

University College Dublin  
School of Computer Science



**Guide For Applicant**  
PhD Scholarship 2025

## Table of Content

1. PhD Scholarship.....	3
2. Eligibility.....	3
3. Guidelines Application Form.....	3
Degree and Transcripts.....	4
English language.....	4
Applicant's Research Project.....	4
Research Project offered by the school.....	5
4. Assessment Process.....	5
5. Notification.....	6
6. Template Application Form 2025.....	7
Contact Details.....	7
Academic Track Records.....	7
Further Track Records.....	9
Personal Statement.....	11
Research Project.....	11
Research Preference.....	12
Referees.....	13
Demographic Details.....	14
7. Research projects offered by the school.....	16
Prediction of long-term clinical risk from psychosis using multi-modal machine learning.....	16
Designing neural network architecture and representations to solve discrete optimisation problems.....	17
Unlocking Parliamentary Data with Large Language Models.....	18
Graph-based Recommender System.....	19
Large Language models for Recommender Systems.....	20
Novel Drug Creation Using Evolutionary Computation.....	21
Abstention and Explanation of Classification of Images.....	22
AI for mining, forecasting, and explaining public opinion using social media polls.....	23
Quantum Machine Learning.....	24
QUANTUM-MIRROR: AI-Enhanced Multi-Layer Secure Quantum Network with Digital	

Twin Integration.....	25
Automated Decision-Making in Ethically Charged Scenarios.....	26
Computer Science Education - Project Negotiable.....	27
Designing AI-Powered Peer Support Systems to Promote Inclusive Mental Health Help-Seeking.....	28
Adaptive Sensory Environments in XR: Leveraging Real-Time Feedback with Diffusion Models... 29	
Information Retrieval for case law and legal statues.....	30
LLM-Powered Security Policies Orchestration and Enforcement in 6G OpenRAN.....	31
Adaptive Bit Allocation for Robust Proactive Deepfake Defense.....	32
Privacy preserving techniques for large languages Models (LLMs).....	33
A Novel Dataset & Framework for Anomaly-Based Intrusion Detection in Software-Defined Networking.....	34
Sustainable Security.....	35
Automated and Intelligent Future Networks (Wireless, Optical, IP).....	36
Automating AI Incident Threat Intelligence.....	37
Distributed ledgers in the quest of fake news detection.....	38
Enhancing Microservice Architectures through Enterprise Knowledge Graph Integration.....	39
Scalable Universal Collective Communication Algorithms for Large Scale Deep Learning on Extreme Scale Heterogeneous Hybrid Platforms.....	40
LLM@Edge: Optimized Deployment of Large Language Models on Distributed Edge Systems	41

## 1. PhD Scholarship

The scholarship will fund applicants intending to pursue full-time doctoral studies in UCD School of Computer Science. The scholarship value is up to €132,000 for 4 years full-time research studies and includes a tax-free stipend (€22,000 annually), [annual registration fee](#), research travel expenses to enable the applicant to carry out activities related to the research project (€3,000 in total) and a new laptop.

In addition, all doctoral candidates will do some demonstration and/or teaching assistant hours in the school as part of their career development.

## 2. Eligibility

### Minimum requirements

The applicant must have a first-class or upper second-class honors bachelor's in an undergraduate degree in Computer Science, Mathematics, Engineering, Science, or a similar technical discipline. If the applicant does not have a minimum of 2.1 grade bachelor's, or the equivalent, degree, they must possess a minimum of 2.1 grade master's degree.

The applicant has to complete the undergraduate studies by June 2025 to be eligible for the scholarship.

### Desirable requirements

Other desirable requirements are outlined in the Project Descriptions offered this year

## 3. Guidelines Application Form

This symbol \* represents a mandatory field. Application submission will fail if fields containing this symbol are unanswered or a document is not uploaded.

The online application does not have a “save and return” option and a submitted application cannot be edited. The applicant is advised to prepare the application offline and when fully satisfied to copy the answers and submit the online form.

## **Degree and Transcripts**

The applicant must upload an official English language version of the degree results. The document has to be endorsed by the academic institution that released it.

If undergraduate examination results are not known at the time of application, the applicant has to upload official transcripts. UCD School of Computer Science may make a provisional offer of a scholarship on condition that the scholar's bachelor's degree result is a first-class or upper second-class honours.

The official english document(s) has to be a single PDF file.

## **English language**

Non-native English speakers require at least IELTS 6.5 (with at least 6 in all components) or equivalent (further details on equivalence of tests are available [HERE](#)).

Uploading the English test is not mandatory at the application stage. Applicants who have not provided proof of IELTS or an equivalent test in the application will be asked to send the document if they are invited to an interview.

## **Applicant's Research Project**

The applicant has to provide a short research project description that fits into one of the Research Area of UCD School of Computer Science. Details of the [research areas](#) are available on the school website. The proposed project cannot exceed 500 words and has to include aims and objectives of the the research idea, how existing literature on the topic has been used to inform the project and how the project will advance state of the art and make a contribution to existing knowledge.

**It is expected that the proposed research project is entirely the applicant's own work.** Random sampling for evidence of plagiarism and excessive duplication will be carried out during the evaluation and award process. In the instance of plagiarism or excessive duplication is identified the application will be deemed ineligible and award offers will be withdrawn.

Plagiarism means using the work of others without acknowledging the original source. This includes presenting ideas, theories, concepts, methodologies or data from the work of another person (including other students, friends, family, or purchasing work from a third party) without acknowledgement and appropriate citation.

## Research Project offered by the school

The applicant has to indicate a project offered by the school that is most interested in. Successful applicants will be working either on the project that they have proposed or on the selected research project proposed by the school.

## Referees

Referees will be contacted if the applicant is shortlisted for an interview. We recommend to inform the referees at application stage.

## 4. Assessment Process

The applicant will be evaluated through a three stage selection process:

### Stage.1 Application form

To assess track record, research potential, evidence of independent thinking, clarity of the proposed research project

### Stage.2 Technical interview

To assess match between the applicant and both the proposed project and the selected project

### Stage.3 Competency-based interview

To assess match between the applicant and the research culture in the school of computer science

Key Dates	
Application deadline	10 Febr 2024 at 17:00 (Irish Time)
Technical interview	February-March 2025
Competency-based interview	April 2025
Scholarship offer	May 2025
PhD Start Date	1 Sept 2025

## **5. Notification**

The applicant will be informed of the outcome at each stage of the selection process but due to the high volume of applications the school of computer science will not be able to provide individual feedback on the application and interview.

