IFN712 Research Project Form

(Submitted to y.feng@qut.edu.au by 30 June 2025)

Project agency (School, industry, funded/HDR)	HDR Project
Industry/project supervisor and contact emails	N/A
Academic Supervisor name(s) and contact emails	Prof. Raja Jurdak (r.jurdak@qut.edu.au) Dr. Gowri Ramachandran (g.ramachandran@qut.edu.au) Dr. Chadni Islam (c.islam@ecu.edu.au)
Information Technology major(s)	Cybersecurity, Software Engineering, Computer Science, Data Science
Project title	Deep Learning-based Explainable Malicious Package Detection System for Next-Gen Software Supply Chain
Brief description of the research problem, aims, method and expected outputs (100~200 words)	**Background:** Modern software development relies heavily on third-party packages from open repositories like PyPI. This has opened new attack surfaces, where malicious actors inject harmful behavior into packages that execute once deployed. Static analysis often fails to detect such threats due to obfuscation or dynamic execution techniques. Dynamic analysis provides execution-level insight into real package behavior. However, interpreting these complex traces manually or with rule-based systems is slow and error-prone. This project uses dynamic analysis traces and deep learning (DL) to detect and explain malicious behavior in Python packages with greater accuracy and interpretability. Unlike traditional ML models, which struggle with high-dimensional data, DL excels at learning patterns directly from raw, temporal data such as system call traces, making it a more robust and scalable solution. **Objectives:** • Model design: Use DL models to process traces and detect malicious packages. • Explainability integration: Apply techniques like attention visualization or SHAP to highlight which parts of the trace influenced classification. • Framework development: Build an automated framework that ingests trace files, performs preprocessing, and outputs threat predictions with explanations. • Evaluation: Benchmark model performance on the dynamic dataset using precision, recall, F1-score, and explanation fidelity. • Scalability testing: Assess the system's ability to generalize across unseen malicious behaviors and new package variants. **Expected Outcomes:** This project will produce a working prototype that accepts dynamic behavior traces as input and returns explainable malicious/benign classifications. With an emphasis on model transparency and real-world applicability, the system will support security analysts in understanding model decisions and identifying high-risk packages. The findings will demonstrate the suitability of DL for behavioral malware detection and offer insights for integrating such tools into CI/CD pipelines or repository vetting systems.
Key words (4-6)	• Malicious Package Detection • Software Supply Chain • PyPI Ecosystem

	• Dynamic Analysis • Security and Privacy
Answerable research questions for 3-5 students (desirable)	• How effectively can deep learning models detect malicious Python packages based solely on dynamic runtime behavior? • Which patterns in dynamic behavior are most indicative of malicious activity in Python packages? • How can explainable AI techniques help interpret and justify deep learning decisions in the context of security threat detection? • How generalizable is the trained detection model across unseen packages or evasion techniques not present in the training dataset?
4-5 key references (desirable) and website resources	1) Mehedi, S.T., Jurdak, R., Islam, C., & Ramachandran, G. QUT-DV25: A Dataset for Dynamic Analysis of Next-Gen Software Supply Chain Attacks. arXiv preprint arXiv:2505.13804 (2025). https://doi.org/10.48550/arXiv.2505.13804 2) Mehedi, S.T., Islam, C., Ramachandran, G., & Jurdak, R. DySec: A Machine Learning-based Dynamic Analysis for Detecting Malicious Packages in PyPI Ecosystem. arXiv preprint arXiv:2503.00324 (2025). https://doi.org/10.48550/arXiv.2503.00324 3) Black Duck Software. 2025 Open Source Security and Risk Analysis (OSSRA) Report. Synopsys, 2025. https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf 4) Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K. Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks. Sensors 2021, 21, 4736. https://doi.org/10.3390/s21144736 5) Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K. Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks. IEEE Access 2022, 10, 123456–123467. https://doi.org/10.1109/ACCESS.2022.1234567
Required major of studies, desirable skill sets, knowledge, and speciality	**Required Skills** • Solid Python programming skills. • Basic understanding of the Python/PyPI ecosystem and software supply chain risks. • Familiarity with Linux and working in command-line environments. **Desirable Skills** • Interest in cybersecurity and common attack techniques in open-source packages. • Experience with sandboxing or monitoring tools (e.g., eBPF). • Basic knowledge of machine learning or deep learning. • Curiosity about explainable AI methods (e.g., SHAP, LIME). • Strong interest in analyzing and interpreting model behavior and results.
Industry-based project: Student IP Agreement. This is the IP model agreed between the parties. Please note that it is QUT policy that where possible students should be allowed to keep their IP. If students	☐ Project IP vests in the student with a license back to the Industry Partner **(licence)** OR ☒ Project IP vests in the Industry Partner/Project owner with a licence back to the student **(assignment)** OR

are asked to assign their work, then please **provide a brief rationale** as additional permissions are needed by QUT to approve.	☐ Academic project (No IP agreement needed)
Number of students (4-5)	5
The message from the supervisor(s) about the acceptance for this project	
Student name(s) (Print your name and submit this form by the end of Week 2)	
Date	
Remarks on conditions of offer	This research is conducted as part of an HDR project. Participating students will be required to sign an Intellectual Property (IP) agreement with the QUT project owners. The supervising team will shortlist candidates following the application process.