School of Information Technology HDR Projects 2020

To express your interest in undertaking a Higher Degree by Research with the School of Information Technology, please review the following projects and email the respective Principal Supervisor, providing the following information:

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

For more information on becoming a research student at Deakin University, please visit:

https://www.deakin.edu.au/research/become-a-research-student

Contents

Anomaly Detection on Blockchain

Principal Supervisor: Dr Lei Pan, lei.pan@deakin.edu.au

Project description:

Anomaly detection is a topic underpinning machine learning practice in expert systems and many other industrial systems. Due to its wide applications, anomaly detection also becomes increasingly popular in blockchain-based systems and blockchain data. Many research papers are recently published on anomaly detection conducted on fraudulent transactions occurred on blockchain transactions like Bitcoin and Ethereum. Such proposed solutions employ deep learning and graph-based methods to improve the accuracy while reducing the false positive rate. The researchers are trying to find new solutions to detect frauds and attacks to the blockchain systems from the finance and security perspectives. Hence, the importance of this project closely aligns with the booming digital economy and digitalized infrastructure.

Project aim:

This project aims to discover novel knowledge and technical approaches in anomaly detection based on blockchain data. The project will firstly establish a comprehensive set of data to benchmark the existing solutions before investigating the cutting-edge approaches in machine learning, including graph-based methods. Through the initial investigations, this project will try to identify the strengths and weaknesses of various solutions through both theoretical analysis and empirical studies. These findings will form an elevated base so that novel and advanced algorithms can be invented. This project aims to solve the following three research questions:

- How do the existing anomaly detection algorithms perform with respect to blockchain data and blockchain systems?
- What are the intrinsic relationships between blockchain systems and their transaction data which help us define anomalies accurately and precisely?
- How will the next generation anomaly detection impact the blockchain systems and their transaction data?
- We strongly encourage the high performing students with a background in deep learning to apply for this project.

Advanced Decomposition Techniques for Multi-Component Optimisation Problems

Principal Supervisor: Dr Sergey Polyakovskiy, sergey.polyakovskiy@deakin.edu.au

Project description:

Real-life optimisation problems often consist of several sub-problems of different nature. Not only do they combine several optimisation aspects into a single problem, but they also emanate from the compounded complexity of conflicting issues in numerous areas like logistics, planning and manufacturing. Solving them requires a thorough understanding of both their compounded and their individual natures. As traditional optimisation methods may demonstrate only limited efficiency for such problems, designing advanced decomposition approaches hybridizing several algorithmic techniques to handle their specificity and non-linear behaviour intrinsic to them appears promising.

Project aim:

The focus of this research is on perspective decomposition methods, search strategies, and learning as a way to tune the search process at the runtime. On the application side, it aims to develop state-of-the-art solution techniques for

a number of multi-component optimisation problems. For a technique to be high-performing, it is of vital importance to be capable to adaptively select sub-problems to solve in a way that ensures fast convergence towards an optimal solution. Tuning the search process appears beneficial, but a posteriori decision-making based on a subset of test instances tends to produce ambiguous settings unsuitable for the whole set. It can ignore promising decisions as the search progresses and thus seriously affect the efficiency of the entire search. More sophisticated decision methods using learning mechanisms during the search should guarantee advanced performance, but require designing new methods to measure the search performance itself. Finding such techniques is a part of this research.

Safety Affordances for Reinforcement Learning Agents

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Agents interacting with the environment may be subjected to potential risks. In reinforcement learning, an alternative is to use a model of the environment. The model is something that imitates or mimics the behaviour of the real environment. Models are used to plan since the action to perform can be decided considering possible future situations before they have actually occurred. One way to model the environment is by the use of contextual affordances where cognitive agents favour specific actions to be performed with specific objects.

Project aim:

In this project, we will use real-world and simulated robots interacting with its environment. By setting up a reinforcement learning task, the agent will use contextual affordances, an extension of the classic Gibson's affordance concept, to establish safety rules which anticipate potential risks.

The project comprises two main stages. In the first stage, it is expected to use visual inputs to determine safe behaviour possibly in different scenarios. A second stage includes to extend the approach to develop a human-robot environment where the robot should perform safe actions taking into account both robot's and human's safety.

