



Candidate Information

Position:	Research Fellow in Cybersecurity and Artificial Intelligence
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	24/112195
Closing Date:	Monday 28 October 2024
Salary:	£39,222 - £46,249 per annum
Anticipated Interview Date:	Thursday 7 November 2024
Duration:	36 Months

JOB PURPOSE:

The purpose of the role is to perform research in the area of AI-enabled cybersecurity (CyberAI). 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, natural language processing, and Document AI models that solve the problem. A key requirement is to design and evaluate novel deep learning and natural language processing architectures reflecting understanding of the cybersecurity datasets and system goals. The role also involves assisting engineering staff in taking the machine learning model into production, in consultation with the partner company.

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 computer science, engineering or physical sciences area.
2. Recent 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 programming skills.
4. Ability to assess and organise resources.
5. 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.
6. Evidence of being a strong communicator with excellent oral and written communication skills.
7. Demonstrate resilience and the ability to work in a fast-changing environment with competing priorities.
8. Demonstrates a high degree of integrity, honesty and openness in professional conduct.
9. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
10. On-site presence required for minimum 3 days per week.

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 Transformer models, with a focus on NLP or Document AI methods and applications.

3. Experience in trustworthy AI/NLP systems and applications such as:
 - Robust document classification
 - Retrieval augmented generation
 - Adversarial training and testing
 - Verification of models
 - Explainability of models.
4. Experience in initiating and developing research plans.
5. Experience in collaborating with industry.
6. Proficient in Python.
7. Experience using PyTorch, Keras, and/or TensorFlow. Jupyter Notebook.
8. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
9. Familiarity with the theory of Machine Learning fundamentals (statistics, optimization, linear algebra, model evaluation, etc.)
10. Demonstrable commitment to the purpose and objectives of CSIT and Cyber AI Hub.

ADDITIONAL INFORMATION:

Informal Enquiries to Paul Miller: p.miller@qub.ac.uk