The Alan Turing Institute

Post-Doctoral Research Associates (x6) – Enhancing Security and Privacy of National Identity Systems

THE ALAN TURING INSTITUTE

There has never been a more significant time to work in data science and AI. There is recognition of the importance of these technologies to our economic and social future: the so-called fourth industrial revolution. The technical challenge of keeping our data secure and private has grown in its urgency and importance. At the same time, voices from academia, industry, and government are coming together to debate how these technologies should be governed and managed.

The Alan Turing Institute, as the UK's national institute for data science and artificial intelligence, plays an important part in driving forward advances in these technologies in order to change the world for the better.

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. The Institute's goals are to undertake world-class research, apply its research to real-world problems, driving economic impact and societal good, lead the training of a new generation of scientists, and shape the public conversation around data and algorithms.
After launching in 2015 with government funding from EPSRC and five founding universities, the Institute has grown an extensive network of university partners from across the UK and launched a number of major partnerships with industry, public and third sector. Today it is home to more than 400 researchers and a talented business team.

PDRA-ID-as-a Service- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about threat modelling and security analysis of possibly future ID infrastructure aligned to national digital identity systems.

ID-as-a-Service is an emerging requirement in many modern societies across the developed and developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into existing and new tools and techniques to support ID-as-a-service, that meets goals for privacy for users, and does not lead to unintended consequences.

This is an opportunity to influence the design of future identity systems around the world - there are many pressures on the design of such systems, and the role should prove fascinating.

PDRA- Pivacy Enhnacing Technologies- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about the design, deployment, and evaluation of Privacy Enhancing Technologies as part of new digital identity systems.

ID-as-a-Service is an emerging requirement in many modern societies across the developed and developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly. However, systems come with strong security requirements, including confidentiality and integrity.

This role in the project entails research into existing and new tools and techniques to support ID-as-a-service, that meets goals for privacy for users, and does not lead to unintended consequences.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into existing and new tools and techniques to support ID-as-a-service, that meets goals for privacy for users, and does not lead to unintended consequences.

PDRA-Real-time Governance- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about the design, deployment, and evaluation of real-time cyber security technologies as part of new digital identity system protection (real-time governance).

The provision of digital infrastructure such as foundational identity systems is an emerging requirement in many modern societies across the developed and developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly. However, systems come with strong security requirements, including confidentiality and integrity.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into existing and new tools and techniques to support such digital infrastructure, that meets goals for privacy for users, and does not lead to unintended consequences.

PDRA- Risk Modelling- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about modeling and quantification of risk in schemes for national digital identity systems.

National identity schemes can be used to support access to services, including financial, healthcare and food, and there is a strong push to support their implementation across the developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly. However, it is vital that such systems are secure against privacy invasions and manipulation by malicious actors.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into understanding the risk to governments, third sector organisations and those enrolled within the scheme. Specifically, the postholder will be involved in the measurement of risk by considering and quantifying harms and likelihood of compromise of the system.

There is a recognized challenge in effective risk quantification, especially in the area of cyber and information risk. This work will be at the interface between applied mathematics, statistics, probability and cyber security. This project will address such issues by developing the metrics and management strategies for risk in national digital identity schemes.

PDRA- Threat Modelling- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about threat modelling and security analysis of schemes for national digital identity systems.

National identity schemes can be used to support access to services, including financial, healthcare and food, and there is a strong push to support their implementation across the developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly. However, it is vital that such systems are secure against privacy invasions and manipulation by malicious actors.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into understanding the vulnerabilities in national identity systems, exploring those actors that may attempt to compromise such systems, and how they might achieve this exploitation. Issues such as access to the system will need to be considered, as well as the motivations and capabilities of those wishing to abuse the system. The project will also seek to define countermeasures to prevent, or mitigate the effects of, threats to the system.

