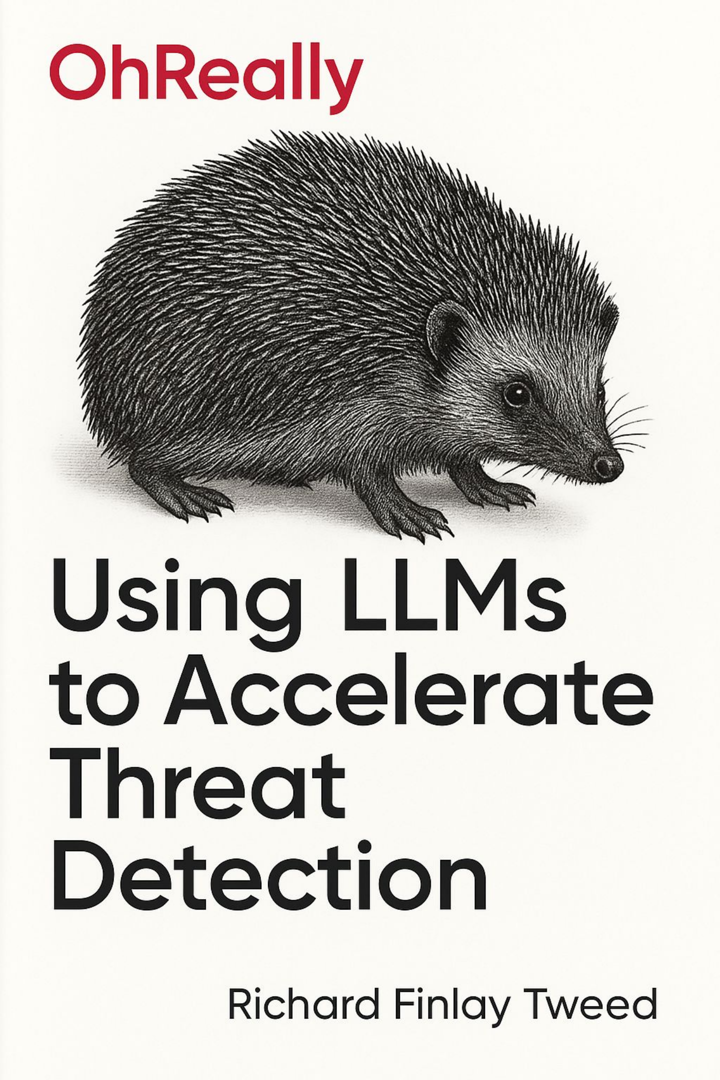


OhReally

Using LLMs to Accelerate Threat Detection

Richard Finlay Tweed

Senior Platform Engineer

at Tessl

infosec.exchange/@RichardoC

tales.fromprod.com

GPT-4o was harmed for these images but no AIs were harmed in the production of this content

All views expressed are my own.

Key takeaways

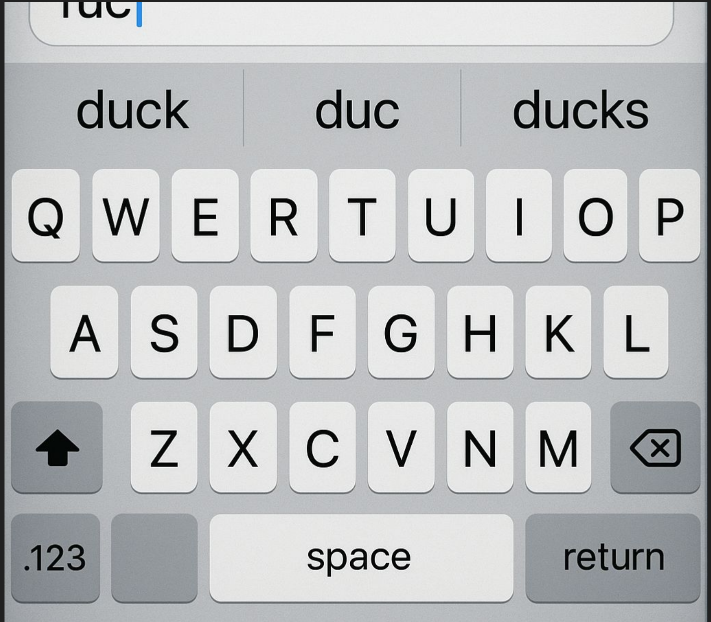
- How Large Language Models (LLMs) function
- How Retrieval Augmented Generation (RAG) works
- Using your existing resources for something new

