Department	School of Computing
Supervisors	Dr Naghmeh Moradpoor, Dr Zakwan Jarouchen, Dr Jawad Ahmad, Professor Leandros Maglaras
Project Title	A novel, secure, and cross platform Intrusion Detection System for protection of Critical National Infrastructure

PROJECT DESCRIPTION

Cyberattacks on Critical National Infrastructure (CNI) appear to be growing in occurrence and strength and Operational Technology (OT) networks have gradually become targets of attack for cyber criminals and state-sponsored hackers. In the past year, 93% of OT organisations experienced an intrusion which makes OT security a growing concern for executive leaders and cyber defenders.

This project aims to address two challenges facing CNI protection. 1) Lack of visibility into CNI networks, which is key for companies managing OT risks. 2) Lack of an early anomaly detection method which is secure against adversaries and can be adopted in various forms of CNI (e.g., clean water and electricity). Therefore, this project seeks to overcome these challenges through a novel, secure, and cross platform early anomaly detection mechanism using a system's energy consumption metrics, machine learning particularly Federated Learning, and Distributed Ledger Technologies.

This research focuses on water treatment systems therefore it will be of great benefit to water suppliers all around the world, improving the security of what will become an ever-greater resource and therefore an increasing target for cybercrime. This work will be based on our existing MPS Filtration System, which is representing a scaled-down version of a one-of-a-kind water treatment system. However, the idea behind this proposal is not tied up to this particular application and can be transferred to other CNI applications such as energy sectors and transportation networks.

The future aim is to have this research adopted by industry and be capable of scale.

Academic qualifications

A first degree (at least a 2.1) ideally in automation & control, industry 4.0, cybersecurity with a good fundamental knowledge of programming languages, OR cybersecurity.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

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

Desirable attributes:

Knowledge of water services (e.g., clean water supply systems and/or clean water treatment systems)

Indicative Bibliography	Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, A. S. (2022). Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. *IEEE Internet of Things Magazine*, *5*(1), 24-29. Robles-Durazno, A., Moradpoor, N., McWhinnie, J., Russell, G., & Tan, Z. (2021). Newly engineered energy-based features for supervised anomaly detection in a physical model of a water supply system. Ad Hoc Networks, 120, 102590. Rosa, L., Cruz, T., de Freitas, M. B., Quitério, P., Henriques, J., Caldeira, F., ... & Simões, P. (2021). Intrusion and anomaly detection for the next-generation of industrial automation and control systems. *Future Generation Computer Systems*, *119*, 50-67. Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764-79800.
Enquiries	For informal enquiries about this PhD project, please contact Dr Naghmeh Moradpoor (n.moradpoor@napier.ac.uk)
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process