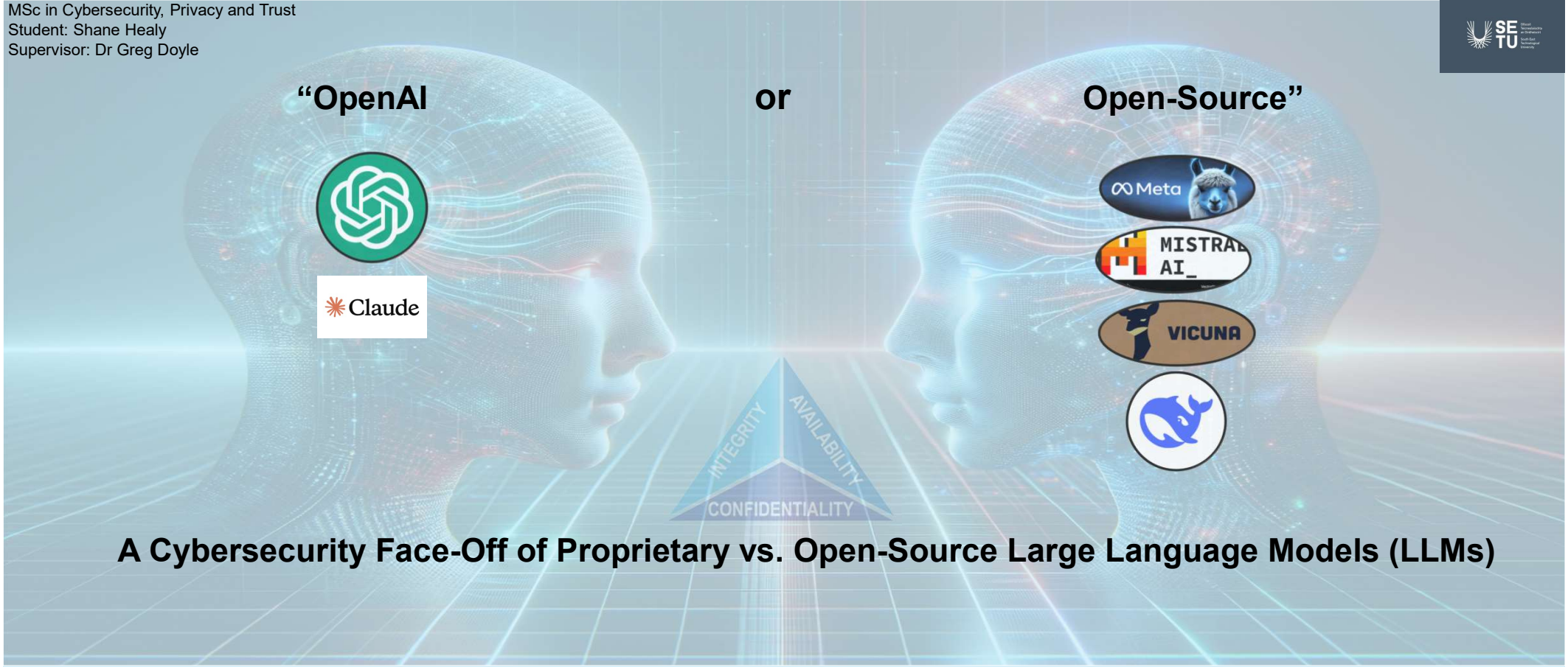
MSc in Cybersecurity, Privacy and Trust
Student: Shane Healy
Supervisor: Dr Greg Doyle



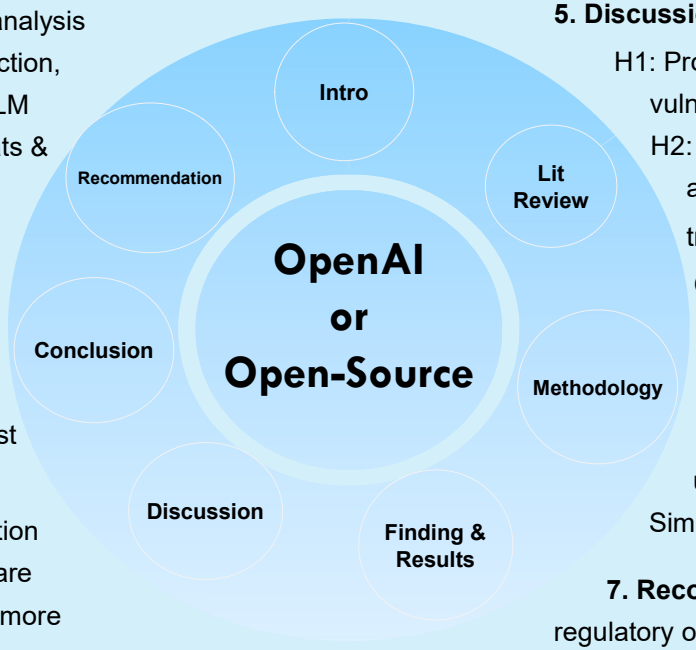
A Cybersecurity Face-Off of Proprietary vs. Open-Source Large Language Models (LLMs)

1. Introduction: A cybersecurity experimental comparative analysis of proprietary vs. open-source LLMs focusing on prompt injection, data privacy/leakage and insecure output handling. Which LLM type is more secure & less susceptible to cybersecurity threats & vulnerabilities .

2. Literature Review: 50+ papers/journal articles reviewed. Gaps in literature - anecdotal evidence lacking validation, applications & LLMs lack real-world testing.

3. Methodology: Mixed method - 75% quantitative (experimental analysis), 25% qualitative (fairness, safety, trust & ethics).

4. Findings & Results: Early indicators show higher evaluation scoring of proprietary vs. open-source LLMs. Ethical issues are evident in proprietary LLMs whereas open-source LLMs are more transparent.



5. Discussion: Initial findings align to hypothesis H1 & H2.

H1: Proprietary Large Language Models (LLMs) have less vulnerabilities and are more resilient to cybersecurity threats...

H2: Open-Source Large Language Models (LLMs) offer more adaptability, public availability and community-driven transparency…..

Consider industry driven LLM testing aligned to governance & regulatory standards.

6. Conclusion: Commercialised and well resourced proprietary LLMs are more secure & suited to general users. Open-source suited to more specific communities. Similar analogy: Are you a Linux or Windows/Mac user?

7. Recommendation: Learn, upskill, test, consider ethical and regulatory obligations, Consider your LLM "use-case".