School of Information Technology
HDR Projects 2020

If you are looking for a rigorous graduate training, and want to make a substantial research contribution to Computer Science, the School of Information Technology at Deakin University offers a fully-funded PhD in Computer Science available over 3 years.

Generous scholarships for outstanding candidates covering tuition fees and a stipend of up to $28,092 annually are available for suitably qualified individuals. PhDs are available in all areas of IT, but we specifically encourage those within the following areas:

- Cybersecurity
- Network Security
- IoT and Distributed Systems
- Cloud Computing
- Software Engineering
- Data Mining and Complex Networks
- Optimisation and Operations Research
- Data Analytics
- Machine Learning
- Computer Vision and Pattern Recognition

This scholarship is available over 3 years:

- Stipend of $28,092 per annum tax exempt.

To be eligible you must:

- Be a domestic or onshore international candidate (domestic includes candidates with Australian Citizenship, Australian Permanent Residency or New Zealand Citizenship)
- Meet Deakin's PhD entry and English Language requirements
- Be enrolling full time and hold an honours degree (first class) or an equivalent standard master's degree with a substantial research component
- For more information please visit Deakin Research – Higher Degrees by Research

To express your interest in this opportunity review the following projects and email the respective Supervisor, providing the following information:

- your CV including details of two referees
- copy of your academic transcripts
- grading scales
- 1-2 page cover letter which outlines your research skills, experience and why this PhD opportunity interests you

Project Title #1: Optimisation and approximation theory

Supervisor Name and Email:
Dr Julien Ugon, julien.ugon@deakin.edu.au

Project description:
In this mathematical research project you will work on approximation problems. Classically, functions are approximated using polynomials, or trigonometric polynomials. In this project, we are looking at extending the classical results to approximation by other families of functions, such as piecewise polynomials, rational functions, etc.

You will be involved in both theoretical investigation and computational experimentation.
You will be working with an international team of researchers, from Australia, France, Spain and Israel.

Project Aim:
The goal of the project is to obtain new results in approximation theory, by combining mathematical tools from optimisation, analysis, and algebra.

Project Title #2: Video Technologies for Distant Working and Learning in Post Pandemic Era.

Supervisor Name and Email:
Dr Glory Lee, glory.lee@deakin.edu.au

Project description:
While the recent pandemic outbreak has induced a huge impact to everyone's lifestyle, it also provides the society with an opportunity to realise that most of the work can be done remotely. In order to empower people with the capability to interact while maintaining social distancing, new video technologies are needed to address the new constraints and limitations under the current complicated scenario. Delays and jitters are always the most significant visual artefacts in real-time video communication applications due to the dynamics of the underlying communication network. In video conferencing applications, the massive number of end-users has introduced more uncertainties in the calculations. To tackle the issues, new machine learning-based video coding schemes will be developed to intelligently process video streams according to the bandwidth and traffic conditions. Missing data can significantly degrade the visual quality of a video. An AI-based video frame reconstruction algorithm will be designed to maintain the subject visual quality of the video at a high standard. The ultimate goal is to deliver a smooth streaming experience in video conferencing applications at 1080p and 60 FPS with the delay controlled at the millisecond level using ordinary equipment. Finally, the project will explore the possibility of applying all the proposing techniques to next-generation immersive video technologies, including 360 videos and VR/AR systems.

Project Aims:
- How to use machine learning to improve video encoding and decoding processes in real-time applications?
- How to use artificial intelligent-based techniques to reconstruct missing information in video streams and maintain subjective video quality?
- How to apply these new proposing techniques on next-generation visual systems, including immersive 360 videos and AR/VR systems.

Project Title #3: Heterogeneous Graph Neural Networks for Scene Understanding

Supervisor Name and Email:
Prof Antonio Robles-Kelly, antonio.robles-kelly@deakin.edu.au

Project description:
Heterogeneous graph networks aim at performing learning and prediction on structured data, whereby each item or entry, abstracted as a node, has attributes that attributes of different types and diverse nature. This is a challenging task that arises in a wide variety of areas spanning from cyber security, mixed text-video classification and social networks to computer vision.

Project Aim:
The project will aim at both, developing methods for feature extraction and relational embedding of the graph structure and leveraging graph context for data mining, classification, clustering and classification and recommendation tasks in scene understanding for computer vision tasks. The project will also explore topics such as federated learning, explainability, robustness and factor graphs as applied to heterogeneous graph networks. Of particular interest are dynamic graphs, non-structured scenarios and scalability.

