EDITH COWAN UNIVERSITY

PROJECT DETAILS

Project Title:

Detecting and Mitigating Emerging Threats of Agentic AI in Australian SMEs.

Project Summary:

This project investigates the emerging threats introduced by Agentic AI systems within Australian Small and Medium Enterprises (SMEs). As autonomous AI agents increasingly perform decision-making, workflow automation, system orchestration and optimization, they may introduce novel threats including goal misalignment, data leakage, adversarial manipulation, tools misuse and cascading operational risks. The project aims to design a Trustworthy Agentic AI Security Framework integrating threat modelling, behavioural monitoring, explainability, and human-in-the-loop oversight. Through real-world SME case studies, prototype development, and risk validation, the research will deliver secure-by-design guidelines and mitigation strategies, strengthen Australia's SME cyber resilience while enabling safe AI-driven innovation and economic growth.

Preferred Applicant Skillset:

The preferred HDR applicant should have a background in AI and the concept of autonomous system. Demonstrated knowledge of machine learning, data analytics, or LLM-based systems is essential. Familiarity with cybersecurity concepts, e.g., threat modelling, adversarial attacks, risk assessment, will be advantageous. The candidate should possess programming skills in Python and relevant AI tools. An interest in trustworthy, explainable, and ethical AI, along with the ability to work collaboratively with industry and SMEs, is highly valued.

Internship Opportunity:

The candidate will have the opportunity to undertake an industry-based internship with an Australian SME or cybersecurity partner organisation. The internship will focus on applying the proposed Agentic AI risk detection and mitigation framework in real-world SME environments. The candidate will engage in threat modelling, AI risk assessment, secure system design, and validation of explainable and human-in-the-loop mechanisms. This experience will provide practical exposure to SME security challenges, strengthen industry collaboration, and enhance translational research impact while supporting career development in responsible AI deployment.

Primary Contact:

Dr. Iqbal Sarker.

m.sarker@ecu.edu.au

+61 480 474 508