The school will not reply to inquiries on the status of personal applications and applicants should check the email spam folder regularly.

## 6. Template Application Form 2025

### Contact Details

Email\*

First Name\*

Last Name\*

### Academic Track Records

Bachelor's degree institution\*

Insert the name of the institution

---

Bachelor's degree graduation date\*

If you have not yet completed your master's degree please indicate your expected completion date.

dd/mm/yyyy

---

Bachelor's degree full qualification type and name\*

Insert your answer

---

Q4. Bachelor's degree final grade or grade point average\*

Please clearly describe the grading scheme that your grade is based on (for example the minimum and maximum values of the scale; e.g.: 9 on a scale of min:5 and max:10).

Insert the name of the institution

---



Bachelor's degree transcript - upload\*

On the online form upload an official English language version of your Bachelor's degree transcript document(s) in a single PDF file. Please also include a description of the grading scale used by your institution. Please name your file "Bachelors\_Transcript\_FN\_LN.pdf" where your FN is replaced with your first name and LN is replaced with your last name.

Master's degree Type

If you do not hold a master's degree leave blank this and the following related questions. If you have yet to complete this degree enter your expected graduation date and leave the final grade section blank  
Delete as appropriate

Taught / Research

---

Master's degree institution

Insert the name of the institution

---

Master's degree graduation date

If you have not yet completed your master's degree please indicate your expected completion date.

dd/mm/yyyy

---

Master's degree full qualification name

Insert your answer

---

Master's degree final grade or grade point average

Please clearly describe the grading scheme that your grade is based upon (for example the minimum and maximum values of the scale; e.g.: 9 on a scale of min:5 and max:10).

Insert your answer

---

Upload an official English language version of your master's degree transcript document(s) in a single PDF file and include a description of the grading scale used by your institution. name your file "Masters\_Transcript\_FN\_LN.pdf" where you FN is replaced with your first name and LN is replaced with your last name.

Are you a native English speaker or have you completed your studies through the medium of English in the last two years\*

Delete as appropriate

Yes / No

---

If you are not a native English speaker please upload a copy of your official English language certification or proof that you carried out your studies through the medium of English within the last two years

For illustration, the list of UCD minimum language requirements is available here:

<https://www.ucd.ie/registry/admissions/elr.html>

Please name your file "English\_Certificate\_FN\_LN.pdf" where you FN is replaced with your first name and LN is replaced with your last name.

## Further Track Records

### Other Education\*

Please provide details of any additional educational achievements not detailed in the previous section (for example other degrees or qualifications).

Insert your answer

---

### Research Achievements\*

Please provide any additional information regarding your research achievements to date such as final year projects, publications, research awards, creation of data sets and databases, conference papers, patents, etc. [Max 250 words]

Insert your answer

---

Journal/Conference/book/etc - Name

If you have one or more publications, select one that you think is most relevant and indicate the venue of the publication (e.g.: name of the journal/conference/book/etc).

Insert your answer

---

Journal/Conference/book/etc - Description

Tell us the novel concepts and approaches of the above publication and how you contributed to the paper  
*[Max 250 words]*

Insert your answer

---

Technical skills & achievements\*

Describe your current level of proficiency in maths, programming (e.g. C++, Java, Python, R) and **knowledge in one of the [School research areas](#)**. Provide evidence to support your assessment. Also provide information regarding your technical achievements to date such as significant systems built, contributions to open source projects, etc. *[Max 250 words]*

Insert your answer

---

Work Experience\*

Please provide details of any relevant work experience, including voluntary work, to date which should include employers' names, job titles, nature of duties and responsibilities, as well as duration of employment. *[Max 250 words]*

Insert your answer

---

ORCID ID

include an ORCID ID to list publications

---

Github Repository

include a Github Repository to show examples of coding projects

---

Google Scholar page

include a Google Scholar page to list publications

---

## Personal Statement

Motivation\*

Please address the following questions:

- Why do you want to pursue a PhD?
- Which of your attributes demonstrate your capability to be a good researcher, e.g. motivation, commitment, thirst for knowledge?
- What research area in Computer Science you are interested most and what skills you think you need to build to work in this domain ? *[Max 500 words]*

Insert your answer

---

## Research Project

Research Project\*

Provide details of your proposed research project to include

- (a) aims, objectives and central research questions of the project,
- (b) how existing literature on the topic has been used to inform the project

(c) how the project will advance state of the art and make a contribution to existing knowledge  
[Max 500 words]

Insert your answer

---

Select a thematic [Research Area](#) for the proposed project.\*

Delete as appropriate

- Bioinformatics and Health Informatics
- Data Science, Machine Learning & Artificial Intelligence
- Emerging Topics
- Foundations of Computing
- Human-Computer Interaction
- Information Systems
- Intelligent Sensing and Multimedia
- Security and Networks
- Software Engineering and Distributed Systems

Name of Collaborator in UCD CS

If you have developed this research project with an academic of UCD School of Computer Science please name them here.

Insert your answer

---

## Research Preference

Indicate the research project proposed by us you are most interested in. If you are offered a scholarship you will develop one of these projects in a co-creating style with the academic who will supervise you.

Indicate your highest preference of proposed projects\*

Select the title of the project from the dropdown list

---

Justification for choosing this project\*

Please outline your reasons for choosing this project and if you have already some knowledge about the topic

Insert your answer

---

IRC Application\*

Have you applied to the "IRC-Postgraduate Scholarship Programme 2025" Call?

Delete as appropriate

Yes/No

---

IRC Application - Supervisor's Name

Provide the name of the academic that supported your proposal if you submitted an application to the "IRC-Postgraduate Scholarship Programme 2025"

Insert your answer

---

## Referees

Contact details of two referees who we will contact if you will be invited to an interview. Include name, institution, email address, phone number, and a short description of your relationship to the referee.

