mèo

Tầng 1: Nhận cạnh, đường viền → Tầng 2: Hình dạng (tai, mũi) → Tầng 3: "A! Con mèo!"

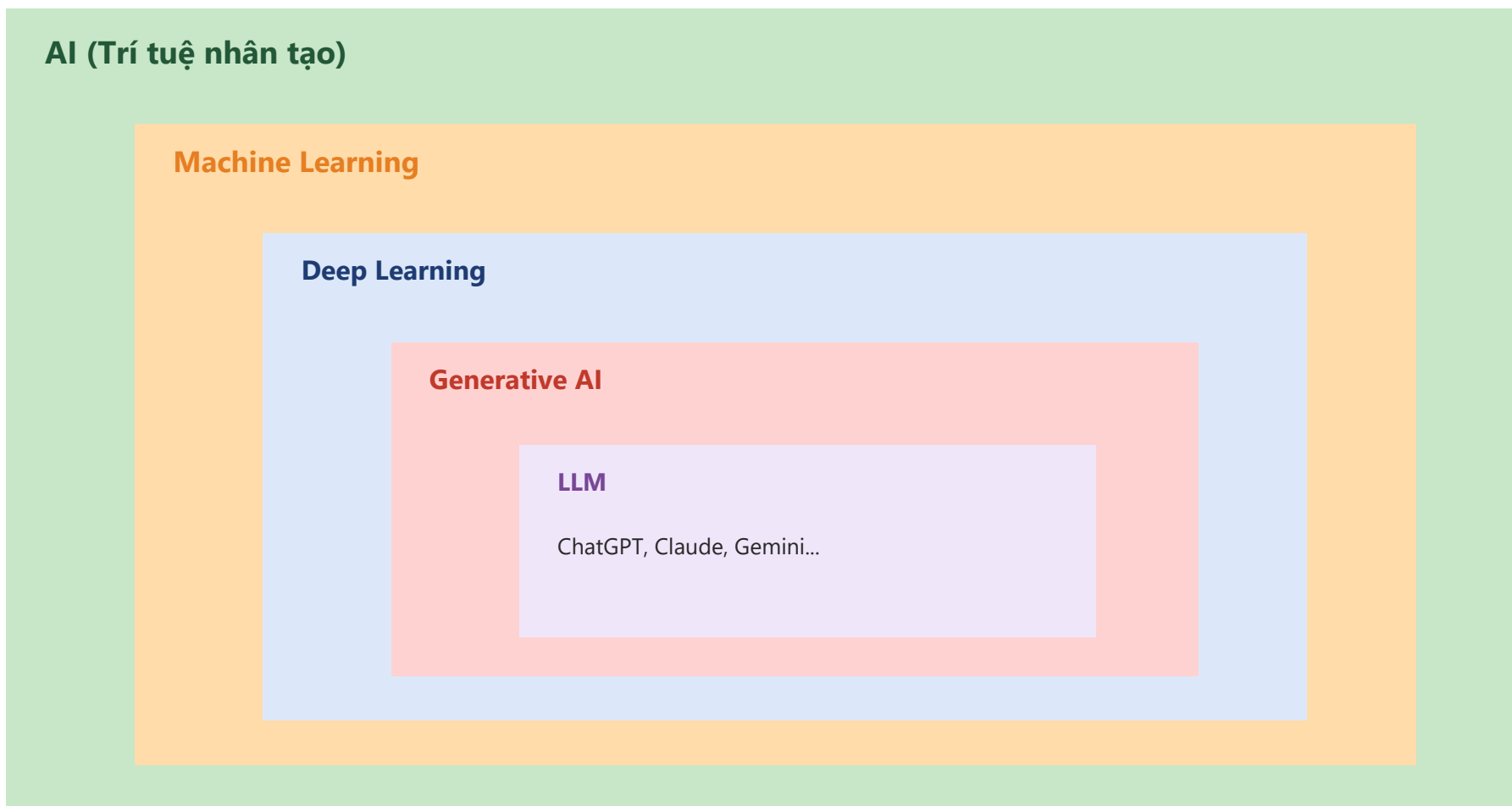
Giống cách não bạn xử lý: từ chi tiết nhỏ → bức tranh tổng thể

## "Deep" = nhiều tầng, không phải "sâu xa" hay "thông thái"

GPT-4 có hàng trăm tỷ tham số (parameters) phân bố trên nhiều tầng neural network.

