

**Research Associate / Senior Research Associate / Research Fellow
in Security Assurance for Agentic AI in Future Networks**

1. JOB DESCRIPTION

Faculty / School: Faculty of Engineering /School of Electrical, Electronic and Mechanical Engineering (EEME)

Faculty/School Address: Merchant Venturers Building, Woodland Road, Bristol BS8 1UB

Job Family:	Research and Teaching		
Grade / Pathway:	Grade I-K (subject to experience)/ Pathway 2	Salary range:	£40,704 - £45,641 (Grade I) or £45,641 - £51,258 (Grade J) or £52,788 - £59,390 (Grade K) per annum depending on experience
Hours of work:	35 hours per week	Contract type:	Open-ended with fixed funding until 29 February 2028
Work pattern:	Full time	Vacancy Reference Number: ACAD108749	

Main Job Purpose

The Smart Internet Lab at the University of Bristol is seeking an outstanding researcher to join the newly funded **AURA (Autonomous Unified RAN Architecture)** project. Project AURA introduces autonomous AI-driven network management across critical network infrastructure, utilising AI agents that sense, decide, orchestrate, and propose configuration changes with minimal human intervention. AURA addresses the security and resilience of private 5G networks deployed across critical infrastructure sectors. The project combines cloud-native private 5G orchestration, zero-trust security, autonomous AI-

driven network management and security assurance, with the ambition of advancing the technology towards operational deployment.

The successful candidate will focus exclusively on addressing the critical security challenges created by the AI-native Future Networks architecture: ensuring that the AI management layer itself is trustworthy, secure, and resilient to compromise. You will be responsible for conducting novel academic and high Technology Readiness Level (TRL) Agentic AI security research to characterise threat landscapes (agentic AI threat modelling), adversarial testing, develop runtime assurance mechanisms, enforce zero trust principles on the autonomous AI layer, behavioural monitoring, and demonstrate autonomous detection and recovery from agent compromise.

Research will be experimentally evaluated using the project partner's agentic AI platform and the University's JOINER national open-networks experimentation infrastructure. The successful candidate will work with the JOINER infrastructure and project partners, to conduct both offensive and defensive Agentic AI security assurance in real-world settings, leveraging the available infrastructure. This role offers a unique opportunity to develop intelligent and innovative solutions that could be integrated with existing security solutions pertaining to agentic AI in future networks. The work will contribute to experimentally validated security mechanisms for autonomous AI-driven network management and to the project's academic, technical and governance outputs. Furthermore, the research aims to advance the applicability of secure and trustworthy agentic AI in future networks. The successful candidate will carry out research for the AURA project with close collaboration with JOINER. JOINER (<https://joiner.org.uk/>) is a national experimentation platform for future connectivity and with cutting edge capabilities. It connects **fifteen** research labs/centres of excellence/universities and is a platform enabling next generation network research to become reality.

The post holder will join the Smart Internet Lab, which is one of the UK's most renowned Information and Communications Technology (ICT) research centres. Our 200 experts address grand societal and industrial challenges associated with 5G/6G radio/wireless, optical communications, and networks. We are challenging the complexity of tomorrow's world by fusing research expertise and innovation in areas such as IoT, 5G/6G & Beyond, Future Transport Networks, Smart Cities, Autonomous Networks, Machine Learning, Artificial Intelligence, Network Convergence, Mobile Edge Computing, and Network Softwarisation. Our unique offering across optical, wireless, IoT, and cloud technologies enable us to bring together end-to-end network design and optimisation, impacting regional, national, and global ICT innovations.

The appointment may be made at **Research Associate (Grade I)**, **Senior Research Associate (Grade J)**, or **Research Fellow (Grade K)** depending on the candidate's qualifications, experience, research independence and track record. You can find more information about the Smart Internet Lab via the links below:

<http://www.bristol.ac.uk/engineering/research/smart/>

Main Statement of Responsibilities

Research Responsibilities

You will work with the AURA project in collaboration with JOINER and focus on the applied agentic AI security in future telecom networks with particular emphasis on Agentic AI Threat Modelling, Trustworthy Agent Execution and Zero Trust AI management, Detection and Autonomous Mitigation of Agent Compromise. You will conduct applied and experimental research with a TRL up to 7. Your main research responsibilities may include:

