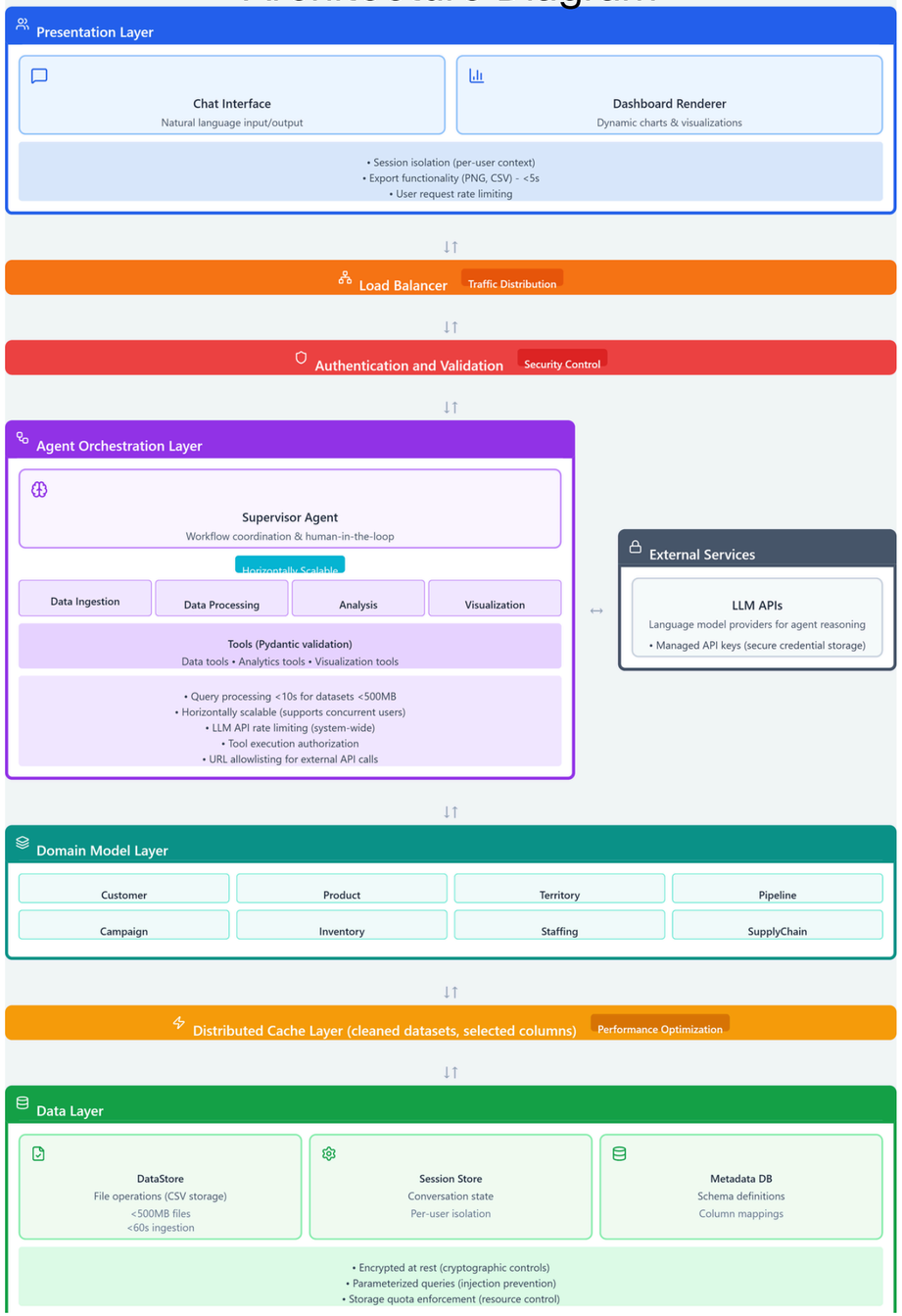
Continuum AI

Group 13

Architecture Diagram



Non-Functional Requirements

Query Performance

Requirement:
The system will process and display visualizations for 90% of natural language queries on datasets under 500MB within 10 seconds

Architecture Support

- Cache Layer stores cleaned data, eliminating repeated reads.
- Supervisor Agent routes queries to the right specialized agent.
- Asynchronous execution reduces waiting time.

Usability

Requirement:
After a 15-minute tutorial, new users must achieve an 80% first-attempt success rate when generating a sales-trend visualization.

Architecture Support

- Chat Interface allows plain-English queries.
- Supervisor Agent provides clarifying prompts (human-in-the-loop).
- Dashboard Renderer gives instant visual feedback.

