Department	School of Computing
Supervisors	Dr. Baraq Ghaleb, Prof. Ahmed Al-Dubai and Dr. Isam Wadhaj
Project Title	Smart, and Energy-Efficient Countermeasures for the IoT Security Attacks

PROJECT DESCRIPTION

The Internet of Things (IoT) paradigm has emerged as a key pillar in the new industrial revolution, namely Industry 4.0, opening the door for a multitude of applications and unprecedented services. However, researchers have identified several vulnerabilities and IoT attacks in the standardized IoT protocols that could crucially limit their applicability in several applications including, for instance, smart homes and healthcare environments where it is crucial to have very robust security measures . Both industry and academia have proposed several solutions to mitigate IoT security vulnerabilities. However, these solutions have limited success in this perspective as there are several security challenges that ought to be addressed to fully unleash the huge potential of such a discipline in the context of health environments. Indeed, Machine-Learning (ML) based solutions have recently opened several windows to address security challenges in IoT and have been mainly utilized to identify abnormal behaviours in IoT-enabled smart networks, however, their potential in the context of IoT standardised applications have not been fully uncovered. Hence, the main aim of this project is to propose ML based security countermeasures for some of the well-known IoT attacks of the standardized IoT protocols including RPL and the 6LoWPAN stacks.

The following objectives are sought to be achieved:

Objective 1: To thoroughly overview the latest advancements of ML based algorithms in detecting IoT attacks. The aim here is to focus on standardised 6LoWPAN stack and the attacks targeting its different layers including Flooding attacks, Sinkhole attacks, Blackhole attacks and Table Falsification attacks.

Objective 2: To develop some ML security countermeasures with the aim at detecting attacks while maintaining acceptable energy consumption profiles and reliable transmissions.

Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervis

Academic qualifications

A first degree (at least a 2.1) ideally in Computer Science with a good fundamental knowledge of programming.

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 Internet of Things (IoT), Machine Learning (ML) and IoT security
- Competent in c/c++ programming
- Knowledge of ML tools
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Indicative Bibliography	1. Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, *14*(100365), 100365. https://doi.org/10.1016/j.iot.2021.100365 2. Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025 3. Al-Amiedy, Taief Alaa, et al. "A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things." Sensors 22.9 (2022): 3400. 4. Verma, Abhishek, and Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review." *IEEE Sensors Journal* 20.11 (2020): 5666-5690.
Enquiries	For informal enquiries about this PhD project, please contact Dr. Baraq Ghaleb at b.ghaleb@napier .ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process