

Privacy Enhanced RAG for LLMs in Healthcare

National University of Singapore

Bryan Ha Wai Kit

2025

Abstract

Large Language Models (LLMs) are increasingly utilized in healthcare for tasks such as clinical note summarization and medical report generation. However, their reliance on proprietary and sensitive patient data introduces significant privacy risks, particularly when using Retrieval-Augmented Generation (RAG). This project proposes a privacy-focused framework that leverages synthetic document generation to mitigate these risks while maintaining response accuracy.

The proposed system follows an agent-based approach, incorporating three key agents: a Search Agent, a Synthesis Agent, and a Review Agent. The process begins with the Search Agent retrieving relevant vector-related text nodes from a vector database. The Synthesis Agent then evaluates the extracted content, filtering and retaining only the necessary information for query responses while removing personally identifiable information (PII). Finally, the Review Agent verifies and refines the synthesized document to ensure privacy compliance before passing it to the LLM.

This thesis evaluates the effectiveness of synthetic document generation in mitigating privacy risks while preserving contextual relevance. Through a series of experiments, the system's ability to reduce PII leakage, maintain medical accuracy, and withstand adversarial attacks is assessed. The findings provide insights into balancing privacy and utility in healthcare-focused LLM applications.

Contents

Abstract	i
Contents	ii
List of Figures	iii
List of Tables	iv
1 Introduction	1
1.1 Background	1
1.1.1 Retrieval Augmented Generation	1
2 Literature Review	2
2.1 Background	2
2.1.1 Retrieval-augmented Generation (RAG)	2
2.1.2 Exploitation of RAG Systems	2
2.1.3 Large Language Model (LLM) Safeguards	2
3 Methodology	4
3.1 Proposal	4
3.2 Implementation	4
3.2.1 Medical Anonymisation	4
3.2.2 System Design	5
3.2.3 Building the RAG Corpus	5
3.2.4 Retrieval	7
3.2.5 Synthetic Report Generation	7
3.3 Moving Forward	8
.1 Appendix	11
A Appendix	12
A.0.1 Report Generation Prompt	12
A.0.2 Synthetic Report Generation Prompt	13
A.0.3 Structured Output Prompt	14
A.0.4 Zero-Shot Result	15
A.0.5 Chain-of-Thought Result	16
A.0.6 Structured Output Result	17

List of Figures

2.1	Example of a Conventional RAG system	3
3.1	System Design	5
3.2	FHIR to sentence	6
3.3	Embeddings to Database	6
3.4	Input Query: Which patients have diabetes?	7
3.5	Zero-Shot Generated Summary V.S. Synthesized Summary	8

List of Tables

Chapter 1

Introduction

LLMs are transforming various industries. They are able to perform tasks such as automated handling of workflows with Agentic frameworks, Natural Language Processing (NLP) tasks such as information extraction, and even rudimentary reasoning in some models. In fields like Healthcare, they can automate clinical note generation and summarization, assist in diagnosis, and provide personalized patient care.

However, they all suffer the same traditional issue, hallucinations, where they generate seemingly coherent but incorrect information. To address this, RAG was developed as a method to provide context to LLMs by incorporating an external knowledge base, allowing them to generate more accurate domain-specific responses. This technique has applications in areas where hallucinations can cause severe harm, such as medicine, legal analysis, and cybersecurity.

While RAG enhances LLM capabilities, it introduces new security risks. Attackers can exploit RAG systems to extract proprietary or sensitive data through prompt injection attacks. This is a critical privacy concern, especially in healthcare where patient confidentiality is important.

In this project, we seek to test and develop an Agent-based synthetic document generation framework to mitigate these risks. By separating the RAG database from the externally facing LLM, we seek to enhance security while preserving the contextual accuracy of responses.

In chapter 1 we describe the workings of a RAG system, as well as the principles behind Medical Anonymization and its methods.

1.1 Background

1.1.1 Retrieval Augmented Generation

Chapter 2

Literature Review

2.1 Background

2.1.1 Retrieval-augmented Generation (RAG)

Retrieval-augmented generation (RAG), first introduced by [1], is a method used to enhance the text generation abilities of LLMs.

It is seeing increased usage in multiple LLM-applications, such as medical chat-bots [2], as well as systems for detecting vulnerabilities in code [3].