# Bản Đồ Quan Hệ

AI > Machine Learning > Deep Learning > Generative AI



Mỗi vòng trong là tập con của vòng ngoài. LLM là một loại GenAI, GenAI là một loại DL, DL là một loại ML, ML là một loại AI.

# Generative AI — AI Biết Sáng Tạo

Tạo ra nội dung mới: văn bản, hình ảnh, code, âm nhạc...

**GenAI không copy-paste. Nó tạo ra thứ MỚI dựa trên pattern đã học.**

Giống như họa sĩ: xem triệu bức tranh → vẽ bức tranh chưa ai vẽ.

**Văn bản:** ChatGPT, Claude, Gemini — viết email, tóm tắt, phân tích

**Hình ảnh:** Midjourney, DALL-E, Stable Diffusion — vẽ từ mô tả

**Code:** GitHub Copilot, Claude Code — viết code từ yêu cầu

**Video:** Sora, Runway, Kling — tạo video từ text

**Âm nhạc:** Suno, Udio — sáng tác nhạc hoàn chỉnh

**Quan trọng: GenAI "sáng tạo" dựa trên XÁC SUẤT, không phải "hiểu biết". Đây là gốc rễ của ảo giác!**

# LLM — Large Language Model

"Bộ não" đằng sau ChatGPT, Claude, Gemini

## LLM hoạt động thế nào?

Được train trên HÀNG TỶ trang web, sách, code, Wikipedia...

Học cách dự đoán: "Cho từ trước, từ tiếp theo khả năng cao nhất là gì?"

VD: "The dog is \_\_\_" → playing (50%), eating (30%), driving (15%), flying (5%)

→ LLM chọn "playing" vì xác suất cao nhất (50%). Đúng hay sai? Phụ thuộc vào ngữ cảnh!

## "Large" cực kỳ lớn:

- GPT-4: ước tính ~1,800 tỷ tham số (parameters)
- Train tốn hàng trăm triệu USD, cần hàng nghìn GPU chạy nhiều tháng

## Phân biệt quan trọng:

- LLM (GPT, Claude, Gemini) = "Bộ não" (model)
- ChatGPT, Claude.ai, Gemini app = "Sản phẩm" (chạy trên model)

Giống như: iPhone (sản phẩm) chạy iOS (hệ điều hành) trên chip A17 (bộ xử lý)

# So Sánh Các Sản Phẩm AI Phổ Biến

Sản phẩm	Công ty	Model	Đặc điểm nổi bật
<b>ChatGPT</b>	OpenAI	GPT-4o, o1, o3	Phổ biến nhất, nhiều plugin, DALL-E
<b>Claude</b>	Anthropic	Opus 4.6, Sonnet 4.6	Dài, chính xác, an toàn, coding mạnh
<b>Gemini</b>	Google	Gemini 2.5 Pro/Flash	Tích hợp Google, multimodal tốt
<b>DeepSeek</b>	DeepSeek (TQ)	V3, R1	Open-source, giá rẻ, reasoning tốt
<b>Copilot</b>	Microsoft	GPT-4o (bên trong)	Tích hợp Office, Windows, Edge
<b>Llama</b>	Meta	Llama 3.3, 4	Open-source, chạy được local
<b>Grok</b>	xAI (Elon Musk)	Grok 3	Tích hợp X (Twitter), ít kiểm duyệt

**Đừng "chạy theo" một sản phẩm. Mỗi AI có thế mạnh riêng — dùng đúng việc!**

Mẹo: Dùng 2-3 AI song song để cross-check kết quả quan trọng.