AI Apology: Beyond Explainable Reinforcement Learning

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Two of the primary aims in explainable artificial intelligence (XAI) is to improve trust and understanding in human users. However, most XAI approaches focus on providing understanding of an AI's decision in the hope that it will improve trust. Trust though also requires the agent to show it understands and considers people's needs. This requires the agent to be able to both illustrate empathy and to be able to alter future behaviour to match that understanding.

One approach to accomplish this is through the human cultural practise of apologising for past mistakes. A genuine apology consist of three stages: acknowledgement - recognition that a behaviour has caused harm; Remorse / Empathy – acknowledgement of how the person would feel as a result of that behaviour; Restitution – an offer of how to alter future behaviour to avoid future harm.

Project aim:

The generation of an apology from an AI system is currently an unexplored domain of XAI. An agent capable of generating an apology will need to perform three primary tasks. The first involves being able to identify when the result of its behaviour (both deliberate and accidental) has caused an undesired outcome for another actor. This process will require modelling of the desired result of the other actors (people) in the environment and the matching

of real outcomes observed against their desired outcomes. Secondly, when significant mismatches are identified the agent would need to provide an expression of understanding of how this has affected the person. This expression of empathy could be provided through an adaptation of a counterfactual explanation between the desired outcome and the actual outcome. Finally, the system should be able to generate a new behavioural constraint on its future behaviour that can inhibit that behaviour in the future and suggest that modification to form the agent's restitution.

The aim of this project is to utilise knowledge engineering and emotion detection approaches to model external actor's desires. Using Multi-objective Reinforcement Learning these desires can be used as a constraint on an agent's primary objective allowing it to optimise its performance while minimising its impact on other actors. When an outcome of the agent's behaviour results in a policy that exceeds the user's model the agent can generate an apology and add new rules to the constraint model to ensure future compliance.

Impact minimisation in dynamic environments

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Imagine a robot is tasked with removing rubbish from a room while. The robot will receive a reward based on how much rubbish there is in the room. The less rubbish the greater the reward. In this simple task the robot will learn to remove all items classed as rubbish.

However, what if someone enters the room and drops new rubbish. The agent will now receive a negative reward because of that person's actions. The robot, wishing to maximise reward, may learn, not only to remove rubbish, but also to prevent people from dropping rubbish in the first place.

Project aim:

In this project you will investigate approaches to Multiple Object Tracking (MOT) approaches to identify external agent interactions with objects and use this information to dynamically identify responsibility for environmental changes. This information will be incorporated into a multi-objective reinforcement learning using impact minimisation to dynamically correct the impact potential function.

This approach will be deployed in both simulated and real-world robotic domains to determine the viability of the technique. In these environments the agent will illustrate that it can still minimise its own impacts while learning to allow other actor's to be uninhibited in their behaviour.

Explainability through Fuzzy Reinforcement Learning

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Reinforcement Learning (RL) observes an environment and determines an action that leads the agent towards its goal. The majority or Deep RL systems use raw state input such as a video image, audio, or other continuous data to represent state information. However, when an RL agent is expected to explain its behaviour it must rely on methods such as saliency maps to identify features of relevance, which have been shown to provide a poor communication technique for explanations. Furthermore, providing explanations of the agent's longer-term intentionality is even more difficult to articulate. One unique alternative approach, called Programmatically Interpretable RL (PIRL) approach raises the possibility of representing state through a programmable structure and using this for generating basic explainable functionality.

Project aim:

In this project we will build upon the idea in PIRL by developing an approach where represents the environmental state through an abstracted model using fuzzy rules where the fuzzy sets are generated through environment interactions. These fuzzy rules will provide a structured ontology for interpreting the state, while the rule inference process will provide the agent's intentionality-based reasoning. The combination of these components will both allow an agent to apply traditional RL learning while also being capable of providing both perception and goal-driven explanations of its behaviour.

This project will be conducted in two stages. The first stage will develop a Fuzzy RL framework capable of learning in traditionally deep learning environments. This agent will then be used to generate explanations of that improves human observers' mental model of its behaviour. This will involve a quantitative and qualitative study of people predicting the agent's future behaviour after being trained on past cases.

