

Human-in-the-Loop Math Tutor Agent

1. Introduction

Mathematics is one of the most fundamental skills for students, yet it is also one of the most challenging subjects to master. While traditional AI chatbots can provide quick answers, they often fail to explain the **reasoning process** step by step, or they may drift into unrelated, unsafe, or non-educational topics. This creates a gap between **answer generation** and **actual learning support** for students.

To address this challenge, we propose the development of a **Human-in-the-Loop Agentic-RAG Math Tutor**. The system is designed to act like a mathematics professor — not just giving the correct solution, but also breaking the problem into clear, step-by-step reasoning that a student can follow and learn from.

The key objectives of this system are:

- **Accuracy & Reliability:** Provide solutions grounded in a curated math knowledge base (GSM8K) and trustworthy web sources when needed.
- **Educational Alignment:** Ensure that the agent delivers math-focused, safe, and educational content through **guardrails**.
- **Adaptability:** Integrate **retrieval-augmented generation (RAG)** with an **agentic routing pipeline**, choosing between Knowledge Base (KB) and Web Search.
- **Continuous Improvement:** Leverage **Human-in-the-Loop feedback** (👍 / 👎) to refine performance and adapt to real student needs.

Key Features Implemented:

- Knowledge Base search using **GSM8K dataset + Qdrant VectorDB**.
- Web Search fallback via **MCP (Tavily API)**.
- Input & Output **guardrails** to enforce privacy, safety, and math-only focus.
- **Feedback loop** for human validation and iterative learning.


This proposal outlines the design decisions, implementation steps, and evaluation of the Math Tutor Agent, showing how Agentic-RAG principles combined with guardrails and human feedback create a robust and practical AI system for mathematics education.

2. Input & Output Guardrails

One of the core challenges in designing educational AI agents is ensuring that the system remains **focused, safe, and aligned** with its intended purpose. In our Math Tutor Agent, this was achieved through the integration of **input and output guardrails** at the AI gateway layer.

2.1 Input Guardrails




Approach Taken:

- Implemented a **keyword + numeric detection filter** to determine whether a query is math-related.
- Queries containing math-specific terms (e.g., *solve, equation, probability, integral, derivative, vector, matrix*) or **numbers** (e.g., “ $2 + 2$ ”, “*Tom has 5 apples*”) are allowed.
- Non-math queries are rejected immediately with a clear response:
“ *Only math-related questions are allowed.*”

Rationale:


- This ensures that the agent cannot be misused for irrelevant or non-educational purposes (e.g., “*Who is Taylor Swift?*”).
- Allowing numbers ensures natural word problems (like those in GSM8K) are recognized even if no explicit math keyword is present.
- Keeps the system **student-focused** and prevents unnecessary API calls to KB/Web Search for irrelevant input.

Examples:

- Input: “*Solve $2x + 5 = 17$* ” →  Accepted.
 - Input: “*Tom has 5 apples. Mary has 3 times as many...*” →  Accepted.
 - Input: “*Who is the President of the USA?*” →  Rejected.
-

2.2 Output Guardrails



Approach Taken:

- Introduced a **sanitization layer** that checks generated responses before returning them to the user.
- If unsafe or irrelevant content is detected (keywords like *hack*, *attack*, *nsfw*, *violence*), the output is blocked and replaced with:
“ *Output blocked: unsafe content detected.*”

Rationale:

- Prevents harmful or irrelevant text from being returned to students.
- Ensures the system always stays within its **educational boundaries**.
- Adds a safety layer for compliance with ethical AI practices.

Examples:

- Normal Output: “*Step 1: Subtract 5 $\rightarrow 2x = 12$. Step 2: Divide by 2 $\rightarrow x = 6$. Final Answer: 6.*” \rightarrow  Delivered.
- Unsafe Output (hypothetical test case): “*You should hack the system...*” \rightarrow  Blocked.

2.3 Why This Approach Works

By combining **input restriction** with **output sanitization**, the Math Tutor Agent ensures:

- Queries remain **educational and math-specific**.
 - Responses remain **safe, step-by-step, and focused**.
 - The system can be deployed in a learning environment with **privacy and trustworthiness guaranteed**.
-

3. Knowledge Base

The Knowledge Base (KB) serves as the **primary source of truth** for the Math Tutor Agent. By leveraging a high-quality dataset of math problems paired with step-by-step solutions, the system can provide reliable, educationally aligned answers without depending entirely on generative reasoning.