The widespread adoption of RAG is due to its flexibility; A pre-trained model can be made to function in different domains simply by making adjustments to its RAG components, bypassing the need for extensive re-training.

Furthermore, numerous advancements are being made in enhancing the capabilities of RAGs, such as advanced techniques that improve retrieval qualities, or modular architectures that allow for specific fine-tuning of RAG components [4].

2.1.2 Exploitation of RAG Systems

Studies ([5]; [6]; [7]) have shown that RAG systems are susceptible to well-crafted prompt attacks during the retrieval stage.


By using targeted as well as untargeted attacks [6], a malicious attacker is able to retrieve personally identifiable information (PII), such as phone numbers and addresses, from a RAG's corpus.

[5] and [7] showcase the ability to affect an LLMs output by inserting specially crafted adversarial passages into its RAG corpus.

This typically affects LLMs that make use of real-time context databases, such as a search engine, which allows an attacker to insert malicious documents into the context database.

2.1.3 Large Language Model (LLM) Safeguards

The widespread usage of LLMs necessitates the development of safeguards to prevent ethical misuse and abuse. These safeguards are often times complex, varying based on application requirements.



`./images/Conventional RAG example.png`

Figure 2.1: Example of a Conventional RAG system

[8] discusses the different components involved in implementing guard rails for LLMs and touches on some of the currently deployed solutions available. In general, safeguards are designed to prevent the LLMs from generating unintended output. This unintended output can be generated in numerous ways, most notably through “hallucinations” as well as targeted prompt attacks known as “jailbreaking”.

Chapter 3

Methodology

3.1 Proposal

Based on research into RAG vulnerabilities, there is a clear lack of security measures designed to preserve the privacy of a RAG corpus. This is especially important in fields like healthcare. As demonstrated in [6], private information can be easily extracted by determined attackers through simple prompt injections. Given that RAG relies on a set of documents as context, and that this is vulnerable to attacks, I suggest generating synthetic context from this set of documents. This set of documents could refer to a patient's records, containing information such as their blood pressure, etc. A separate LLM will analyze the set of records retrieved by the user's query, comparing the two and extracting relevant information. The LLM will then generate a synthetic record containing all the information needed to answer the query, whilst removing PII at the same time. This separates the context given to the LLM from the RAG corpus, whilst still ensuring that its response remains contextually relevant.


3.2 Implementation

To design an adequate system that can preserve a patient's privacy, we must first understand the different types of methods associated with this task.

3.2.1 Medical Anonymisation

According to [9], the three main methods in preserving medical privacy are Pseudonymisation, De-identification and Anonymisation. Pseudonymisation refers to the replacement of attributes with pseudonyms. De-identification refers to the removal of PII from patient records. Anonymisation refers to the distortion of data such that any record lacks individuality.

The method we will be focusing on is the process of anonymisation. There are two different ways this is achieved. Recalculation, which involves turning absolute dates into relative representations (such as turning a patient's date of birth into their equivalent age representation), and Perturbation, which involves directly modifying a patient's medical records away from their original form.



