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 Kehinde Babaagba (Email: k.babaagba@napier.ac.uk)
- 2ND SUPERVISOR: tbc

Subject Group: Computer Science

Research Areas: Computer Science

Project Title: Quantum Computing for Malware Analysis and Detection

Project description:

In recent years, the threat landscape in cybersecurity has grown exponentially, with increasingly sophisticated malware variants targeting critical infrastructure, financial systems, and personal data. Traditional methods of malware detection and analysis, primarily relying on signature-based techniques, heuristics, and machine learning, are struggling to keep pace with the rapid evolution of these threats. As quantum computing emerges as a transformative technology, it holds the potential to revolutionize the field of cybersecurity. This PhD project aims to explore the application of quantum computing to malware analysis and detection, focusing on leveraging quantum algorithms to enhance the identification and mitigation of advanced persistent threats (APTs) and metamorphic/polymorphic malware.

The primary objectives of this research are as follows:

1. Exploration of Quantum Algorithms for Malware Detection:

- Investigate the potential of quantum algorithms, such as Grover's algorithm, quantum annealing, and quantum machine learning, in enhancing the efficiency and accuracy of malware detection systems.

- Develop quantum-based models that can outperform classical machine learning models in identifying zero-day exploits and novel malware variants that traditional systems may fail to detect.

2. Quantum-enhanced Pattern Recognition and Anomaly Detection:

- Implement quantum computing techniques to improve pattern recognition in large datasets, enabling the identification of subtle anomalies and behavioral patterns associated with malware.

- Explore the use of quantum support vector machines (QSVMs) and quantum neural networks (QNNs) for real-time anomaly detection in network traffic and system logs.

3. Development of Quantum-resistant Malware Detection Systems:

- Analyze the implications of quantum computing on existing cryptographic systems and explore the creation of quantum-resistant malware detection frameworks.

- Investigate how quantum-resistant algorithms can be integrated into malware detection systems to secure them against future quantum-based cyber threats.

4. Scalability and Practicality of Quantum Malware Detection:

- Assess the current state of quantum hardware and its suitability for real world malware detection applications.

- Develop hybrid classical-quantum models that utilize quantum computing's strengths while mitigating current hardware limitations, ensuring the feasibility and scalability of the proposed solutions.

Methodology:
The research will be conducted in multiple stages, beginning with a comprehensive literature review of existing malware detection methods and quantum computing advancements. The candidate will then focus on designing quantum algorithms tailored for malware analysis, followed by their implementation on quantum simulators and actual quantum hardware as it becomes available.

1. Literature Review: Explore current quantum computing applications in cybersecurity and identify gaps in the literature related to malware analysis.

2. Algorithm Design: Develop quantum algorithms, focusing on their theoretical advantages over classical approaches in terms of speed, accuracy, and ability to handle large datasets.

3. Simulation and Testing: Implement the designed algorithms on quantum simulators such as IBM Qiskit or Google Cirq. Evaluate their performance against traditional methods using malware datasets from sources like VirusTotal and other cybersecurity databases.

4. Hybrid Models: Develop hybrid models combining classical and quantum approaches, testing their efficiency on real-world data.

5. Evaluation: Benchmark the performance of quantum algorithms against classical ones in various scenarios, including detection speed, false positive rates, and adaptability to new malware variants.

Candidate characteristics

Education:

The ideal candidate should have a first degree with at least a 2:1 classification in one of the following subjects: Computer Science, Mathematics, Cybersecurity or similar subjects.

Subject knowledge:

The ideal candidate will have a strong background in computer science, with a focus on cybersecurity, quantum computing, or a related field. Experience with machine learning, malware analysis, and programming languages such as Python is essential. Familiarity with quantum computing frameworks like Qiskit, Cirq, or D-Wave would be advantageous.

Essential attributes:

- Strong Analytical and Problem-Solving Skills
- Solid Foundation in Quantum Computing and Algorithms
- Proficiency in Programming
- Background in Cybersecurity
- Research Experience
- Mathematical Competence
- Ability to Work Independently and Collaboratively
- Communication Skills
- Adaptability and Curiosity
- Attention to Detail