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. Luigi La Spada (Email: L.LaSpada@napier.ac.uk)
- 2ND SUPERVISOR: Prof. Bill Buchanan

Subject Group: Cyber Security and System Engineering

Research Areas: Cyber Security, Internet of Things, Machine Learning, Quantum Computing

Project Title: Machine Learning Algorithms for Improving Predictive Maintenance in Industrial Automation Systems

Project description:

The literature indicates significant advancements in securing IoT networks, especially against quantum computing threats. Bagchi 2023 proposes a post-quantum lattice-based secure framework called LAS-AIBIoT for ambient intelligence-assisted blockchain-based IoT applications. It utilizes aggregate signatures and demonstrates robustness against potential attacks, including quantum computing security threats. Biswas 2023 introduces a scalable meta-learning-based model for securing IoT networks. The model combines edge models and metadata-based learning to detect various attacks in IoT devices, improving accuracy and performance. Building on the ideas from Bagchi and Biswas about making IoT networks safer, this project mix Quantum Metamaterials, Artificial Intelligence (AI), and Large Language Models(LLMs) to create stronger security for IoT networks.

At the heart of this project is the creation and tailoring of Quantum Metamaterials to improve IoT security. These metamaterials will form the basis of a new physical security layer, enabling hidden communication, better intrusion detection, and secure data transfer within IoT networks.

Generative AI will be crucial in automatically designing and refining these quantum metamaterials. Using Generative Adversarial Networks (GANs) or similar algorithms, the project seeks to find new metamaterial structures with quantum features that enhance security. The generative models will continuously create and assess various metamaterial designs, speeding up the search for the best configurations to improve IoT security.

At the same time, Large Language Models (LLMs) will be used to create a smart security analysis framework. This framework will constantly examine the many interactions within the IoT network and the broader digital environment to spot potential security threats. The LLMs, trained on a wide range of cybersecurity texts and real-world intrusion data, will be able to identify complex cyber-attack patterns and suggest immediate solutions.

Moreover, a cooperative feedback loop between the LLM-driven analysis and the Generative AI-driven metamaterial design will be formed. Insights from LLM analysis will guide the generative algorithms, helping to continuously improve the quantum metamaterials to tackle emerging security threats. On the other hand, the actual performance data of the quantum metamaterials will be used to enhance the LLMs' understanding and prediction accuracy regarding cybersecurity challenges in IoT.

By blending quantum physics, artificial intelligence, and cybersecurity the goal is to develop a resilient, adaptable, and smart IoT security infrastructure that can foresee and counter a wide range of cyber threats in an increasingly interconnected digital world.

References:

[1] Bagchi, P., Bera, B., Das, A.K., Shetty, S., Vijayakumar, P., & Karuppiah, M. (2023). Post Quantum Lattice-Based Secure Framework using Aggregate Signature for Ambient Intelligence Assisted Blockchain-Based IoT Applications. IEEE Internet of Things Magazine, 6, 52-58.

[2] Biswas, K., Ghazzai, H., Sboui, L., & Massoud, Y. (2023). A Scalable Meta Learning-Based Model to Secure IoT Networks. IEEE Internet of Things Magazine, 6, 116-120.

Candidate characteristics

Education:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Cybersecurity, Electrical and Electronic Engineering, Computer Science, Artificial Intelligence or Machine Learning

Subject knowledge:

- Networking and Internet of Things (IoT)
- Quantum Mechanics
- Mathematics
- Physics
- Communication Systems

Essential attributes:

- Strong Analytical Skills
- Technical Proficiency
- Research Aptitude
- Innovative Thinking
- Effective Communication Skills
- Creative Problem-Solving Skills

Desirable attributes:

- Multidisciplinary Background
- Industry Experience
- Publication Record
- Teaching or Mentoring Experience
- Advisory or Consultancy Experience