Please inform your referees about this application and required reference.

Referee 1\*

Name and Surname

Insert your answer

---

Email\*

Insert your answer

---

Institution and relationship to the applicant\*

Insert your answer

---

Referee 2\*

Name and Surname

Insert your answer

---

Email\*

Insert your answer

---

Institution and relationship to the applicant\*

Insert your answer

---

## Demographic Details

How do you currently describe your gender identity?

To assist us in ensuring diversity among the student cohort, we request an indication of gender.

Delete as appropriate

Female/Binary/Male/Transgender/Other/Prefer Not to Say

---

What's your nationality, i.e.: your passport-issuing country?\*

Insert your answer

---

In what country are you currently located?\*

Insert your answer

---

How did you hear about this PhD Scholarship?\*

Select one and delete the remaining

- LinkedIn
- Facebook
- Twitter
- [Jobs.ac.uk](http://Jobs.ac.uk)
- Computer Science Website
- Friend
- My Supervisor
- Websearch
- FindaPhD
- Google Group
- Other:



## 7. Research projects offered by the school

### Research Area

Bioinformatics and Health Informatics

### Project Title

Prediction of long-term clinical risk from psychosis using multi-modal machine learning.

### Project Overview

Psychosis, a severe mental disorder characterized by a disconnection from reality, often delays treatment by six months to a year, underscoring the need for improved detection and intervention. Affected conditions include schizophrenia and severe mood disorders. Existing detection models primarily use single-source data (e.g., behavior, genetics, or neuroimaging). Although effective in controlled settings, these models struggle to translate into real-world clinical practice due to several factors.

### Research Objectives

The central goal is to develop a user-centred machine learning model to assess mental health risk. This model will incorporate multimodal data streams, including available clinical data, behavioural patterns and self-reported state with the aim of exceeding the current benchmarks of predictive performance. A secondary goal is to assess feasibility and acceptability of this model among individuals with psychosis and clinical professionals. The research will be conducted in collaboration with clinical partners at the Dublin & East Treatment & Early Care Team, a specialist service that supports individuals experiencing distressing perceptual disturbances. This setting will provide access to existing datasets to support model development.

This scholarship intersects three core research themes: AI, Human-Computer Interaction, and Digital Health. It has the potential to positively impact psychosis treatment and will directly foster a new collaboration between the School of Computer Science, the School of Psychology, and DETECT. Additionally, it will provide vital data and partnerships to pursue further grants. If awarded, we will apply for the Irish Research Council PhD scheme in October 2025, returning any unused funds.

### Keywords

digital health, machine learning, human computer interaction

### Desirable Requirements

2.1+, undergraduate in Computer Sci, Math, Eng or Science, real world Eng and Data Science experience.

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Designing neural network architecture and representations to solve discrete optimisation problems

## Project Overview

Combinatorial optimisation problems arise naturally in many areas of computer science and other disciplines, such as business analytics, operations research, bioinformatics and electronic commerce. Since many of these optimisation problems are NP-hard, applications typically rely on meta-heuristic frameworks, approximation algorithms and carefully designed heuristics for specific instance classes to solve them efficiently. However, the resultant solutions can be very far from optimal and the development of good algorithms often require significant human effort. The goal of this PhD project is to augment the human ability to design good algorithms and data structures by using machine learning techniques to explore the search space efficiently. Specifically, we would like to explore the design of neural network architecture and representations to solve discrete optimisation problems, such as those arising in the context of graphs and geometry. The representations should ideally generalise the known approximation algorithms for classical problems.

Our research group has done a lot of work in this area and this PhD project will build on this research. "Effectiveness of SDP rounding using Hopfield Networks" Learning on Graphs 2024

"A scalable learning approach for the capacitated vehicle routing problem." Computers & Operations Research 2024

"Learning fine-grained search space pruning and heuristics for combinatorial optimization." Journal of Heuristics 2023

I encourage students with a background in CS, mathematics, physics, engineering or business analytics to get in touch with me. Students with a background in algorithms or theoretical computer science are particularly encouraged to apply.

## Keywords

Machine Learning, Combinatorial Optimisation, Algorithm Design, Graph Algorithms, Graph Neural Networks, Operations Research

## Desirable Requirements

Ideally, some background in machine learning and optimisation/algorithms.

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Unlocking Parliamentary Data with Large Language Models

## Project Overview

Parliaments are fundamental to modern democracies, yet citizens often find it challenging to keep track of their activities. Although open-access data policies aim to promote transparency, the sheer volume of information and the limitations of existing user interfaces often prevent the public from fully benefiting from these initiatives. This project aims to address these challenges by integrating large-scale, open-access parliamentary data with the latest advancements in large language models (LLMs), with the core goal of enhancing transparency around parliamentary activities. The methods developed during the project will enable users to perform natural language queries on parliamentary data, simplifying the process of finding information relevant to their interests in specific topics and policy areas. To maintain the integrity of the information provided, key objectives of the project will include: 1) mitigating the risk of potential "hallucinations," where responses may appear coherent but are factually incorrect or nonsensical; and 2) supporting verification by explaining responses through the citation of relevant sources in the original data. The project will also involve collaborating with political scientists at the UCD Connected\_Politics Lab to ensure that the project's outputs can facilitate greater transparency and accessibility, allowing the public to engage more effectively with parliamentary activities.

## Keywords

AI, Natural Language Processing, LLMs, Interdisciplinary Research

## Desirable Requirements

Ideally some prior familiarity with Natural Language Processing

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Graph-based Recommender System

## Project Overview

Recommender systems play an instrumental role in enhancing user experience across various e-commerce platforms, such as Amazon, eBay, etc., by suggesting relevant content, products, or services. Recent advances in graph-based recommender systems have demonstrated excellent performance by capturing intricate relationships and interactions among users, items, and contextual information. This proposal aims to investigate and develop novel graph-based approaches that capture and integrate user dynamic behaviours. The research seeks to bridge gaps in scalability, recommendation performance, and explainability, enabling a new generation of personalized/non-personalized and interpretable recommender systems, which will contribute to both academia and industry by pushing the boundaries of recommender system capabilities.

