IFN712 Research Project Form

(Please submit to [y.feng@qut.edu.au](mailto:y.feng@qut.edu.au) by 30 June 2025)

|  |  |
| --- | --- |
| Project agency (School, industry, funded/HDR) | School of computer science, Datellite Pty Ltd |
| Industry/project supervisor and contact emails | Datellite pty ltd/ Khurram Malik  malik@datellite.org |
| Academic Supervisor name(s) and contact emails | Dr Bhargavi Goswami  bhargavi.goswami@qut.edu.au |
| Information Technology major(s) | Computer Science, Data Science, Software Development |
| Project title | Zero-Day Attack Detection Using Machine Learning Methods |
| Brief description of the research problem, aims, method and expected outputs (100~200 words) | Zero-day attacks exploit unknown vulnerabilities and often bypass traditional rule-based security mechanisms, making them difficult to detect using signature-based methods. This project aims to develop a machine learning-based approach to detect zero-day cyberattacks by identifying anomalous patterns in network behavior. Using public datasets containing both normal and known attack traffic, the project will train unsupervised and semi-supervised machine learning models capable of learning normal behavior and flagging deviations. Techniques such as Isolation Forest, One-Class SVM, and Autoencoder-based models will be explored. Data preprocessing will include normalization, dimensionality reduction, and feature engineering. The performance of selected models will be evaluated using metrics like precision, recall, and F1-score, with a specific focus on their ability to detect previously unseen attack types. Expected outcomes include a functional detection model, a comprehensive performance report, and practical recommendations for improving early threat detection in real-world environments. |
| Key words (4-6) | Zero-Day Detection, Anomaly Detection, Machine Learning, Cybersecurity, Unsupervised Learning, Threat Intelligence |
| Answerable research questions for 3-5 students (desirable) | * How effectively can unsupervised or semi-supervised ML models detect zero-day attacks by modeling normal network behavior? * Which machine learning techniques offer the best balance between detection performance and false positive rate? * How do different feature selection and preprocessing methods affect anomaly detection accuracy? * What are the limitations of using public datasets for simulating zero-day attack scenarios? |
| 4-5 key references (desirable) and website resources | 1. Sommer, R., & Paxson, V. (2010). “Outside the closed world: On using machine learning for network intrusion detection.” *IEEE Symposium on Security and Privacy*. 2. Javaid, A., et al. (2016). “A deep learning approach for network intrusion detection system.” *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*. 3. Chandola, V., Banerjee, A., & Kumar, V. (2009). “Anomaly detection: A survey.” *ACM Computing Surveys*, 41(3), 1–58. 4. CIC-IDS2017 Dataset – https://www.unb.ca/cic/datasets/ids-2017.html 5. NSL-KDD Dataset – https://www.unb.ca/cic/datasets/nsl.html |
| Required major of studies, desirable skill sets, knowledge, and speciality | Required: Cyber Security or Data Science majors  Desirable Skills: Python, Scikit-learn, anomaly detection, data preprocessing, network traffic analysis  Speciality: Interest in proactive threat detection and adversarial-aware cybersecurity methods |
| **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 are asked to assign their work, then please **provide a brief rationale** as additional permissions are needed by QUT to approve. | Project IP vests in the student with a license back to Industry Partner **(licence)**  OR  Project IP vests in the Industry Partner/Project owner with a licence back to the student **(assignment)**  OR  Academic project (No IP agreement needed) |
| Number of students (4-5) | 4 |
| The message from 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 |  |