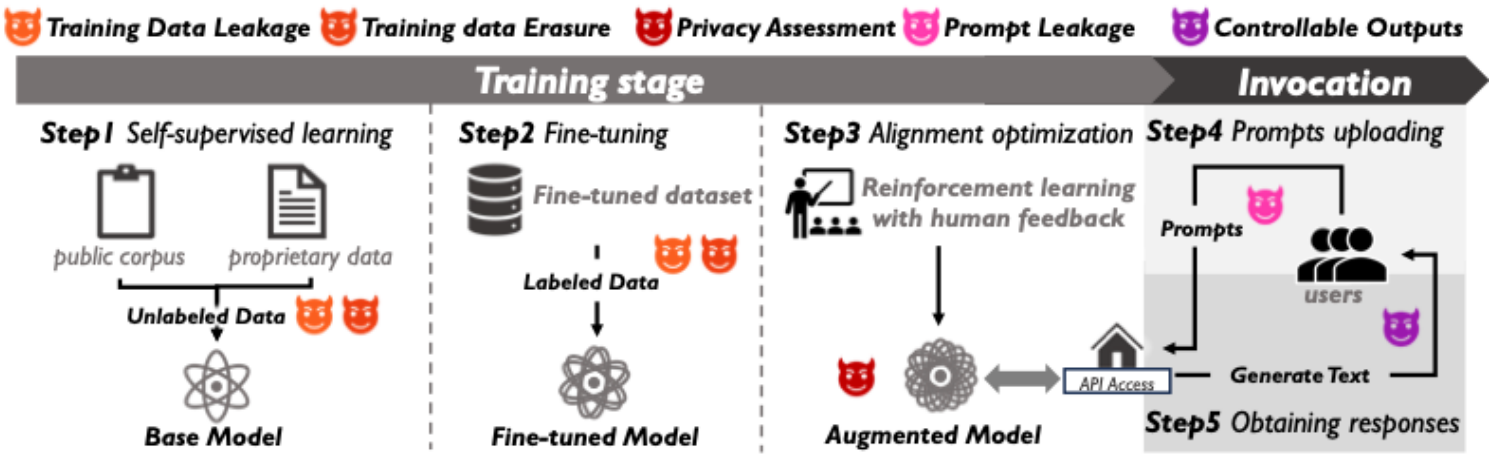
Privacy Dilemmas and Opportunities in Large Language Models: A Brief Review

Hongyi LI, Jiawei YE, Jie WU

Frontiers of Computer Science, DOI: 10.1007/s11704-024-40583-8

Problems & Investigation

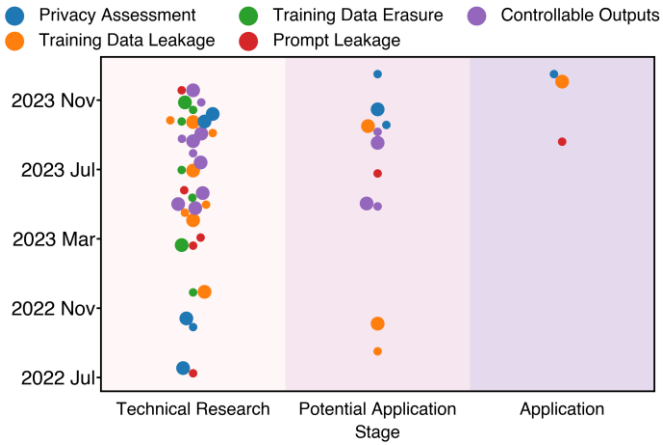
- Problems of LLM privacy:
  - LLMs face significant privacy risks, making privacy research essential.
  - Existing surveys explore LLM security while often overlooking specific attention to privacy.
- Investigation: A comprehensive exploration of LLM privacy issues related to text-sensitive information.
  - A detailed analysis of five privacy issues and solutions in LLM training and invocation.
  - Delving into three privacy-centric research focuses in LLM application that are not mentioned previously.



LLM Process and Privacy Issues.

Analysis & Outlooks

- **Technology Maturity Analysis:**
  - Current LLM privacy research is still in a technical exploration phase, with a certain gap from practical application.
- **Outlooks:**
  - Five potential research directions for further LLM privacy research;
  - Three innovative prospects for LLM native security mechanisms.



Distribution of Surveyed Research. The abscissa represents the research stages, the ordinate represents the research publication time, and the point size represents attention.

Further Research Directions

- ***Diverse Scalability***
  - *Multi-form Sensitive Information Protection*
  - *Multi-granularity Privacy Assessment*
  - *Multi-dimensional Task Prompt Protection*
- ***Cross-domain Generalizability***
  - *Applicability of Methods*
  - *Generalizability of Methods*
- ***Privacy-preserving Robustness***
  - *Privacy-Utility Tradeoff in LLMs*
  - *Designing Effective Privacy-Preserving Methods*
- ***Collaborative Security***
  - *Access Management and Data Traceability*
  - *Collaboration privacy-preserving techniques*
- ***Multimodal Impact***
  - *Multimodal inputs' impact on LLM privacy*

Native Security Insights

Privacy Boundary Framework

↓

Authentication Framework

↓

Data Security Isolation Framework