## Keywords

Recommender Systems, Graph Learning

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Large Language models for Recommender Systems

## Project Overview

This project aims to exploit the extraordinary ability of large language models to improve the performance of recommender systems. Recommender systems try to learn user preferences so they can suggest an item or service which the user will prefer. However, in many situations, additional contextual information about the user preferences is missing. Large language models are good at generating synthetic information which can be used to augment the training data for recommender systems. This LLM augmented data can enhance the personalisation of recommender systems, improve the training time and increase the performance. This research project will examine ways to enhance knowledge graph structures which can be exploited by the recommender system to improve its performance. Some knowledge of recommender systems and large language models is desirable.

## Keywords

recommender systems, LLM, machine learning, personalisation, knowledge graphs

## Desirable Requirements

computer science

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Novel Drug Creation Using Evolutionary Computation

## Project Overview

Protein design and discovery is the foundation of many medical advances, from drug and MRI contrast design, to creating proteins for cellular reprogramming. Recent advances in structural protein prediction have enabled rapid design of proteins with desired structural properties. However, understanding how to design proteins with specific functional or multi-functional properties is not well-understood. This is critically important for smaller proteins – peptides – where there is little to no secondary/tertiary structure to predict. This project aims to broaden the scope of Evolutionary Computation (EC) based Machine Learning in the area of peptide/protein design. EC based protein design differs from Protein Language Model (PLM) approaches as improved, novel peptides can be discovered with very few examples. This is crucially important peptides, such as anti-cancer peptides, will be novel and very few will exist, therefore building a large library, necessary to train a PLM, is unfeasible. This will be achieved by accelerating directed evolution of active variants via the creation of new software tools and other related tools that will allow multi-functional computational modeling to be an essential part of targeting different protein/peptide functions. The overall goal of the project will be to create state-of-the-art ML algorithms for multi-functional peptide prediction.

## Keywords

Optimisation, Evolutionary Computation, Peptides, LLMs

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

Abstention and Explanation of Classification of Images

## Project Overview

Abstention of prediction and explanation of the reason for abstention is a very important field, which is more relevant as more AI systems become a part of our day to day life.

Classification models can make predictions if a datapoint is from a class or another. Such models are used in many practical and often critical applications. Sometimes it is better not to predict the class of a datapoint because it is ambiguous with respect to the models, so that the decision can be left to the human experts. To assist the human experts it would be also beneficial to explain why the model did not predict and consider the datapoint ambiguous, give generated examples of what changes to the datapoint would have made the model to confidently predict that datapoint, etc.

This project will focus on the image domain to develop methods which can abstain from prediction which it is not confident, provide explanation of the reason for abstention, as well as provide robust counter-factual and semi-factual explanation datapoints which avoids ambiguous regions.

The overall high level objectives of the project are:

1. Generate a robust image classification system to identify ambiguous regions and quantify it
2. Use this to abstain from prediction
3. Generate visual examples (counterfactual/semi-factual, saliency maps) to explain why the abstention was done"

## Keywords

machine learning, abstention, robustness, xAI, image processing

## Desirable Requirements

Familiarity of machine learning algorithm internals, experiment methods will be a plus.

## Research Area

Data Science, Machine Learning & Artificial Intelligence

## Project Title

AI for mining, forecasting, and explaining public opinion using social media polls

## Project Overview

Public opinion is traditionally measured via surveys, but they often result in biased estimates of public opinion. Recently, other sources of information about public opinion rose in prominence: nearly a million informal polls are published on social media platforms each month. While social media polls tend to be more biased than traditional polls, these biases can be corrected. Our prior works show that bias-corrected social polls are more accurate in estimating popular support for the US presidential elections of 2016, 2020, and 2024 than traditional polls (see [socialpolls.org](https://socialpolls.org)).

The key objective of the project is to develop and evaluate the next generation of AI-powered methods to infer and explain the dynamics of public opinion based on social media polls. The project will develop and apply machine learning methods to infer attributes of users interacting with such polls, including age, gender, ethnicity, and partisanship. Then, the project will generate insight into the dynamics of public opinion on politically-relevant topics including: elections in multiple countries, such as the US, the UK, and India; and emerging issues of interest, such as support for military aid to Ukraine. The research will involve development of LLM-based systems for classification of polls, multimodal neural networks for user attribute classification, and (deep) autoregressive models forecasting election outcomes. The project will result in a groundbreaking data repository that will enable multiple areas of downstream research in various domains and will involve collaboration with world-class researchers from the US and Europe.

## Keywords

AI, NLP, models, computational politics, digital media, social polls



## Research Area

Emerging Topics

## Project Title

Quantum Machine Learning

## Project Overview

Understanding how and when to leverage machine learning for and/or with quantum computing is still in its infancy. Machine learning can be used to optimize quantum algorithms, and quantum computing can be used to develop new machine learning algorithms. This project will explore one of these directions (depending on the interest of the candidate). In quantum machine learning, i.e. using quantum computers to develop new machine learning methods, there are many challenges to solve: how to prepare data, developing new methods, interpreting the output of the quantum computer, handling error/noise etc. Similarly, when applying machine learning methods to quantum problems (e.g. controlling quantum systems, quantum error mitigation, quantum optimisation etc.) the challenge is to balance a rich understanding of the quantum system(s) with sufficient machine learning expertise to develop toolkits of value to the domain. Thus, the purpose of this PhD topic is to generate valuable tools and methods to further the understanding of where machine learning and quantum computing can benefit each other and identify meaningful application areas.

## Keywords

quantum computing, machine learning, optimisation

## Research Area

Emerging Topics

## Project Title

QUANTUM-MIRROR: AI-Enhanced Multi-Layer Secure Quantum Network with Digital Twin Integration

## Project Overview

This research project aims to revolutionize quantum network management through an advanced digital twin ecosystem. The system architecture integrates three cutting-edge elements: quantum network infrastructure, comprehensive digital twin simulation, and artificial intelligence (AI)-enhanced real-time optimization, creating an unprecedented level of network visibility and operational control in quantum systems.