Scenario

NETWORK TRAFFIC
SECURITY OPERATIONS CENTER
NEW ALERT
THREAT DETECTION
SYS TIMG MONITORING

How Large Language Models (LLMs) function

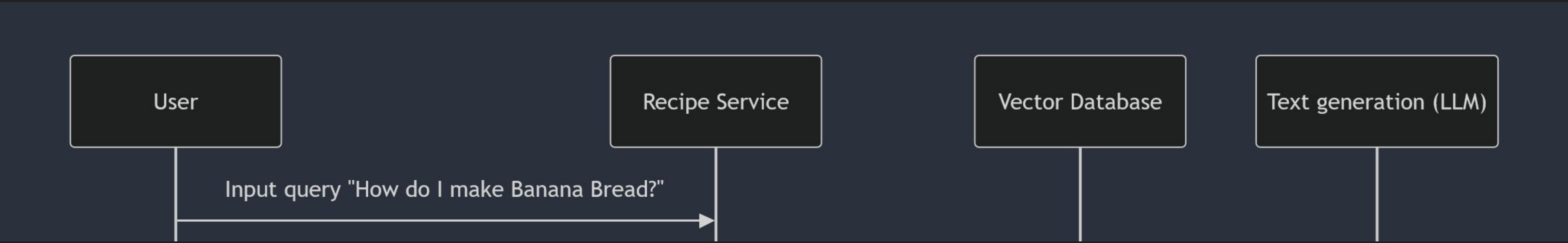
They’re the evolution of “next word prediction” on your phone keyboard



Retrieval Augmented Generation (RAG)

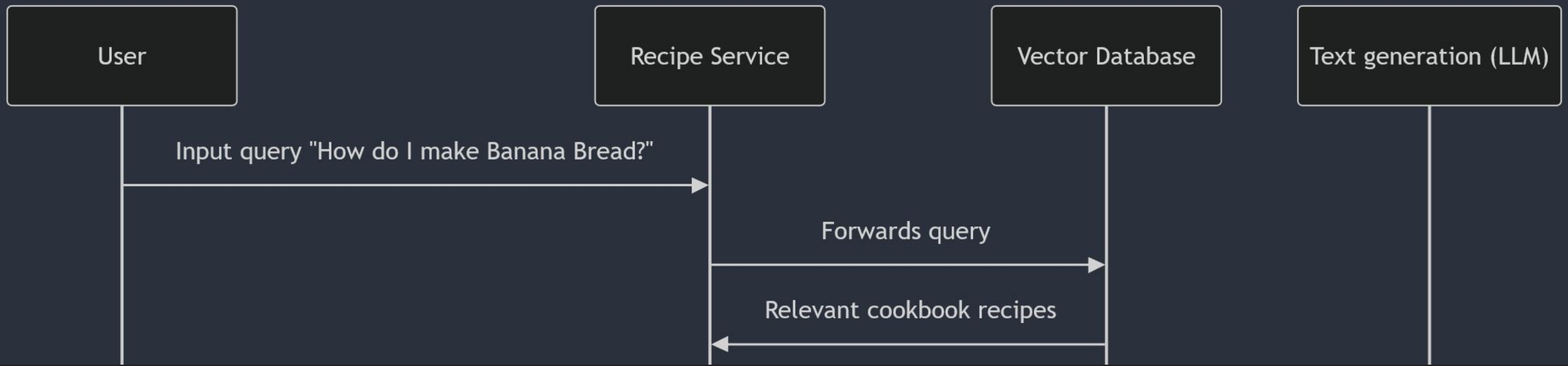
Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." *Advances in Neural Information Processing Systems* 33 (2020): 9459-9474.

