Sensational

GenAI Capability with guardrails

Created - Stephen Adebola & Andrita

Sensational

GenAI

fundamentals & frameworks,
Implementations, governance & guardrails.

A hands-on intro, on how to use AI to achieve your objectives

Sensational

Welcome to the AI Capability Hands-on tailored for SMEs.

This interactive session is tailored to equip both technical and non-technical individuals with a thorough grasp of GenAI, its practical uses, and essential guidelines, particularly focusing on containment and alignment. As GenAI becomes increasingly integrated into our daily lives, establishing robust guardrails will be pivotal for responsible deployment.

During the program, attendees will explore the complexities of various models and frameworks, grapple with the ethical considerations of AI, and gain hands-on experience in developing their own GenAI applications, agents, and chatbots, among other subjects.

Sensational

Understanding AI and Its Foundations

First part focuses on introducing participants to AI and its foundational concepts. The sessions are designed to be interactive, with hands-on exercises complementing theoretical knowledge.

The highlights include:

- Demystifying Models, Weights, and Biases
- The differences between tunning vs Prompting
- Introduction to AI frameworks with a spotlight on Langchain
- Exploring no-code AI solutions with LangFlow and Flows

Sensational

Implementing, Testing, and Safeguarding AI

Part two shifts the focus towards implementing, testing, and safeguarding AI solutions. Participants will gain insights into testing AI models, addressing safety concerns, and understanding the ethical considerations in AI.

The highlights include:

- Testing and evaluating models using tools like LangSmith and LangForge
- Introduction to GuardRails for AI to ensure business safety
- Practical hands-on session to build a simple AI project