Project Title #4: Security issues in blockchain networks

Supervisor Name and Email:
Dr Luxing Yang, luxing.yang@deakin.edu.au

Project description:
Over the past decade, blockchain technology has attracted tremendous attention from both academia and industry. The popularity of blockchains was originated from the concept of crypto-currencies to serve as a decentralized and tamper-proof transaction data ledger. Nowadays, blockchains as the key framework in the decentralized public data-ledger have been applied to a wide range of scenarios far beyond crypto-currencies, such as the Internet of Things, healthcare, and insurance, etc.

Although with the advantages such as open access, disintermediation, and pure self-organisation, open-access/permission less blockchains rely on the condition of honest majority to guarantee the data integrity and service security, especially when the Nakamoto consensus protocol based on proof-of-work (PoW) is adopted. Since permission less blockchain networks admit no identity control, they can be vulnerable to a series of attacks by malicious consensus nodes. Those attacks are applicable to a wide range of blockchain-based resource trading services and systems, resulting in tremendous economic losses. Consequently, it is urgent and of practical significance to develop effective security enhancement solutions to defending against the emerging attacks in blockchain networks.

The student will conduct research in security issues of blockchain networks, which aligns with the goals of SIT and its vision towards expanding and growing research of high quality and impact. The research will be conducted under the University's Cyber Security Research and Innovation Centre (CSRI), which is one of the University's strategic research centres and one of its research focuses is cyber defence. During PhD, the student will participate in activities of CSRI and gain technical support from the researchers at CSRI.

Project Aim:
The student will focus on common security issues in blockchain. In particular, it is intended to develop novel security enhancement solutions for blockchain networks against a variety of attacks, including self-

mining attacks, majority attacks and distributed denial-of-service (DDoS) attacks, etc. To prevent such an attack, it is crucial to analyse strategies of the miners and pools as well as the interaction among them. Optimisation, game theory, machine learning, and networking techniques are expected to be utilised. The outcomes of this project will significantly enhance the understanding of blockchain and provide guidelines to develop more secure blockchain systems.

Project Title #5: Energy Efficient Engineering of Software Systems

Supervisor Name and Email:
Prof Jean-Guy Schneider, jeanguy.schneider@deakin.edu.au

Project description:
Software systems are becoming increasingly challenging to design and implement, both with regards to size and complexity. To address these challenges, many software engineering methods focus on a mix of functionality and a selected few quality aspects of software systems. However, very few software engineering methods take energy efficiency of the system to be developed as one of the core criteria in both design and implementation – if at all, this is only considered as an afterthought. Energy efficiency of software systems –across a variety of domains – is becoming an increasingly important quality that needs to be explicitly addressed during design and implementation. Therefore, there is a clear need to augment existing software engineering methods in such a way that software engineers are given appropriate tools and techniques to explicitly deal with energy efficiency as one of the core trade-offs under consideration.

Project Aim:
Over the years, software engineering methods have devised various techniques to deal with functional requirements as well as a number of quality aspects (e.g., performance, maintainability, usability) of software systems. However, to the best of our knowledge, none of the existing software engineering methods give software engineers appropriate guidance in how to design and implement software systems that need to meet given energy constraints. The aim of this project is to advance the state-of-the-art of software system design to address this shortcoming and invent novel techniques and tools for software engineers to treat energy efficiency as a first-class entity in software design. The techniques and tools are to be evaluated across a number of selected application domains to demonstrate their effectiveness.

Project Title #6: Threat Intelligence Management Framework

Supervisor Name and Email:
Chang Tsun Li, changtsun.li@deakin.edu.au

Project description:
Threat intelligence is the practice of analysing, integrating disjointed cyber data to extracting evidence-based insights regarding an organization's unique threat landscape. This helps explain who the adversary is, how and why they are comprising the organization's digital assets, what consequences could happen following the attack, what assets actually could be compromised, and how to detect or respond to the threat. Threat intelligence creates a significant difference to the organization's ability to manoeuvring threat countermeasure mechanisms into place, prior to and during the attack. Every organisation is different and therefore threat intelligence frameworks should be custom-tailored to the business process

itself and the organization's risks, as there is no 'one-size-fits-all' in cyber. Implementing threat intelligence is challenging for two key factors:

- The increasing volume and the quick evolution of the threat landscape makes organizations unimmune to the evolving capabilities of modern cybercrimes that consists of a multitude of complex attacks
- The complexity of organisation's cyber data; With the massive amount of operational and business data, many organizations are not able to prioritize the most meaningful data, accurately discern patterns and pinpoint trends. Poor cyber data management and analytics means too many false alarms; and thus, a higher risk of successful breaches. Without a precise systematic analysis to classify and make sense of collected data, and more importantly log the right data, organizations would not be able to discover data-driven competitive features in cyber data.