Retrieval Augmented Generation (RAG)



Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." *Advances in Neural Information Processing Systems* 33 (2020): 9459-9474.

Retrieval Augmented Generation (RAG)



User

Recipe Service

Vector Database

Text generation (LLM)

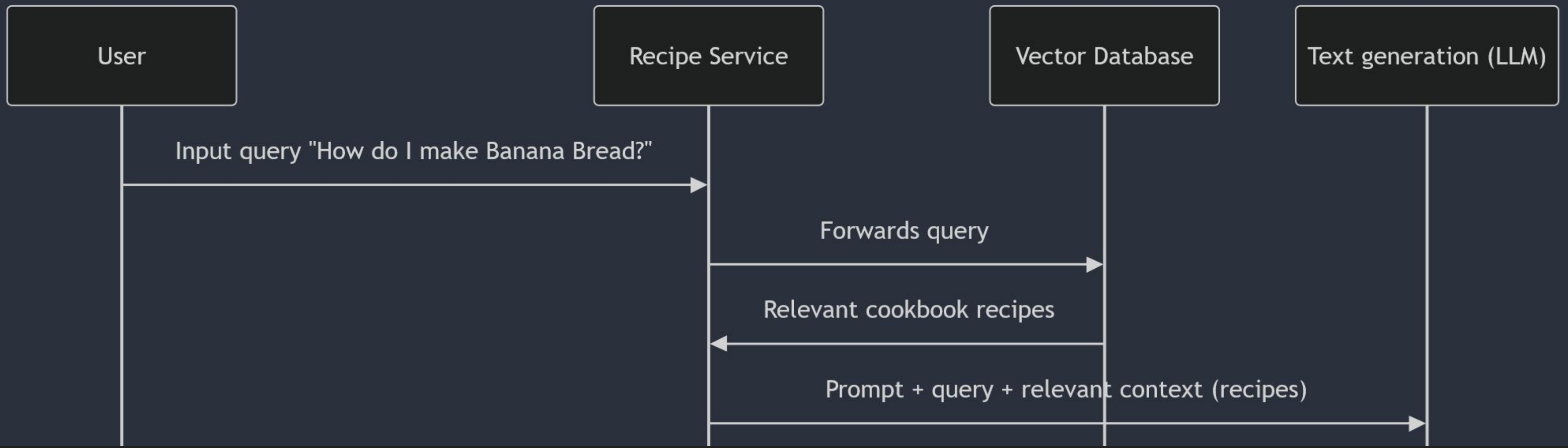
Input query "How do I make Banana Bread?"

Forwards query

Relevant cookbook recipes

Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." *Advances in Neural Information Processing Systems* 33 (2020): 9459-9474.

Retrieval Augmented Generation (RAG)



User

Recipe Service

Vector Database

Text generation (LLM)

Input query "How do I make Banana Bread?"

