School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Funding and application details

Funding status: Self funded students only

Application instructions:
Detailed instructions are available at https://blogs.napier.ac.uk/scebe-research/available-phd-student-projects/

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Mouad Lemoudden (Email: M.Lemoudden@napier.ac.uk)
- 2ND SUPERVISOR:

Subject Group: Cyber-security and system engineering

Research Areas: Cyber Security, Quantum Computing, Machine Learning

Project Title: Investigating Quantum Machine Learning for Cyber Security

Project description:

Quantum Machine Learning (QML) is an emerging field of research that leverages quantum computing to improve the classical machine learning approach to solve complex real-world problems. QML has the potential to address cyber security-related challenges, and this PhD project aims to investigate and apply QML for offensive and/or defensive cyber security use cases.

The project will focus on exploring the potential of QML for cyber security applications, identifying research gaps, and developing novel QML-based algorithms for cyber security. The project will involve developing novel QML-based

algorithms for cyber security applications, evaluation of developed algorithms using quality datasets and comparing the performance against classical machine learning algorithms and identifying further research gaps in the field of QML-based cyber security to address.

Research gaps in the field of QML-based cyber security include: - Lack of Resources: Due to the novelty and complex architecture of QML, resources are not yet explicitly available that can allow cyber security researchers to experiment readily with this emerging technology. - Limited Research: There is limited research on the application of QML for offensive and/or defensive cyber security use cases. This project aims to address this research gap. - Algorithm Development: There is a need for the development of novel QML-based algorithms that can uncover new avenues for machine learning and leverage the unique properties of quantum computing.

In this PhD project, the successful candidate will explore the current state of the art and aim to address these research gaps and contribute to the development of novel QML-based algorithms for cyber security. The project will provide an opportunity to work with cutting-edge technologies and contribute to the development of innovative solutions for cyber security challenges.

References:

[1] Tehrani, M., Sultanow, E., Buchanan, W. J., Amir, M., Jeschke, A., Chow, R., & Lemoudden, M. (2023). Enabling Quantum Cybersecurity Analytics in Botnet Detection: Stable Architecture and Speed-up through Tree Algorithms. arXiv preprint arXiv:2306.13727.

[2] A. Gouveia and M. Correia, “Towards quantum-enhanced machine learning for network intrusion detection,” in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). IEEE, 2020, pp. 1–8.

[3] A. Zeguendry, Z. Jarir, and M. Quafafou, “Quantum machine learning: A review and case studies,” Entropy, vol. 25, no. 2, p. 287, 2023.

Candidate characteristics

Education:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Cyber Security or Computer Science

Subject knowledge:

- Cyber Security

Essential attributes:

- Competent in Cyber Security
- Knowledge of Machine Learning
- Good written and oral communication skills
- Strong motivation
- Good time management

Desirable attributes:

- knowledge of quantum computing and mathematics would be beneficial