Project Aim:
The key objective of this research project is to help organisations to combine, process, aggregate and analyse historical threat data, existing and possible attack vectors and vulnerabilities, threat actors and models that are specific to the business operations, to find the needle in the haystack that will yield the relevant intelligence that could minimise the threat landscape in the future. The main innovation aspect of this project is to enable effective cyber data management to achieve threat intelligence. Cyber data management will provide organizations with a better understanding of their threat landscape to automate and speed risk management and incident response; allowing developing effective and measurable security controls. Threat intelligence will turn the cyber data into useful insights to drive effective decisions to defend against potential cybersecurity threats.

Project Title #7: Predicting Critical Data Breaches with AI Powered Solutions

Supervisor Name and Email:
Dr Seng Loke, seng.loke@deakin.edu.au

Project description:
Organizations handle a vast amount of sensitive personal, financial and business data, some of which are governed by laws and regulations in local and international jurisdictions. Reported data leakage incidents have reached their highest level; 2019 was a record-breaking year for the numbers of publicly reported data breaches and exposed records worldwide with millions of dollars of losses. Australian organisations have had a sizable number of critical data breaches, with millions of dollars of losses. Because of such high incidents of critical data breaches, the Australian government recently introduced a mandatory data breach notification scheme that requires businesses to publicly disclose data breaches including Australian Government agencies, businesses and organisations. This amplify the relentless challenge of staying ahead of security vulnerabilities to protect against movement of sensitive data outside organisations' secure perimeter, to ensure compliance with the new data breaches notification schema. Reports shows that outsider hackers are the primary cause of data breaches; however, organizations implement defence mechanisms that focus only on insider hackers and enterprise users to detect internal or accidental data breaches. On the other hand; according to many data breach detection gap analysis studies, most data breach incidents could take several months to be discovered.

Within the noise of big data, enterprises need sophisticated security tools to find deep insights in their data to detect anomalies and prevent data breaches. Data breaches are usually a result of advanced persistent threats (APTs) that happen over a large period of time, to enable hackers remain anonymous and hidden to

gain access to enterprise systems, compromise infrastructure and steal data. Detecting APTs is very challenging as it requires effective correlation and deep analysis of system events, that are spaced out over a large period in a distributed environment that originate from different resources.

Project Aim:
In this project, we aim to develop a new AI-powered security solution that can stop emergent critical data breaches for organisations that process and store a huge amount of confidential data. It is designed to ultimately predict and prevent data breaches at the initial stages before data exfiltration can take place, by monitoring, mining and detecting security flaws that might lead to future sudden or gradual data leakage. This solution will add significant visibility to the organisational data usage across the enterprise and ultimately prevent critical data breaches. Through Machine Learning (ML) optimisations, this solution will enable businesses to deter, disrupt and defeat cyber adversaries, and increase the probabilities of detecting exploitation measures before they are successful. This project will focus on preventing external data breaches that are a result of external hacking activities. This is not like existing approaches that focus on deploying data discovery agents within enterprise's devices to track and monitor corporate data by monitoring internal users. The resultant proof-of-concept system will prevent data breaches from becoming major incidents, by detecting security threats existing in enterprise's infrastructure that could lead to data exfiltration. This will enable businesses to know what confidential information is about to leave corporate's endpoints and through which channels, before data is moved outside an organisation's secure perimeters. Implementing building blocks of practical AI and ML together with security solutions, facilitates automation and orchestration to build autonomic security solutions that can keep up with the scale, speed, complexity and adaptability of today's cybersecurity threats.

Project Title #8: A Comprehensive Cyber Risk Management Framework

Supervisor Name and Email:
Prof Jean-Guy Schneider, jeanguy.schneider@deakin.edu.au

Project description:
The cost of a security breach has risen significantly over the past 5 years and costs millions of dollars of losses. These rising losses are representative of financial impact of breaches, increased regulation and the complex process of managing cyber risks. A comprehensive security plan based on a pragmatic risk profile can spare much unnecessary business and associated reputational and financial losses. Every organisation is different and therefore needs a carefully tailored security plan, as there is no 'one-size-fits-all' defence strategy.

