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: Sana Ullah Jan (Email: S.Jan@napier.ac.uk)
- 2ND SUPERVISOR: Bill Buchanan

Subject Group: Cyber-security and system engineering

Research Areas: Artificial Intelligence and Cyber Security

Project Title: Adversarial machine learning for intrusion detection system

Project description:
The demand of secure and reliable communication infrastructure has never been higher due to elevated number of applications in the present-day world such as the Internet of Things (IoT). The integration of numerous IoT-based applications in various aspects of our lives, e.g., industrial automation, smart healthcare, smart cities, and intelligent transportation has resulted in a continuously growing amount of heterogeneous data generated and shared among IoT devices. This situation has constituted grounds for intruders to attack on the ubiquitous IoT devices and security against these attacks is considered one of the biggest barriers in adopting IoT. The aim of this project is to design adversarial machine learning-based

intrusion detection system (IDS) that can discriminate between normal samples and the samples under zero-day adversarial network attacks.

References:

[1] He, Ke, Dan Dongseong Kim, and Muhammad Rizwan Asghar. "Adversarial machine learning for network intrusion detection systems: a comprehensive survey." IEEE Communications Surveys & Tutorials (2023).

[2] Alotaibi, Afnan, and Murad A. Rassam. "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense." Future Internet 15, no. 2 (2023): 62.

Candidate characteristics

Education:

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

Subject knowledge:

- Computing Fundamentals
- Programming C/C++, Python, Java, Matlab or any other relevant tool

Essential attributes:

- Committed to pursue higher education in the field
- Motivated to do PhD
- Eager to work on development of solutions for today's problems