The core innovation lies in our novel approach to quantum network management through an intelligent digital twin framework. Our system creates a complete virtual replica of the quantum network, including quantum repeater nodes, quantum memories, and entanglement distribution channels. This digital twin, powered by deep learning and reinforcement learning algorithms, enables unprecedented capabilities: real-time simulation of quantum state evolution, predictive analysis of network behaviour, and optimization of quantum routing protocols. The system maintains a dynamic model of critical parameters, including entanglement fidelity, decoherence rates, and quantum state transfer efficiency, enabling proactive network management and resource optimization.

The project will deliver a proof of concept demonstrating: (1) A comprehensive digital twin platform that mirrors and predicts quantum network behaviour in real-time, (2) An AI-driven optimization system for quantum network operations, including automated resource allocation and protocol selection, and (3) A scalable virtual testing environment for future quantum network protocols and technologies. This innovative approach enables network operators to visualize, optimize, and manage complex quantum networks through an intuitive digital interface. The technology has immediate applications in quantum internet development, distributed quantum computing, and quantum network research, positioning us at the forefront of quantum network management technology.

## Keywords

Digital Twin, Quantum network, Artificial intelligence, Quantum entanglement

## Research Area

Emerging Topics

## Project Title

Automated Decision-Making in Ethically Charged Scenarios

## Project Overview

Increasingly, human lives are affected by automated decision-making in various domains. These range from allocative decisions such as loan-appraisal or parole risk assessment to representational decisions such as image tagging in cultural contexts. These decisions have the potential to be ethically unsound, and therefore must be detected and computed accordingly. The development of ethical artificial agents is a multi-disciplinary endeavour, which requires a good understanding of philosophical tenets of good judgement, as well as the ability to forecast implications of decisions on various stakeholders. Examples such as Pro-Social Rule Bending and Virtue Ethics demonstrate why simplistic decision mechanisms such as utility functions and rule-based decisions are grossly insufficient. Deliberate decisions of pro-social rule-bending underscore the intricate nature of ethical choices in real-world scenarios.

This research will look at multi-agent simulations of decisions made by autonomic systems, and try to compute whether ethical values of stakeholders are violated, and to what extent. The research will aim to identify robust mechanisms of decision-making as well as rigorous mechanisms of validating such decisions. Integrating such decision-making abilities into socio-technical systems will also require the application of software engineering principles.

## Keywords

computational machine ethics, artificial intelligence, software engineering

## Desirable Requirements

Preference will be given to candidates with prior experience in agent-based modelling

## Research Area

Foundations of Computing

## Project Title

Computer Science Education - Project Negotiable

## Project Overview

My area of research is computer science education. More specifically I am interested in tools and techniques that can help:

- 1) students learning to program,
- 2) non-native students learning to program through English,
- 3) assessment and management of group software engineering projects

I would like the specific project to be driven by the interests of the student as long as it is within my general area of research. Below is a list of exemplar projects:

- IDE or LMS integrated visualisation of memory utilisation for early-stage programming students (like Python Tutor)
- IDE or LMS integrated representation of programs as frame-based constructs (like Strype or Stride)
- Web-based Intelligent tutoring systems for early-stage programming students. Potentially AI driven, with an aim towards mastery-based learning.
- Tools for management and analysis of version control systems for team-based software engineering projects. This could include analysis of individual contributions as well as peer-review components.
- Tools for automated assessment in computer science classes, with possibilities including parsons problems, explain in plain English problems, programming problems (output based), programming problems (design based/static analysis), code tracing problems, and other similar concepts

A successful candidate would expect to gain a grounding in the area of computer science education as well as other areas depending on their project. This could include web technologies, AI/ Machine Learning and other similar areas:

LMS: Learning Management System like Moodle

Python Tutor: <https://pythontutor.com/>

Strype: <https://strype.org/>

Stride: <https://www.stride-lang.net/>

## Keywords

Computer Science Education, Visualisation, Mastery Learning, Tools, Assessment

## Research Area

Human-Computer Interaction

## Project Title

Designing AI-Powered Peer Support Systems to Promote Inclusive Mental Health Help-Seeking

## Project Overview

Social isolation and a lack of relatable experiences often discourage young people from seeking help for mental health challenges. While digital platforms aim to address these issues, they frequently fall short in harnessing the power of peer experiences to inspire help-seeking behaviour.

This project will explore how behavioural modelling, supported by AI, can provide social proof and encourage help-seeking. By showcasing examples of peer actions, the research will investigate how a system can foster relatability and motivate users to seek support. The research will also investigate how AI can personalise these experiences to cater to the diverse needs of different user groups, including underrepresented and minority populations.

Using a user-centred design approach, the project will identify the needs, preferences, and challenges faced by a wide range of users. AI-driven features, such as adaptive content delivery and real-time insights, will ensure the system remains inclusive and relevant to various demographics. Ethical considerations, including trust, privacy, and representation, will be at the forefront of the design process.

This interdisciplinary project integrates insights from psychology, human-computer interaction, and AI to inform the design of a scalable, impactful intervention. The work has the potential to significantly enhance digital mental health platforms by fostering a sense of community and inclusivity while leveraging technology to address critical gaps.

## Keywords

mental health, artificial intelligence, user centred design, behavioural modelling

## Desirable Requirements

Background in HCI or some relevant experience working in the mental health space.

## Research Area

Human-Computer Interaction

## Project Title

Adaptive Sensory Environments in XR: Leveraging Real-Time Feedback with Diffusion Models

## Project Overview

Extended Reality (XR) technologies have demonstrated significant potential in healthcare, particularly in reducing pain through immersive distraction techniques. Building on this foundation, this research investigates the integration of XR with Brain-Computer Interfaces (BCI) to create adaptive sensory environments. The primary focus will be on sensory sensitivities, such as those experienced by individuals on the autism spectrum, by dynamically adjusting visual stimuli in response to real-time feedback. By leveraging XR's HMD's sensor capabilities and the adaptability of BCIs, the project seeks to extend the benefits of XR to healthcare, training, and entertainment applications.

The proposed system employs an XR HMD to overlay augmented visuals onto the real world while a BCI monitors user states, such as stress or discomfort. Inspired by advancements in diffusion models, such as those demonstrated in "Oasis Minecraft AI" and "Gamengen"—where real-time diffusion models generated versions of Minecraft and Doom—this research aims to take a similar approach using diffusion models. The system iteratively modifies the visual environment by dimming bright areas or reducing visual noise to optimise user comfort and sensory experience.

