CREATING AN AI ASSISTANT

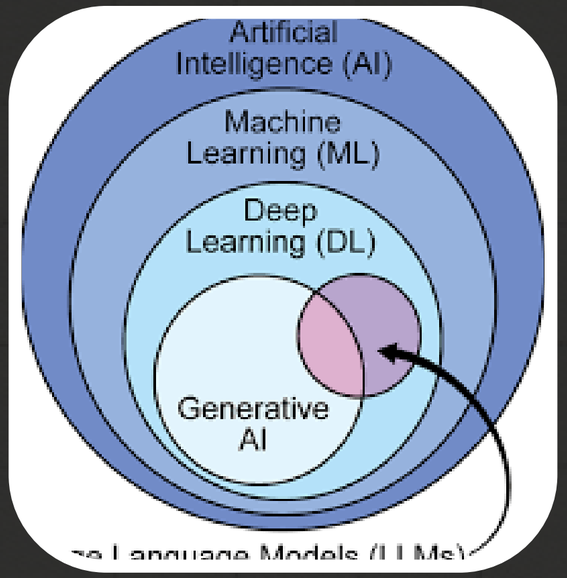
By Roheender Singh Sahota

$whoami

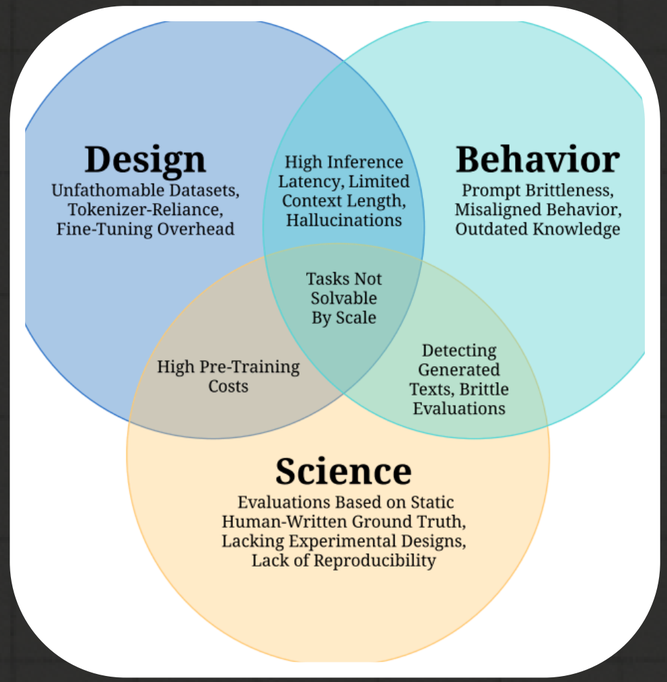
- NAME: ROHEENDER SINGH SAHOTA😃
- STUDENT AT APU(ASIA PACIFIC UNIVERSITY)
- ACTIVE CTF PLAYER
- SECURITY RESEARCHER
- DIRECTOR OF CTF CHALLEMGE CREATOR AT APU

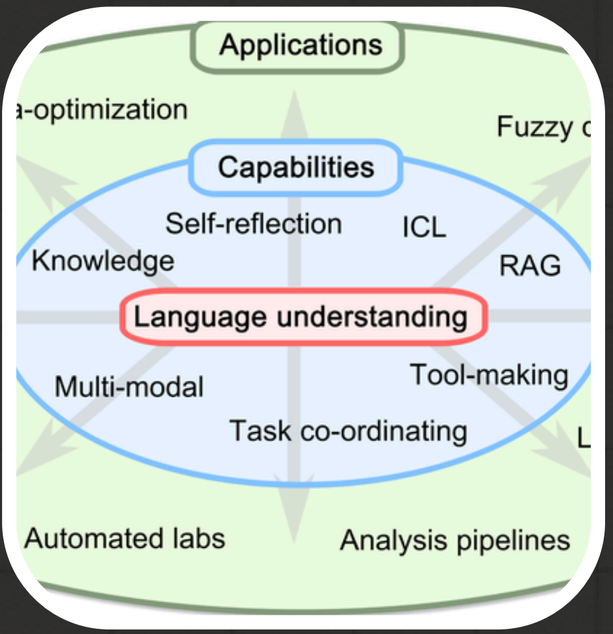
TODAY'S AGENDA

- Introduction
- About me
- What are LLM
- What will we build
- Tech Stack
- Demo
- Application
- Conclusion



WHAT ARE LLM





- LLM are algorithms that are equipped to summarize, predict, understand and generate text

- Broad field focused on creating systems that perform tasks requiring human intelligence. Example: self-driving cars, facial expression.