PDRA-Trust Framework Development- Enhancing Security and Privacy of National Identity Systems

THE ROLE

This position is about the design, deployment, and evaluation of a Trust Framework to be used in the development of national digital identity systems.

National identity schemes can be used to support access to services, including financial, healthcare and food, and there is a strong push to support their implementation across the developing world. New techniques for deployment at scale promise to improve the assurance of users' rights to access to various digital and physical resources, vastly more easily, cheaply and quickly. However, it is vital that such systems are trustworthy, since there are many actors that aim to abuse the system.

DUTIES AND RESPONSIBILITIES

This role in the project entails research into developing Trust Frameworks to Support National Identity Systems. There has been some good initial work in developing the principles for such Trust Frameworks by both NIST and OIX. This work will develop on those efforts to develop a trust framework that covers the privacy and security requirements in an evolving world. For example, the 2018 NIST work (https://doi.org/10.6028/NIST.IR.8149) highlights the need for *Recognizing & Communicating Conformance*. This project will address such issues by developing the metrics and conformance assessment mechanisms for the Framework being developed.

PERSON SPECIFICATION

The successful candidate will have:

ESSENTIAL

- Successful candidates will hold (or be close to completing) a PhD in Computer Science or related dsicpline .Appointment at Research Associate level is dependent on having a PhD or having equivalent skills and experience through non-academic routes. Where a PhD has yet to be awarded appointment will initially be made as a research assistant and amended to research associate when the PhD is awarded.
- Experience of or aptitude for rigorous computer system and security design, implementation, measurement and evaluation, including experiment design, data capture, and data analysis. This may have been gained in commercial or industrial settings as well as through production of academic papers. Good to substantial Knowledge of Privacy Enhancing Technologies capabilities and limitations is essential, especially basic privacy technologies, but also newer technologies, e.g. secure enclaves, differential privacy, and secure multi-party computations (for example).
- Ability to communicate clearly in English, in both written and spoken forms.

- Experience of working independently and in medium to large-scale teams, on collaborative and interdisciplinary research projects with academic and industrial partners. Dealing with users in the real world will be very important.
- Evidence of an excellent publication record, commensurate with level of experience. Candidates from outside academia may be able to evidence this by providing examples of technical writing or system design and implementation, published or distributed through channels other than academic conferences and journals, e.g., blog posts and/or software repositories.

DESIRABLE

- Familiarity with data science techniques and applications, including machine learning and statistics.
- Other language skills may be an asset.
- The post holder may be required to travel within the UK and internationally.

TERMS AND CONDITIONS

This full-time post is offered on a fixed term contract until 2022, with possibility for extension (funding permitting).starting as soon as possible. We are happy to talk flexible working.

The salary range offered for this role is £35,000 – £41,000 (dependent on experience and skills). A competitive benefits package is also available (https://www.turing.ac.uk/work-turing/why-work-turing/employee-benefits).

APPLICATION PROCEDURE

If you are interested in this opportunity, please click the apply button below. You will need to register on the applicant's portal and complete the application form including your CV, covering letter and contact details for your referees.

Please specify in your cover letter which of the six PDRA specialisms you are most interested in.

If you have questions or would like to discuss the role further with a member of the Institute's HR Team, please contact them on 0203 862 3394 or 020 3862 3357, or email recruitment@turing.ac.uk.

EQUALITY, DIVERSITY AND INCLUSION

The Alan Turing Institute is committed to creating an environment where diversity is valued and everyone is treated fairly. In accordance with the Equality Act, we welcome applications from anyone who meets the specific criteria of the post regardless of age, disability, ethnicity, gender, gender reassignment, marital and civil partnership status, pregnancy, religion or belief or sexual orientation. Reasonable adjustments to the interview process can also be made for any candidates with a disability.

Please note all offers of employment are subject to continuous eligibility to work in the UK and satisfactory pre-employment security screening which includes a DBS Check.

Full details on the pre-employment screening process can be requested from HR@turing.ac.uk***.***