Due to the exponential increase in security breaches, organisations need to secure their digital infrastructure by adopting appropriate risk management plans and investment in cybersecurity. However, convincing a board to invest in cybersecurity is challenging as such investments are costs and cannot be directly mapped to profit. Executives and decision makers in big organisations bring cyber risks as an essential topic on their agendas to know how well cyber risk is being managed in their organizations and what exactly is needed, in terms of cyber investments. Executives should approach cyber decisions with caution since cyber breaches can impact their organisations, leading to significant punitive fines and damages. Therefore, decision makers should equip themselves with the required cyber risk knowledge and tools to take the right decision.

The optimal level of cyber investments depends on a detailed cost-benefit analysis. Usually, the costs of cyber investments are compared to the expected benefits. Whenever a security investment decision needs to be made, decision makers do that based on the potential financial loss against digital assets, according to risks and remediation actions prioritisation. Unfortunately, cyber investments are often the target of financial cuts because they do not result in direct revenue impact.

Generally speaking, a cyber-risk is a type of operational risk, which means the potential for business losses including; financial, reputational, operational, regulator, etc. In big organisations; it is an established business practice to prioritise investment decisions based on Return on Investment (ROI) calculations and prioritisation of cyber investments requires extending the concept of ROI to Return on Security Investment (ROSI). Cyber investments primarily focus on minimising financial losses to the organisation, and ROSI is usually much higher than 100% (~1000%-2000%). Such large percentage seems to be counter-intuitive as ROI is traditionally less than 25%. Here comes the problem of how a decision maker could interpret ROSI to the board. Moreover, the biggest challenge here is how organisations could estimate the financial losses attributed to a cyber-breach to outweigh the cost-benefit analysis. Estimating financial losses attributed to cyber breaches is challenging as it depends of many factors and organisations usually depend on a cyber-expert to estimate losses based on the probable frequency of successful cyber threats and risks.

Project aim:

In this project, we aim to develop a new comprehensive cyber risk management framework that enables organisations to understand cyber risks as more clearly as business risks that happens in the digital domain, by measuring ROSI much more effectively. The proposed framework advances the use of risk-based approaches to achieve proactive cybersecurity, in order to help decision makers identify and focus on the important elements of cyber risk and investments based on pragmatic facts and data of the organisation itself to create a custom-tailored security plan. The proposed framework enables decision makers to understand, model, profile and prioritise the different components of cyber risk for cybersecurity efforts and investments.

The objective of this project is to support decision makers by providing precise risk models with clear alignment from the board to the front line. This means that an organization will no longer need to implement security controls everywhere; rather, the focus will be on building the appropriate controls for those that target the business's most critical areas. The benefits are not quantifiable but have great added value to business operations and success. The main innovation aspects of this project are:

- Systematically modelling the risk profile of organizations digital infrastructure, to identify possible risks based on the business nature, digital infrastructure and networks, policies, services, etc. Threat modelling plays a central role to assess security posture, however; it only reflects one side of the assessment process and usually not enough to pinpoint which security threats are the most relevant at a given time for a specific business.
- Enabling organizations to prioritize cyber investments based on accurate and pragmatic calculations to reduce risk. Prioritising the identified risks based on accurate estimates of ROSI and the cost of security breaches rather than the experience of cyber experts, so security investments can be financially justified in terms of profits for decision makers.

Existing solutions do not provide any appropriate analysis reflecting the impact of a security investment or the cost of a breach based on scientific analysis for the business digital components. Existing ROSI frameworks are built with the concept of one-size-fits-all and they work on approximations based on experience resulting in false estimations. Existing tools also do not take into consideration the cost of a

security breach when calculating the ROSI. On the other hand; existing efforts to calculate the cost of a given breach work on historical data for breaches after they have occurred, which it is ineffective in decision making and protecting the organisation assets. Moreover, existing commercial tools focus only on calculating the cost of a data breach only, using simple formulas based on manual user inputs. Several factors come into play when determining the precise cost of a security breach that organizations may incur, including location, type of currency, company size, industry and type of business data, number of affected users, the underlying digital infrastructure complexity, operational costs, breach aftermath, investigation costs, public disclosure, class-action lawsuits, sales or mergers, etc.

