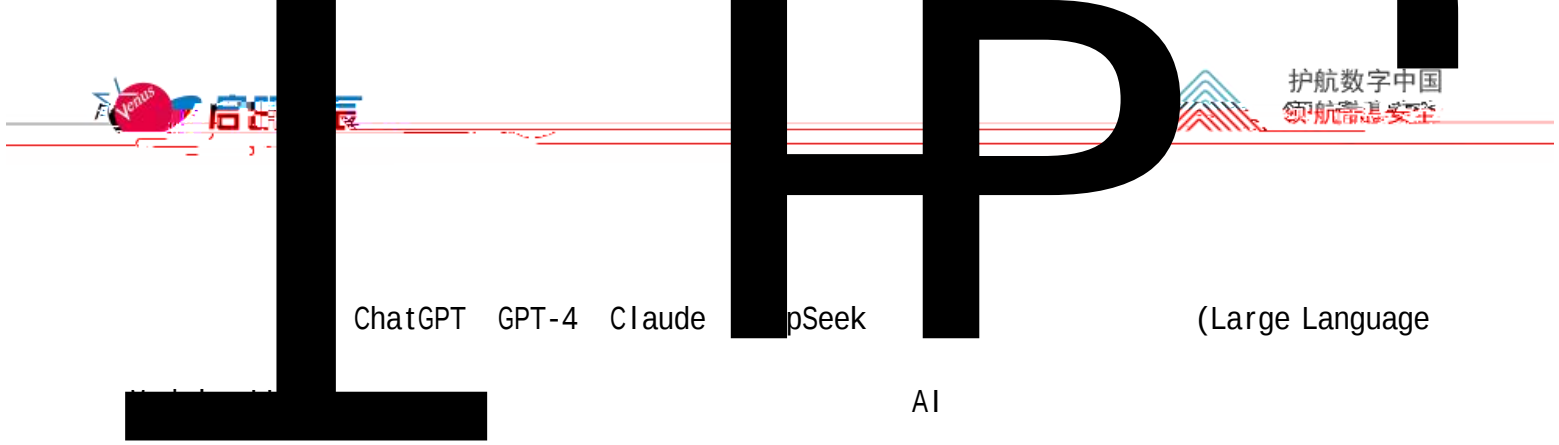




n Pts

2003

j Y 5

TensorFlow PyTorch Numpy

●

API

API

Ollama

“

” “ ”

APP

DeepSeek APP

APP

2.2

●

“ ”

2.3

2.4

AI

AI

AI

Web

(

XSS)

AI

(

AI

)

AI

AI

AI

AI

- Web

Web

API

XSS

SQL

CSRF

API

- API

●

AI

AI-R-IAM

AI

AI Identity

Non-Human Identity, NHI

RAG

IAM

RAG

API

API

(

)

IAM

- 1 AI AI-R-IAM . 2025 2 .
- 2 AI Demon AI Security Handbook 2025 5 .
- 3 DeepSeek . 2025 4 .
- 4 OWASP Top 10: LLM & Generative AI Security Risks <https://genai.owasp.org>.

EU AI ACT

2024

5 8 2025 2

AI AI

AI AI

- ISO/IEC 42001 ()

ISO IEC AI

AIMS

AI AI

- IEEE AI (IEEE AI Ethics Guidelines)

IEEE AI

- /

“ ”

“ ”

2023 8

1.0 2024 9

4

2.

AI

- OWASP Top 10 for LLM Applications 2025

Web

0 ğ "

- MIT AI Risk Repository

Google DeepMind

FSF Frontier Safety Framework

DeepMind

AI

SAI

FSF

● OpenAI AI

OpenAI LLM AI

“OpenAI Safety Framework”

AI

I

I

ES # A

91 H9)

6

88 (88) 71