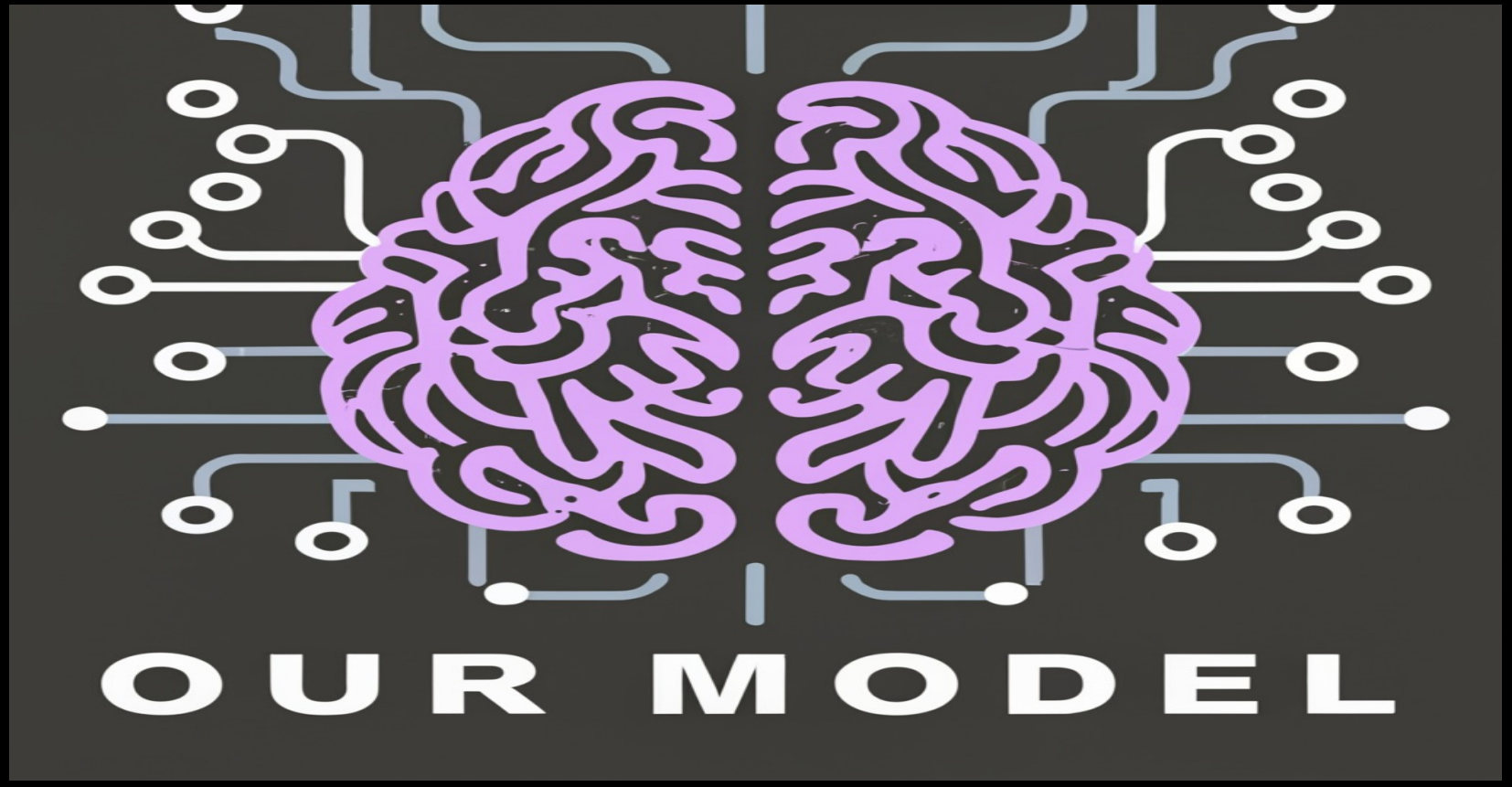
Sensational

Key Takeaways at the end of this interactive session, participants will

- Have a clear understanding of AI, models, weights, and biases.
- Be familiar with various AI frameworks and tools.
- Gain hands-on experience in building AI applications.
- Understand the importance of safety and ethics in AI.
- Be equipped with the knowledge to scale AI solutions for their businesses.

Sensational

What is a Model



Sensational

Your Objectives
&
Key Results

Inference Call

Like finally baking the perfect cookies and sharing them

Prompting

Like asking Can you make the cookies chocolate flavoured

Tuning

Like baking and tasting cookies to make them perfect.

Weight & Biases

Like the amounts of sugar and flour. Adjust them to make cookies taste better.

Model

Think of this like the recipe for cookies. It tells us the ingredients and steps.

Sensational

Tunning Vs Prompting

Sensational

Tuning

Modular Fine-Tuning of Pre-existing Models For domain-specific tasks, Fine Tuning of existing models is vital. It customizes pre-trained models for specific tasks using domain data. However, this can be costly, as it modifies millions of parameters, needing extensive data and infrastructure. Full fine-tuning risks catastrophic forgetting and results in large, non-modular models. Solutions like Parameter Efficient Fine Tuning (PEFT) offer modular fine-tuning that conserves resources and is cost-efficient.

Your Objectives & Key Results

GenAI Frameworks & Applications

Your Models LLM

Prompting

Prompt Engineering Pre-existing Models Fundamentally, obtaining anticipated results from Large Language Models requires meticulous engineering of prompts. This method entails designing appropriate prompts and inputs to draw out the specific reactions from the model. Engineering prompts is a crucial approach for numerous applications, particularly when general feedback is adequate.