The PhD aims to research how such an XR system could be created that can cater to diverse sensory requirements. The ultimate objective is to develop an adaptive, inclusive XR experience that improves quality of life for users.

## Keywords

XR,VR,BCI,Diffusion models

## Desirable Requirements

Computer Science / Cognitive science

## Research Area

Information Systems

## Project Title

Information Retrieval for case law and legal statutes

## Project Overview

Having advanced significantly in recent years, modern Natural Language Processing (NLP) methods, including Large Language Models (LLMs), have the potential to revolutionise the processes of analysing, summarising and searching legal text (e.g. legislation, regulation, court judgments, contracts, etc.). This in turn has the potential to contribute efficiencies to legal practitioners in the form of semi-automatic technology-assisted search and analytics tools.

However, legal documents have their own particular characteristics that have been demonstrated to pose problems for modern approaches, including extremely long sequence lengths, complex semantics and structure, specialised vocabulary, jurisdictional differences and data imbalance. Additionally, trust in these technologies is a significant obstacle to real-world deployment, particularly due to the black-box nature of deep-learning-based approaches such as LLMs.

The primary objective of this project is to investigate and develop solutions to the problem of Legal Information Retrieval: identifying case law and/or legislation that is relevant to user queries provided by domain experts. This is closely aligned to the goals of the annual COLIEE Legal Case Retrieval and Statute Law Retrieval tasks (<https://draft.coliee.org/overview>). The research will focus not only on the quality of retrieval, but also consider the explainability and trust of such systems, along with considering the impact of jurisdiction-specific characteristics and legal language.

## Keywords

Information Retrieval, Legal Informatics, Natural Language Processing, Large Language Models, Artificial Intelligence, Computational Linguistics

## Research Area

Security and Networks

## Project Title

LLM-Powered Security Policies Orchestration and Enforcement in 6G OpenRAN

## Project Overview

This PhD project focuses on designing an innovative framework for end-to-end orchestration and enforcement of security policies in 6G OpenRAN networks. The research leverages the capabilities of fine-tuned Large Language Models (LLMs) to address complex security requirements through natural language processing, bridging the gap between human operators and machine-executed security functions in OpenRAN environments.

The project investigates the integration of LLMs for holistic and adaptive security management in 6G OpenRAN. This includes mining, gathering, and processing knowledge to understand and mitigate threats in dynamic network conditions. Key advancements include continuous feedback loops to refine the LLM's decision-making, creating an adaptive and self-optimizing security system.

### Objectives:

1. Design an LLM-driven framework for automating threat intelligence management in OpenRAN environments, including automated CTI report analysis and regex generation for SIEMs.
2. Implement real-time, multi-domain monitoring to detect security anomalies in OpenRAN.
3. Enable network operators to input high-level security commands via a natural language interface, translated into actionable security policies.
4. Develop and enforce corrective actions for detected threats, integrating security across network slices, edge, and cloud domains.

The final phase of the PhD involves validation and performance evaluation of the developed framework using UCD NetsLab's real-world ORAN testbed (<https://netslab.ucd.ie/testbed/>). Expected outcomes include improved accuracy in security policy enforcement; automation of threat intelligence processes; seamless multi-domain security orchestration; and establishing benchmarks for energy efficiency and adaptability in 6G OpenRAN security operations.

## Keywords

6G, Security, OpenRAN, AI, LLM, Anomaly detection



## Research Area

Security and Networks

## Project Title

Adaptive Bit Allocation for Robust Proactive Deepfake Defense

## Project Overview

The rise of Deepfake (DF) technology has enabled the creation of highly realistic manipulated content, raising concerns about its misuse for misinformation and fraud. To address these issues, two main defense methods have emerged: Passive Deepfake Detection (PD) [1] and Proactive Deepfake Defense (PDD) [2]. PD helps to mitigate damage but is unable to fully eliminate it. In contrast, PDD focuses on preventing DF creation at the source that can be divided into two main categories: Disruption and Watermarking. [2] shows that while current PDD methods show effectiveness, their success rate drops significantly when watermarked images modified. [3] introduces adaptive blind watermarking, which can detect relative positions in the image adaptively, even when face images undergo slight modifications. However, existing methods face challenges, including limited bit length that may not suffice for identifying content associated with specific models. Therefore, this research aims to develop adaptive bit allocation techniques that dynamically adjust the number of embedded bits based on content complexity. This research focuses on the following questions:

1. How can image entropy, texture analysis, and edge detection be effectively integrated to assess content complexity?
2. What methods can be dynamically allocated bits across different regions, ensuring both optimal watermark strength and minimal distortion in high-detail areas?
3. How can adaptive bit allocation be implemented in a computationally efficient manner for large-scale applications, such as social media platforms?

[1] [10.36227/techrxiv.173273016.63626046/v1](https://arxiv.org/abs/10.36227/techrxiv.173273016.63626046/v1)

[2] [10.36227/techrxiv.173121245.50797124/v1](https://arxiv.org/abs/10.36227/techrxiv.173121245.50797124/v1)

[3] [10.1016/j.jvcir.2024.104094](https://arxiv.org/abs/10.1016/j.jvcir.2024.104094)

## Keywords

Proactive\_Deepfake\_Defense, Deep\_Learning, Adaptive\_Watermarking, Bit\_Allocation, AI\_Security

## Desirable Requirements

Deep learning research, python programming, first author of research papers published, working experience in research projects.

## Research Area

Security and Networks

## Project Title

Privacy preserving techniques for large languages Models (LLMs)

## Project Overview

Privacy preserving techniques for large languages Models (LLMs)

The rapid adoption of large language models (LLMs) in sensitive domains such as healthcare, finance, and personal communication has raised significant concerns about user privacy. These models, trained on massive datasets, often capture and potentially memorize sensitive information, creating risks of unintended leakage during inference or when accessed by adversaries. For instance, LLMs used in medical diagnosis might reveal patient-specific information, while those applied in financial settings could expose confidential transaction details. The primary goal of this research is to explore and develop effective privacy-preserving mechanisms tailored for LLMs, ensuring secure AI deployment.

