Candidate Information

Position:	Research Fellow - AI Centric Datacentre Security
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	24/112196
Closing Date:	Monday 7 October 2024
Salary:	£46,249 per annum
Anticipated Interview Date:	Thursday 24 October 2024
Duration:	3 years

JOB PURPOSE:

In this role as a Post-doctoral Research Fellow the candidate will actively contribute to a major collaborative project between NVIDIA R&D labs and the Centre for Secure Information Technology (CSIT) Cyber-AI Hub. The candidate will engage in challenging cyber security related research projects to enhance GPU Data and DPU based AI centric Datacentre security, investigate threat detection techniques, and benchmark hardware accelerated DPU use-cases. The candidate is expected to undertake novel research and actively participate in the development of Proof-of-Concept demonstrators and performance benchmarking in close collaboration with NVIDIA R&D labs staff.

MAJOR DUTIES:

1. Investigate various forms of security threats to datacentre networks and cloud SAAS.
2. Investigate threat specific signatures that can be effectively extracted in real-time and utilised for AI/ML-based threat detection.
3. Develop and customise AI/ML algorithms, specifically emerging AI algorithms underpinning LLMs, transformers and advance anomaly detection for datacentre threat intelligence and prediction.
4. Utilise NVIDIA GPU technology, CUDA and Morpheus Cybersecurity Framework to develop and train various inference engines for threat intelligence and prediction.
5. Explore how NVIDIA DPU technology can be effectively utilised as real-time telemetry and feature extraction device.
6. In collaboration with Nvidia staff, design and develop proof-of-concept prototypes to demonstrate the viability and effectiveness of AI-centric DPU/GPU enabled datacentre security solutions.
7. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
8. Prepare, in consultation with supervisor, material for publication in national and international journals and presentations at international conferences.
9. Assist grant holder in the preparation of funding proposals and applications to external bodies.
10. Carry out routine administrative tasks associated with the research project/s to ensure that projects are completed on time and within budget.
11. Carry out occasional undergraduate project supervision within the post holder's area of expertise and under the direct guidance of a member of academic staff.
12. Any other duties that may reasonably be requested by the programme supervisor.

ESSENTIAL CRITERIA:

1. Normally have or about to obtain a PhD in engineering or physical sciences area.
2. Recent high quality research experience in AI-enabled cybersecurity, machine learning/AI or cybersecurity, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Academic research experience in either:
   • Deep learning neural networks such as CNNs, autoencoders, transformers or self-attention networks, including ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets; OR
   • Analysis of malware and ransomware indicators and behaviours, or network threat analysis and detection.
4. Software programming skills, evidenced through experience at systems or embedded level, preferably in C, C++, or Python.

5. Ability to assess and organise resources.
6. A consummate team player is prepared to work closely with other members of a large multidisciplinary research and development team, as well as with industrial collaborators.
7. Evidence of being a strong communicator with excellent oral and written communication skills.
8. Demonstrate resilience and the ability to work in a fast-changing environment with 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 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 initiating and developing research plans.
3. Experience in collaborating with industry.
4. Commercial software development experience.
5. Experience using PyTorch, TensorFlow, and or Keras. Jupyter Notebook.
6. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc).
7. Good understanding of GPU/DPU technologies.
8. Good understanding of security architectures, resource isolation and segregation approaches.
9. Demonstrable commitment to the purpose and objectives of CSIT and Cyber AI Hub.

ADDITIONAL INFORMATION:

Informal enquiries may be directed to: Professor Sakir Sezer at s.sezer@qub.ac.uk