Back-dooring Federated Learning and Mitigations

Principal Supervisor: Dr Leo Zhang, leo.zhang@deakin.edu.au

Project description:

Standard machine/deep learning requires a centralized dataset for model training. Google and other industry leaders strongly advocated for federated learning because it enables distributed users to learn a model collaboratively. Federated Learning aggregates different ML model updates submitted from participants through an aggregation centre. It eases the concern of privacy leakage since data is not directly exposed to the centre or other participants. However, this architecture increases the attack surface, including data/model poisoning and back-dooring. In particular, back-dooring aims to control the model's behaviour on specific attacker-chosen inputs via implanting a backdoor to the model during training/fine-tuning.

Project aim:

This research project is a discovery project in both AI and cybersecurity fields. Despite its academic nature, this project is closely aligned with the latest advancements of AI technologies used in leading companies like Google, Microsoft, Amazon, and alike. Hence, the outcomes of this project apply to both academia and the industry. This project also investigates one of the most prominent attacking methods against AI models through planting backdoors. This project aims to find the balance between the feasibility requirement imposed by the real-world needs and datasets and the increasing security and privacy needs through theoretical analysis and empirical studies. To research the techniques for back-dooring federated learning and its mitigations, it is necessary to:

- Review federated learning for the differently partitioned databases (horizontal, vertical, hybrid) and the associated optimization techniques;
- Review the back-dooring methods and the mitigations on the traditional learning paradigm for different network frameworks, like CNN, RNN, and etc. under the identified threat model.
- Identify the new threat model for federated learning and implant backdoor to CNN, RNN in the federated learning scenario through optimizing a backdoor-associated loss.
- Mitigate the backdoor attacks to federated learning with techniques like anomaly detection or removing the backdoor through fine-tuning/generative adversarial training.

Narrative generation in complex group decision making

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Modelling and representing decisions made by a team under complex environment is very challenging. Some examples include decisions made by health professionals in hospitals and army commanders in battle fields. These decisions can be critical and have to be made quickly considering the current context and information available. Understanding the rationale/story behind decisions made previously is important to understand the context for future decision making. Knowledge representation, argumentation modelling and narrative theory can be useful to generate narratives for such complex decisions.

There might be a possibility to engage and collaborate with hospitals and/or defence partners (e.g., DST Group).

Project aim:

This PhD project aims to develop a framework to generate narratives for complex decisions made by a team. The plan is to extend the idea of Generic/Actual Argument Modelling (GAAM) to create a story for a decision made. In GAAM, knowledge is represented as a tree structure called 'Generic Argument Structure' (GAS). It captures context variables, relevant data with reasons for relevance, inference with reasons and claims. Each argument is an instantiation of GAS. The two layered abstractions separating generic and actual argumentation provides flexibility to consider different opinions. Because GAAM captures context, data (setting) and claim (resolution), it can be used to generate a story based on the narrative theory. The research may be based on case studies from domains such as defence, health and/or law. A candidate with some background in knowledge engineering, programming, text mining and machine learning will be preferred.

Deep Topic Modelling for Text Analysis in Fog Computing

Principal Supervisor: Dr Feifei Chen, feifei.chen@deakin.edu.au

Project description:

As the booming development of topic modelling algorithms and word embedding techniques, the researchers started to chase for the better performance of topic modelling and text analysis with more meta-information in the local computing environment, namely Fog computing. Given these, in this research project, we will investigate how different embedding techniques and meta information could benefit the topic modelling as well as textual analysis and application in Fog computing.

Project aim:

The project aims to improve the deep topic modelling performance in Fog computing, it actually can benefit in more trending text analysis tasks and undiscovered machine learning areas. As a critical task in textual analysis, topic modelling in Fog computing has achieved several researchers' attention to exploring. Besides, with the boosting of advanced neural network technology and localized computing facility, topic modelling in Fog computing has a potentially large area to investigate. In both the supervised and unsupervised learning area, there have been several attempts of improving the performance of topic modelling in various domain-specific for localized services. For example, added word embedding into word-occurrence model as well as encoded a character embedding in topic modelling in for a domain specific use case.

