# RAG Security Architecture with AltaStata

## The Problem

Traditional RAG implementations expose enterprise data through:

- **Storage**: Admins can access unencrypted documents
- **Retrieval**: Data transmitted without end-to-end encryption
- **Processing**: Confidential data in unprotected memory
- **Compliance**: No audit trails or version control for GDPR/HIPAA/SOC 2

## Data Flow

### Document Ingestion (Write Path)

1. Enterprise uploads document → AltaStata encrypts with AES-256
2. Document chunked and compressed for speed/cost optimization
3. Encrypted bytes stored in multi-cloud backend (AWS/IBM/MiniIO/GCP/Azure)
4. Version metadata created for audit compliance

### RAG Retrieval (Read Path)

1. LangChain loader requests `altastata://` URL
2. fsspec routes to AltaStata filesystem
3. Authenticates user credentials and permissions
4. Downloads encrypted bytes from cloud storage
5. Decrypts locally within application's memory space
6. Returns plaintext to RAG application (text splitter → embeddings → vector store)

## Key Security Features

**End-to-End Encryption**: AES-256 encryption per file, Zero-Trust architecture prevents admin access

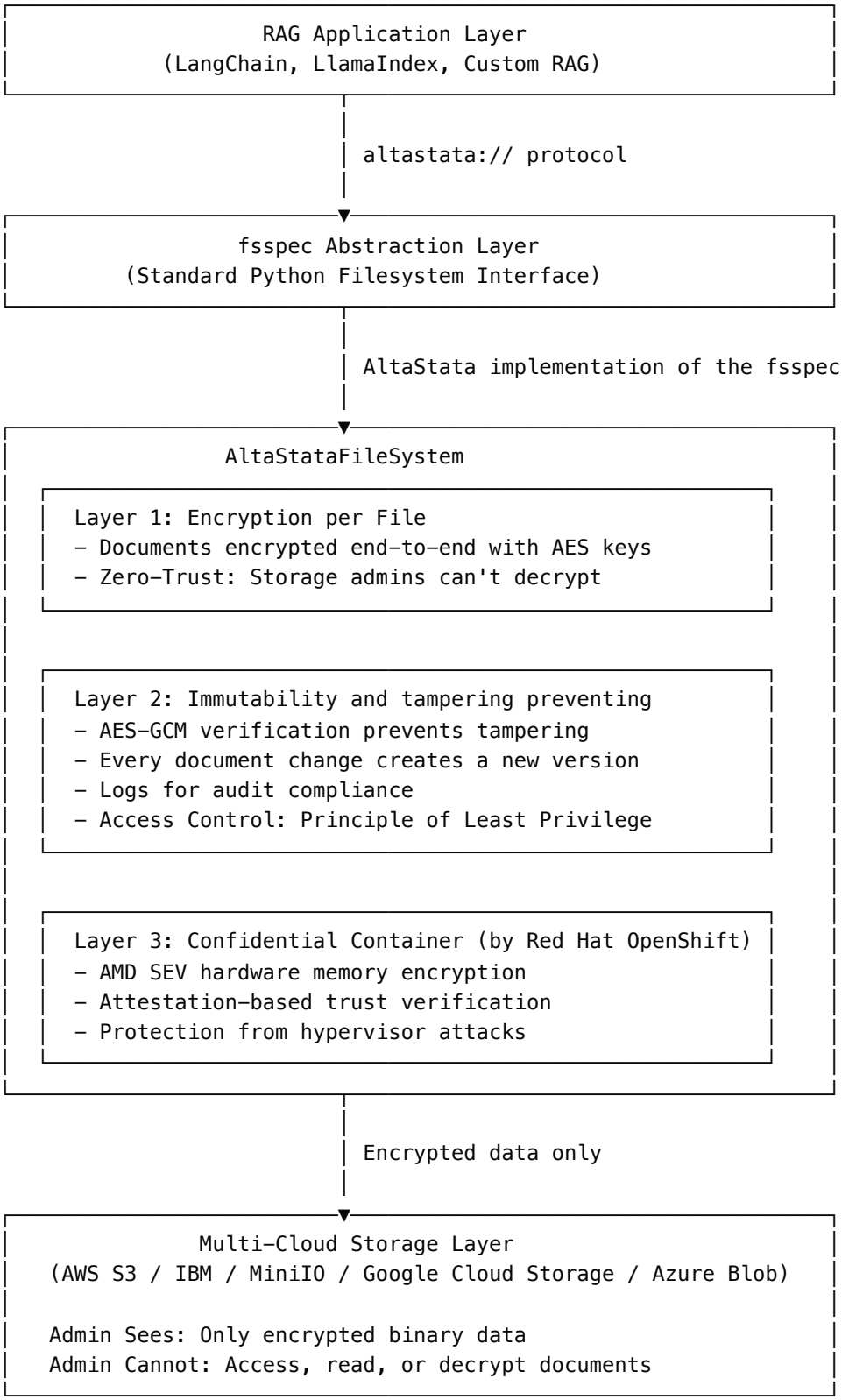
**Immutable Versioning**: Every change creates new version with AES-GCM verification to prevent tampering

**Access Control**: Account-based isolation with credential authentication and role separation

**Confidential Computing**: Optional Confidential Container via Red Hat OpenShift

# The Solution: Multi-Layer Security Architecture

AltaStata implements defense-in-depth security specifically designed for RAG systems:



### Working Example

See **test_rag.py** for a complete, production-ready RAG implementation that demonstrates:

- Uploading documents to encrypted storage
- Loading documents via fsspec
- Creating vector embeddings
- Semantic search with similarity scoring
- Automatic cleanup

## Deployment Models

1. **On-Premises**: Maximum control, data never leaves trusted environment (finance, healthcare, defense)
2. **Hybrid Cloud**: RAG in public cloud with encrypted storage, zero-trust security
3. **Confidential Computing**: Confidential Container for end-to-end protection (mission-critical AI)

## Compliance

**GDPR**: Encryption, version control, audit trails, right to erasure **HIPAA**: End-to-end encryption, access controls, audit logs **SOC 2**: Authentication, key management, monitoring

## Security Comparison

| Feature | Traditional RAG | AltaStata RAG |
|---|---|---|
| **Storage** | Provider-managed keys | Client-side AES-256 (zero-trust) |
| **Processing** | Plaintext in memory | Optional Confidential Container |
| **Audit Trail** | Manual logging | Automatic version history |
| **Compliance** | Custom implementation | Built-in GDPR/HIPAA/SOC 2 |
| **Integration** | Custom per backend | Standard fsspec interface |