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://www.napier.ac.uk/research-and-innovation/research-degrees/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: Christos Chrysoulas (Email: C.Chrysoulas@napier.ac.uk)
- 2ND SUPERVISOR:

Subject Group: Computer science

Research Areas: System Architecture, Distributed Computing, Smart Grids

Project Title: Building the next Generation of Smart Grid Infrastructures

Project description:

Building the future of Smart Grid infrastructures involves leveraging advanced technologies and integrating renewable energy sources, enhancing grid resilience, improving efficiency, and implementing intelligent monitoring and control systems. To achieve this goal this research will mostly fouced, but not limited to the following aspects:

a) Advanced Metering Infrastructure (AMI): Deploy smart meters to enable real-time monitoring of energy usage, provide consumers with detailed information, and support demand-side management programs.

b) Internet of Things (IoT) and Sensors: Install sensors and IoT devices across the grid for real-time data collection, enabling proactive maintenance and optimizing grid performance.
c) Advanced Analytics and Artificial Intelligence (AI): Utilize AI algorithms to analyze the vast amount of data generated by smart meters and sensors, predicting load patterns and optimizing energy distribution, and Implement AI-based predictive maintenance to reduce downtime, improve reliability, and extend the lifespan of grid components.
d) Demand Response Programs: Implement demand response initiatives to incentivize consumers to reduce energy consumption during peak periods, optimizing load distribution and reducing strain on the grid.
e) Cybersecurity and Privacy: Implement robust cybersecurity measures to protect smart grid infrastructure from cyber threats and ensure the privacy and security of consumer data.

By following this multi-faceted approach, we can build a resilient, efficient, and sustainable smart grid infrastructure that supports the integration of renewable energy and meets the growing energy demands of the future.

References:

[1] A. F. Blomstedt et al., "The arrowhead approach for SOA application development and documentation," IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, USA, 2014, pp. 2631-2637, doi: 10.1109/IECON.2014.7048877.

[2] B. L. L. Ferreira et al., "Arrowhead compliant virtual market of energy," Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, Spain, 2014, pp. 1-8, doi: 10.1109/ETFA.2014.7005193.

[3] C. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.

[4] D. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 371-390, doi: 10.23919/CYCON.2018.8405026.

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Computer Science or Electrical and Computer Engineering

Subject knowledge:

- Fundamental knowledge of Machine Learning,
- Good programming skills in Object Oriented Languages
- Basic Security algorithms and programming (eg. Python).
- An inquisitive and analytical mind, self-motivation and the ability to work independently, are consid

Essential attributes:

- Experience in Service Oriented Architectures (SOA)
- Experience of fundamental Machine Learning and/or Cybersecurity techniques.

- Knowledge of Machine Learning and/or Cybersecurity theory.
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- A master's degree with courses on Machine Learning, and/or Security/Cybersecurity.
- Background in machine learning (deep feed-forward neural networks, deep recurrent neural networks, deep convolutional neural networks, etc.).
- Background in cybersecur