Main Tasks and Responsibilities

- Identify and document the threat landscape across the data ingestion, intent interface, and execution layers of the Agentic AI system and develop an adversarial data injection framework to test the resilience of the telemetry ingestion pipeline against corrupted or malicious inputs.
- Simulate and demonstrate agent misuse and multi-agent coordination attack scenarios on the live platform of another AURA's partner to establish a concrete attack landscape.
- Design and implement intent-to-policy mapping to translate agent intent into formal policy constraints that can be verified before execution.
- Develop a runtime decision validation engine to evaluate proposed configuration actions against cross-layer security dependency models.
- Implement a dynamic trust scoring mechanism that evaluates agents based on historical behaviour and performance under validated security models.
- Create an adaptive decision assurance loop where trust scores determine the level of scrutiny applied to an agent's subsequent decisions.
- Implement continuous behavioural monitoring across both agent-layer decision patterns and network-layer security impacts, such as QoS metrics and resource usage.
- Develop automated mitigation strategies that do not require human intervention, including rollback mechanisms that restore the network to its last verified configuration state.
- Design agent isolation protocols to remove compromised agents from the actuation loop, ensuring the network degrades gracefully to a safe operating mode.
- Publish research findings in high-impact journals and present at leading conferences, including but not limited to, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, ACM Transactions on Privacy and Security, IEEE Symposium on Security and Privacy, ACM CCS, USENIX Security Symposium.

You will contribute to the preparation and submission of project deliverables, milestone documents, research proposals, standards applications and patent applications, and contribute towards further evolving the existing experimental facilities and assist in project management duties.

Administration Responsibilities

Support organisation of events relating to the project as well as research dissemination (e.g. industrial workshops, scientific knowledge, and skills exchange days, etc.)

Teaching Responsibilities

As this role is a Pathway 2 (Research) role, there are no formally specified teaching duties required of the role holder. However, other commitments permitting, the role holder may be given development opportunities to undertake activities such as teaching on Masters and Doctoral programmes and/ or supervising MSc dissertations within the school, as appropriate.

Relationships

The post holder will work with Dr Rasheed Hussain, Dr. Yulei Wu, and Professor Dimitra Simeonidou, and collaborate with other members of the Smart Internet Lab.

Line manager: Dr. Rasheed Hussain

Job Hazards/Safety Critical Duties

N/A

PERSON SPECIFICATION

2.1. Relevant Experience, Skills and Knowledge

Essential (all candidates)

- Knowledge of **cybersecurity, network security, and artificial intelligence in network security with in-depth understanding of fundamental cybersecurity concepts, including threats, vulnerabilities, attack surfaces and security controls.**
- Good working knowledge of telecom standard and specs, e.g., ORAN specs and standards, 3GPP Specs and Standards, ETSI, etc.
- Experience of conducting experimental research and/or technical investigations using systematic and evidence-based approaches.
- Programming experience, preferably using **Python** or another suitable programming language, working in a **Linux/Unix-based research or development environment.**

- Ability to work independently on defined research tasks while contributing effectively to a research team and meet agreed project milestones, deliverables and deadlines and to understand and critically evaluate academic and technical literature.
- Willingness and ability to learn new technologies, tools and research methods relevant to agentic AI and future networks.

Essential (Candidates for Grade J positions)

In addition to the above, candidates appointed at Grade J should demonstrate:

- Substantial research or equivalent professional experience in **cybersecurity, AI security, network security, artificial intelligence, and telecommunication networks**.
- Specialist knowledge in at least one area directly relevant to Stream 4, such as:
 - AI/ML security;
 - agentic or autonomous AI;
 - cybersecurity threat modelling;
 - adversarial AI;
 - network security;
 - anomaly detection;
 - zero-trust security; or
 - security monitoring and assurance.
- Knowledge of E2E Agentic Orchestration, Agentic MCP tools, Opensource AI frameworks and models (Ollama, Huggingface), Langchain and vLLM
- Experience with any cloud platform, e.g., azure, aws, gcp, hands on skills with relevant opensource orchestration and observability frameworks and tools

Essential (Candidates for Grade K positions)

In addition to the above, candidates appointed at Grade K should demonstrate:

- Substantial postdoctoral or equivalent research experience in a relevant area.
- A strong and demonstrable specialist research profile relevant to AI in **cybersecurity, AI security, autonomous/agentic AI security, networking, telecommunications or related fields**.
- Evidence of **independent research leadership**, including responsibility for defining research questions, methodologies or technical directions.
- Experience with E2E Agentic Orchestration, Agentic MCP tools, experimental prototyping and demonstrations

Desirable (all candidates)

The following experience, skills and knowledge would be advantageous:

- Experience in **agentic AI, autonomous AI systems or multi-agent systems**.
- Knowledge of security challenges associated with AI systems that can use external tools, APIs, or infrastructure.
- Experience with **AI security, adversarial machine learning or AI red teaming**.

