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/ Usman Mushtaq  usman@datellite.org |
| Academic Supervisor name(s) and contact emails | Dr Zhenguo Shi  zhenguo.shi@qut.edu.au |
| Information Technology major(s) | Computer Science, Data Science, Software Development |
| Project title | Binary vs. Multiclass Evaluation of IoT Cyber Attacks |
| Brief description of the research problem, aims, method and expected outputs (100~200 words) | Intrusion detection systems (IDS) are essential for identifying malicious activity in IoT environments, where networks are often constrained and highly vulnerable. Most detection models follow either a binary classification approach (normal vs. attack) or a multiclass approach (e.g., DoS, DDoS, MitM, Infiltration). This project aims to compare the effectiveness and limitations of both methods using the same IoT cyber attack dataset (such as CIC-IoT-2023). Students will train and evaluate standard machine learning classifiers (e.g., Random Forest, SVM, XGBoost) on both binary and multiclass-labeled datasets. The models will be evaluated based on metrics such as accuracy, F1-score, confusion matrix, and false positive rate. The project will explore which approach provides better real-world applicability in terms of detection precision and deployment complexity. Expected outcomes include a comparative analysis report, visualization of results, and practical recommendations on when to use binary or multiclass IDS depending on organizational needs. |
| Key words (4-6) | IoT Security, Binary Classification, Multiclass Detection, Intrusion Detection, Cyber Attacks, Model Evaluation |
| Answerable research questions for 3-5 students (desirable) | * How does binary classification performance compare with multiclass models in IoT cyber attack detection? * What are the trade-offs in terms of accuracy, false positives, and interpretability between both approaches? * Which attack types are most frequently misclassified in a multiclass setup? * How should model complexity and use case requirements influence the choice between binary and multiclass IDS? |
| 4-5 key references (desirable) and website resources | 1. Hodo, E., et al. (2016). “Machine learning approach for detection of DoS attacks in IoT systems.” *Information*, 7(3), 67. 2. Ferrag, M. A., et al. (2020). “Deep learning approaches for cyber security intrusion detection: A review.” *Future Generation Computer Systems*, 105, 347–375. 3. CIC-IoT-2023 Dataset – https://www.unb.ca/cic/datasets/iot.html 4. cikit-learn: <https://scikit-learn.org/> 5. Khan, M. A., et al. (2021). “A survey on IDS techniques in IoT: Binary vs. multiclass classification.” *Sensors*, 21(8), 2566. |
| Required major of studies, desirable skill sets, knowledge, and speciality | **Required**: Cyber Security or Data Science majors  **Desirable Skills**: Python, Scikit-learn, feature selection techniques, ML model evaluation, pandas/numpy  **Speciality**: Interest in interpretable AI and lightweight security models for IoT |
| **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 |  |