Candidate Information

Position:	Research Fellow in Edge AI security
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	25/112741
Closing Date:	Monday 25 August 2025
Salary:	£41,519 per annum
Anticipated Interview Date:	Tuesday 2 September 2025
Duration:	12 months

JOB PURPOSE:

The emergence of edge AI systems-AI deployed on resource-constrained, often battery-powered, devices at the edge of the network-presents critical security challenges. These systems are increasingly vulnerable to hardware-level threats, including side-channel attacks, fault injections, and malicious approximations, particularly when optimized for performance through approximate computing.

This Research Fellow position focuses on AI security in the context of hardware-constrained edge devices, investigating how hardware-supported approximate computing can be leveraged to improve performance and energy efficiency without compromising system robustness. The role involves designing secure AI accelerators, analyzing attack surfaces introduced by approximation, and developing a performance-security trade-off framework to guide secure AIoT deployment.

MAJOR DUTIES:

1. Undertake novel research on the security of edge AI systems with a focus on hardware vulnerabilities and the impact of approximate computing.
2. Investigate and model attack surfaces introduced by approximation techniques, including side-channel leakage, RowHammer vulnerabilities, and fault propagation.
3. Develop and evaluate mitigation strategies and trade-off models to balance security, performance, and energy efficiency.
4. Design and prototype AI accelerators on FPGA platforms (e.g. AMD Zynq UltraScale+), with hardware-level approximation.
5. Contribute to impactful publications and present research at major international venues in AI security and hardware-aware systems (e.g. IEEE S&P, USENIX, DAC, CHES, SATML, etc).
6. Collaborate with the wider project team, including researchers at CSIT, and contribute to industry-facing dissemination activities.
7. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
8. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
9. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Have or be about to obtain a PhD in computer science, engineering, mathematics or physical sciences area.
2. Recent high quality research experience in machine learning/AI, Embedded Systems or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Proficiency in Python, familiarity with hardware design (Verilog/VHDL), and FPGA-based acceleration.
4. A consummate team player who is open-minded and is prepared to work closely with other members of a large multidisciplinary research and development team, as well as with industrial collaborators.
5. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
6. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. PhD in hardware-aware AI security, approximate computing, or secure embedded AI systems.
2. Hands-on experience in Edge AI.
3. Experience in embedded systems security.
4. Experience in AI security and/or Trustworthy AI.
5. Experience in initiating and developing research plans.
6. Experience in collaborating with industry.
7. Experience with platforms such as PYNQ, FINN-R, hls4ml, Vivado HLS.
8. Experience using PyTorch, Keras, and/or TensorFlow. Jupyter Notebook.
9. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc.)
10. Demonstrable commitment to the purpose and objectives of CSIT and Cyber-AI Hub.
11. Ability to assess and organise resources.
12. Evidence of being a strong communicator with excellent oral and written communication skills.
13. Demonstrate resilience and the ability to work in a fast-changing environment with competing priorities.
14. Demonstrates a high degree of integrity, honesty and openness in professional conduct.