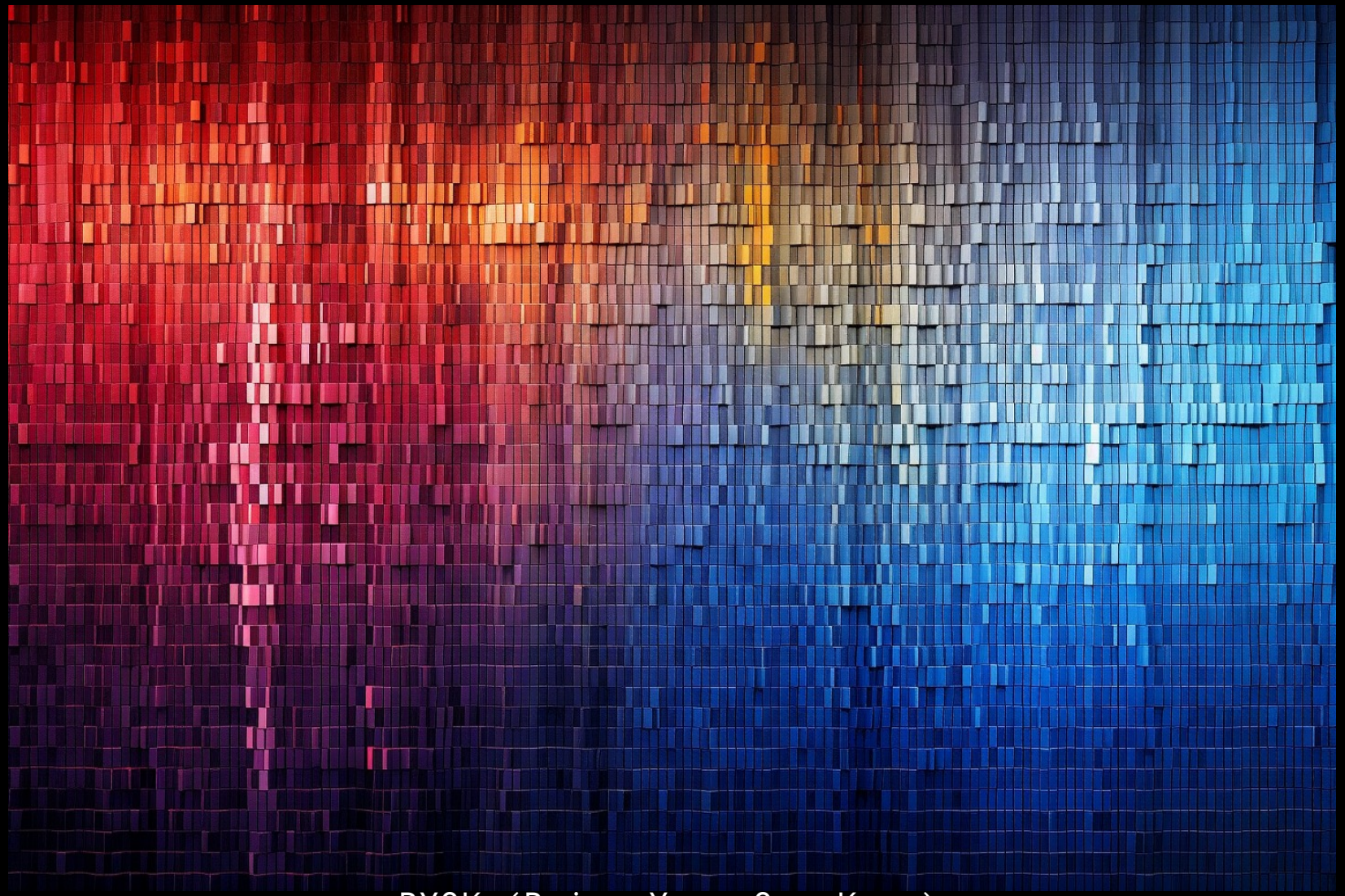
Tunning:(PEFT-LoRA, QLoRA)

Llama 2
GPT-3-Turbo
PALM 2

Prompting: (MRKL, REAct, COT, RAG, Zero Shot)

Llama 2
GPT-3-Turbo
GPT-4
PALM 2
Claude 2

Sensational



BYOK (Bring Your Own Keys)

Sensational

Your Keys

Your Objectives & Key Results

Your Privacy

GenAI Frameworks & Applications

Your Vector Stores

Your Models (LLM)

Your API

Your Key Vault

Sensational

GenAI Integrations and Guardrails

Sensational

IAM & Security

Multi Modal Applications

Fast NoCode Application Development

Autonomous Agents

Promt Engineering & QA

GenAI Frameworks

Pront Engineering	Pronpt Chaining	RAG	REAct MRKL COT	LangChain
Tools	Toolkits	Functions Calling	Retrievers	LlamaIndex
Memory	Vector DBs	Splitters	Embeddings	HF Transformers
				Functions Calling

