Candidate Information

Position: Research Fellow
School/Department: School of Electronics, Electrical Engineering and Computer Science
Reference: 26/113326
Closing Date: Monday 15 June 2026
Salary: £41,519-£46,704 per annum
Anticipated Interview Date: Thursday 25 June 2026
Duration: 36 months

JOB PURPOSE:

This role addresses research in applying novel AI approaches to detect and respond to cyber threats against critical infrastructure, such as gas, water and electrical grids. The role requires a deep understanding of Agentic AI frameworks, unsupervised learning and anomaly detection, Large Language Models (LLMs) and Transformers. Experience in how to model the patterns and behaviours of cyber adversaries, such as advanced persistent threats (APTs) in IT and OT networks and devices is highly desirable, as this will be the use case of the AI models to be developed . It will focus on adapting transformer architectures to parse heterogeneous data streams, enabling the detection of subtle, multi-stage threats that traditional signature-based tools miss. Beyond detection, it will investigate the use of agentic AI, developing autonomous systems capable of reasoning across complex security alerts, threat intelligence and system constraint data, to execute real-time, context-aware responses to maintain system stability and operations, ensuring that critical infrastructure remains resilient in the face of evolving adversarial tactics.

MAJOR DUTIES:

1. Undertake high-quality and novel research in the areas of transformer-based AI modelling and agentic AI approaches for cyber threat detection and response applied to critical infrastructure environments.
2. Design, develop, and refine experiments to evaluate performance of anomaly detection and agentic AI approaches.
3. Perform critical evaluation and interpretation of AI outputs using appropriate analytical frameworks and technical methodologies.
4. Coordinate research tasks, work packages, deliverables and publications with external academic research partners and industrial collaborators, including external visits where appropriate.
5. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
6. Prepare material, in consultation with the line manager, for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy, ACM Computer and Communications Security, NeurIPS and AAAI.
7. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
8. 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, mathematics, engineering or physical sciences area (*must be obtained within 3 months of closing date of post).
2. Significant, relevant 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. Hands-on experience in clustering and anomaly detection methods and/or experience in AI agentic systems.
4. Software programming skills.
5. Excellent oral and written communication skills. Articulate, confident, and able to clearly communicate complex concepts.
6. Ability to work closely with other members of a large multidisciplinary team.
7. Prepared to work closely with industrial collaborators.
8. Ability to assess and organise resources and balance 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.
11. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. Have or be about to obtain a PhD in an area related to AI and machine learning.
2. Experience in deep learning for modelling heterogenous data sources.
3. Experience in Agentic AI.
4. Experience in LLMs and Transformer architectures.
5. Experience in initiating and developing research plans.
6. Experience in initiating and developing research plans.
7. Experience in collaborating with industry.
8. Experience in successful research with external partners (e.g. joint research publications or deliverables).
9. Proficient in Python.
10. Experience using PyTorch, Keras, and/or TensorFlow. Jupyter Notebook.
11. Experience using AgenticAi frameworks such as Autogen, CrewAI or OpenAI Agents SDK.
12. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
13. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc).
14. Domain knowledge of critical infrastructure related technologies (IT-OT, CPS, ICS, etc).
15. Familiarity with the theory of Agentic Systems (MCP, A2A, orchestration, etc).
16. Experience in trustworthy AI.
17. Experience leading, coordinating or managing research across multiple institutes or industry partners.

ADDITIONAL INFORMATION:

Informal enquiries may be directed to: Paul Miller at p.miller@qub.ac.uk.