Research Objectives:

- Conduct a comprehensive analysis of potential privacy vulnerabilities, including data leakage, inference attacks, and model exploitation.
- Evaluate the impact of existing privacy-preserving techniques on these vulnerabilities.
- Design an efficient privacy preserving approaches for LLM considering advanced cryptographic methods such as homomorphic encryption, secure multi-party computation, and differential privacy.
- Optimize the balance between privacy guarantees and model utility for LLM.

## Keywords

Privacy, LLMs, differential privacy, homomorphic encryption

## Desirable Requirements

Strong background in Cryptographic (homomorphic encryption, secure multi-party computation, and differential privacy), ML , and LLM

## Research Area

Security and Networks

## Project Title

A Novel Dataset & Framework for Anomaly-Based Intrusion Detection in Software-Defined Networking

## Project Overview

The aim of this project is the development an efficient anomaly-based Intrusion Detection System (IDS) for enhancing Software-Defined Networking (SDN) security. Leveraging Deep Learning (DL) algorithms, the proposed IDS will offer a flexible, robust solution for modern attack detection within SDN environments, a crucial element to ensure more widespread adoption of SDN as the dominant networking model. The main objective is to create a lightweight DL-based attack detection and mitigation framework, capable of classifying network attacks as anomalies in SDN environments. This will require a comprehensive SDN-specific dataset that accurately reflects real-world conditions. While previous work by the UCD team has focused on virtual SDN attack datasets, this project seeks to overcome the shortcomings of existing datasets by developing a new, publicly available, real-world dataset to enhance collaborative research in this underserved domain. To achieve this, the project proposes the construction of a hybrid virtual-physical testbed that connects physical hosts and infrastructure to virtual networks, replicating real-world architectures. High granularity standard network traffic will be captured directly within the network and via the SDN controller Southbound Interface (SBI) API. Normal and attack traffic will be simulated and captured, including new SDN-specific attack types such as Controller Spoofing and Communication Channel Eavesdropping.

## Keywords

SDN, IDSs, Machine Learning, attack detection

## Desirable Requirements

At least one research paper published in a peer reviewed journal or conference as the main/first author; At least one year experience in machine learning and network engineering.

## Research Area

Security and Networks

## Project Title

Sustainable Security

## Project Overview

Cyberphysical systems (CPS), integrating software, hardware, and human operators, are increasingly vulnerable to security threats due to misconfigurations, third-party vulnerabilities, and human error. These vulnerabilities are exacerbated by the dynamic nature of CPS, making it challenging to maintain security. This proposal seeks to address the critical gap between attack detection, diagnosis, and mitigation to improve the resilience and sustainability of CPS security.

## Problem Statement

Current security approaches for CPS are siloed, with limited integration between detection, diagnosis, and mitigation. While anomaly detection techniques can identify previously unknown attacks, they fall short in diagnosing attack types or automatically applying appropriate security controls. Penetration testing, though effective, is often impractical for live systems such as smart homes and lacks adaptability to runtime-detected anomalies. Moreover, evolving system configurations introduce new security requirements that traditional methods fail to manage effectively. Addressing these challenges requires innovative solutions to bridge these gaps while sustaining human engagement and measuring security performance.

## Research Objectives

**Integrated Attack Management:** Develop a framework that seamlessly integrates attack detection, diagnosis, and automated mitigation, enabling dynamic and informed responses to evolving threats.  
**Evolving Security Requirements:** Create logic-based learning mechanisms, such as inductive learning, to adapt security policies and requirements in response to system configuration changes.  
**Human–Machine Collaboration:** Design human-centered security interfaces that enhance situational awareness and promote stakeholder engagement across various expertise levels.  
**Sustainable Security Metrics:** Define and measure sustainable security by evaluating system robustness, stakeholder participation, and user experience.

## Keywords

Adaptive Security, Software Engineering, HCI

## Research Area

Security and Networks

## Project Title

Automated and Intelligent Future Networks (Wireless, Optical, IP)

## Project Overview

This PhD project aims to develop innovative solutions for the next generation of networks, spanning wireless, optical, and IP domains. The project focuses on integrating automation for enhanced resource management and optimization, leveraging artificial intelligence (AI) to improve efficiency, capacity, and minimize latency, while supporting open models for multi-vendor collaboration. The research will utilize cutting-edge tools and methodologies, including machine learning frameworks (e.g., TensorFlow, PyTorch), network simulation platforms (e.g., ns-3, OMNeT++), software-defined networking (SDN) controllers (e.g., OpenDaylight, ONOS), and network function virtualization (NFV).

Key Research Areas:

- AI-Driven Radio/Optical Access Network Optimization: Developing AI algorithms to dynamically optimize resource allocation and performance in radio and optical access networks.
- Market Design for Network Infrastructure Sharing and Resource Allocation: Applying game theory and economic models to design fair and efficient mechanisms for resource sharing.
- Automated Root Cause Analysis for Network Operations: Creating AI-powered systems for real-time fault detection and diagnosis in complex network environments, improving reliability and reducing downtime.
- Machine Learning for Traffic Prediction and Load Balancing: Leveraging machine learning models to predict network traffic patterns, enabling proactive resource management and efficient network provisioning.
- Network Slicing: Developing advanced techniques for creating virtualized network slices on shared infrastructure, supporting multiple services with diverse performance requirements.
- Edge Computing Integration: Bringing computation closer to data sources through edge computing, reducing latency for time-sensitive applications.
- Energy-Efficiency Optimization in Satellite Communications: Exploring energy-efficient strategies for satellite communication networks for Low Earth Orbit (LEO) constellations.

## Keywords

Wireless communications, Optical Networks, 6G, Future Networks, Open Radio Access Networks

## Research Area

Security and Networks

## Project Title

Automating AI Incident Threat Intelligence

## Project Overview

Artificial intelligence (AI) systems will soon seamlessly share and process information, aid businesses, governments and healthcare. This rapid integration of AI comes with challenges. Sometimes, AI systems will fail and generate potentially dangerous incidents, despite the risk management and AI governance controls envisioned by the EU AI Act. To respond promptly, cyber threat intelligence (CTI) systems automate the sharing of incident data. Managing AI incidents would benefit from similar incident-sharing systems, and enable integrating AI incident handling with cyber incident handling. The OECD published an initial report seeking to define AI incidents in October 2023.

