Project Write-Up: Velonix AI Security: Secure RAG System Tool

Project Title: Securing Enterprise AI Systems through Role-Aware tools for RAG systems.
Organization: Velonix AI Security
Date: April 2025

1. Executive Summary

Velonix is pioneering an advanced AI security infrastructure designed to revolutionize data protection and controlled knowledge dissemination within large language model (LLM) systems. Our innovative platform seamlessly integrates Role-Based Access Control (RBAC) within Retrieval-Augmented Generation (RAG) pipelines, ensuring that sensitive information reaches only authorized users with appropriate credentials.

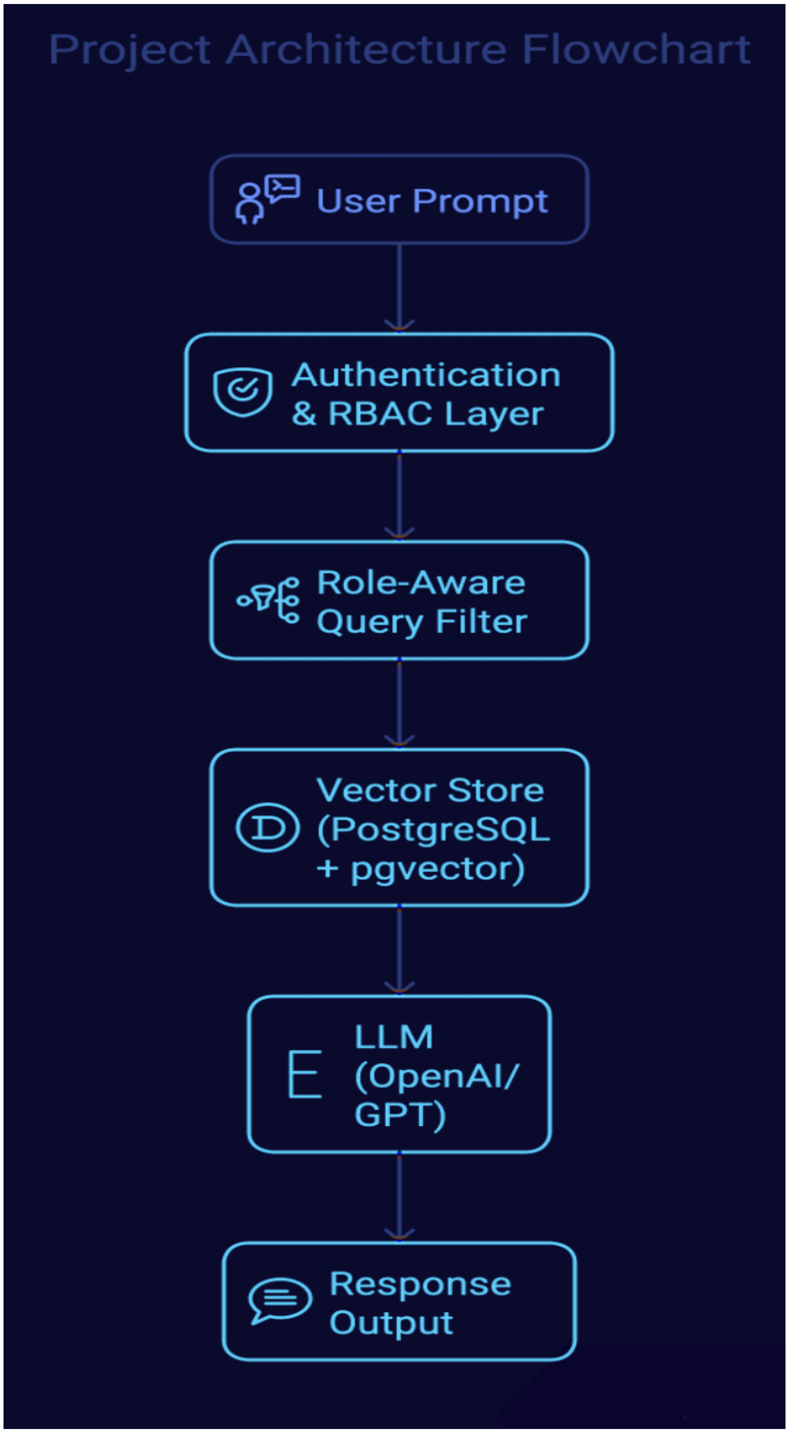
This strategic initiative directly supports Saudi Vision 2030's core pillars of digital transformation, secure smart infrastructure, and innovation leadership. By providing enterprise-grade security for AI interactions across critical sectors, including healthcare, energy, defense, and government, Velonix enables:

1. **Guaranteed data sovereignty** through granular access control mechanisms
2. **Enhanced digital trust** in AI-powered systems
3. **Accelerated AI-driven economic diversification** with built-in security

Key Differentiator: Unlike conventional approaches that treat security as an afterthought, Velonix embeds protections at the retrieval layer, where knowledge access decisions occur, preventing unauthorized information exposure before it can happen.