Next Generation Authentication and Privacy Protection Scheme for Vehicular Fog Infrastructure

Principal Supervisor: Prof Robin Doss, robin.doss@deakin.edu.au

Project description:

Intelligently connected vehicles are one of the key nodes in the fog infrastructure as the extension of cloud computing. It is a distributed computing infrastructure and can provide timely responses to the various service requests within the tolerable network latency. Fog computing has competencies in terms of certain mobility integrating network, computing, storage and application on the edge of the network near the object or data source. For the purpose of achieving a secured interconnected vehicular edge system, this project proposes an IoT device/context fingerprint based next generation authentication scheme for autonomous vehicular within the fog infrastructure.

Project aim:

Aiming to establish an edge fog computing infrastructure to provide a real-time, safe and converged services, where the core authentication technique is integrated with privacy-preserving techniques (e.g., LBS) to interconnect the vehicle network.

The expected outcome of this research includes:

- A new classification method for connected users and information in vehicular network meets the needs analysis.
- An intelligent system for discovering connected vehicles and information. A new trust-built scheme is developed and maintained sustainably.
- New algorithms/models for next-generation IoT device level authentication and reconstruction based on new technologies (for instance, context fingerprinting, blockchain trust network).

Research Activities:

- Be part of the team, fortnightly project meetings closely
- Literature review on blockchain, malware/ransomware detections, privacy preservation techniques.
- Launch attacks: Use of Veins Simulation Platform with attacks, such as Miral attacks, Man-in-the-middle attacks etc.
- Explore learning schemes, such as Federated Learning scheme and Deep Reinforcement Learning scheme.

Heterogeneous IoT Data Stream Analysis to Enhance Network Security

Principal Supervisor: Dr Keshav Sood, keshav.sood@deakin.edu.au

Project description:

Due to continue skyrocket growth of large scale multi-technology and multi-tenant Internet of Things (IoT) networks the networks are expected to be extremely heterogeneous. This heterogeneity will give unique challenges on real-time network security. There are some limited solutions in this problem domain which alleviate the current heterogeneity challenges. Still we observe that the heterogeneity of IoT node's data will substantially increases in future which can play an adverse role in large scale IoT network security management. We believe that a deep understanding and analysis of heterogeneous data streams can promisingly help us to alleviate network security issues in future.

Project aim:

Therefore, in this project, firstly we will investigate how the heterogeneous data streams alter or affect the decision making ability of intelligent and autonomous security systems. Secondly, we will propose an approach to alleviate the complexity of heterogeneity in data streams. So that the real-time data processing and intelligent decisions making will be easier for a security management system. Following this, the proposed approach will be tested and validated. Finally, based on the proposed approach an autonomous network security management system will be proposed.

This study will expands our knowledge to design an autonomous IoT security architecture. The autonomous and intelligent architecture will be capable to a) early alarm the risk of cyber-attacks, b) timely detection of anomaly connections, and c) will helps to avoid any unplanned network maintenance. This eventually would enhance network security to great extent, improve user experience and would save significant operational and capital expenditure cost.

Machine Learning for Financial Risk Management

Principal Supervisor: Dr Wei Luo, wei.luo@deakin.edu.au

Project description:

Management of financial risk is critical for organisations, particularly those relying on risk exposure for competitive advantage. The task, however, has become increasingly complex due to the fast-changing risk landscape. This project will leverage the latest advances in artificial intelligence (AI) to develop better models for identifying and measuring risks. It will produce novel machine learning algorithms that can assist decision-makers to turn the risk into business performance.

Project aim:

Our project aims to develop novel yet highly applicable machine learning algorithms that can provide reliable and accurate risk measures to support risk-related decision making. The main objectives include:

- To conduct a systematic survey of the current machine-learning techniques used for managing financial risks.
- To develop robust machine-learning algorithms to measure and mitigate the risk of large-scale financial portfolios.
- To develop an AI-driven decision-support system assisting the financial risk management process.

Computer Vision for 3D Scene Understanding

Principal Supervisor: Dr Duc Thanh Nguyen, duc.nguyen@deakin.edu.au

Project description:

Scene understanding is a fundamental topic in Computer Vision with a wide spectrum of applications in many research fields such as robotics and virtual reality. The project will develop novel Computer Vision and Machine Learning models to address the current challenges in 3D scene understanding from large-scale and real-world data. In the project, contemporary computational models and technologies in Computer Vision and Machine Learning such as mobile-based real-time 3D reconstruction, big data processing, and deep learning will be advanced. The outcomes of the project will be applied in real-time navigate robots and mobile-based virtual reality systems.

