Securing Generative AI Applications with Defense-in-Depth

A Focus on OWASP Top 10 for LLMs Mitigating using AWS Bedrock and Services

Presented by

Shilpa Shivapuram
Ayyanar Jeyakrishnan

Agenda

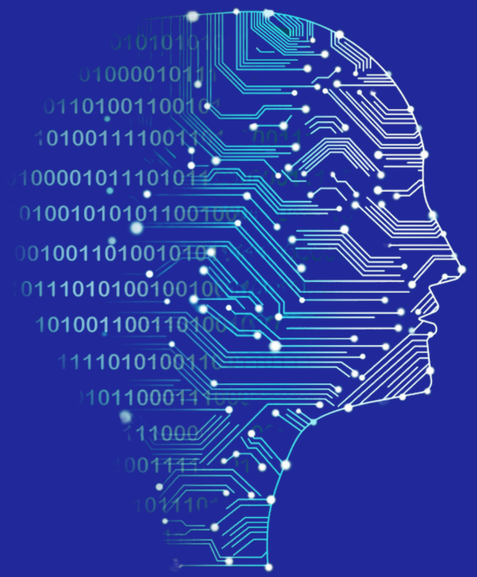
01 Introduction to Generative AI, Usecase and LLM Journey.

02 Understanding OWASP Top 10 for LLMs

03 Real-World Use Case: A Generative AI Chatbot

04 Leveraging AWS Bedrock and Other AWS Services for Secure AI Development

What is Generative AI



Generative AI refers to artificial intelligence systems capable of creating content, such as text, images, and music, by learning from vast amounts of data

Generative AI - Usecases

Boost Employee Productivity

- Employee Assistant
- Code Generation
- Automated Report Generation

Improve Customer Experiences

- Chatbots and Virtual Assistants
- Conversational Analytics
- Agent Assist
- Personalization

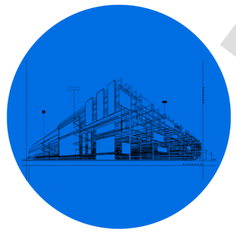
Enhance Creativity & Content Creation

- Marketing
- Sales
- Product Development

Accelerate Process Optimization

- Document Processing
- Data Augmentation
- Supply Chain Optimization

LLM Journey - Quick Introduction



Choice of your foundation Model

- Properietry or Opensource or Restricted Use
- Parameters
- Speed,
- Context Window,
- Finetunable
- Training Dataset, Quality.