The primary aim of this research is to enhance the efficiency, accuracy, effectiveness of AI incident data sharing through by adapting existing cyber threat intelligence (CTI), sharing data formats and protocols, e.g. the open source MISP (Malware Information Sharing) platform, and the development of new metrics, tools and methods for AI incident classification, enrichment and normalisation, especially by working on symbolic methods like the AI Risk Ontology and combining them with neural processing techniques to rapidly consume data and test to identify threats and responses.

The proposal spans AI incident management, cybersecurity, and data-sharing. A gap exists in machine-readable reporting in AI incidents, and AI-generated incidents are often overlooked in cybersecurity. This research aims to fill these gaps, paving the way for new advances in effectively governing AI to make it more trustworthy by enabling a more controlled and automated response to AI incidents.

## Keywords

Cybersecurity, AI governance, knowledge graphs, machine learning

## Research Area

Software Engineering and Distributed Systems

## Project Title

Distributed ledgers in the quest of fake news detection

## Project Overview

In this line of research, we will design and implement an auditable and ever-growing decentralised knowledge base that stores information regarding news creation, i.e., the list of agencies, reporters, articles, and artefacts, which is added by autonomous crawlers and is maintained by a network of distributed nodes of corroborators.

The design of such a knowledge base is challenging and requires the design and development of (i) multiple communication protocols that support the participation of multiple crawlers and corroborators at a global scale, (ii) efficient and reliable storage architectures to store ephemeral and permanent information, and (iii) incentive mechanisms that motivate self-interested entities to dedicate part of their resources to the function of the framework.

## Keywords

distributed ledgers, consensus protocols, decentralised systems, fake news, microservices

## Research Area

Software Engineering and Distributed Systems

## Project Title

Enhancing Microservice Architectures through Enterprise Knowledge Graph Integration

## Project Overview

This project aims to determine whether enterprise knowledge graphs can be effectively integrated into microservice architecture and to assess the impact on the system's design, performance, maintainability, and evolvability. A key aspect of the research will be to explore how this integration can be achieved and to define a methodology and associated toolkit to support it.

It will achieve this by: Demonstrating the feasibility of integrating knowledge graphs and microservice architecture through a number of case studies; Exploring the potential impact of knowledge graphs on current pitfalls of microservices system design, and the impact of mitigations on performance, and scalability; and how Knowledge Graphs can enhance Software Engineering Practice through the definition of a methodology and associated toolkit for the creation of knowledge graph enabled microservices-based systems.

Key Research Objectives: (RO1) To identify the main pitfalls of current best practices with microservices architecture; (RO2) To explore how distributed knowledge graphs can be used to mitigate some of these pitfalls; (RO3) To identify a methodology and toolkit to support the application of distributed knowledge graphs to microservices architecture; (RO4) To evaluate the effectiveness of the methodology and proposed mitigations by applying them to an existing application.

## Keywords

Microservices, REST, Semantic Web, Linked Data

## Desirable Requirements

Experience with: Distributed Systems/Microservices, REpresentational State Transfer (REST), Linked Data/Semantic Web



## Research Area

Software Engineering and Distributed Systems

## Project Title

Scalable Universal Collective Communication Algorithms for Large Scale Deep Learning on Extreme Scale Heterogeneous Hybrid Platforms

## Project Overview

Deep learning applications have become pervasive, energizing technological innovations in several fields, including speech recognition, autonomous driving, medical diagnosis, and natural language processing. Large-scale deep learning applications require training deep neural networks (DNN) on large datasets to make better predictions. However, the training times increase drastically with the size of the DNN. Therefore, accelerating the training of large-scale DNNs is a formidable challenge. Parallel deep learning has become a natural and effective strategy to address the challenge.

Parallel deep learning methods rely critically on a subset of optimized collective communication routines (allreduce and alltoall) to deliver high performance. The project aims to develop scalable and universal collective communication algorithms for this subset to accelerate large-scale deep learning on extreme-scale heterogeneous hybrid and AI-specific computing platforms.

## Keywords

deep learning, parallel computing, MPI, collective communication, allreduce, alltoall

## Research Area

Software Engineering and Distributed Systems

## Project Title

LLM@Edge: Optimized Deployment of Large Language Models on Distributed Edge Systems

## Project Overview

Deploying Large Language Models (LLMs) across distributed edge systems presents opportunities for enabling low-latency, energy-aware, and scalable AI applications. However, the inherent resource constraints and heterogeneity of edge nodes introduce significant challenges in ensuring efficient execution, particularly for compute-intensive models like LLMs. This research project addresses these challenges by leveraging distributed systems principles, focusing on resource scheduling and orchestration mechanisms, to optimize LLM deployment and operation in edge environments. This project considers distributed deployment frameworks to partition LLMs into lightweight components for execution on edge nodes, reserving more complex computations for cloud backends or higher-capacity nodes. Dynamic resource scheduling mechanisms will allocate edge resources based on workload characteristics, device capabilities, network conditions, and energy-aware metrics. The geo-distribution of edge nodes must be considered for context-sensitive scheduling and place tasks closer to data sources or end-users. The resource scheduling must also optimize the carbon footprint of LLM operations by allocating tasks to energy-efficient nodes or renewable energy-powered regions to minimize environmental impact. In addition, robust orchestration mechanisms are critical for overcoming the scalability challenges of dynamic workloads in distributed LLM deployments. These mechanisms will leverage container orchestration platforms (e.g., Kubernetes) for dynamic placement, serverless orchestration frameworks for event-driven scaling across the edge-cloud continuum, and workflow orchestration tools to coordinate multi-step LLM processes. This project unlocks the potential of LLMs in real-world applications, including smart cities, healthcare, and IoT ecosystems.

## Keywords

Edge Cloud Continuum, Large Language Models, Resource Scheduling, Orchestration Frameworks, Sustainable Computing, Distributed AI

## Desirable Requirements

The candidate should have publications in the related areas.