./images/Synthesis LLM RAG example.png

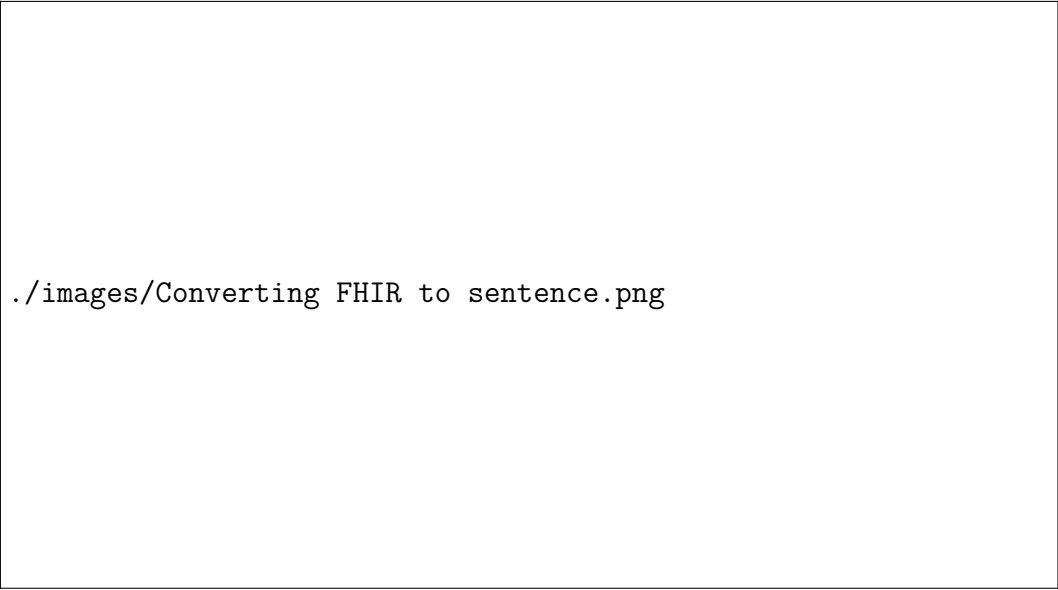
Figure 3.1: System Design

3.2.2 System Design

The proposed system design is outlined in figure 3.1. The system is similar to figure 2.1, with the inclusion of an intermediary step that passes both the user query as well as the retrieved context documents to a secondary LLM for synthesis. The secondary LLM is responsible for both information extraction as well as synthetic document generation. To mimic privacy requirements, a locally run LLM is used here to ensure that the RAG corpus remains air-gapped. The use of an adequately sized LLM is critical here, and in our case we will be using Mistral’s Nemo-12B. The synthesized document is then returned to the front-facing LLM along with the user’s query to generate an appropriate response.

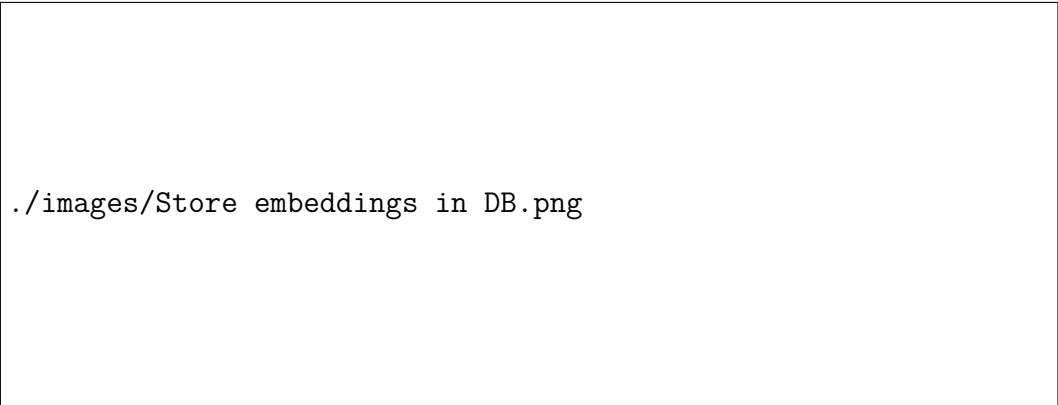
3.2.3 Building the RAG Corpus

RAG systems can make use of either structured or unstructured data. For our case, we will be making use of a synthetic FHIR dataset, generated by Synthea [10]. FHIR is a structured healthcare standard that defines how healthcare information can be shared between different systems regardless of how they are stored. Individual FHIR patient records are stored in what is known as resources. A resource can take on



```
./images/Converting FHIR to sentence.png
```

Figure 3.2: FHIR to sentence



```
./images/Store embeddings in DB.png
```

Figure 3.3: Embeddings to Database

different types, and each type contains information necessary for its specific use case. FHIR records can appear in the form of JSON, XML or RDF. Here we will be making use of JSON FHIR files to create our RAG corpus.

Firstly, we convert FHIR resources to basic sentences. This is to avoid repeatedly embedding the same key-value token pairs and wasting embedding tokens. Refer to figure 3.2 for an example. This can be further truncated. For example we can simply embed only the name of the reading and its associated value.