Prompting – Few Shot, ReAct, Zero, RAG

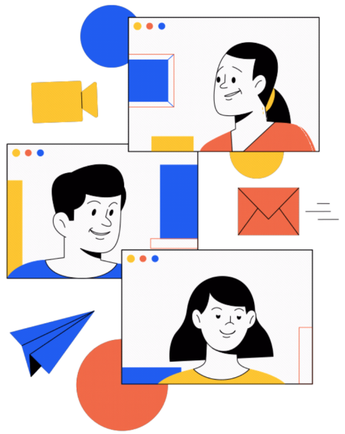
FineTuning – PeFT, LoRA, QLoRA

RLHF

PreTrain the Model

LLM - Personas

Providers
People who build FM

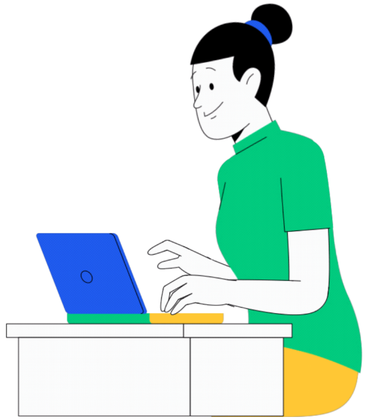


E.g) AWS, Azure, GCP, COHERE, ANTHROPIC, Stability.ai, Mistral, Meta-LLAMA

Large Language Model - FineTuners
Use the FM and Finetune for their Domain

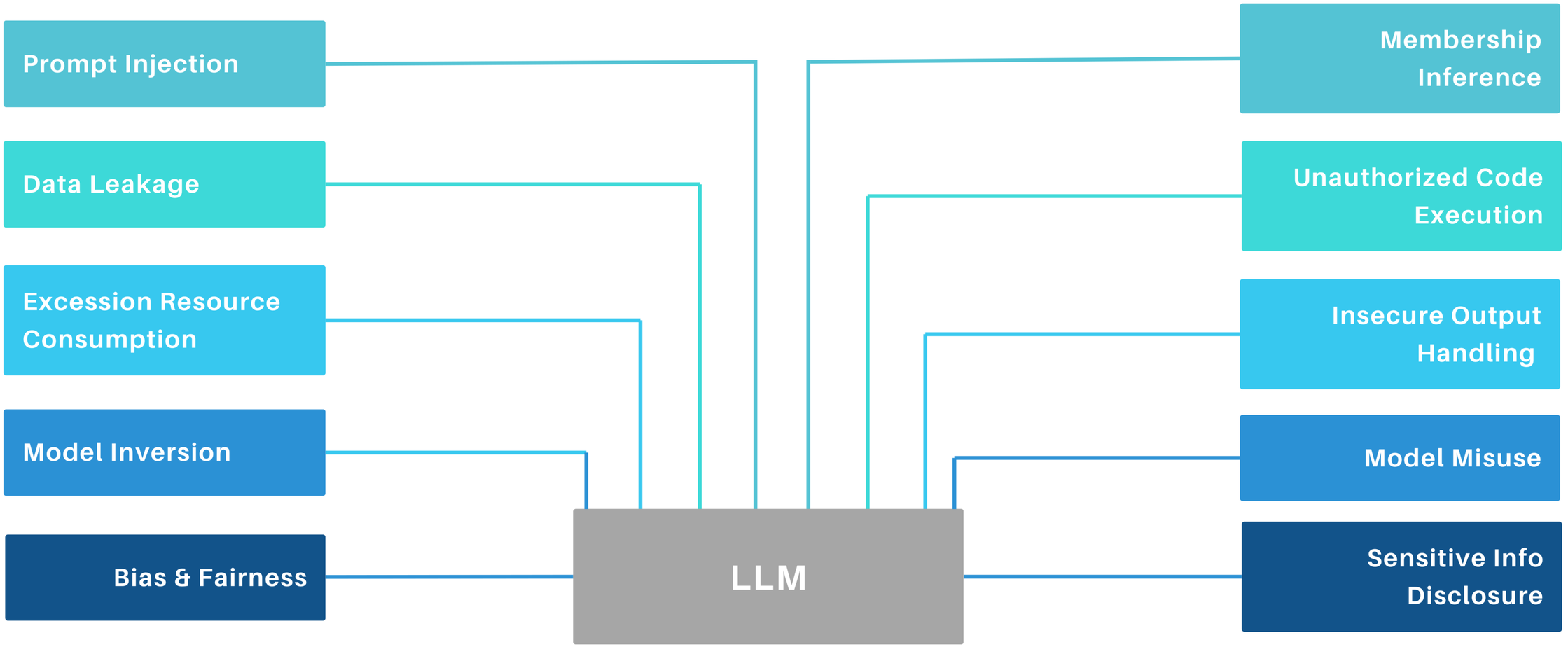
This can be Enterprise like us, Or using Cloud Provider and finetune FM using your data and Host Foundation Model