Project aim:

This project aims to develop Computer Vision and Machine Learning models to solve the following problems:

- High-quality and real-time 3D reconstruction
- 3D-2D reasoning
- Semantic scene segmentation
- 3D object recognition
- Scene modelling

Data-driven Online IDS for IoT Streaming data using Machine Learning

Principal Supervisor: Dr Adnan Anwar, adnan.anwar@deakin.edu.au

Project description:

Cybersecurity in IoT space is gaining significant relevance due to increased network attacks and data breaches reported in this area. Also, the level of sophistication and complexity of cyber-attacks is increasing with adversarial learning and AI-based malware being used. Traditional machine learning algorithms are good for prediction of attacks with static and known features. However, the continuous change in network behaviour and rapidly evolving cyber-attacks necessitates developing a flexible intrusion detection system (IDS) that will be dynamic and lightweight in nature for classifying unforeseen and unpredictable cyber-attacks.

Project aim:

Although machine learning has been extensively used for IDS with static data, still there is a huge scope to explore the security aspects for IoT streaming data. In this project, different machine learning algorithms will be evaluated for classification of attacks based on IoT datasets. This study will gauge if different ensemble learning approaches can improve the efficacy of intrusion detection systems while maintaining their light-weight property for online adoption that would be suitable for near real-time operations. This type of study facilitates to identify the best algorithm which will improve the detection accuracy and computational efficiency of detecting future IoT cyber-attacks.

Automated Privacy Compliance Evaluation

Principal Supervisor: Prof Gang Li, gang.li@deakin.edu.au

Project description:

Privacy breaches are a regular occurrence in contemporary society with the public becoming increasingly concerned with how their digital data will be handled. Hence, regulatory organizations through the world, are formulating data privacy legislations, such as the EU's GDPR. Those data related regulations are requiring significant manual effort to determine whether a compliance violation has occurred. This project aims to develop an automated privacy compliance verification system, in which the bounds of privacy loss on the targeted individual can be quantified.

Project aim:

Students are expected to be with statistical background, and data science technical skills. The research project aims to make novel contribution in the theory of automated privacy compliance checking, and implement a prototype system which can deliver satisfactory results for popular privacy preserving methods evaluated on benchmark datasets.

Adversarial attacks on medical machine learning

Principal Supervisor: Dr Sutharshan Rajasegarar, sutharshan.rajasegarar@deakin.edu.au

Project description:

Medical practitioners and researchers are developing and deploying many AI-driven systems to aid medical diagnosis, treatment, and even insurance claims. However, adversarial attacks, as a new form of attacks against machine learning and deep learning models, become an emerging threat to the medical field. This project involves the application of adversarial machine learning in the field of medical AI systems. This project will evaluate the reliability and security of medical AI systems: when, how, and why they fail under the adversarial setting. This project aims to develop novel set of both adversarial attack and defence methods during this project.

Project aim:

Based on the attackers' knowledge, the adversarial attacks can be developed under different settings: white-box, where the attacker has perfect knowledge about the model and how it was trained, and the next one is the black-box, where the attacker has only a query access to the target model. Black-box (or zero-order) optimization methods can be used to craft black-box attacks while gradient-based (e.g., first-order or second-order) optimization methods can be used to craft white-box attacks. Defence methods are generally developed under a white-box setting to ensure maximum robustness under the worst-case vulnerabilities.

Moreover, the methodology used for defence methods will be robust optimization: incorporating the robustness objectives into the standard performance objective to form a bi-level optimization problem. In detail, this project attempts to achieve the following objectives:

- Develop adversarial attack methods to evaluate the vulnerability and reliability of medical machine learning systems.
- Develop adversarial defence methods to protect medical machine learning systems.
- Provide useful understandings of the weakness of existing medical AI systems: when and why they can fail.
- Bring new attack/defence/evaluation methodologies to the adversarial machine learning community.

Applicants who have a strong background in machine learning and even industry experiences are strongly encouraged to consult one of the supervisors via email.