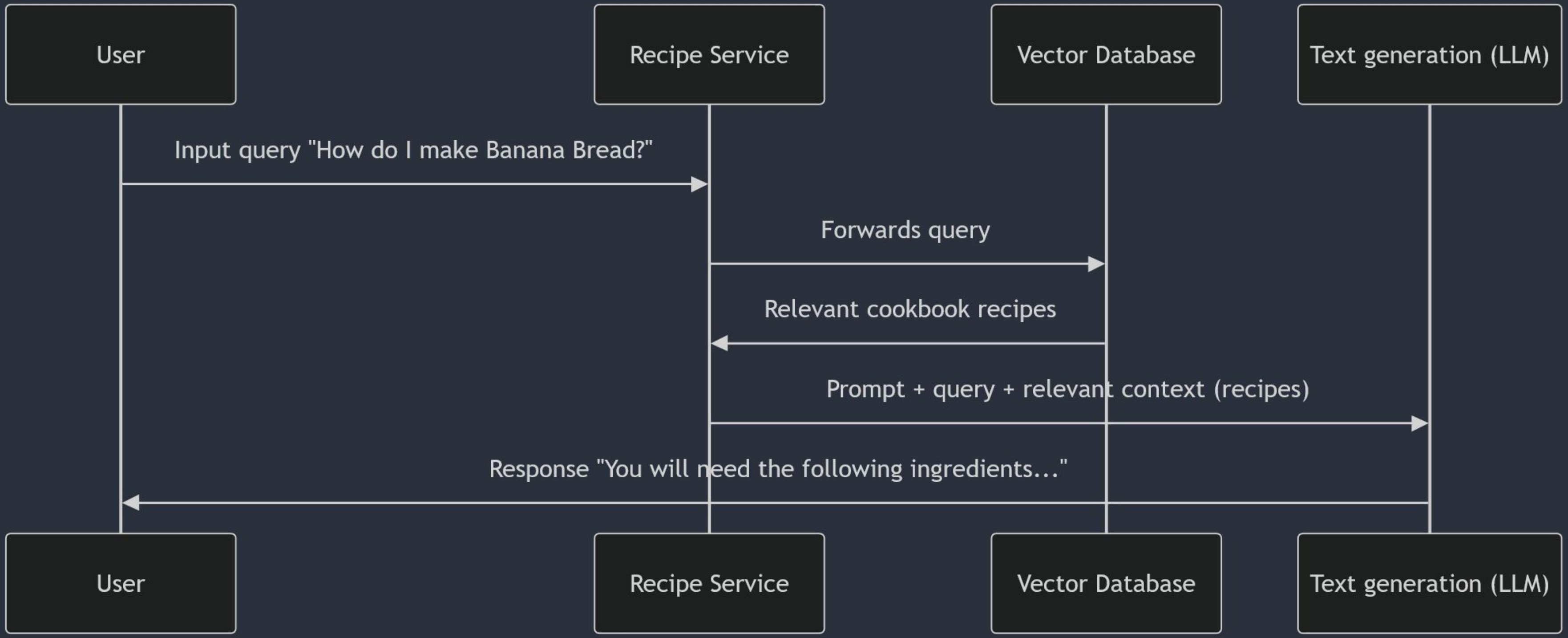
Forwards query

Relevant cookbook recipes

Prompt + query + relevant context (recipes)

Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." *Advances in Neural Information Processing Systems* 33 (2020): 9459-9474.

Retrieval Augmented Generation (RAG)


User
Recipe Service
Vector Database
Text generation (LLM)
Input query "How do I make Banana Bread?"
Forwards query
Relevant cookbook recipes
Prompt + query + relevant context (recipes)
Response "You will need the following ingredients..."
User
Recipe Service
Vector Database
Text generation (LLM)

Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." *Advances in Neural Information Processing Systems* 33 (2020): 9459-9474.

So, what?

Live demo?

Next steps

Next steps

- Use your existing runbooks to create updated detections

Next steps

- Use your existing runbooks to create updated detections
- Use these techniques to accelerate your investigations

