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 | Feature Selection Impact on IoT Attack Detection Accuracy |
| Brief description of the research problem, aims, method and expected outputs (100~200 words) | As the Internet of Things (IoT) expands across smart homes, cities, and industries, securing IoT environments from cyberattacks becomes increasingly critical. IoT traffic datasets often contain a large number of features, many of which may be irrelevant or redundant, reducing model performance and interpretability. This project aims to investigate how different feature selection techniques affect the accuracy and efficiency of IoT attack detection models. Using datasets such as CIC-IoT-2023, the project will apply various selection methods—including ANOVA F-test, mutual information, and recursive feature elimination (RFE)—to identify the most relevant features. These feature sets will be used to train and evaluate traditional machine learning models (e.g., Random Forest, SVM, XGBoost), comparing accuracy, F1-score, training time, and model complexity. The project will produce a ranked list of impactful features, a performance comparison report, and practical insights for designing more effective and lightweight intrusion detection systems in IoT networks. |
| Key words (4-6) | IoT Security, Feature Selection, Intrusion Detection, ANOVA, Mutual Information, Cybersecurity |
| Answerable research questions for 3-5 students (desirable) | * How do different feature selection techniques influence the performance of ML models in detecting IoT-based attacks? * Which features are most frequently selected across different selection methods? * What trade-offs exist between model accuracy, interpretability, and training time when using reduced feature sets? * Which feature selection technique offers the best performance-to-complexity ratio for lightweight intrusion detection? |
| 4-5 key references (desirable) and website resources | 1. Ferrag, M. A., et al. (2020). “Deep learning approaches for cyber security intrusion detection: A review.” Future Generation Computer Systems, 105, 347–375. 2. Liu, H., et al. (2010). “Feature selection and its application in intrusion detection.” ACM Computing Surveys, 43(3), 1–40. 3. Chandrashekar, G., & Sahin, F. (2014). “A survey on feature selection methods.” Computers & Electrical Engineering, 40(1), 16–28 4. CIC-IoT-2023 Dataset – https://www.unb.ca/cic/datasets/iot.html 5. Scikit-learn Feature Selection Guide – https://scikit-learn.org/stable/modules/feature\_selection.html |
| 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 |  |