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: Baraq Ghaleb (Email: B.Ghaleb@napier.ac.uk)
- 2ND SUPERVISOR: Ahmed Al-Dubai, and Isam Wadhaj

Subject Group: Cyber-security and system engineering

Research Areas: Computer Science

Project Title: Safeguarding the Internet of Things: A Machine Learning Driven Security Paradigm

Project description:

The integration of Machine Learning (ML) techniques within the domain of Internet of Things (IoT) security has emerged as a critical research area due to the escalating risks posed by sophisticated cyber threats. This proposed doctoral research aims to investigate the efficacy of ML algorithms in enhancing the security of interconnected IoT networks. By conducting a comprehensive analysis of existing vulnerabilities and attack vectors, the study seeks to design and implement ML-driven solutions that can effectively detect and mitigate potential security breaches in real-time.

The research methodology involves the collection and analysis of diverse IoT network data, followed by the development of advanced ML models tailored to the unique characteristics and requirements of IoT environments. Through the systematic evaluation of the proposed ML-based security measures, this study aims to contribute to the development of robust and adaptive security protocols capable of safeguarding IoT networks against an array of potential cyber-attacks.

The anticipated outcomes of this research endeavor include the identification of optimized ML frameworks for IoT security, the validation of their effectiveness through extensive experimentation, and the formulation of guidelines for the integration of ML-based security strategies within existing IoT infrastructure. This proposal seeks to make a significant contribution to the field of cybersecurity, fostering a safer and more resilient IoT ecosystem in the face of evolving security challenges.

References:

Candidate characteristics

Education:

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

Subject knowledge:

- Computing
- Computer Engineering

Essential attributes:

- Strong Background in Computer Science and Cybersecurity
- Competent in fundamental programming language
- Knowledge of IoT standards, and machine learning
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Innovative Problem-Solving Skills
- Passion for Research and Self-Motivation