Consumers
Build a Product using FM/ Finetuned Model

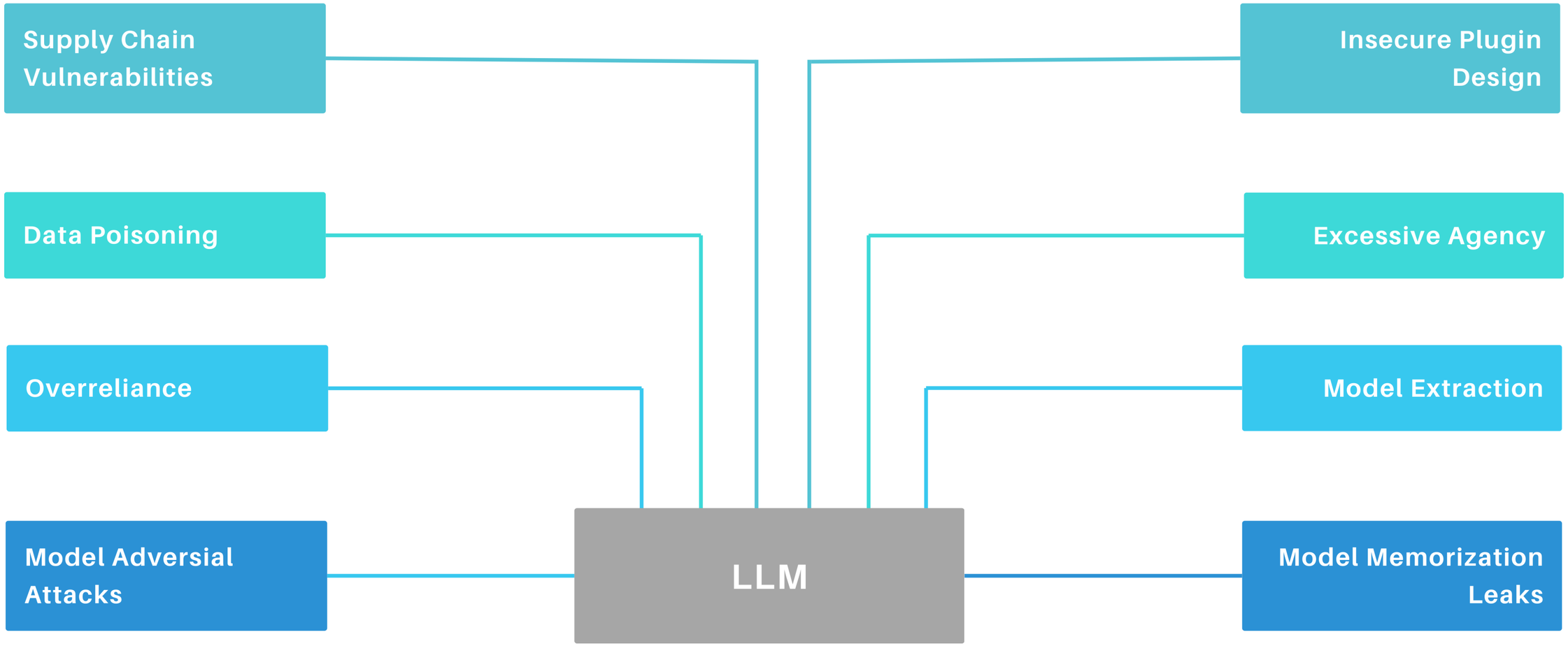


Consume FM as API and build a product or intergrate with-in their workflow/process