Your Data

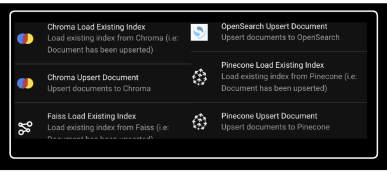
Your Company GuardRails

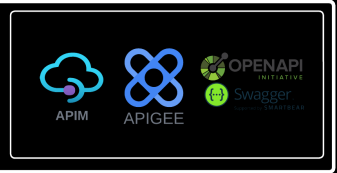
Embeddings Model

Your Vectorised Data

Your Private & Proprietry Models

Your APIs

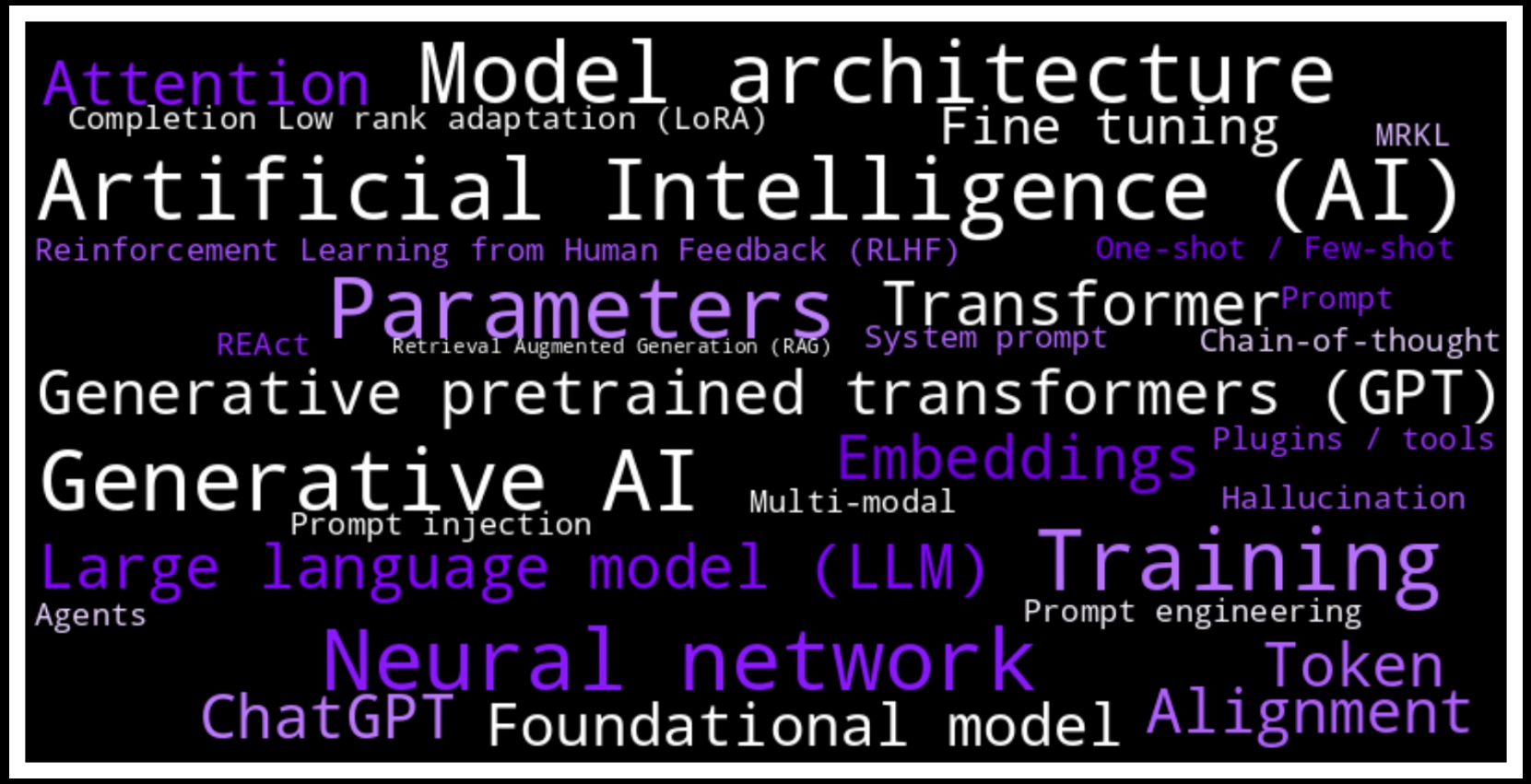




GenAI Capability

Sensational

Glossary Terms



Sensational

Term	Description
Neural network	Network modelled on the brain
Parameters	Weights that control neural network calculations
Model architecture	Components of a complex AI model
Training	Improving model performance on data
Generative AI	Models that generate text/images from prompts
Generative pretrained transformers (GPT)	Popular large language model
ChatGPT	Conversational version of GPT
Large language model (LLM)	AI model that handles language
Transformer	Popular neural network architecture
Token	Encodes text numerically for models
Embeddings	Represent words/text semantically
Attention	Allows models to understand context

