AI Workshop Series

Introduction to the Workshop Series

Exploring AI and Large Language Models in Application Logic

Purpose of the workshop

Understand how to integrate AI-powered language models into applications.

Expected outcomes

Gain hands-on experience in leveraging AI APIs for real-world use cases.

Workshop schedule

6 meetings covering prompt engineering, API integration, AI agents and security considerations.

Session 1: Introduction to Prompt Engineering

Mastering the Art of Effective Communication

Understanding Prompts

Explore how different prompts shape AI responses and outcomes.

Best Practices

Learn techniques like specificity context-setting and role-based prompting.

Hands-on Examples

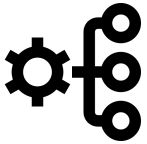
Experiment with real-world scenarios to craft precise and useful prompts.

Session 2: Advanced Prompt Engineering Techniques

Enhancing AI Performance with structured input

Few-shot & Zero-shot technique

Utilizing context examples to improve AI predictions and generalization.



System messages & structured prompts

Guiding AI behavior with predefined instructions and formatted inputs.

Controlling output reliability

Techniques to refine responses for consistency, accuracy, and robustness.

Session 3: AI Integration with application

Connecting AI models to real-world systems

When to use AI

Determining which tasks to outsource to AI Models and which to retain

Key aspects

Key considerations for developing applications with LLM Integration

QA and debugging

Exploring tools for maintaining and enhancing LLM-based applications

Session 4: Chaining calls & memory management

Enhancing AI with Contextual Awareness

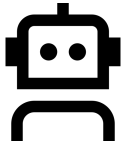
Chaining API calls
Link multiple requests for complex workflows and advanced logic.

Memory using embeddings
Store and retrieve relevant data for better AI context retention.

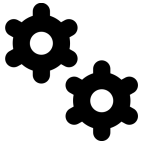
Enhancing AI interactions
Improve user experience with AI that remembers and adapts.

Session 5: Concept of AI agents

Building (partially?) autonomous and Intelligent AI Systems



What AI agents are?
Understanding AI-driven decision-making systems.



Combining multiple LLM calls
Integrating AI models with structured workflows for intelligent decision logic.

Real-world applications
Exploring use cases such as chatbots, automated assistants and process automation.

Session 6: Security considerations in AI Applications

Protecting AI systems from threats and vulnerabilities

Understanding AI security risks

Identifying vulnerabilities ins AI models and applications.

Data protection & Prompt injections

Preventing unauthorized access and malicious manipulations.

Compliance & best practices

Ensuring AI implementations adhere to security standards.