Learning the Focus of Attention to Detect Distributed Coordinated Attacks

Principal Supervisor: Dr Sutharshan Rajasegarar, sutharshan.rajasegarar@deakin.edu.au

Project description:

Cyber security has become a strategic national priority given the dependence of modern society on Internet-based services. While cyber defences have improved, attackers are also becoming more sophisticated in the design of their attacks in order to evade defences. Distributed coordinated attacks have grown, in which attackers use a large number of infected hosts that are widely distributed across the Internet to generate malicious traffic in a coordinated manner. The aim is to accurately detect these attacks from the massive volume of data in a timely manner. This project is part of an ARC DP grant project.

Project aim:

Cyber security analysts need to detect and respond to the coordinated attacks as soon as possible, to minimise the damage attackers can inflict. However, the growth in highly distributed attacks that span multiple networks has meant that massive volumes of data need to be analysed. While machine learning techniques can help filter the data, we

need techniques that can automatically provide a focus of attention for analysts on the most relevant observations. The aim of the project is to propose novel suite of deep learning-based algorithms that can focus the search of security analytics techniques, which substantially improve the accuracy and efficiency of distributed coordinated attack detection in high volume distributed security data streams.

Energy consumption modelling and monitoring in power networks

Principal Supervisor: Dr Sutharshan Rajasegarar, sutharshan.rajasegarar@deakin.edu.au

Project description:

Microgrids are some of the important part of the power grid for providing reliable and economic energy. The main sources of energy in microgrids are the renewable energies. Analysis of energy consumption and supply are important for effective monitoring and management of the network assets, including microgrids. Customer profiling and monitoring environmental conditions can help to perform reliable prediction on the consumption patterns, and hence to aid with the energy management in the network. The data collected from the various sources are mainly time series measurements. Hence it is important device accurate models using time-series to perform forecasting and anomaly detection in the system.

Project aim:

Energy consumption analysis involve univariate and multivariate time-series analysis to identify patterns and perform reliable forecasting in long and short term. In this project various machine learning and deep learning models will be evaluated and novel algorithms will be proposed to achieve reliable and accurate forecasts incorporating heterogeneous time-series data from energy, environment, electrical assets, customer profile data and sensor data. Candidates interested in this project need to have WAMS over 80 or H1, and publications in reputed venues in the related field of the work, namely deep learning and computer science areas.

Data-dependent kernel similarity

Principal Supervisor: Dr Sunil Aryal, sunil.aryal@deakin.edu.au

Project description:

Because the distance between two data objects is independent of data distribution, distance-based kernel functions' performances vary significantly in different datasets/applications. There has been a couple of data-dependent (dis)similarity measures proposed (e.g., Mp-dissimilarity and random forest-based similarity measures) where the (dis)similarity of two objects is distribution dependent. They have been shown to produce better results than data-independent distance measures in various tasks. Some of these data-dependent dissimilarity measures are not valid kernels. Some prior studies have used data-dependent kernel functions using random forest-based similarity. Because of their grid-based implementation, they do not work well in high dimensional spaces.

Project aim:

First, this project aims to do comprehensive comparative study of existing data-independent and data-dependent kernel similarity functions to understand their strengths and limitations. A recently comparative study has shown that the data-dependent (dis)similarity measure of Mp-dissimilarity produces better results than distance-based data-independent and random forest-based data-dependent (dis)similarity measures, particularly in high dimensional problems. However, Mp-dissimilarity is not a valid kernel because of its definition. The main aim of this project is to extend Mp-dissimilarity into a valid data-dependent kernel and study its properties. It is believed that such kernel will produce better results than existing distance-based and random forest-based kernel functions, particularly in high

dimensional data sets. The proposed and existing kernel functions will be assessed in publicly available benchmark datasets.

Augmented reality enhanced analytics

Principal Supervisor: Dr Shaun Bangay, **shaun.bangay@deakin.edu.au**

Project description:

This project extends on a research project undertaken in conjunction with a local primary school to develop an augmented reality (AR) application to support student engagement during the kindergarten/primary school transition. This utilizes the forest classroom experience which is a physical room providing a calming environment for disengaged students. During this process an opportunity was identified to use the AR experiences to collect and present learning analytics, to enhance existing data collection and teacher reflections mechanisms.

Project aim:

This project aims to advance the use of teaching analytics through integrating data collection into augmented reality applications used to enhance the classroom environment, and to provide opportunities to present this information to teachers in ways that effectively support the learning process. The process involves closely collaborating with our partner school, and identifying candidate curriculum topics.