Sensational

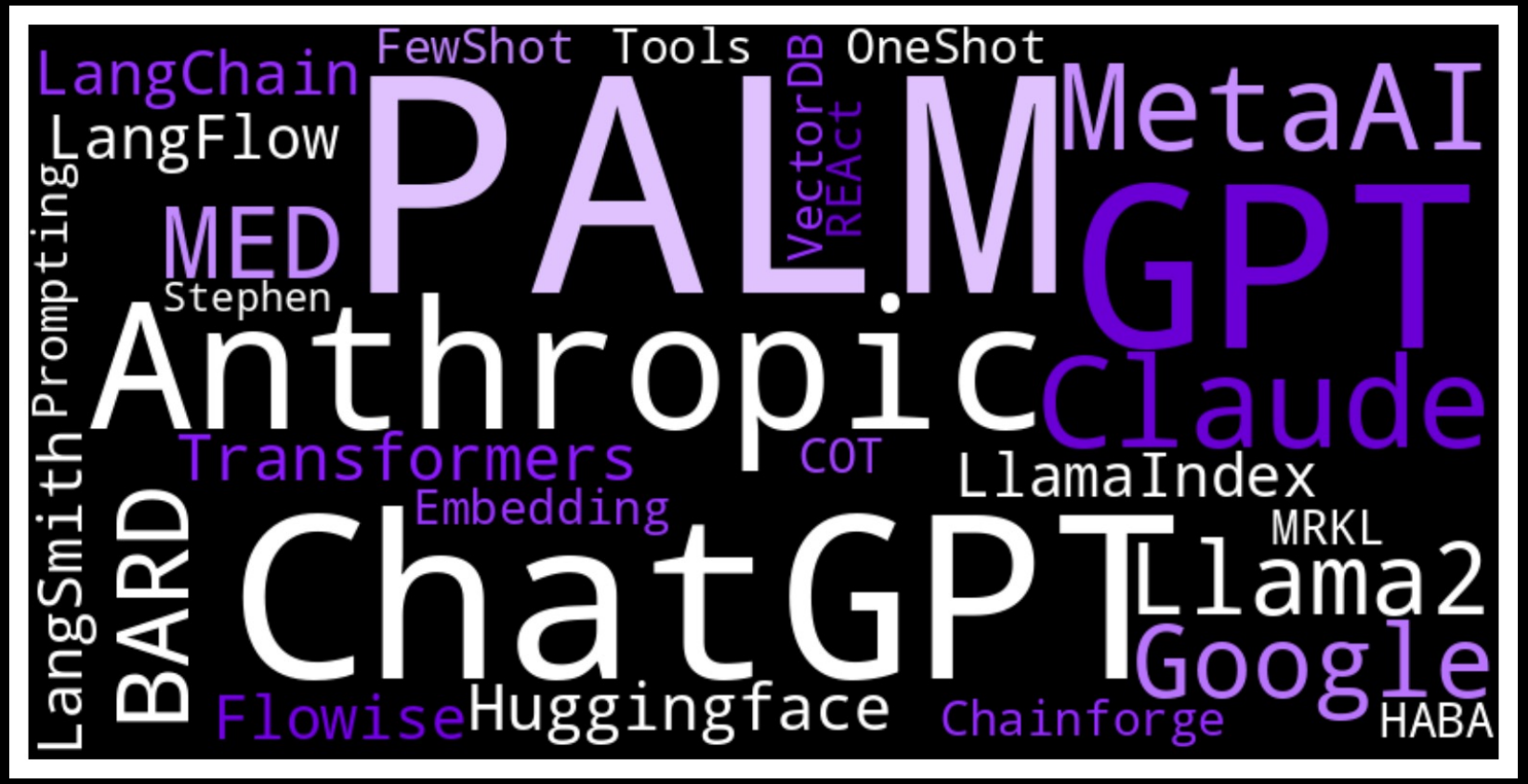
Term	Description
Alignment	Steers models towards ethical output
Foundational model	Broadly trained model
Fine tuning	Tailoring model to specific tasks
RLHF	Reinforcement Learning from Human Feedback to improve models
Low rank adaptation (LoRA)	Efficient fine-tuning method
Multi-modal	Handle mixed text/image input
Prompt	Text input to models
Completion	Text output from models
Hallucination	Fictional/incorrect output
One-shot / Few-shot	Types of prompting
System prompt	Defines model characteristics
Prompt engineering	Developing effective prompts

Sensational

Term	Description
Prompt injection	Subverting models via input
Chain-of-thought	Improves reasoning via breakdown
REAct	Read Evaluate and React
MRKL	Modular Reasoning, Knowledge & Language
Agents	Versatile AI tools
Plugins / tools	Expand capabilities via APIs
Retrieval Augmented Generation (RAG)	Supplementing with searches

Sensational

Appendix



Sensational

Term	Description	Links
Nvidia Guardrails	Stop AI systems getting out of control	
Langchain:	1.Chaining large language models together, allowing them to converse	https://www.langchain.com
Flowise	Flowise: Workspace for building AI flows visually	https://flowiseai.com
Chainlit	Service for running computations on GPT models	https://docs.chainlit.io/overview
LangFlow	Framework for creating AI pipelines with Python	https://www.langflow.org
LangSmith	Platform for searching AI models and chaining them together	https://smith.langchain.com
Retrieval Augmented Generation (RAG)	Supplementing with searches	
LLM's	(GPT-4, Anthropic, PALM 2, Llama 2)	https://openai.com https://www.anthropic.com https://cloud.google.com/vertex-ai https://ai.meta.com