- Experience with cybersecurity threat modelling and attack scenario development.
- Knowledge of **zero-trust architectures and security principles**.
- Knowledge of **5G, private 5G, 6G**, network functions, network orchestration, NFV, SDN, Open RAN or network slicing **and future telecommunications networks**.
- Experience with network telemetry, observability, cloud-native technologies, containerised environments, and working with experimental network/testbed environments.
- Experience with cloud-native technologies and/or containerised environments.
- Demonstrable experience conducting research specifically in **AI security, agentic AI security, autonomous systems security or network security**.

2.2. Relevant Qualifications

Essential

- A PhD or near completion or equivalent R&D experience in computer science, networks or communications, and/or demonstrated experience with at least 3 of the following areas, industrial setting or clinical setting equivalent to a PhD. Applied AI/ML in (future) networks security.
- Agentic AI security in 5G and Beyond networks
- Threat Modeling Security and vulnerability assessment
- Agentic AI security
- Zero Trust frameworks and adversarial AI
- AI/ML/container orchestration and MLOps platforms

2.3. Communication and Interpersonal Skills

Essential (all candidates)

- Excellent verbal and written communication skills with a proven ability to work and communicate well across functional groups and with a wide range of people
- Excellent ability to work as part of a team and to be open-minded and cooperative
- Ability to produce clear and well-structured technical reports, research papers and project documentation.
- Ability to present research findings effectively to academic and/or technical audiences.
- Ability to listen to, consider and incorporate feedback from colleagues and collaborators.
- Ability to lead technical discussions within areas of specialist expertise.

Essential (Candidates for Grade J positions)

- Demonstrable ability to communicate specialist research findings confidently to academic

and industrial audiences.

- Ability to explain complex cybersecurity, AI or networking concepts to researchers from other disciplines.
- Experience contributing to collaborative research outputs and technical presentations.
- Ability to develop effective working relationships with external project partners.
- Ability to represent the research team appropriately in technical meetings and research events.
- Ability to provide constructive technical guidance to less experienced researchers or students.

Essential (Candidates for Grade K positions)

- Experience in presenting research results in technical meetings and contributing to standardisation activities
- Excellent ability to communicate complex and novel research clearly to **academic, industrial and wider stakeholder audiences**.
- Demonstrable ability to lead technical and research discussions and ability to communicate research strategy, technical risks and research findings effectively to senior colleagues and project stakeholders.
- Demonstrated ability to represent the University and research project professionally in external engagements and demonstrated ability to mentor and support less experienced researchers.

2.4. Additional Criteria

Essential

- Ability to prioritise and work to deadlines while demonstrating a track record for innovation and creativity.
- Ability to update and acquire new skills and knowledge in line with advances in the relevant subject area.

2.5. Selection Criteria

Selection will be done in two stages with research presentation and interview, and practical tasks to demonstrate some of the aforementioned skills.

3 CAREER PATHWAY AND OTHER RELEVANT INFORMATION

3.1. Career Pathways

All members of academic staff have a clear career pathway involving a series of levels with distinct role profiles, each with its unique requirements. Each profile sets out what is expected of an academic at the particular level. The role profiles also set out a collection of competencies expected for each level. Progression or promotion to the next level will occur after these competencies have been attained and where a role at the higher level is available.

The academic pathways are as follows:

Career Pathway One - academic roles that combine teaching, research and administrative duties.

Career Pathway Two - academic roles focusing on research and associated administrative duties.

Career Pathway Three – academic roles focusing on teaching and associated administrative pathways.

This post is located on Pathway Two. Role Summaries setting out what is expected of an academic at each particular profile level on pathway two can be found below. Please note that an appointment may be made at any level of the pathway.

A schematic diagram of the career pathways can be found at

<http://www.bristol.ac.uk/hr/grading/academic/>.

For Pathway Two roles progression to the next level will only occur where a role has been identified as being eligible for progression, having reached the relevant point on the salary scale and after the relevant competencies have been attained. A progressable role is a role at Level b or Level c that has been determined as being eligible for progression by the Head of Department, based on departmental needs, priorities and funds. Individuals in progressable roles at Level b or Level c are expected to develop their skills, knowledge and experience in order to ultimately progress to Level c or Level d, as applicable. A non-progressable role is one either at Level a (which are not subject to formal progression arrangements, although there may be opportunities to develop into a Level b role, based on departmental needs, priorities and funds), or at Level b or c for which the Head of Department has identified an ongoing need at that particular level. Movement to Level e will be by promotion only.

