Candidate Information

Position:	Research Fellow in Cybersecurity and Artificial Intelligence (2 posts)
School/Department:	Centre for Secure Information Technologies
Reference:	23/111040
Closing Date:	Monday 17 July 2023
Salary:	£36,333 - £43,155 per annum.
Anticipated Interview Date:	Thursday 10 August 2023
Duration:	Fixed Term 3 years, or available until 31/03/2026, whichever is sooner

JOB PURPOSE:

To perform research in the area of AI-enabled cybersecurity, called Cyber-AI. The role will involve gaining deep understanding of a cybersecurity problem of relevance to a partner company and, using both proprietary and public cybersecurity datasets, design, implement, train and test machine learning and reasoning models that solve the problem. A key requirement is to design novel deep learning and reasoning architectures reflecting understanding of the unique structure of cybersecurity datasets. Assisting engineering staff to take the machine learning model or reasoning into production.

MAJOR DUTIES:

1. Undertake high quality and novel research in the area of CyberAI.
2. Design, develop and refine experiments in order to evaluate CyberAI algorithm performance.
3. Carry out analyses, critical evaluations, and interpretations using methodologies and other techniques appropriate to CyberAI.
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, often in consultation with line manager, material for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy, 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 success of the project 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. Substantial high quality research experience in machine learning/AI or cybersecurity, or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Software or hardware programming skills.
4. Ability to communicate complex information in a variety of formats clearly.
5. Ability to build contacts and participate in internal and external networks.
6. Ability to assess and organise resources.
7. 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.
8. Must be prepared to work closely with industrial collaborators.

DESIRABLE CRITERIA:

1. Normally have or be about to obtain a PhD in the area of machine learning/AI, cybersecurity or cyberAI.
2. Experience in deep learning neural networks such as CNNs, auto-encoders, transformers and self-attention networks. Adversarial training and testing. Reasoning with uncertainty.

3. Experience in cybersecurity applications such as:
   • threat intelligence and monitoring,
   • ICS malware detection and network intrusion detection,
   • device/service identification,
   • device trust,
   • hardware or embedded systems security,
   • security and verification of AI
   • and threat prediction and prevention.
4. Experience of collaborative research working in a team with industry.
5. Experience in initiating and developing research plans.
6. Proficient in Python, C/C++ or Verilog.
7. Experience using PyTorch, Keras, and/or TensorFlow. Jupyter Notebook.
8. Ability to design, train and test machine learning/AI systems using appropriate datasets.
9. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc.)