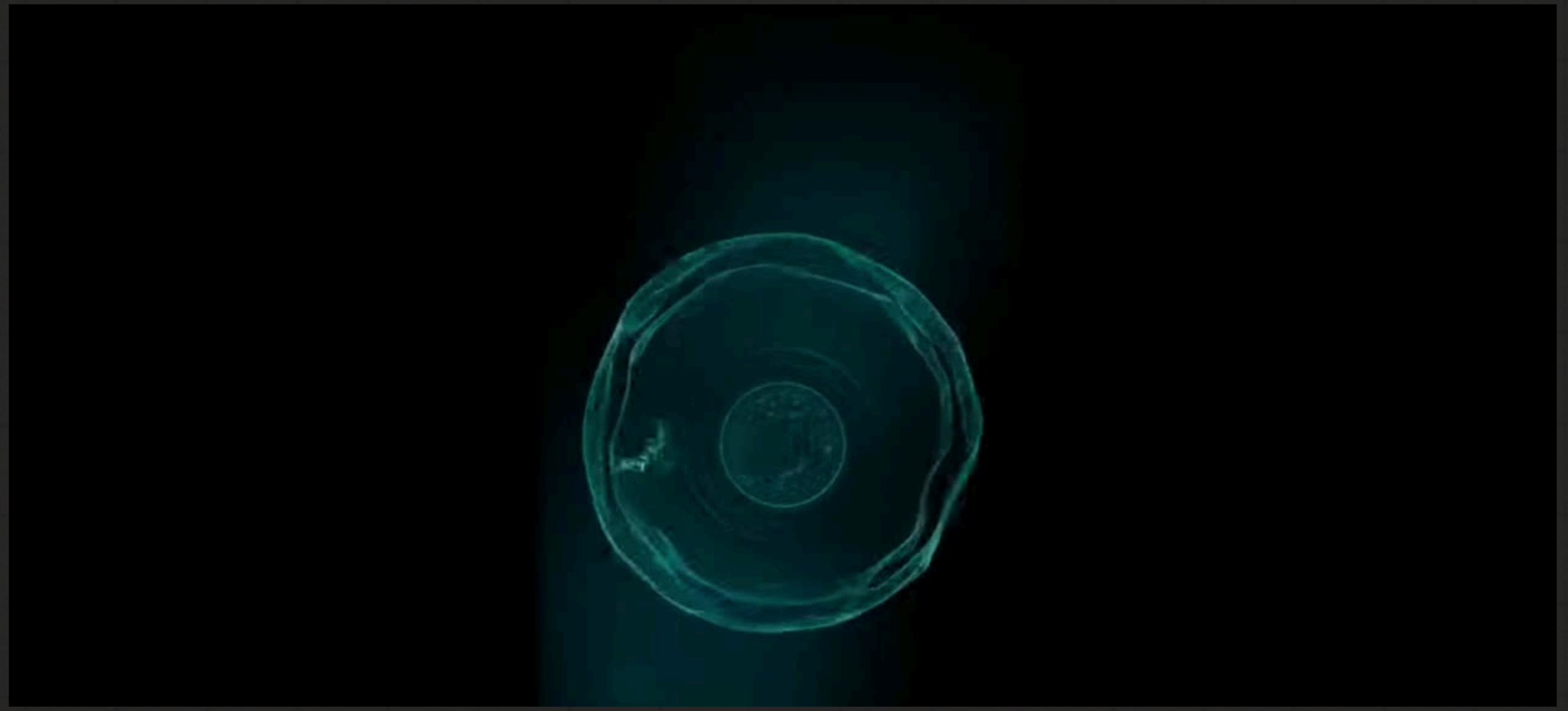
Capabilities of LLM:

- **Text Generation**
- **Language Translation**
- **Summarizing text**
- **Generating code**

Limitations of LLM:

- **Biased**
- **Ethical Concerns (Can be Bypassed)**
- **Hallucination**
- **Data Quality**

WHAT WE WILL BE BUILDING 🧨



TECH STACK

Python

LM Studio

Open Interpreter


DEMO WEEEEE

PROJECT APPLICATION

- Be used to create self replicating malware. 🦠🪰
- Can bypass AV 👨‍💻
- Can be used as a C2 💀

CONCLUSIONS

Connect with me😀

THANK YOU!