
# SENTINEL

## INTELLIGENCE PLATFORM

The Definitive Field Guide for Java Developers building Secure, Air-Gapped RAG Applications.

CLASSIFICATION: TOP SECRET // NOFORN
VERSION: 1.0.1

# 1. THE MISSION

You are tasked with presenting **Sentinel** to a high-security client. Their problem is simple but critical: **They cannot use ChatGPT.**

### THE PROBLEM: DATA LEAKS

Every time an analyst pastes a document into a public AI, that data leaves the secure perimeter. For banks, defense, and healthcare, this is unacceptable.

### THE SOLUTION: "AIR-GAPPED" RAG

Sentinel runs **entirely on the local machine**. Cables unplugged. No WiFi.

- **Local Brain:** We replace OpenAI with `Ollama` (Llama 3).
- **Local Memory:** We replace Vector Databases with local `MongoDB`.
- **Java Backend:** We orchestrate it all with `Spring Boot`.

# 2. ARCHITECTURE

Don't be intimidated by the "AI" buzzwords. This is a standard 3-tier Java application.

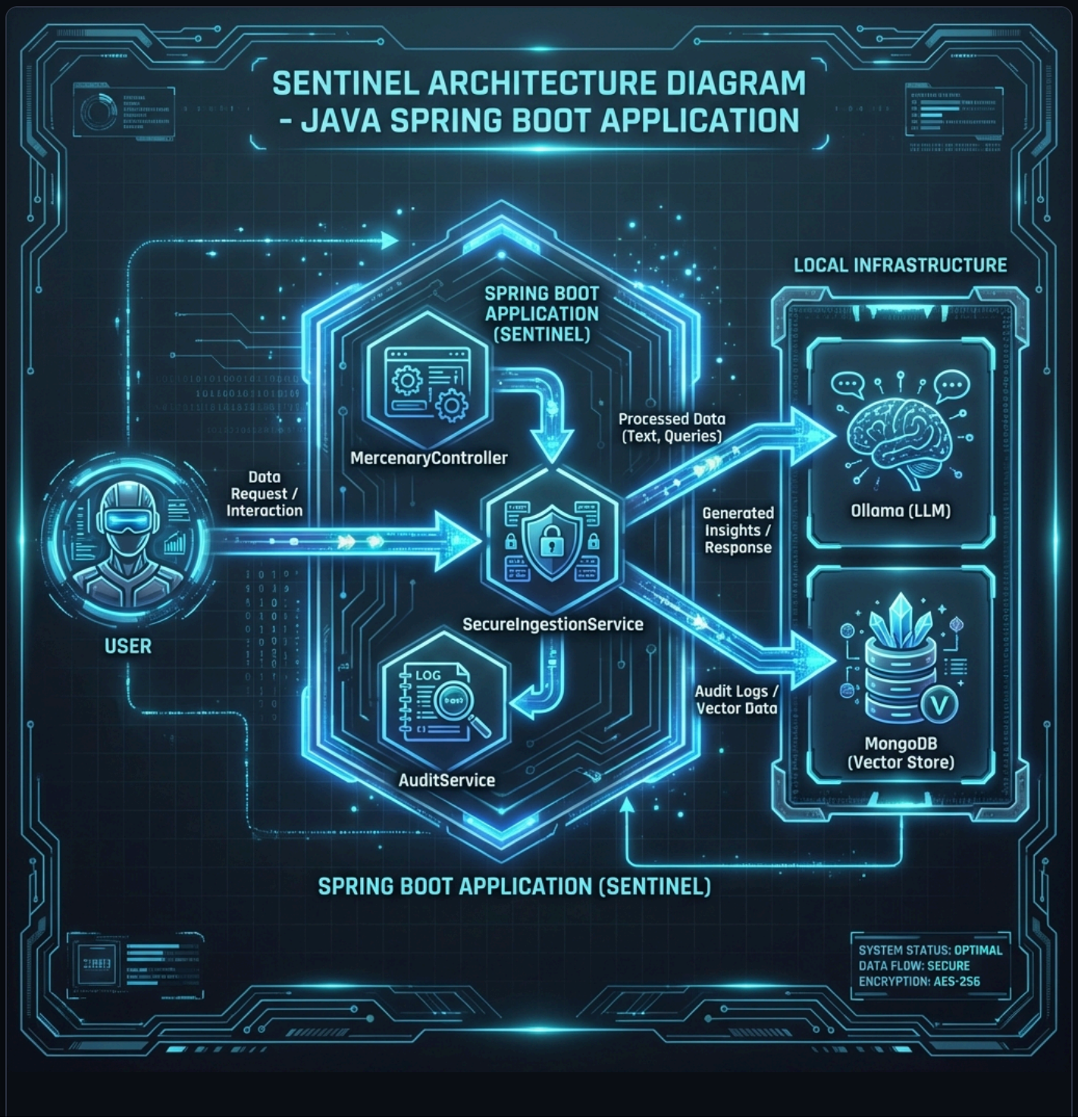

*Figure 1: High-Level System Architecture*

### THE CONTROLLER

`MercenaryController.java`

The "Traffic Cop". It accepts HTTP requests, checks **Security Clearance**, and routes queries to the AI.

### THE SERVICE

`SecureIngestionService.java`

The "Translator". It takes PDF files, cleans them (removes SSNs), and turns them into math (Vectors).

# 3. CORE CONCEPT: VECTORS

How does a computer "understand" meaning? It converts text into lists of numbers called **Embeddings**.


*Figure 2: Semantic Space Visualization*

Imagine a 3D space. The words "King" and "Queen" are close together. "Apple" is far away.

## RECOMMENDED RESOURCES

**Video: Vector Embeddings Explained**

IBM Technology (6 mins) - Excellent visual explanation.

### Video: Spring AI RAG Tutorial

Dan Vega (20 mins) - The best Java-focused breakdown.

# 4. THE INTERFACE

We built a "Glass Box" UI. Unlike ChatGPT which is a "Black Box" (you don't know why it said that), Sentinel shows its work.

*Figure 3: The Sentinel Operator Dashboard*

## KEY SELLING POINTS

- **Telemetry Bar:** Shows low latency (running locally).
- **Citations:** Clicking `[file.pdf]` opens the source document.
- **Security Warnings:** Red banners for classified data.

# 5. THE CODE

The magic happens in `MercenaryController.java`. Here is the critical security logic:

```
// HARDENED SECURITY CHECK
User user = SecurityContext.getCurrentUser();

if (user == null) {
    auditService.logAccessDenied(...);
    return "ACCESS DENIED";
}

// CHECK CLEARANCE LEVEL
if (!user.canAccessClassification(dept.getClearance())) {
    return "ACCESS DENIED: Insufficient Clearance";
}

// ONLY THEN -> EXECUTE AI QUERY
vectorStore.similaritySearch(query);
```

This proves to the customer that **Java Security** runs *before* the AI ever gets the prompt.