3.1.1 Role Summaries

Research Associate (Level a)

Role holders at this level are concerned with *assisting* an individual research leader or team to conduct a particular study (or group of studies). They will generally be involved in data generation and/or

collection using standard and well-defined methods developed by others. They will be working under close supervision by, and direction from, a more senior researcher, who will be ultimately responsible for the project. This may be the entry level for some staff who are expected to train and/or develop to take on more senior researcher roles. Role holders will be provided with academic and pastoral support within the department (including counselling on realistic career opportunities) and training will be available designed to develop their competences and to prepare them to take on more responsibilities associated with a higher grade.

Senior Research Associate (Level b)

Role holders at this level will be experienced and professional researchers (or have considerable professional experience) and will be specialists in a particular area or methodology, drawing upon knowledge gained from postgraduate research and/or working within a Level a role. They will be *associated* with a particular project (or projects) and will contribute ideas, and/or enhancement of techniques or methodologies. They will be expected to do some writing for dissemination outside the Department. They will still be working under supervision, but will be expected to take significant initiatives in their work and consult with the Principal Investigator over the details of the project. They may, where practical, contribute to the department's teaching, through supervision of projects, overseeing practical classes, or taking small group classes. They will be provided with academic and pastoral support within the department and training will be available designed to develop their competences (including counselling on realistic career opportunities) and prepare them to take on more responsibilities associated with a higher grade.

Research Fellow (Level c)

Role holders at this level will have substantial experience of research (normally not less than six years). They will initiate and take responsibility for some research projects and may be Principal Investigators or, where a Research Council does not permit this, act as though they were Principal Investigators. They will be involved in administration relevant to their projects (e.g. helping to prepare bids for research funding), managing other researchers and monitoring research budgets. They will be expected to be undertaking research individually and/or collectively and to be advancing the state of knowledge and understanding within their particular area of expertise. They will be publishing regularly in high quality outlets. They are likely to provide some teaching support for the department (consonant with the terms of their funding). They will be expected to be establishing a growing reputation within their particular research field and academic discipline and to be developing and demonstrating intellectual independence.

Senior Research Fellow (Level d)

Role holders at this level will have extensive experience in research and research management. They will normally be Principal Investigators, leading collaborative research bids and research teams, or driving forward innovative research themselves. They will be involved in scholastic projects (e.g. editing

journals and academic books), and be making a significant leadership and/or management contribution within their department or the wider university, to be participating in national/international academic networks and conferences. They may be transferring their knowledge through some teaching and/or supervision to undergraduate or graduate students (consonant with the terms of their funding). Role holders at this level will be independent researchers and will have an established national and growing international reputation within their academic discipline generally and research field in particular.

Professorial Research Fellow (Level e)

Role holders at this level will have very extensive experience of research leadership and related management/administration. They will enjoy a wide recognition for their expertise within the academic community internationally (as evidenced by conference invitations, journal editorships, office holding in specialist groupings, associations with appropriate Research Councils etc.). They will have made recognised and significant contributions to the developing knowledge and understanding of their research area. They will already have responsibilities for the creation, initiation, development and overall management of significant research programmes. They will “profess” their discipline within the Department, as appropriate and consonant with the terms of their funding. They may also carry significant leadership roles within the Faculty or University.

3.2. Smart Internet Lab

The Smart Internet Laboratory is one of the UK's most renowned Information and Communications Technology (ICT) research centres. Our 200 experts address grand societal and industrial challenges associated with 5G/6G radio/wireless, optical communications, and networks. We are challenging the complexity of tomorrow's world by fusing research expertise and innovation in areas such as IoT, 5G/6G & Beyond, Future Transport Networks, Smart Cities, Autonomous Networks, Machine Learning, Artificial Intelligence, Network Convergence, Mobile Edge Computing, and Network Softwarisation. Our unique offering across optical, wireless, IoT, and cloud technologies enable us to bring together end-to-end network design and optimisation, impacting regional, national, and global ICT innovations.

This is an open-ended position starting as soon as possible, with fixed funding until 29 February 2028 in the first instance.

Informal enquiries should be addressed to Dr. Rasheed Hussain (rasheed.hussain@bristol.ac.uk).