Model Context Protocol: A Technical Overview

The Model Context Protocol (MCP) is an open standard introduced by Anthropic in November 2024.
It provides a universal interface for AI systems to integrate with external tools and data sources.
MCP defines how language models communicate with applications through a structured protocol.
The protocol supports three transport modes: stdio for local subprocess communication,
SSE for server-sent events over HTTP, and streamable-http for bidirectional streaming.
Each MCP server exposes tools that Claude Desktop can discover and invoke at runtime.
Tools have typed input schemas, making them safe and predictable for automated use.
LanceDB is used as the underlying vector store for semantic search capabilities.
Documents are chunked into overlapping segments and embedded using sentence-transformers.
The embedding model used is all-MiniLM-L6-v2 which produces 384-dimensional vectors.
Semantic similarity is computed using cosine distance in the vector space.
The system supports ingestion of PDF Word PowerPoint Excel HTML and image formats.
MarkItDown is used to convert all these formats into plain Markdown text.
Content deduplication is performed using SHA256 hashes of the source bytes.
Multiple libraries allow organizing documents into separate searchable collections.