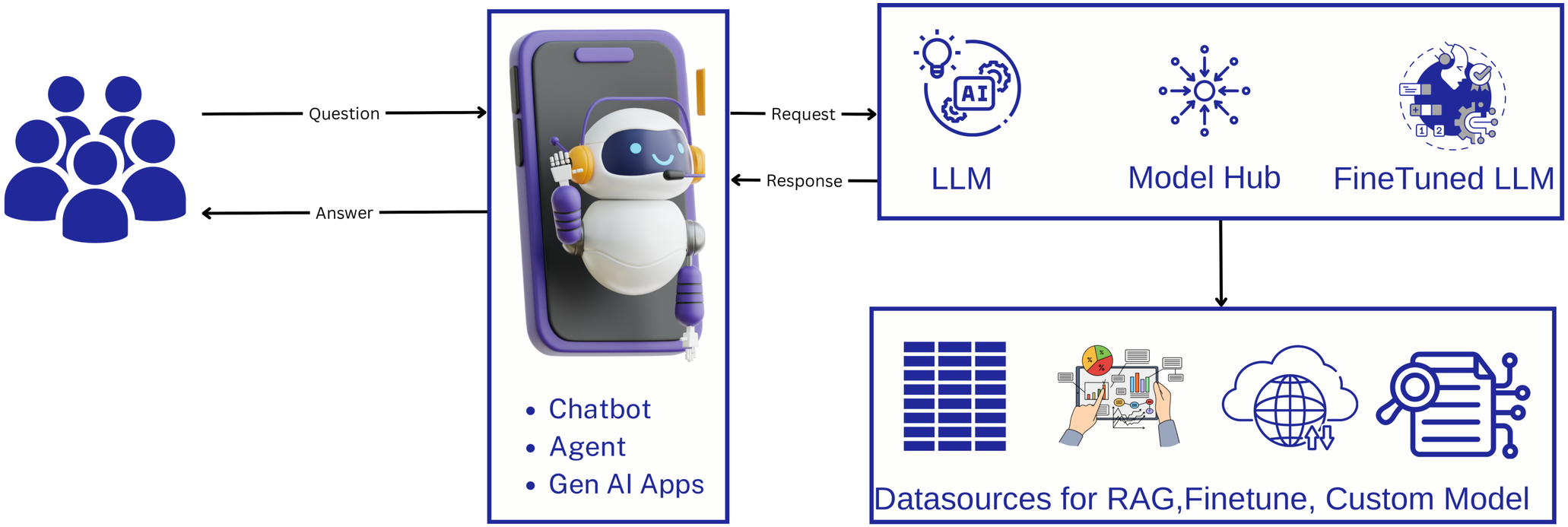
COMMON VULNERABILITIES



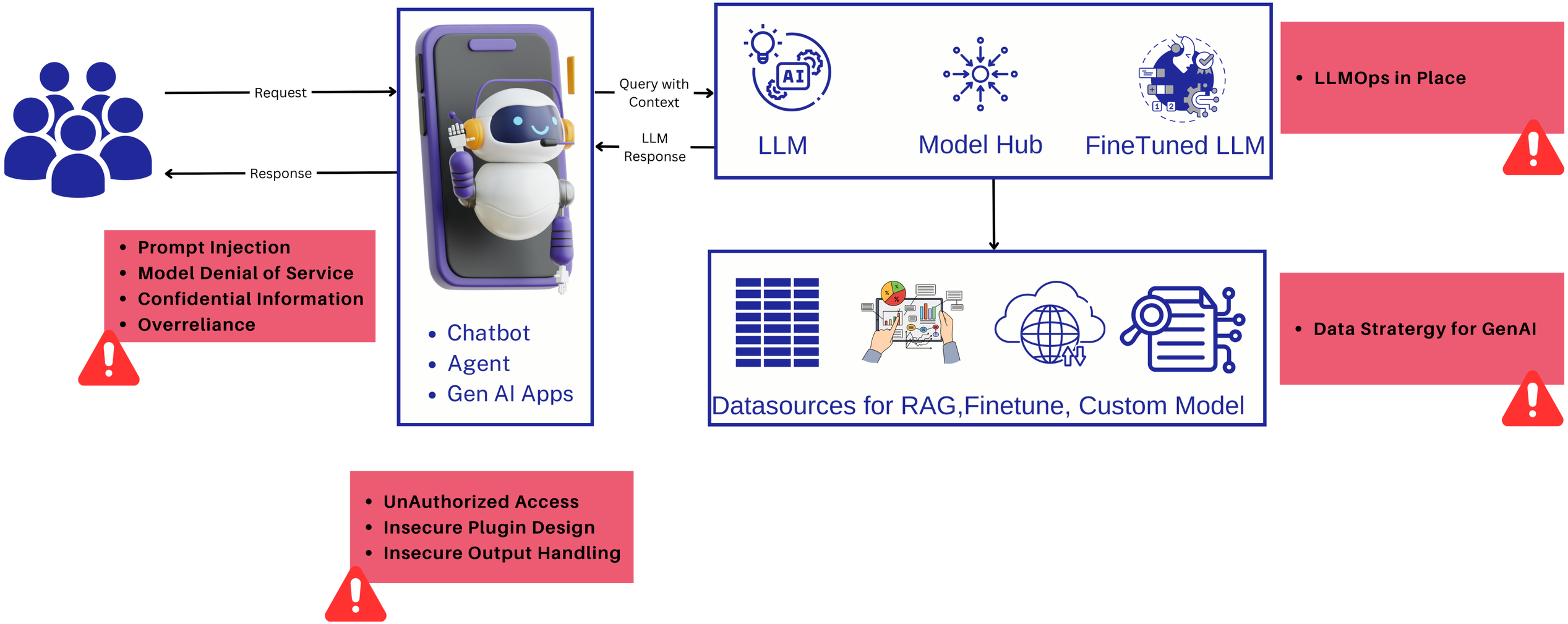
NEW VULNERABILITIES



