Candidate Information

Position:	Research Fellow in Trustworthy AI
School/Department:	Centre for Secure Information Technologies
Reference:	24/111952
Closing Date:	Monday 17 June 2024
Salary:	£37,841 per annum
Anticipated Interview Date:	Monday 1 July 2024
Duration:	24 months

JOB PURPOSE:

To conduct research into advanced machine learning techniques and their trustworthiness (security/privacy/reliability) for use in hardware security and contribute to the planning and delivery of research project activities associated with the Research Institute in Secure Hardware and Embedded Systems (RISE).

MAJOR DUTIES:

1. Conduct research into the trustworthiness of machine learning techniques, with hardware security as a use-case.
2. Present annual progress reports on research for funders and to the UK research community via RISE, to CSIT industry advisory board members or to external audiences to disseminate and publicise research findings.
3. Prepare, in consultation with supervisor, material for publication in national and international journals and presentations at international conferences.
4. Assist in the preparation of funding proposals and applications to external bodies.
5. Read academic papers, journals and textbooks to keep abreast of developments in own specialism and related disciplines.
6. Carry out occasional undergraduate/postgraduate student project supervision, demonstrating or lecturing duties within the post holder's area of expertise and under the direct guidance of a member of academic staff.
7. Any other duties that may reasonably be requested by the programme supervisor.

ESSENTIAL CRITERIA:

1. 2:1 Honours degree in Computer Science/Electrical and Electronic Engineering/ Mathematics (or related discipline).
2. Have, or be about to obtain, a PhD in a relevant subject.
3. Recent relevant research experience in ML/DL modelling.
4. Evidence of a strong publication record commensurate with career stage and experience.
5. Ability to contribute to broader management and administrative processes.
6. Ability to contribute to the School's outreach programme by establishing links with industry, community groups etc.
7. Sufficient breadth and depth of specialist knowledge in the discipline and of research methods and techniques to work within established research programmes.
8. Good written and verbal communication skills.
9. Ability to communicate complex information clearly.
10. Ability to innovate and rapidly contribute to research projects.
11. Willingness to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.

DESIRABLE CRITERIA:

1. Expertise in adversarial AI attacks and/or explainable AI.
2. Background in Hardware Design.
3. Expertise in Hardware Trojan design and/or detection.
4. Ability to build contacts and participate in internal and external networks.
5. Experience of collaborative research or working in a team is desirable.