- **Are you an ICT graduate in computer science or cognate discipline looking to pursue a PhD?**
- **Do you want to make a real contribution in the area of cybersecurity for the IoT?**
- **Do you want to study with a world leading SFI research centre?**

Science Foundation Ireland (SFI) Centre for Future Networks and Communication in partnership with Munster Technological University (MTU) and Waterford Institute of Technology (WIT) is seeking to recruit a PhD student to contribute to the area of cybersecurity for the Internet of Things (IoT).
The student will be a member of the SFI CONNECT research centre and will be physically based in MTU, jointly supervised by Prof Donna O'Shea (MTU), Dr Mubashir Hasain Rehmani (MTU) and Dr Bernard Bulter (WIT).
The structured PhD position is a fully funded position for 4 years.

The student will be expected to contribute to CONNECT Education and Public Engagement (EPE) activities with the aim of bridging the gap between the research community and society. The successful candidate will be expected to carry out a minimum of 2 engagement activities per year and engage with the EPE activities for the centre. This can include participating in public events to promote research, writing media articles or contributing to educational activities. Researchers will be supported by ongoing training and the EPE team. For more examples of CONNECT EPE activities see here: https://connectcentre.ie/public-engagement/.

Further information on the project is outlined below:
The student will be expected to carry out innovative research in Zero Trust (ZT) security for the Internet of Things (IoT) providing an alternative to existing perimeter-based approaches to network security. The concept of a Zero Trust (ZT) model for cybersecurity was first introduced by John Kindervag at Forrester Research. ZT treats every network user as a possible danger, requiring vetting before receiving access. This flips the traditional perimeter-based approach to network security, leveraging firewalls and VPNs, where it often assumed that everyone on the inside of an organizations network was a good actor and did not pose any security threat. Prior to Industry 4.0, a limited attack surface meant that the network was considered secured within the established perimeter. With Industry 4.0, there is an ever-expanding number of new attack vectors meaning that this assumption can no longer be taken for granted. Perimeter based security, using firewalls and VPNs, also means that once network access is granted, users have full access to resources inside the network which increases risk of east-west movement and lateral based attacks. Given this context, the research aim of this project is to undertake pioneering scientific research in ZT and to evaluate this approach to network security to deal with the increased threat landscape introduced through IoT, complex digital supply chains and increased remote workers.

To apply, please send a CV, Motivational Letter, Proof of Degree and Transcript of Results, and English Language certification (if required) to Donna O'Shea at info@cyberskills.ie