Generative AI and LLMs in Networking and Security

Roopa Prabhu | Netdev0x17/31Oct2023

Security Applications of Machine Learning

Classification and Clustering

- Malicious URL detection
- Network Traffic Analysis
- Detection of new classes of malware
- Network Traffic anomaly detection
- Network traffic log analysis
- Identifying SQL injection
- DOS/DDOS detection
- And many more …

GenAI

What and Why

What is GenAI ?

- Generative AI models use neural networks to identify the patterns and structures within existing data to generate new and original content

Applications of GenAI

- Large language models (LLM's) are language based generative models which are used in translation, code generation, summarization, understanding genetic sequences, …
- Synthetic data generation to improve efficiency and accuracy of existing AI systems
- Help Automate and accelerate tasks and processes
- Create new text, Audio and visual content

GenAI and Security

GenAI and Security

Security Applications of GenAI

Synthetic Data Generation

- In most cases, anomalies are rare, making it hard to find the required data to train models
- Synthetic data can bridge the gap by producing the data for anomalies

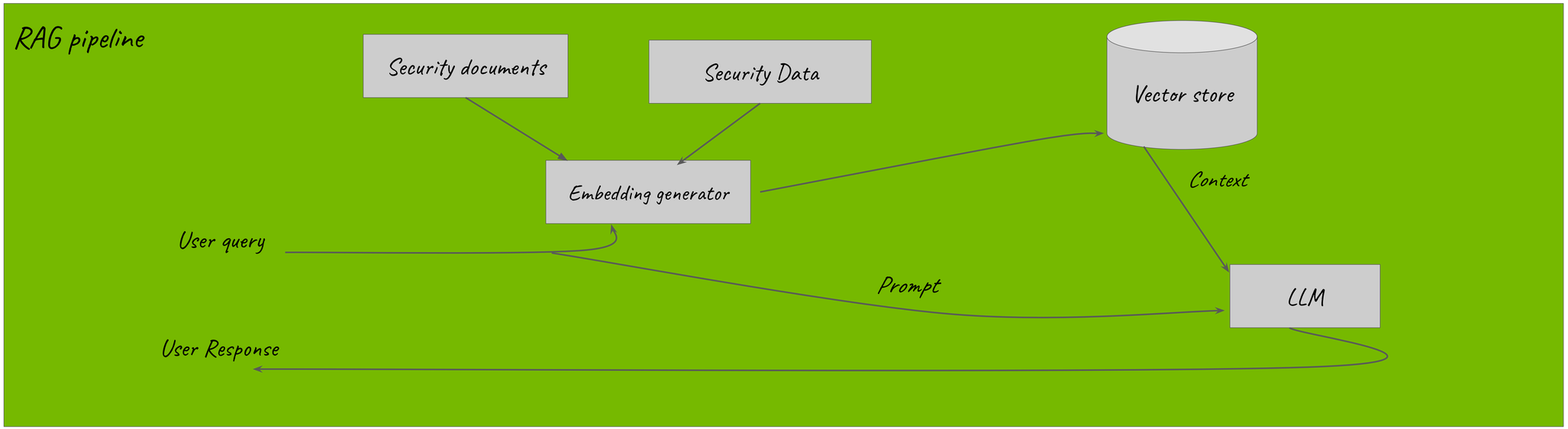
Code Generation

- Security co-pilot
  - Large Language Model with security specific capabilities

GenAI and Security

Large Language Models

- Interact with your security data using Natural language
- SecOps using Natural Language
- LLM's can provide summaries of relevant threats, exploitable vulnerabilities
- Retrieval Augmented Generation (RAG) for improving the quality of LLM generated responses

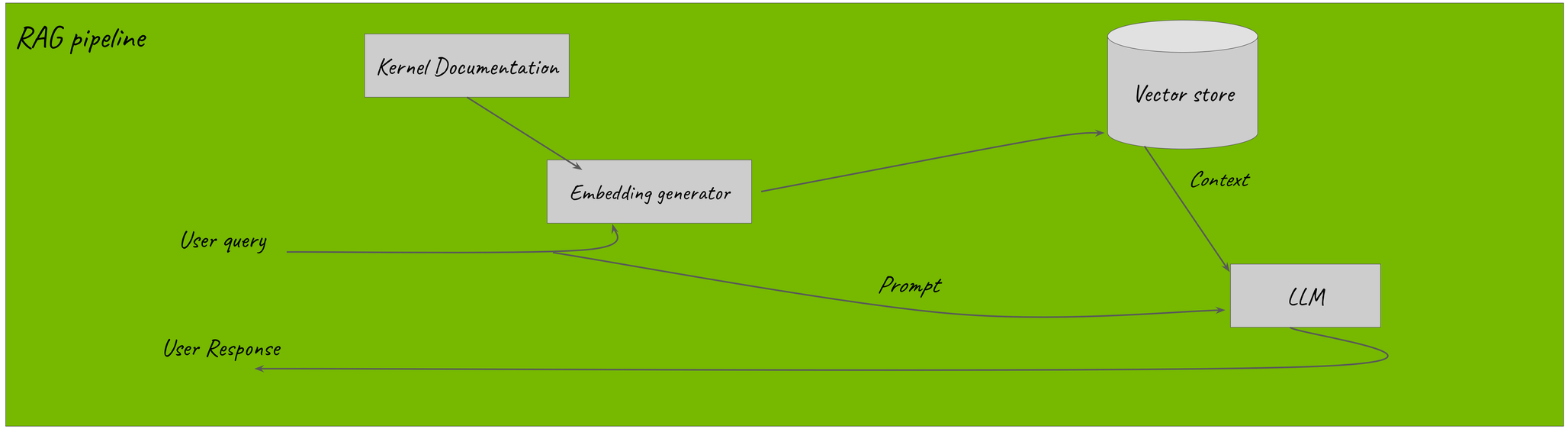


Bringing LLM’s and GenAI to Linux Networking

GenAI and LLM's for Linux Networking

Food for thought

- Kernel development co-pilot
  - Fine tune a LLM for kernel code
- Kernel Patch Review helper
  - Summarize patch reviews
- Kernel Documentation chatbot
  - RAG pipeline with Llamaindex or other frameworks (I can see this being very useful for outreachy-kernel)
- Augment Syzkaller reports with more context



GenAI and LLM's for Linux Networking Operations

Food for thought - Imagine you could talk to Linux TC in natural language :)

```
$show me qdisc on interface enp0s1

Executing 'tc qdisc show dev enp0s1'

qdisc fq_codel 0: root refcnt 2 limit 10240p
flows 1024 quantum 1514 target 5.0ms interval
100.0ms memory_limit 32Mb ecn
```

```
$show me qdisc counters on interface enp0s1

Executing 'tc -s qdisc show dev enp0s1'

qdisc fq_codel 0: root refcnt 2 limit 10240p
flows 1024 quantum 1514 target 5.0ms interval
100.0ms memory_limit 32Mb ecn

Sent 1008193 bytes 5559 pkt (dropped 233,
overlimits 55 requeues 77)

backlog 0b 0p requeues 0
```