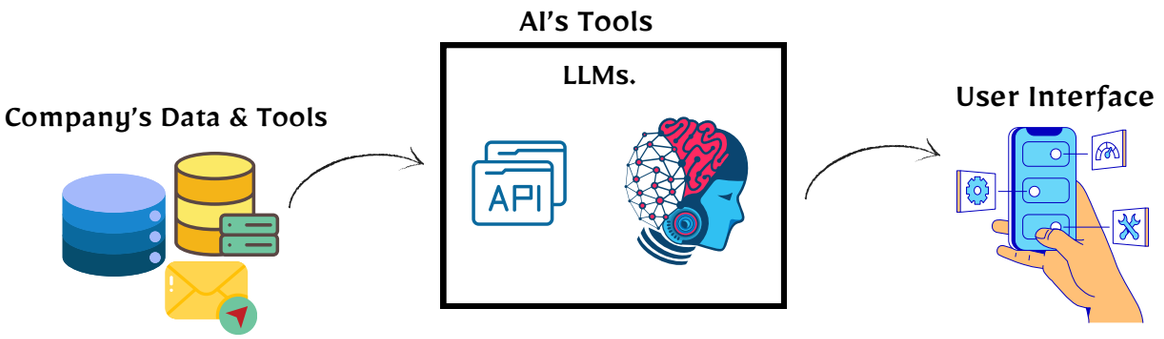
AI Engineer Roadmap

خارطة طريق لمهندس الذكاء الاصطناعي

What is AI Engineer ?

AI Engineering is the profession of building real, production-ready systems that use AI models (like LLMs) to solve business problems.



As it's appearing for you , you are not gonna to build new AI's models like chatgpt or deepseek but you will use them to solve a real business problem for companies that what they search for .

So remember you must focus :

Practical skills , Not deep math

You don't build models from scratch (that's ML Research).

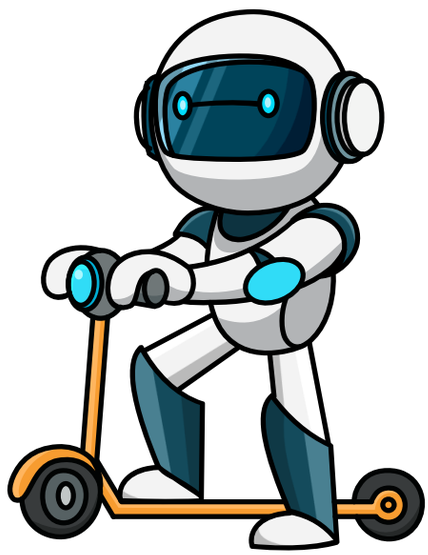
Instead you use existing models (OpenAI, HuggingFace, LLAMA, DeepSeek, etc.) and integrate them into systems.

System building, Not research

AI Engineering = connecting:

- AI Models
- Databases
- APIs
- Tools
- Vector stores
- Memory
- Reasoning strategies
- Monitoring
- Deployment

Into a working product.



Business-focused

Your job is delivering:

- automation,
- assistants,
- agents,
- tools,
- internal workflows,
- data-connected LLMs.

Not doing statistics or training neural networks manually.

PHASE 1 — Solid Foundations

🎯Goal: Become comfortable writing software and working with data.

1. Python (must master)

You must know:

- variables, loops, conditions
- functions
- classes
- modules
- error handling
- file handling
- virtual environments
- pip
- requests library
- working with JSON

Why?

Because every AI system = Python scripts connecting APIs + data + models.

2. Git + GitHub

- create repos
- push/pull
- branching
- version control

Why?

No AI engineer works without Git. Period.

3. Basic Linux & Terminal

- navigating folders
- environment variables
- running scripts
- installing packages

Why?

Servers = Linux.

AI systems run in Linux containers.

4. Data Handling Basics (Very Important for AI Engineers)

You must know:

- Reading & cleaning data with Pandas (CSV, Excel, JSON)
- Basic SQL (SELECT, WHERE, JOIN)
- Handling files: PDF, DOCX, images

Why?

Because AI systems rely on real company data — and RAG, agents, and pipelines all require clean, structured data.

PHASE 2 — AI Interaction Skills (LLM Skills)

🎯Goal: Understand how to control models, not just ask questions.