Project Title #9: Data After Death

Supervisor Name and Email:
Dr Arash Shaghghi, arash.shaghaghi@deakin.edu.au

Project description:
Most of us live two lives - the physical one and a virtual mirror of it online. When we die, our physical existence comes to an end, but what happens to all the data and content we have created on our online accounts (Facebook, Twitter, Gmail, etc.)? What happens to all that we have stored in the cloud and, unknowingly, in servers across the globe? In fact, the increased digital activities of people are continuing to grow exponentially with estimates indicating about 2.5 quintillion of data being generated per day. Supposing this data becomes inaccessible as a result of the owner's death, there are issues of what happens to the data. A recent study by the University of Oxford has revealed that Facebook could have 4.9bn dead users by 2100.

Generally, the person's testament decides the legacy of a person when s/he passes away. However, this typically does not include the digital assets of a user stored online. Even if it does, it is very unclear what can be done and who could execute them. There are concerns as to what data a user has actual control over and what may be defined as personal property in this context. From a security perspective, the threat models, adversaries, and challenges involved in this domain are rather obscure. It is also challenging identifying types of solutions that will be effective and reliable across different services and jurisdictions.

Project Aim:
- To determine users and organization's understanding of "data after death".
- To review and critically analyse existing "data after death" solutions.
- To carry out an extensive investigation to define the characteristics of working solutions while considering the requirements of users and organizations.
- IV. To implement innovative technical solutions and evaluate them for their effectiveness. For this, we will need to create evaluation frameworks, which do not exist.

Project Title #10: Deep-Learning, Text and Image analytics

Supervisor Name and Email:
Prof Peter Eklund, peter.eklund@deakin.edu.au

Project description:
Convolutional neural network is a class of deep neural networks, most commonly applied to analysing visual imagery. They are also known as shift invariant or space invariant artificial neural networks, based on their shared-weights architecture and translation invariance characteristics. Bidirectional Encoder Representations from Transformers (BERT) is a technique for NLP (Natural Language Processing) pre-training developed by Google and is a deep learning approach to text analytics. The research applies these deep learning methods where either may be fit for purpose, depending on the problem domain.

Project Aim:
The research team are experimenting with Deep Learning Methods in various domains including sentiment analysis in text analytics and image clarification in medical domains. A wide variety of problem domains are available for PhD study with the common thread of the application of convolutional neural networks or Bidirectional Encoder Representations from Transformers.

Project Title#11: Ambiguity Management in Requirements Engineering

Supervisor Name and Email:
Dr Muneera Bano, muneera.bano@deakin.edu.au

Project description:
Natural Language (NL) is the most commonly used vehicle for requirements specification. NL is easy to understand by most stakeholders and requires no a-priori training. Despite these advantages, NL is prone to challenges, such as ambiguity, abstraction and vagueness (AAV). This research project targets the detection of these constructs in NL requirements. The main objective of this research is to investigate how in a certain instance we can one utilize contextual information for managing AAV in requirements.

In this project we will be having an external researcher involved, Professor Didar Zowghi from University of Technology Sydney.

Project aim:
The aim of the project is to investigate the challenges of ambiguity, vagueness and abstraction in software requirements engineering. The candidate will research on the state-of-the-art and state-of the-practice in requirements engineering focusing on technical and linguistic aspects of AAVs. The project would further develop human-centric techniques and automated tools for effective management of AAVs in requirements. The enabling technologies for this project will be natural language processing and machine learning.

Project Title #12: Securing Machine Learning Software Systems

Supervisor Name and Email:
A/Prof Mohamed Abdelrazek, mohamed.abdelrazek@deakin.edu.au

Project description:
Machine learning techniques have seen a remarkable rate of adoption in recent years across a broad spectrum of industries and applications to automate many of the complex tasks. However, adversarial machine learning techniques (attempt to fool machine learning models through malicious inputs) are growing in use to attack or cause malfunction of the machine learning models and systems that rely on these models. We still see (i) a lack of understanding of how ML models work; (ii) an absence of appropriate software & security analysis tools; (iii) an absence of engineering best practices & life-cycle management; (iv) a lack of explainability; and (v) a lack of trust in the solution given the degree of uncertainty in the input training data.