Data Ingestion Performance

Requirement:
A 100MB CSV file will be ingested, processed, and made ready for analysis in under 60 seconds.

Architecture Support

- Data Ingestion Agent handles file uploads and schema validation in parallel.
- Data Processing Agent cleans and transforms data (missing values, types, outliers).
- Distributed Cache Layer stores cleaned datasets for immediate reuse.
- Metadata DB registers schema definitions, speeding up later queries.

Security Risks and Justifications

Injection Attacks

Malicious input execution via queries or uploads (e.g., SQL/CSV injection).

- Validation Middleware scans all user inputs. (Security Middleware)
- Strict Pydantic Schemas enforce typed, safe input. (Agent Orchestration)
- Parameterized SQL Queries block injection even if earlier layers are bypassed. (Data Layer)

Broken Access Control

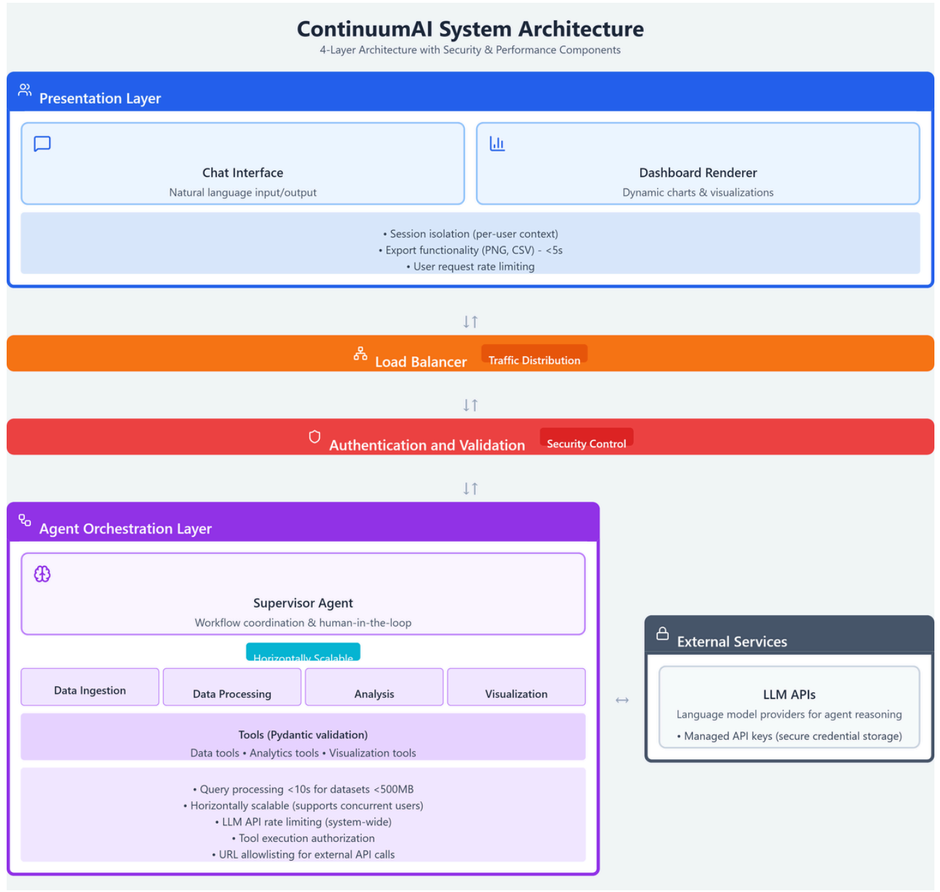
Unauthorized access to data or functionality beyond user permissions.