We perform this operation on the patient's record, extracting Observations and Procedures, separating them by date, and extracting a patient's diagnosed conditions, medications, as well as allergies, and storing them in a separate document. These documents are then converted into vectors through the use of a text-embedding model. For this, we will be using the *bge-base-en* embedding model. The embeddings are then stored in a Postgres database utilizing the *pgvector* extension.

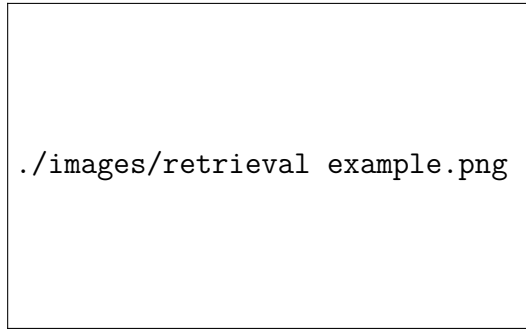


Figure 3.4: Input Query: Which patients have diabetes?

3.2.4 Retrieval

With the RAG corpus built, we can now move onto retrieving documents associated with a query. The query goes through the embedding process and its resulting vector is compared to other document vectors in the database. The top k results are returned, with k being an adjustable variable. What determines the chunk's relevance is its cosine similarity to the input query. Cosine similarity is defined as the following:

$$\text{Cosine Similarity} = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|}$$

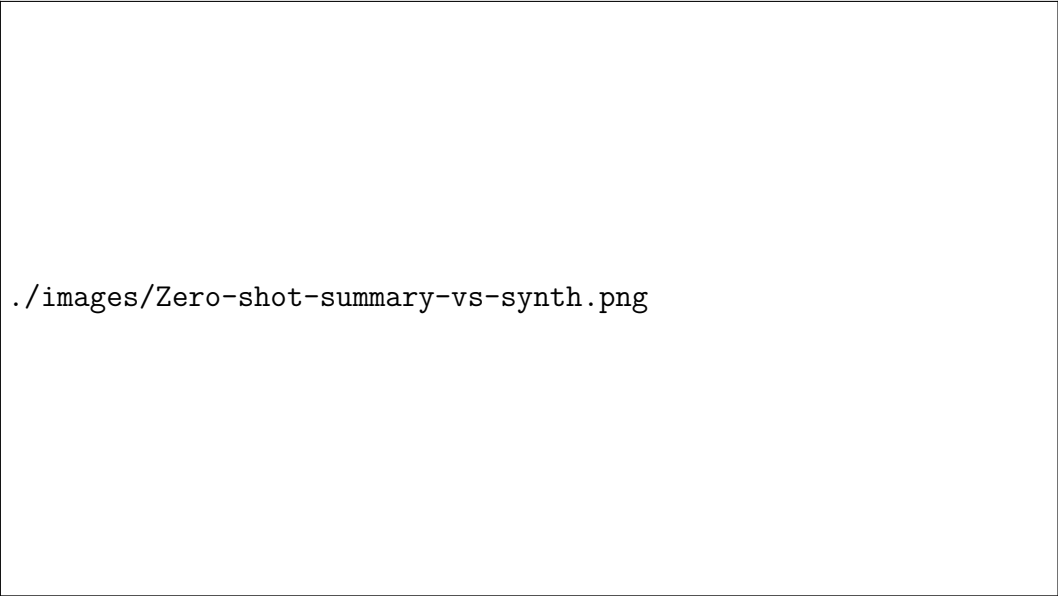
and returns a score between 0.0 to 1.0. Here we can set a minimum cut-off for cosine similarity to adjust the relevance of returned information. Refer to figure 3.4 for an example of the returned chunks.

3.2.5 Synthetic Report Generation

LLMs differ in capabilities in accordance to their size. To determine if the chosen LLM (Mistral Nemo 12B) was sufficient for what I needed it to do, I tested its summarization and generation abilities. Firstly, I merged the previously processed FHIR record for a single patient into a combined document. This document was then passed to LLM along with a set of instructions. The specific prompt provided to the LLM is in the appendix, but to summarize:

- Break the summary into clear sections with headers
- Include exact numerical values
- Use precise dates
- Report conditions with specific terminology
- Summarize readings into a range spanning from min-max

The generated report summary was then passed to the LLM with instructions to anonymize information by rounding values as well as removing ages, dates, and names. This was done for three different types of prompting strategies, Zero-Shot, Chain-of-Thought, and Structured Output.