Recent research efforts have shown that ML models (including widely-used deep neural networks or DNNs) are vulnerable to maliciously modified inputs - adversarial examples - that can deceive a ML model to misclassify input instances. Even worse, these adversarial examples can be used to mislead other ML models developed for the same AI/ML tasks using the same (or different subsets) of the original training data. This implies that an attacker can mount an attack that appears to an AI-powered system as a legitimate behaviour, an example would be to assume control of an autonomous vehicle using deliberately designed inputs, or misleading an AI-powered cyber security (e.g. spam filter) with malicious email that looks legitimate. These flaws threaten the future of ML adoption in such mission critical applications.

Furthermore, there have been many examples of dataset poisoning, where attackers portray malicious examples as virtuous (or virtuous examples as malicious) and inject these data into training set. This in turn leads to either malfunction or a biased and skewed ML model. Furthermore, ML models can be reverse engineered - learning the underlying data distribution - from the actual model in both discrete and continuous data cases. Thus violating the veracity of the training data and potentially exposing data which may contain private or personal information.

To understand the security challenges introduced by AI/ML, it is important to understand how Machine learning (ML) works and how AI-powered systems are developed. ML models are data-driven, this means: (i) a high-quality ML model depends extensively not only on the size of the data, but importantly on the authenticity, integrity, and quality of the dataset used to train the system; (ii) the model evolves (after retraining) when the underlying dataset changes - 'concept drift'. This is partly a feature of ML-system since under normal circumstances it affords learning models ability to adapt to changes occurring in a dynamic environment or to adapt to individual preferences and behaviour without the need to manually reprogram the model as in traditional computer systems. On the other hand concept drift can be used to subvert the system away from the model derived from correct training input; and (iii) the model is a representation of the business domain knowledge/rules reflected in the dataset that was used to train the model and as such, these rules may change over time.

Project Aims:
1) ML Models Security Weaknesses Landscape: There exists a Common Weakness Enumeration (CWE) database for traditional software systems, but not for AI/ML-powered systems. A first step is to conduct a detailed analysis to identify weaknesses in ML models (some of them are already known and mentioned such as evasion and data poisoning attacks) as well as AI-powered system weaknesses. The

result is a weaknesses landscape, as well as AI-powered Software Systems Attack Surface. We will then investigate the root causes of such security weaknesses. As in the current CWE, each weakness will elaborate its severity, consequences, likelihood and so on. This task will inform the research activities in the rest of the project including: (i) developing attack resilient ML models; (ii) security analysis of the end product AI-powered software system, and (iii) in developing secure deployment pipelines of the ML/AI-Powered Systems.

2) Developing resilient ML Models: Once the weaknesses repository is developed, you will then work on developing new techniques to prevent or mitigate these ML weaknesses. This might require modifying existing ML learning algorithms or processes using techniques like defensive distillation, using model ensembles, or developing new training algorithms that can help assess the security and soundness of a ML model after training.

Project Title #13: Using Computer Vision For Systems Engineering

Supervisor Name and Email:
A/Prof Mohamed Abdelrazek, mohamed.abdelrazek@deakin.edu.au

Project description:
Over the last years deep learning methods have shown to outperform many state-of-the-art machine learning techniques in several fields including computer vision as one of the challenging tasks in machine learning. Computer Vision, CV, seeks to help computers "see" and understand the content of images and videos. We use CV in many applications: OCR, Retail, surveillance, object detection, object segmentation, object recognition, etc. CV has been used in many areas, but not yet in software engineering.

Project Aim:
In this project, we aim to investigate how computer vision can assist in automating many of the tasks in the software engineering process. There are multiple areas of interest that the candidate can choose from, depending on their background and research interests, including: software (and GUI) testing of the software, assessing the usability and accessibility of the software/app, understanding developer key activities/practices and assess their productivity, their mental health and wellbeing, their working environment, and many more

Project Title #14: Using Generative Models in Requirements Engineering

Supervisor Name and Email:
A/Prof Mohamed Abdelrazek, mohamed.abdelrazek@deakin.edu.au

Project description:
Generative Models can learn the data distribution of the training dataset using unsupervised learning so we can generate new data points with from the same distribution. One of the most commonly used approaches is the Generative Adversarial Networks architecture (GANs), which is based on game theory approach with an objective to find Nash equilibrium between the two networks: Generator and Discriminator.

Project Aim:
This project aims to investigate the practicality of using generative machine learning models to support different software engineering practices. The candidate would be able to choose, depending on their background, from the following challenges: augmenting test cases, augmenting system requirements, UX/UI screens of apps, augmenting and understanding source code.