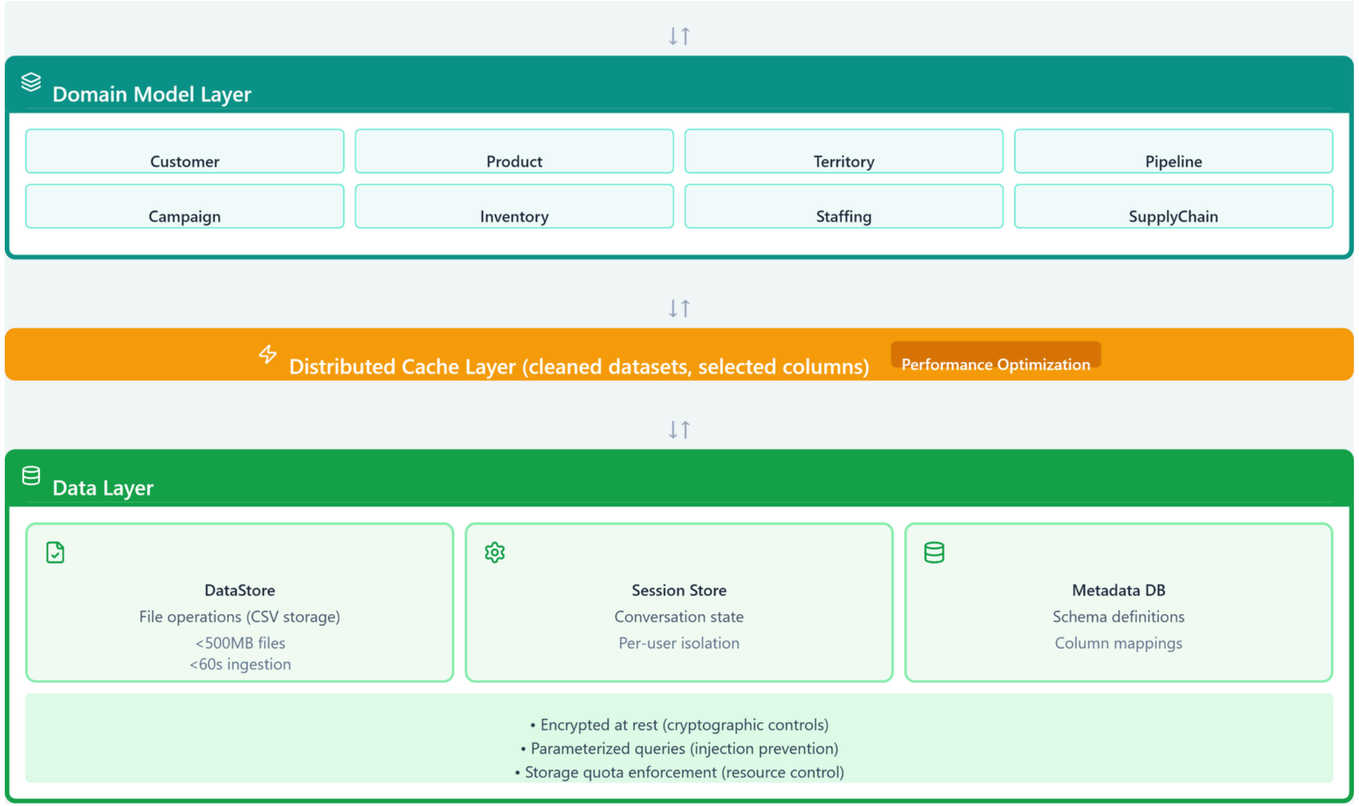
- Session Isolation ensures user-specific data contexts. (Presentation Layer)
- Security Middleware authenticates & blocks unauthorized requests. (Auth and Validation)
- Per-User Data Isolation keeps user data strictly separated in all layers. (Data Layer)

Cryptographic Failures

Exposure of sensitive data due to weak encryption or poor key handling.

- Encryption at Rest for all stored data. (Data Layer)
- Secure Credential Management via runtime key retrieval & no logging. (External services)
- Encrypted Communication ensures all data in transit is protected, even between internal layers. (Cross Layer)


ContinuumAI System Architecture
4-Layer Architecture with Security & Performance Components
Presentation Layer
Chat Interface
Natural language input/output
Dashboard Renderer
Dynamic charts & visualizations
• Session isolation (per-user context)
• Export functionality (PNG, CSV) - <5s
• User request rate limiting
Load Balancer
Traffic Distribution
Authentication and Validation
Security Control
Agent Orchestration Layer
Supervisor Agent
Workflow coordination & human-in-the-loop
Horizontally Scalable
Data Ingestion
Data Processing
Analysis
Visualization
Tools (Pydantic validation)
Data tools • Analytics tools • Visualization tools
• Query processing <10s for datasets <500MB
• Horizontally scalable (supports concurrent users)
• LLM API rate limiting (system-wide)
• Tool execution authorization
• URL allowlisting for external API calls
External Services
LLM APIs
Language model providers for agent reasoning
• Managed API keys (secure credential storage)


Domain Model Layer
Customer
Product
Territory
Pipeline
Campaign
Inventory
Staffing
SupplyChain
Distributed Cache Layer (cleaned datasets, selected columns)
Performance Optimization
Data Layer
DataStore
File operations (CSV storage)
<500MB files
<60s ingestion
Session Store
Conversation state
Per-user isolation
Metadata DB
Schema definitions
Column mappings
• Encrypted at rest (cryptographic controls)
• Parameterized queries (injection prevention)
• Storage quota enforcement (resource control)