2. Project Architecture: The Velonix Security Layer

Velonix delivers a sophisticated middleware security layer that integrates seamlessly between existing enterprise user-facing applications and foundational LLM-based RAG systems. Our role-aware middleware enforces fine-grained access control at every stage of data processing.


Project Architecture Flowchart
User Prompt
Authentication & RBAC Layer
Role-Aware Query Filter
Vector Store (PostgreSQL + pgvector)
D
E
LLM (OpenAI/ GPT)
Response Output

Core Architectural Components

Component	Function	Key Innovation
Middleware Access Gateway	Intercepts user queries, authenticates sessions, and applies RBAC policies before data reaches vector databases or LLMs	Real-time query transformation with role context
RBAC Policy Engine	Applies configurable, organization-specific access policies with inheritance and exceptions	Semantic understanding of documents and queries
Multi-Layer Filtering System	Enforces restrictions through combined metadata, semantic, and contextual filters	The hybrid filtering approach preserves relevance
External RAG Integration Layer	Connects with existing RAG systems (OpenAI API, LangChain, private LLM stacks)	Non-invasive implementation reduces adoption friction
Comprehensive Audit & Governance Module	Captures detailed access logs, policy enforcement decisions, and provides compliance reporting	Executive dashboards with risk visualization

Our middleware architecture eliminates the need for enterprises to rebuild existing RAG workflows, providing a scalable and secure plug-in layer that respects existing technology investments.

3. Technical Advantages and Innovation

Role-Aware Filtering & Semantic Security

Velonix implements multi-dimensional security that goes beyond simple access control lists:

1. **Semantic Understanding:** Documents are evaluated against both role metadata and semantic relevance to prevent information leakage
2. **Contextual Query Analysis:** Natural language understanding identifies potential attempts to circumvent access controls
3. **Real-Time Role Inference:** The system adapts dynamically to session-level role changes or contextual access rules

Enterprise-Ready Architecture

1. **Modular Infrastructure:** Each component is pluggable, allowing compatibility with diverse enterprise tools and cloud environments
2. **High-Performance Design:** Low-latency pipelines with caching, batching, and parallelism ensure minimal delays despite sophisticated security layers
3. **Scalability:** Handles millions of documents and thousands of concurrent users without performance degradation

Security-First Implementation

1. **Defense-in-Depth:** Multiple control layers prevent single points of failure
2. **Transparent Audit Trail:** Comprehensive logging for regulatory compliance and threat detection

4. Strategic Alignment with Saudi Vision 2030

Saudi Vision 2030 establishes ambitious goals for the Kingdom as a global hub for AI, innovation, and cybersecurity. Velonix directly supports these national priorities:

Digital Trust & Data Sovereignty

1. Enables organizations to adopt advanced AI capabilities without compromising sensitive data
2. Ensures all data processing adheres to local regulations and sovereignty requirements
3. Provides granular control over knowledge flows within and across organizational boundaries

Smart Government & Secure Cities

1. Facilitates AI adoption in public services with strict access controls and audit trails
2. Supports secure knowledge sharing across government entities while preventing unauthorized access
3. Enables intelligent infrastructure that protects sensitive citizen and operational data

National Cybersecurity Readiness

1. Aligns with National Cybersecurity Authority (NCA) and Saudi Data & AI Authority (SDAIA) guidelines
2. Enhances protection of critical national infrastructure through secure AI systems
3. Provides technology sovereignty in key AI security capabilities

Private Sector Transformation

1. Accelerates secure AI adoption across financial institutions, energy companies, and healthcare providers
2. Reduces compliance risks while maximizing AI benefits
3. Creates competitive advantage through secure innovation capabilities

Our technology directly supports flagship initiatives, including NEOM, The Line, and other giga-projects by enabling secure AI deployment across decentralized environments with varying security requirements.

5. Conclusion: Securing the AI-Powered Future

In the rapidly evolving AI landscape, organizations must not be forced to choose between intelligence and security. Velonix bridges this critical gap by embedding sophisticated access control mechanisms deep within the knowledge retrieval process, enabling enterprises to:

1. Deploy powerful LLM capabilities with confidence
2. Protect sensitive information from unauthorized access
3. Maintain comprehensive audit trails for governance
4. Accelerate AI adoption across regulated industries

Our vision is to establish Velonix as the gold standard for secure enterprise AI systems, contributing significantly to Saudi Arabia's leadership in global cybersecurity innovation and trusted AI deployment.

Prepared by:
Velonix team.
April 2025