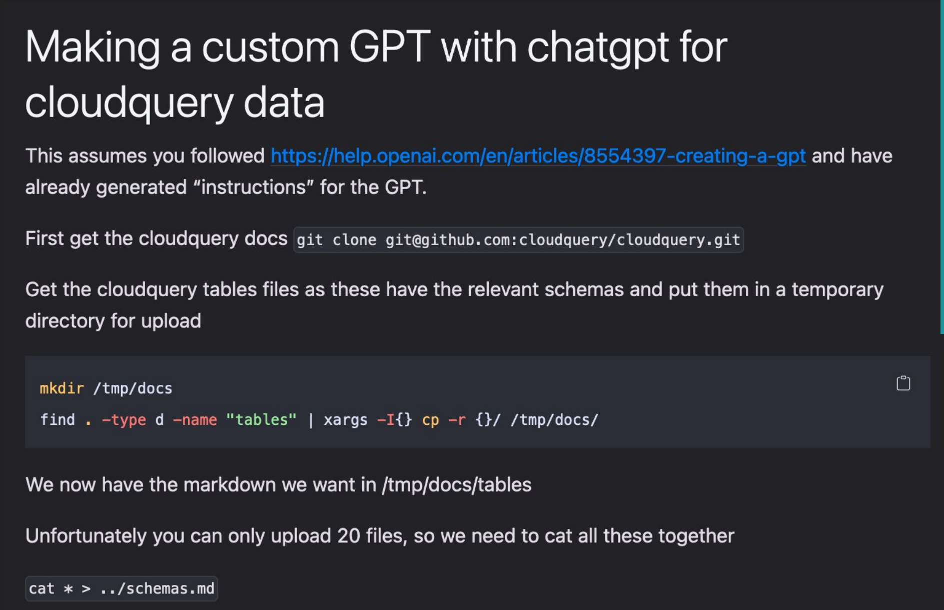
Next steps

- Use your existing runbooks to create updated detections
- Use these techniques to accelerate your investigations
- Discover for yourself that these LLMs are limited

Key takeaways

- How Large Language Models (LLMs) function
- How Retrieval Augmented Generation (RAG) works
- Using your existing resources for something new

Useful resources



Making a custom GPT with chatgpt for cloudquery data

This assumes you followed https://help.openai.com/en/articles/8554397-creating-a-gpt and have already generated "instructions" for the GPT.

First get the cloudquery docs `git clone git@github.com:cloudquery/cloudquery.git`

Get the cloudquery tables files as these have the relevant schemas and put them in a temporary directory for upload

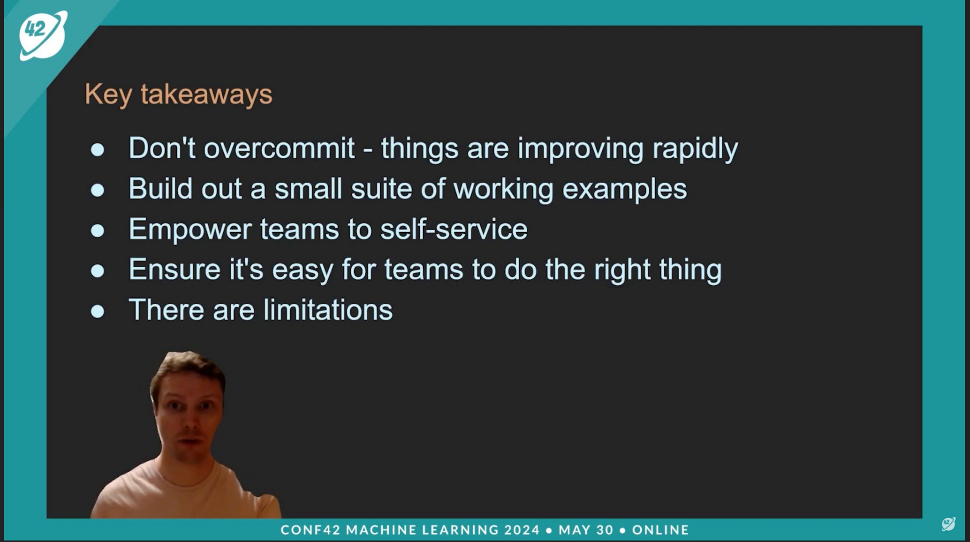
```
mkdir /tmp/docs
find . -type d -name "tables" | xargs -I{} cp -r {}/ /tmp/docs/
```

We now have the markdown we want in /tmp/docs/tables

Unfortunately you can only upload 20 files, so we need to cat all these together

`cat * > ../schemas.md`

https://tales.fromprod.com/2024/067/custom-chatgpt-cloudquery.html



Key takeaways

- Don't overcommit - things are improving rapidly
- Build out a small suite of working examples
- Empower teams to self-service
- Ensure it's easy for teams to do the right thing
- There are limitations

CONF42 MACHINE LEARNING 2024 • MAY 30 • ONLINE

Example architectures for these tools https://www.youtube.com/watch?v=KeAO1lgzoBQ

AI Native Tools (open source data) https://landscape.ainativedev.io/