A Database-Independent LLM Framework for Real-Time Authorization in Retrieval-Augmented Generation

Halil Yesil[1], Sumeyye Gultekin[2], Fatma Bozyigit[3], Baris Tekin Tezel[1], Moharram Challenger[3]

[1]Dokuz Eylul University, Izmir, Turkey | [2]Cankaya University, Ankara, Turkey

[3]University of Antwerp and Flanders Make, Antwerp, Belgium

Problem

RAG systems face critical security challenges when handling sensitive information:

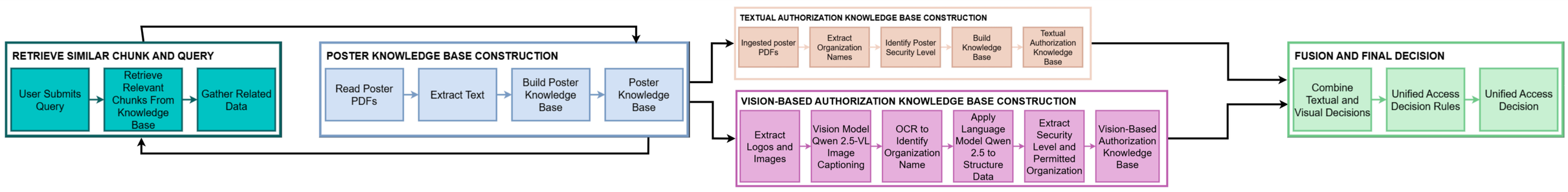
- ✓ Risk of unauthorized data access during retrieval and generation
- ✓ Accidental exposure of confidential documents
- ✓ Current solutions require extensive preprocessing or manual database construction
- ✓ Scalability limitations in enterprise deployments

Our Solution

Database-independent framework with real-time access control

- ✓ No manual database construction required
- ✓ Three specialized knowledge bases for dynamic security
- ✓ Multimodal access control (text + images)
- ✓ Automated email-based organization identification
- ✓ Real-time authorization decisions without preprocessing
- ✓ Scalable deployment for enterprise environments

Methodology



1. Retrieval Phase

User submits query → System retrieves top-5 similar chunks from Poster Knowledge Base using cosine similarity on embeddings

2. Authorization Phase

Extract user org from email → Query text & vision-based authorization KBs → Apply LLM reasoning (qwen2.5:72b) to verify permissions

3. Generation Phase

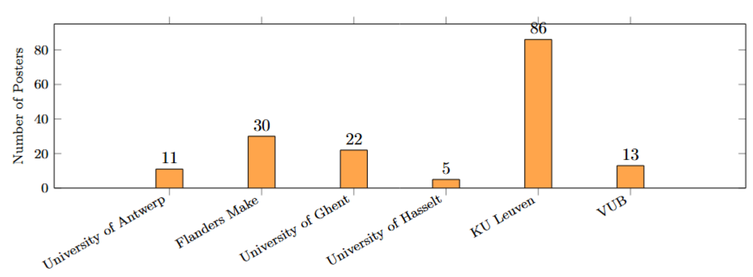
Combine textual and visual access decisions → Unified access control → Generate response only from authorized chunks

System Architecture

1. Query — User submits query → **2. Retrieve** — Top-5 similar chunks via embeddings → **3. Verify** — Dual-layer access control check → **4. Generate** — Answer from authorized docs only

Dataset

167 Research Posters from 6 organizations:



Hybrid Annotation Strategy:

We added organization logos and security level indicators to posters

Security levels: Confidential, Private, Copyright, Public

Formats: Text-only, Image-only, Hybrid indicators

Data Preprocessing:

- Modified raw posters with security classifications (confidential, private, copyright, public)
- Kept some posters with original public status for access level diversity
- Added organization logos and security level indicators as visual elements
- Enables visual identification of ownership and security levels
- Supports both human and automated access control verification

Key Components

Knowledge Base Creation:

- ✓ **Poster Content KB:** Document embeddings using mxbai-embed-large for semantic retrieval
- ✓ **Text Access KB:** Organization-level and security-level permissions extracted from document text
- ✓ **Image Access KB:** Visual logo analysis using qwen2.5vl:72b vision-language model

Knowledge Base Construction Process:

1. **Poster Content KB:** Supports RAG mechanism → Extract text from PDFs → Generate embeddings → Store in vector database → Enable answer generation from relevant pieces matching user queries
2. **Text Access KB:** Two-level access control → Organization-level permissions (based on affiliation) → Security-level permissions (based on document classification)
3. **Image Access KB:** Process visual content with qwen2.5vl:72b → Extract organizational ownership and security classifications

Access Control Process:

1. Extract user organization from email domain
2. Query text & image access control databases
3. qwen2.5:72b analyzes overlap between permissions
4. Generate response only from authorized documents

Results & Performance

Text Access Control	Image Access Control	Combined System
92%	**78%**	**93%**
Accurate extraction and classification from document text	Visual content analysis and logo recognition	Multimodal fusion improves overall accuracy

Multimodal fusion combines text and visual analysis for superior access control performance

Evaluated on	Across
167 Research Posters	**6** Organizations

Key Contributions

- ✓ First database-independent access control framework for RAG systems
- ✓ Novel multimodal security classification combining text and visual analysis
- ✓ Three specialized knowledge bases architecture for dynamic access control
- ✓ Automated organization identification through email domain extraction

Conclusion

- ✓ Achieved 93% overall accuracy combining text (92%) and vision (78%) modalities
- ✓ Successfully evaluated on 167 research posters from 6 organizations
- ✓ Demonstrated scalability and quick deployment capability
- ✓ Eliminates extensive preprocessing while maintaining high accuracy

Impact: Enables secure RAG deployment in sensitive domains (healthcare, legal, finance) where data privacy and access control are critical requirements