# Vì Sao AI Hay "Ảo Giác"?

Hallucination — Vấn đề lớn nhất của LLM hiện nay

## Ví dụ: Ông Tiến Sĩ IQ 160 Nhưng EQ Gần 0

- Đọc hết mọi sách trên đời → kiến thức bao la (= LLM đọc internet)
- Nhưng KHÔNG có trải nghiệm thực tế, không có common sense
- Hỏi gì cũng trả lời rất tự tin — kể cả khi SAI (vì IQ cao = overconfident)
- Không biết nói "Tôi không biết" — vì được train để luôn có câu trả lời

## Nguyên nhân kỹ thuật:

- LLM = máy dự đoán xác suất
- Chọn từ "có vẻ đúng nhất"
- KHÔNG kiểm chứng sự thật
- KHÔNG có nguồn dữ liệu đáng tin

## Ví dụ thực tế:

- Bịa ra trích dẫn luật không tồn tại
- Tạo link Wikipedia giả
- Cho số liệu "rất thuyết phục" nhưng hoàn toàn sai

**Quy tắc vàng: KHÔNG BAO GIỜ tin 100% output của AI. Luôn double-check thông tin quan trọng!**

# Ảo Giác — Hiểu Sâu Hơn

Tại sao "ông Tiến Sĩ" không thể ngừng bịa?

## LLM dự đoán từng từ một, giống autocomplete trên điện thoại:

Hỏi: "Thủ đô Việt Nam là gì?" → "Thủ" → "đô" → "Việt" → "Nam" → "là" → "Hà" → "Nội" [DUNG]

Hỏi: "Ai phát minh WiFi?" → tự tin ghép: "Nikola Tesla phát minh WiFi năm 1896" [SAI]

### 1. Không có nút "Tôi không biết"

LLM được train để LUÔN tạo ra câu trả lời. Nói "không biết" = thất bại trong training.

### 2. Tự tin đều nhau

Dù đúng hay sai, giọng văn đều tự tin như nhau. Không có cơ chế "nghĩ ngờ bản thân".

### 3. Pattern > Sự thật

LLM tìm pattern nghe hợp lý. "Tesla + phát minh" = pattern phổ biến → ghép lại dù sai.

### 4. Không có bộ nhớ thật

Không có database fact-check. Mọi thứ đều từ "cảm giác" xác suất.

# Tầm Quan Trọng Của Prompt

Prompt = Câu lệnh / Yêu cầu bạn đưa cho AI

## AI giỏi đến mấy mà prompt dở → kết quả dở.

Có ông Tiến Sĩ IQ 160 làm trợ lý, nhưng bạn chỉ nói "làm cái gì đó đi" → ổng sẽ làm bừa.  
Phải biết CÁCH ra lệnh! Đó chính là Prompt Engineering.

### Prompt dở:

"Viết email"

"Tóm tắt cái này"

"Giúp tôi với"

→ Thiếu context, mơ hồ, AI phải đoán

### Prompt tốt:

"Viết email chuyên nghiệp cho đối tác, ngắn gọn 5 dòng, xác nhận meeting thứ 3 lúc 10h, giọng lịch sự nhưng thân thiện"

## Công thức nhanh: Vai trò + Context + Nhiệm vụ cụ thể + Format mong muốn

"Bạn là chuyên gia marketing" + "cho công ty logistics, khách B2B" +  
"viết 3 tiêu đề" + "dạng bullet, tối đa 50 từ mỗi cái"

# Tổng Kết

**AI** = Khái niệm rộng nhất — máy làm việc cần "trí tuệ"

**ML** = Máy tự học từ dữ liệu, không cần lập trình từng luật

**Deep Learning** = ML dùng neural networks nhiều tầng

**GenAI** = AI tạo nội dung mới (text, ảnh, code, nhạc...)

**LLM** = "Bộ não" của ChatGPT, Claude... dự đoán từ tiếp theo

## 3 Điều Quan Trọng Nhất:

1. AI rất mạnh nhưng KHÔNG hoàn hảo — luôn kiểm chứng output (đặc biệt số liệu & trích dẫn)
2. Prompt tốt = Kết quả tốt — đầu tư thời gian vào cách hỏi, không chỉ cái hỏi
3. AI là CÔNG CỤ — người dùng giỏi mới tạo ra giá trị, không phải AI tự tạo

## Q & A

Hỏi gì cũng được — không có câu hỏi sai!

## Bài sau:

Bài 2: Prompt Engineering chuyên sâu!

Làm Quiz: [tranlamhuan.vn/quiz/ai-bai-1](https://tranlamhuan.vn/quiz/ai-bai-1)