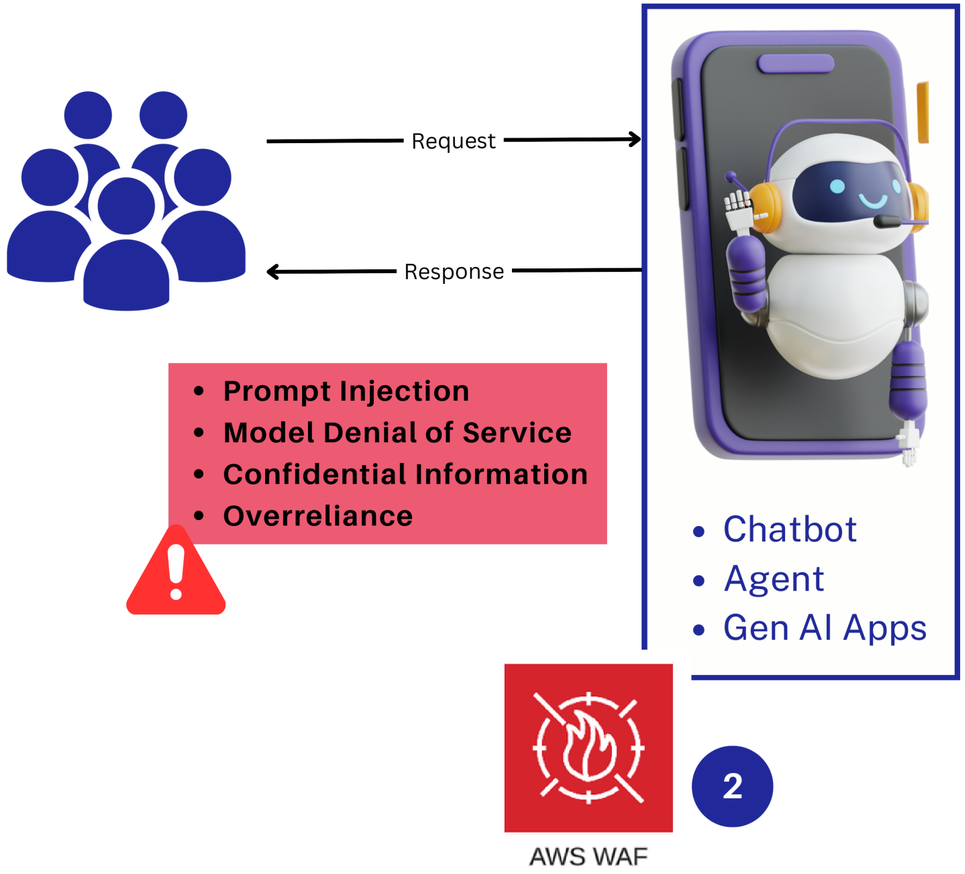
GenAI Application

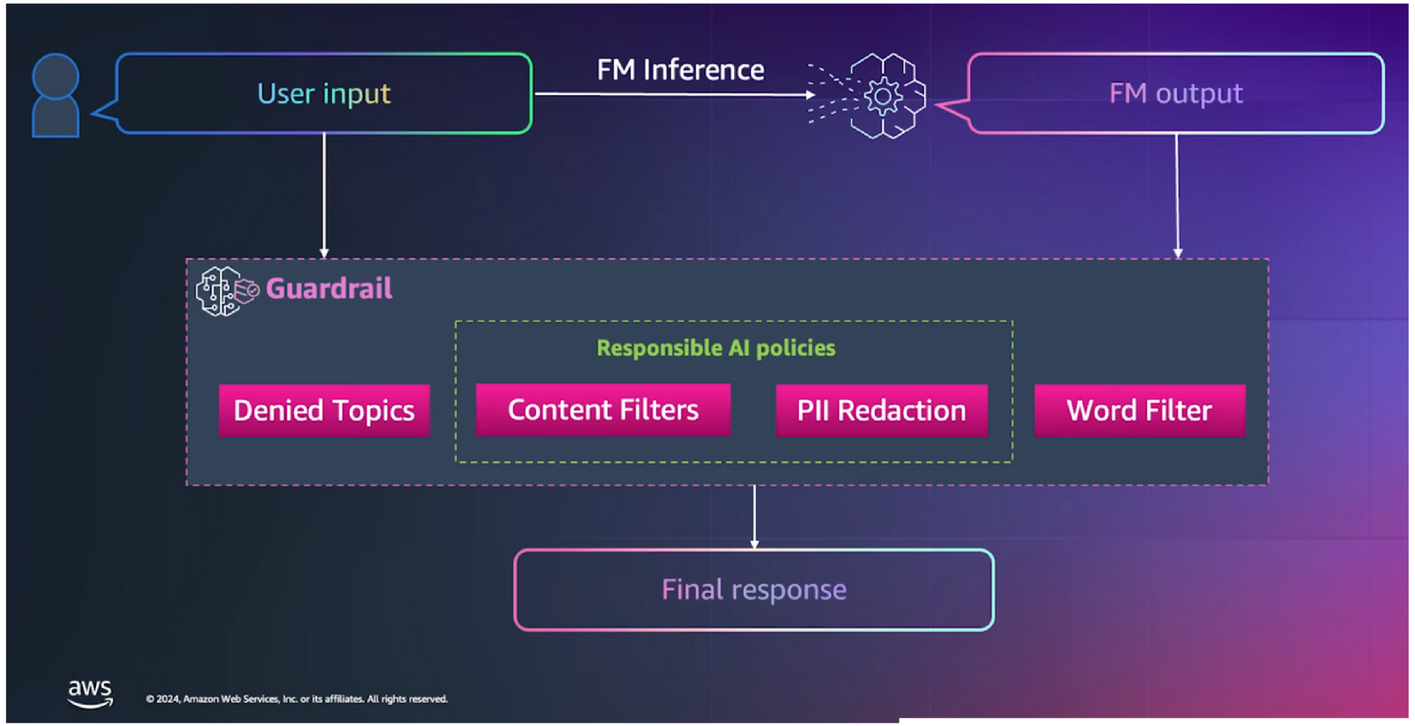


GenAI Application - OWASP Vulnerabilities



GenAI Application - OWASP LLM Top 10 Mitigation using AWS Bedrock and Services





1 • AWS Bedrock Guardrails

THANK YOU FOR LISTENING!