Arun Ragavendhar
Software Developer, AI and Cybersecurity Enthusiast
Melbourne, VIC
+61 0410692290
arunragavendhar.1999@gmail.com

4 June 2025

Dr. Shigang Liu
Distributed Systems Security Team
CSIRO Data61
Clayton, VIC

Dear Dr. Liu,

I have always been the kind of person who wants to know how things work under the hood, someone who keeps asking "why" and "how." That curiosity is what pulled me into programming in the first place. Over time, I realised I am most interested in problems that sit right at the edge of software, AI, and security, especially when a system looks fine on the outside but behaves unexpectedly underneath. That is exactly why this internship on LLM prompt injection stood out to me. It is not just a technical challenge; it is the kind of problem I naturally think about and would genuinely enjoy working on.

At Swinburne, I have been focusing on projects that combine AI and security. One that stands out is **CyberShield AI**, a full-stack malware detection system I built using a hybrid AI model, an Autoencoder to detect anomalies and a Random Forest to classify malware types (if malware is found). I trained both models, cleaned and structured the dataset, built the backend using Flask APIs and MySQL, and integrated it with a Vue.js frontend. The system includes features like scan logs, admin retraining, anomaly scoring, and even a future risk predictor. That project taught me how models behave with noisy or unexpected input, which I now understand is a key part of LLM alignment and failure detection.

In another project for my Internet Security unit, I conducted a **deep memory forensic analysis** of a simulated ransomware attack based on APT38. I used Volatility 3 to analyse the memory dump. The attack involved Defender bypass through PowerShell, SYSTEM-level execution, and a batch script that ran in-memory hundreds of times without ever being saved on disk. I learnt how to spot failure patterns, look beyond surface logs, and think like both an attacker and a defender. That experience helped me understand how attackers hide traces and how systems behave in ways we might not always expect.

That is why this internship caught my eye. CSIRO's focus on identifying unintended LLM behaviours such as deception, policy bypass, and context failures, and building a real

dataset around them is exactly the kind of work I want to do. I love the idea of being in a team that is focused on doing this seriously, carefully, and transparently. I also respect how CSIRO supports open science and mentorship. I value that kind of space where people ask questions, test ideas, and improve together as a team.

I believe I can bring not just skills, but also energy and curiosity to this role. I ask when I do not know, I explore until I find answers, and I genuinely enjoy working with people who care about building safe and reliable systems.

I have also adapted quickly to the Australian academic and workplace culture and value the openness and innovation it encourages. I am confident that I can communicate clearly, work effectively in team settings, and contribute positively to the goals of any organisation I am placed with. I am proficient in tools like MS Teams, GitHub, and Zoom, and I am comfortable managing project tasks under deadlines.

Thank you for taking the time to read my application. I have attached my resume and academic transcript. I would be happy to talk further if selected.

Warm regards,
Arun Ragavendhar