QUEEN'S
UNIVERSITY
BELFAST

Candidate Information

Position:	Research Fellow In AI For Malware Detection On Internet Of Things (IoT) Devices
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	24/112287
Closing Date:	Monday 25 November 2024
Salary:	£39,922 per annum
Anticipated Interview Date:	Thursday 12 December 2024
Duration:	36 months

JOB PURPOSE:

To perform research in AI for Internet of Things (IoT) malware detection. The role involves gaining a deep understanding of how AI systems can be applied to design IoT malware detectors. The key requirements are to design deep neural network (DNN) malware detection solutions that generalise across multiple platforms and can run efficiently on low-resource embedded IoT hardware.

MAJOR DUTIES:

1. Undertake high-quality and novel research in deep-learning-based Internet of Things (IoT) malware detection. This will involve developing deep-neural-network-based malware detectors that use multi-task learning for improved cross-platform robustness, then adapting these networks to run on low-resource IoT devices using novel pruning and distillation techniques.
2. Design, develop, and refine experiments to evaluate deep-learning-based IoT malware detection performance.
3. Carry out analyses, critical evaluations, and interpretations using methodologies and other techniques appropriate to AI for IoT security.
4. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
5. Prepare material, often in consultation with the line manager, for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy and ACM in Computers and Communication Security.
6. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
7. Undertake supplementary duties relevant to the project's success, including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Normally have or about to obtain a PhD in engineering or physical sciences area.
2. Recent high-quality research experience in machine learning/deep learning or cybersecurity, or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Proficient in a high-level programming language such as Python, C++ etc.
4. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
5. Demonstrable ability to assess and organise resources.
6. Evidence of being a team player with a proven ability to work with other members of a large multidisciplinary research and development team, as well as with industrial collaborators.
7. Evidence of being a strong communicator with excellent oral and written communication skills.
8. Demonstrate the ability to work in a fast changing environment with competing priorities.
9. Demonstrates a high degree of integrity, honesty and openness in professional conduct.
10. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.

DESIRABLE CRITERIA:

1. Normally have or be about to obtain a PhD in the area of machine learning/AI, cybersecurity or cyberAI.
2. Experience with deep-learning based malware detection techniques.

3. Experience with techniques for adapting neural networks to lowresource devices, such as pruning and distillation.
4. Experience in initiating and developing research plans.
5. Experience in collaborating with industry.
6. Experience in IoT security in hardware and software.
7. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc.)
8. Demonstrable commitment to the purpose and objectives of CSIT.