Bespoke AR applications specific to those topics and with enhanced data collection capabilities will then be deployed in the classroom. The research will evaluate the accuracy and relevance of the data collected. We also investigate the opportunities that presentation of this data provides to enhance teaching practices through interviews with teachers. The outcome is anticipated to advance practices in educational data collection and augmented reality experience design practices, and has potential for subsequent commercialisation.

Privacy-Preserving Federated Learning in Edge Computing

Principal Supervisor: Dr Longxiang Gao, longxiang.gao@deakin.edu.au

Project description:

Due to the demand of low latency and data privacy, edge computing becomes efficient architecture for data storage and processing. Amounts of data private in nature is stored in edge devices, especially in some particular scenarios such as medical service. These rich data could be utilized to construct intelligent applications for users. For example, automatic text summarization or detection model could be built for human activity recognition. These intelligent tasks are performed by training machine learning models via data on user's devices.

Project aim:

Compared to conventional approaches to train models on centralized data centres, training models on decentralized edges bring challenges in many aspects. How edge devices update parameters locally? How updating information is aggregated to train a global model on cloud server? For tackling solutions, the concept of federated learning was introduced by Google in 2016 to define this emerging machine learning paradigm. However, even though some studies contribute to this area recently, there are only a few industrial applications of federated learning due to the challenges related to data privacy, communication efficiency and heterogeneous data. One of the biggest research questions is approaches for model aggregation with consideration of three limitations mentioned above. The project aims to develop optimization algorithms and suitable model architecture to update the model for cross-silo applications where data is not allowed to share with other clients.

Device-centric Smart Neuromorphic Computing

Principal Supervisor: Dr Frank Jiang, frank.jiang@deakin.edu.au

Project description:

Next-generation IoT Systems aim at delivering the device-specific adaptability in the contested tactical environments, that evolves the IoT device/system itself to cope with the ever-changing context/anomalies in an intelligent manner for future heterogeneous and hostile environments while maintaining the cyber-safe sufficiency for users. However, the adaptable devices also exhibit the vulnerability, as a result of certain level of "openness" due to the adaptability, to the attacks explicitly and implicitly. In this project, an adaptable IoT system with smart Neuromorphic computing algorithms, Spiking Neural Network (SNN) and new protocols will be further developed, validated for smart anomaly detection/diagnosis in low-powered IoT devices.

Project aim:

The aim of the proposed project is to develop and design the embedded system with the adaptable intelligent algorithms and protocols that can be quickly deployed in the contested tactical environments, such as battle fields, while maintaining the acceptable level of data security.

The expected outcome of this research includes:

- Developing a sustainable and maintainable IoT networked architecture by using biomimetic mechanisms, satisfying the performance goals (e.g., robustness and scalability), and economic goals (e.g., finance feasibility);
- Creating a scalable and adaptable decision-making facility enabled by the local intelligence from "Reasoning" capability referring to the distributed biological algorithm.
- Develop new algorithms/models for next-generation IoT device level authentication and adversarial detection based on FPGA embedded platforms.

Research Activities:

- Be part of the team, fortnightly project meetings closely.
- Literature review on Neuromorphic computing, malware/ransomware detections, privacy preservation techniques.
- Launch attacks: Use of Simulation Platform with attacks, such as DDos, Miral attacks, Man-in-the-middle attacks etc.
- Explore other learning schemes to improve the system interoperability across platforms.
- Produce new patent on the basis of our existing FPGA patent as a practical outcome.

Autism Screening by Deep Learning

Principal Supervisor: Dr Shang Gao, shang.gao@deakin.edu.au

Project description:

Autism spectrum disorder (ASD) is a neurodevelopmental disorder that affects communication and behaviour. Detecting ASD as early as possible is desirable as early detection of ASD enables timely intervention and early treatment on the children affected by ASD. However, conventional autism assessment tools usually take long time to diagnose, which is not clinically applicable or convenient. The research topic of this project includes early ASD diagnosis prediction and novel screening algorithm development. It will develop innovative and interactive ASD screening tools

that incorporate artificial intelligence technologies to empower parents and the paediatricians to act on early concerns.