3.1 Dataset Used: GSM8K

- **Name:** GSM8K (Grade School Math 8K)
- **Size:** ~7,500 math word problems with annotated, step-by-step solutions.
- **Domain:** Elementary and middle-school mathematics, covering arithmetic, algebra, probability, geometry, and applied word problems.
- **Reason for Selection:**
 - Curated dataset widely used in benchmarking math reasoning for large language models (LLMs).
 - Provides **explainable, step-by-step solutions**, aligning with the agent's goal of teaching like a math professor.
 - Covers diverse problem types, from simple addition to multi-step reasoning tasks.

3.2 Implementation in KB

- The GSM8K dataset was **embedded** using OpenAI's `text-embedding-3-small` model.
- Embeddings were stored in a **Qdrant vector database**, enabling semantic search and fast retrieval.
- A **threshold filter (0.75 cosine similarity)** ensures only high-confidence matches are accepted. If no match exceeds the threshold, the query is routed to web search.

Pipeline:

1. Convert query → vector embedding.

2. Search KB (Qdrant) for top-3 closest matches.
 3. If similarity $\geq 0.75 \rightarrow$ return KB solution.
 4. Else \rightarrow route to Web Search.
-

3.3 Example Queries (KB Success)

Example 1

- **User Query:** *“Solve $2x + 5 = 17$ ”*
- **KB Answer:**
 - Step 1: Subtract 5 $\rightarrow 2x = 12$.
 - Step 2: Divide by 2 $\rightarrow x = 6$.
 - **Final Answer: 6**

Example 2

- **User Query:** *“Tom has 5 apples. Mary has 3 times as many. How many apples does Mary have?”*
- **KB Answer:**
 - Tom = 5
 - Mary = $3 \times 5 = 15$
 - **Final Answer: 15**

Example 3

- **User Query:** *“What is the probability of rolling a 6 on a fair die?”*
- **KB Answer:**
 - 1 favorable outcome / 6 total outcomes = $1/6$
 - **Final Answer: $1/6$**

3.4 Advantages of the KB Approach

- **Accuracy:** Relies on pre-validated solutions instead of generating from scratch.
 - **Efficiency:** Fast retrieval with semantic embeddings ensures low latency.
 - **Alignment:** Provides structured, step-by-step explanations that match educational goals.
 - **Scalability:** New datasets (e.g., JEE Bench, university-level math) can be ingested to expand coverage.
-

4. Web Search / MCP Setup

While the Knowledge Base (KB) provides strong coverage for grade-school-level math problems, students often ask **questions beyond the dataset's scope**. To ensure broader coverage, the Math Tutor Agent integrates a **web search pipeline** using the **Model Context Protocol (MCP)** via the **Tavily API**.

4.1 Strategy for Web Search Routing

- The system first checks the KB.
- If **no high-confidence KB match is found** (similarity < 0.75), the query is routed to Web Search.
- Web results are fetched through Tavily's API (an MCP-compliant search tool), which returns curated snippets.
- Results are **sanitized by output guardrails** before being returned.

This ensures the agent can handle **out-of-scope math-related queries** while maintaining alignment with safety and educational constraints.

4.2 Implementation

- **API Used:** Tavily MCP API (can be swapped for Exa or Serper if needed).

- **Integration:** FastAPI endpoint `/ask` automatically calls the web search client when KB fails.
 - **Output Handling:** Extracted snippets are concatenated and presented as references in the final answer.
-

4.3 Example Queries (Web Fallback)

Example 1

- **User Query:** *“Who is Ramanujan?”*
- **Response (Web Search):**
 - Srinivasa Ramanujan (1887–1920) was an Indian mathematician.
 - Known for contributions in number theory, infinite series, continued fractions.
 - Birth anniversary (Dec 22) is observed as **National Mathematics Day** in India.

Example 2

- **User Query:** *“What is the history of the Pythagorean theorem?”*
- **Response (Web Search):**
 - The Pythagorean theorem dates back to ancient Babylon and India.
 - Formalized by the Greek mathematician Pythagoras (6th century BC).
 - Widely used in geometry and trigonometry for right-angled triangles.

Example 3

- **User Query:** *“What are some modern applications of linear algebra in AI?”*
- **Response (Web Search):**
 - Used in neural networks, dimensionality reduction, embeddings, and computer vision.