Project Title#15: Requirements Engineering for AI Systems

Supervisor Name and Email:
Dr Chetan Arora, chetan.arora@deakin.edu.au

Project description:
With the emergence of IoT and AI systems, software and systems engineering practices, in particular the requirements engineering practices, have changed substantially in the past decade. The requirements elicitation and specification need to account for the concomitant uncertainty and lack of visibility in the inner workings of these systems. The research project is targeted at building an understanding of the state-of-the-practice in RE for AI systems and propose changes.

Project Aim:
The PhD project will investigate the requirements engineering (RE) practices in AI projects. The candidate will research on the current industrial practices and the challenges faced by the practitioners, when defining and building predictive components for software and systems engineering. The project would further develop human-in-the-loop techniques and tools for effective requirements elicitation, specification and management. The enabling technologies for this project will be natural language processing and machine learning.

Project Title#16: Representation Learning over Dynamic Network Data

Supervisor Name and Email:
Dr Jianxin Li, jianxin.li@deakin.edu.au

Project description:
In the real-world scenarios, the dynamic graph is the very common case such as the social graphs in Twitter, citation graphs in DBLP, student learning history. It needs some graph embedding technologies to solve the dynamic changes and scalable problems. The graph embedding is used to turn a graph into a low dimensional space. The research provides a unified data model to represent different types of graphs, such as homogeneous graph, heterogeneous graph, attribute graph. By preserving the complex graph features, it can be applied to analyse downstream applications such as knowledge enrichment, link prediction and recommendation. However, most of the existing graph embedding methods focus on the statics graph and involves the low efficiently issue. Thus, how to design effective graph embedding methods in dynamic domains is a very practical and valuable research topic.

Project aim:
Through this project, the PhD candidate expects to have a better understanding for graph neural network techniques and solve the practical and challenging problems in analysing network data. She/he will also explore the feasibility and performance of current state-of-art graph embedding algorithms, and develop novel deep learning techniques with the strong prediction capability in dynamic network environment. In

this project, we will collect the IT related course information in Australia, generate the course map based network data, and analyse the relatedness and the suitability of courses, especially for the short course application scenario. At the end of this project, the PhD candidate will publish several scientific research articles in top-tier venues, and release the demo system for public access.

Project Title#17: Stability of trajectories in optimal control problems

Supervisor Name and Email:
Dr Musa Mammadov, musa.mammadov@deakin.edu.au

Project description:
Asymptotic behaviour of optimal solutions has important applications in a wide range of real life problems in almost all areas of human activity. The phenomenon of stability of optimal trajectories is often called the turnpike property. Simply saying this property states that, regardless of initial conditions, all optimal trajectories spend most of the time within a small neighbourhood of some optimal stationary point when the planning period is long enough. In a simple case when the time horizon is infinite, this property is often defined as a convergence of all optimal solutions to a unique stationary point. The interest to this theory has grown significantly in recent years. This project is motivated by several important research directions and their applications.

There are different definitions for the turnpike property and a number of powerful theoretical approaches have been suggested. These studies have been undertaken for continuous and discrete systems separately, leading to different techniques for both directions. Some convexity conditions are sufficient for discrete systems; however, rather restrictive assumptions are usually required for continuous time systems that restrict their applications to many real world problems.

Another area is the extending this theory to optimal control problems described by time-delay systems. Theory and applications of time delay systems represent an important part of modern nonlinear dynamics. These equations are natural mathematical models for a number of real life phenomena whose dynamics are governed by the presence of aftereffects. Time delay systems find various applications in biology and medicine, where the time-delay arises naturally, for instance, as a time-lag required for cells to start dividing after they activated. Thanks to the advances in cell tracking devices and methodologies, many similar models are expected to come in the near future covering different aspects of biological and medical processes. Some other applications are in epidemiology and population dynamics, laser optics, power systems and neural networks, physiological processes, life sciences and economics, and other natural sciences.

Project aim:
The project is aimed at the study the qualitative behaviours of optimal trajectories and to relate these to particular models from applications in several areas, including biology, medicine, economics, and other fields. The project will emphasize stability of optimal trajectories in non-linear optimal control problems, as well as stability of optimal trajectories in problems described by a special class of time-delay systems having relevance to several important applications. Applications of the theoretical outcomes into several classes of applied models, including models of the immune system will be considered. This partly includes

- nonlinear continuous time systems with both integral and terminal type functionals; and
- time-delay systems governed by practical models in medicine and biology.