1. Prompt Engineering

- structure prompts
- system prompts
- few-shot examples
- chain-of-thought prompting
- tool prompting
- role prompting
- style control
- evaluation prompts

Why?

This is the core of AI system behavior.

2. Use AI APIs

Learn to call:

- OpenAI APIs
- DeepSeek APIs
- Meer-Ai APIs // This is an Iraqi mode 👽
- OpenRouter
- HuggingFace Inference API // very important one 💀👽
- Groq API

Understand:

- model parameters
- tokens
- cost control
- temperature / top_p
- streaming responses

Why?

AI engineers don't use ChatGPT only — they integrate LLMs into applications.

PHASE 3 — AI System Building

🔗 LangChain — Build Real AI Systems

LangChain lets you connect models, tools, memory, and logic into multi-step workflows.

This is where you move from simple prompts to full AI systems that follow a structured process.

🔥 Must-Learn Skills

☐ Understand chains, tools, memory, and agents

☐ Connect multiple models in one workflow

☐ Pass data between steps and manage context

☐ Add business logic and conditions

☐ Build a small multi-step automation project

Bottom Line: LangChain is the backbone of creating real AI applications.

📚 RAG — Retrieval-Augmented Generation

RAG lets AI use your real data instead of relying only on what it was trained on.

It powers enterprise search, customer support bots, and knowledge assistants.

🔥 Must-Learn Skills

☐ Chunk documents

☐ Create embeddings

☐ Use vector databases for search

☐ Inject retrieved results into prompts

Bottom Line: RAG connects AI with up-to-date and accurate information.

🤖 AI Agents — AI That Takes Action

Agents don't just answer questions — they plan and execute tasks.

They can call APIs, update databases, read emails, create notes, automate workflows, and collaborate with other agents.

🔥 Must-Learn Skills

☐ Let agents call APIs or databases

☐ Build RAG-enabled agents

☐ Create multi-agent systems

☐ Manage memory and context

☐ Automate repetitive tasks

Bottom Line: Agents turn AI into real business automation.

🧩 MCP — Model Context Protocol

MCP creates a safe layer between agents and external systems.

It standardizes access, ensures security, and removes the need for custom connectors.

🔥 Must-Learn Skills

☐ Agent–MCP server communication

☐ Connect APIs/databases through MCP

☐ Set permissions and scopes

☐ Log and monitor agent actions

☐ Apply security policies

Bottom Line: MCP provides safe, controlled, and standardized integrations for AI systems.

⚙️ LLMOps — Operating AI in Production

Once your AI system is deployed, LLMOps keeps it fast, reliable, cost-efficient, and continuously improving.

🔥 Must-Learn Skills

☐ Full lifecycle understanding

☐ Track prompts and responses

☐ Test & optimize RAG pipelines

☐ CI/CD for model updates

☐ Monitor latency, cost, satisfaction

☐ Alerts and dashboards

☐ Evaluation and safety ensure your AI system is reliable, secure, and trusted by companies.

Bottom Line: LLMOps ensures your AI system stays stable and scalable after launch.

PHASE 4 — Deployment & DevOps

🎯 Goal: Make AI systems run in real production.

Learn:

- FastAPI (build backend)
- Docker
- Deploy on:
  - AWS / Azure
  - Vercel
  - HuggingFace Spaces
  - Render
- Logging & Monitoring
- Rate limits
- Cost optimization

Why?

Real companies need stable, deployed systems — not Jupyter notebooks.

PHASE 5 — Portfolio Projects (VERY IMPORTANT)

Build at least 5 strong AI projects, such as:

- AI email assistant
- AI document search (RAG)
- AI summarizer for company PDFs
- An automated chatbot connected to your database
- Multi-agent workflow automation system
- AI that fills reports automatically
- AI coding helper
- AI form-filling bot

Document everything with:

- README
- screenshots
- live demo
- short video

PHASE 6 — Certifications (Optional but Strong)

- Azure AI Engineer
- Databricks Generative AI Engineer
- AWS Machine Learning Specialty
- DeepLearning.AI LLM Engineering

Helps build trust for employers.

I created this roadmap based on my own experience, combined with insights from multiple trusted sources. Phase 3 in particular aligns closely with the structure explained by Mr. Baraa on his YouTube channel “Data with Baraa”, after deep research and validation across real industry practices.

Naser Almurad