`./images/Zero-shot-summary-vs-synth.png`

Figure 3.5: Zero-Shot Generated Summary V.S. Synthesized Summary

Refer to figure 3.5 for a side-by-side comparison for Zero-Shot generation. Full results for each are present in the appendix. Overall, the LLM was effective in following instructions as well as working with a large amount of context.

3.3 Moving Forward

With the RAG corpus built, and the abilities of the LLM confirmed, the next steps are as follows:

- Evaluate LLM’s ability to extract relevant information from retrieved chunks
- Create a pipeline that connects the retrieval, synthesis and inference stages
- Compare LLM’s responses when presented with the original and synthesized information
- Test the system through prompt attacks (information-query attacks)

References

- [1] Patrick Lewis et al. *Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks*. 2021. arXiv: 2005.11401 [cs.CL]. URL: <https://arxiv.org/abs/2005.11401> (cit. on p. 2).
- [2] Mingyu Jin et al. *Health-LLM: Personalized Retrieval-Augmented Disease Prediction System*. 2024. arXiv: 2402.00746 [cs.CL]. URL: <https://arxiv.org/abs/2402.00746> (cit. on p. 2).
- [3] Xueying Du et al. *Vul-RAG: Enhancing LLM-based Vulnerability Detection via Knowledge-level RAG*. 2024. arXiv: 2406.11147 [cs.SE]. URL: <https://arxiv.org/abs/2406.11147> (cit. on p. 2).
- [4] Yunfan Gao et al. *Retrieval-Augmented Generation for Large Language Models: A Survey*. 2024. arXiv: 2312.10997 [cs.CL]. URL: <https://arxiv.org/abs/2312.10997> (cit. on p. 2).
- [5] Zhen Tan et al. "Glue pizza and eat rocks" – Exploiting Vulnerabilities in Retrieval-Augmented Generative Models. 2024. arXiv: 2406.19417 [cs.CR]. URL: <https://arxiv.org/abs/2406.19417> (cit. on p. 2).
- [6] Shenglai Zeng et al. *The Good and The Bad: Exploring Privacy Issues in Retrieval-Augmented Generation (RAG)*. 2024. arXiv: 2402.16893 [cs.CR]. URL: <https://arxiv.org/abs/2402.16893> (cit. on pp. 2, 4).
- [7] Jiaqi Xue et al. *BadRAG: Identifying Vulnerabilities in Retrieval Augmented Generation of Large Language Models*. 2024. arXiv: 2406.00083 [cs.CR]. URL: <https://arxiv.org/abs/2406.00083> (cit. on p. 2).
- [8] Yi Dong et al. *Building Guardrails for Large Language Models*. 2024. arXiv: 2402.01822 [cs.CL]. URL: <https://arxiv.org/abs/2402.01822> (cit. on p. 3).
- [9] Aryelly Rodriguez et al. "Current recommendations/practices for anonymising data from clinical trials in order to make it available for sharing: A scoping review". In: *Clinical Trials* 19.4 (June 2022), pp. 452–463. DOI: 10.1177/17407745221087469 (cit. on p. 4).
- [10] Corporation MITRE. *Synthea*. 2024. URL: <https://synthetichealth.github.io/synthea/> (visited on 11/29/2024) (cit. on p. 5).
- [11] John Chong Min Tan et al. *TaskGen: A Task-Based, Memory-Infused Agentic Framework using StrictJSON*. 2024. arXiv: 2407.15734 [cs.AI]. URL: <https://arxiv.org/abs/2407.15734>.

- [12] Meenatchi Sundaram Muthu Selva Annamalai, Andrea Gadotti, and Luc Rocher. *A Linear Reconstruction Approach for Attribute Inference Attacks against Synthetic Data*. 2024. arXiv: 2301.10053 [cs.LG]. URL: <https://arxiv.org/abs/2301.10053>.

.1 Appendix

Appendix A

Appendix

A.0.1 Report Generation Prompt

A.0.2 Synthetic Report Generation Prompt

A.0.3 Structured Output Prompt

A.0.4 Zero-Shot Result

A.0.5 Chain-of-Thought Result

A.0.6 Structured Output Result