



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

PHD STUDENT PROJECT

Application instructions:

Detailed instructions are available at:

<https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply>

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: Dr Naghmeh Moradpoor (Email: n.moradpoor@napier.ac.uk)
- 2ND SUPERVISOR: tbc

Subject Group: Cyber Security and System Engineering

Research Areas: Computer Science, Engineering

Project Title: Communication Efficiency for Federated Learning in Critical Infrastructure

Project description:

Federated learning is a machine learning approach that enables multiple parties to collaborate in developing a shared model while safeguarding the distribution and privacy of their data. The application of federated learning to critical national infrastructure protection offers several advantages, including enhanced security, efficiency, and privacy. Nevertheless, various security issues and concerns persist. In this Ph.D. research, our focus is on addressing one of these challenges, specifically concentrating on Communication Efficiency within the context of federated learning for Critical National Infrastructure.

We aim to discover novel techniques to minimize the volume of communication required between the central server and the participants. Our goal is to reduce the communication overhead while ensuring model security and accuracy.

References:

- [1] Novikova, E., Doynikova, E., & Golubev, S. (2022). Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case. *Algorithms*, 15(4), 104.
- [2] Jalali, N. A., & Chen, H. (2023). Security Issues and Solutions in Federate Learning Under IoT Critical Infrastructure. *Wireless Personal Communications*, 129(1), 475-500.
- [3] Jalali, N. A., & Chen, H. (2023). Federated Learning Security and Privacy-Preserving Algorithm and Experiments Research Under Internet of Things Critical Infrastructure. *Tsinghua Science and Technology*, 29(2), 400-414.

Candidate characteristics

Education:

A second-class honour degree or equivalent qualification in automation & control, industry 4.0, cybersecurity

Subject knowledge:

- Programming Languages, OR Cybersecurity

Essential attributes:

- Experience of fundamental cybersecurity
- Competent in software development and algorithmic design
- Knowledge of /interest in application of machine learning, critical national infrastructure protection
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management