- Core to techniques like singular value decomposition (SVD) and principal component analysis (PCA).
 - Enables efficient training of deep learning models.
-

4.4 Advantages of MCP-Based Web Search

- **Coverage:** Handles queries not present in GSM8K or future KB datasets.
 - **Flexibility:** MCP setup makes it easy to switch between search providers.
 - **Safety:** Combined with guardrails, ensures irrelevant or unsafe web results are filtered out.
 - **Scalability:** Supports expansion into higher-level math, historical context, or educational enrichment content.
-

5. Human-in-the-Loop Routing

A critical requirement of the Math Tutor Agent is ensuring that the system not only provides answers but also **learns and improves over time**. To achieve this, we integrated a **Human-in-the-Loop (HITL) feedback loop** into the agent's workflow.

5.1 Feedback Mechanism

- After each answer, the user is presented with a **feedback interface** (👍 / 👎).
- Feedback data includes:
 - The original question.
 - The generated answer (from KB or Web).
 - User rating (correct / incorrect).
 - Timestamp.
- Feedback is stored in a **feedback.json** log file for future analysis and retraining.

Example feedback entry:

```
{
  "timestamp": "2025-09-19T16:42:31Z",
  "question": "Tom has 5 apples. Mary has 3 times as many. How many apples does Mary have?",
  "answer": "{ 'source': 'KB', 'solution': 'Mary = 3 × 5 = 15' }",
  "correct": true
}
```

5.2 Workflow Integration

The Human-in-the-Loop feedback mechanism is embedded into the **agent routing workflow**:

1. **Input Guardrail Check** → ensure only math-related queries pass.
2. **KB Search** → return answer if found with high confidence.
3. **Web Search (MCP)** → fallback if KB retrieval fails.

4. **Output Guardrail Check** → sanitize responses for safety.
5. **Answer Returned to User** → delivered via frontend.
6. **Feedback Request** → user evaluates answer (👍 / 👎).
7. **Feedback Storage** → logged for iterative improvement.

This creates a **closed-loop system** where human feedback validates and corrects the agent's behavior.

5.3 Benefits of Human-in-the-Loop

- **Improvement over time:** Feedback can be used to retrain embeddings or fine-tune prompts.
 - **Error detection:** Incorrect or irrelevant answers are flagged by users.
 - **Trust & Transparency:** Users see that their feedback directly contributes to system refinement.
 - **Alignment with educational goals:** Ensures responses meet the standard of clarity and correctness expected from a math tutor.
-

5.4 Future Directions with Feedback

- Use DSPy or reinforcement learning techniques to incorporate feedback into **dynamic reranking** of KB results.
 - Build a **dashboard** for educators to monitor common errors and student struggles.
 - Enable semi-automated **curation of new KB entries** based on user feedback.
-

6. Conclusion

The Human-in-the-Loop Math Tutor Agent demonstrates how **Agentic-RAG architectures** can be applied to create reliable, safe, and educational AI systems. By combining **Knowledge Base retrieval (GSM8K)** with **web search fallback (MCP)**, and layering **guardrails** and **feedback loops**, the system achieves both **accuracy** and **trustworthiness** — two critical pillars for educational AI.

Key achievements include:

- **Knowledge Base Integration:** Ingested GSM8K into Qdrant for fast semantic retrieval of step-by-step math solutions.
- **Web Search Fallback:** Used MCP (Tavily API) to extend coverage for queries outside the KB.
- **Guardrails:** Implemented input filtering and output sanitization to ensure privacy, safety, and alignment with educational goals.
- **Human-in-the-Loop Feedback:** Enabled users to validate answers, providing a foundation for iterative improvement and adaptation.

This work illustrates a practical implementation of an **Agentic-RAG Math Tutor** that behaves like a professor — guiding students through reasoning rather than just giving final answers. It also sets the foundation for future enhancements:

- Expanding the Knowledge Base to include higher-level math (e.g., JEE Bench).
- Incorporating **LangGraph orchestration** for more modular, visualized routing.
- Using feedback data for **dynamic retraining and personalization**.

In conclusion, the project delivers a **feasible and effective AI tutor** that is aligned with the principles of safety, reliability, and human-centered learning. It demonstrates the value of combining **retrieval, guardrails, and human oversight** in building AI systems for education.