Project aim:

This project aims to apply advanced deep learning methods to create a highly sensitive and accurate early diagnostic classifier for the prediction of ASD. It will also identify genomic mutations associated with ASD that might enable more effective treatment. On completion of this project, a comprehensive ASD diagnosis tool based on specific deep learning models will be delivered, together with various analytical ASD data, such as brain and facial images, genetic variants, demographics, and behaviour data, etc.

This project will further facilitate the collaboration with Olga Tennison Autism Research Centre, La Trobe University for autism-related data support and attract more potential collaboration opportunities from other autism research institutions/hospitals. Meanwhile, considering that the Australian government is investing more in Mental Health, there is a big potential to work with health institutions for ARC linkage projects and other funding opportunities.

Deep learning-based voiceprint authentication system for IoT

Principal Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au

Project description:

Voice biometrics gains increasing popularity. Analogy to fingerprints, voiceprints carry the acoustic information of human in a speech and provide a distinctive biometric identity for individuals. Further, voiceprints can be easily collected and using voiceprints greatly simplifies interactions between human and devices. These qualities enable voiceprints to work as passwords for high-level security services, particularly in the realm of Internet of Things (IoTs). The voice control smart home assistant and Advanced Driver Assistance Systems (ADAS) are two promising IoTs applications. However, the state-of-the-art solution utilising voice biometrics lacks of required robustness, efficiency and safety.

Project aim:

One of the major challenges in the voiceprint authentication system is the consistency of accuracy and recall simultaneously. Deployment is another significant problem. Communication latency, storage, and computing resources limit a deep learning model running as usual on edge devices. Instead, an optimized model is in demand to retain consistency while enhancing usability on edge devices. Moreover, given that voiceprints systems are particularly vulnerable to certain conditions such as malicious voice input attacks, security problems are also highly desired under IoT.

This project proposes to integrate deep learning-based voiceprint authentication system into IoT edge devices with the following aims:

- Robustness: The voiceprint authentication system can have consistent accuracy and recall in various application scenarios.
- Efficiency: The voiceprint authentication system can be deployed onto edge devices with minimum requirement for computation and network resources
- Safety: The voiceprint authentication system can resist various state-of-the-art attacks including adversarial attacks and Trojan attacks.

Point Cloud Driven Scene Understanding

Principal Supervisor: Dr Xuequan Lu, xuequan.lu@deakin.edu.au

Project description:

3D geometric data is becoming increasingly prevalent nowadays. It mainly consists of two types of data: mesh and point cloud. With the increasing availability of consume-grade sensors, point cloud data can be easily captured. As a result, understanding of point cloud data especially scene point cloud data is of great importance in many fields, such as VR/AR, entertainment, vision, graphics, robotics and so on. It will also provide great potential to commercialization by boosting intelligence, accuracy and user interaction. As such, it is significant to understand complex scenes based on point cloud data.

Project aim:

This project will mainly target at scene understanding based on point cloud data. The aims are as follows:

- Develop a series of robust and novel approaches for scene understanding;
- Identify significant factors in point cloud based scene understanding;
- Introduce various methods to handle the identified factors;
- Integrate methods into a prototype platform;
- Disseminate research outcomes, e.g., publication and present in prestigious conferences.

Combinatorics of polytopes

Principal Supervisor: Dr Guillermo Pineda Villavicencio, guillermo.pineda@deakin.edu.au

Project description:

A *polytope* is the intersection of all convex sets containing a finite set of points in the Euclidean space, its *vertices*. The dimension of a polytope is the maximum number of affinely independent points in the polytope minus one; the maximum number of affinely independent points in R^d is *d+1*. A polytope is structured around other polytopes, its faces. A *face* of a polytope P is P itself, or the intersection of P with a hyperplane that contains P in one of its closed half-spaces. In a d-dimensional polytope, or d-polytope for short, the vertices are its 0-dimensional faces, and the *edges* are its 1-dimensional faces. The vertices and edges of a polytope form *graph*, where two vertices are adjacent if they belong to the same edge.

Project aim:

The project aims to gain insights into graphs of polytopes, and to pinpoint to what extent they explain properties of polytopes. Two questions make these aims concrete:

- Given the graph of a polytope, what properties can we infer about the polytope?
- Given a class of polytopes, what properties characterise their graphs?

The outcome of the project will be a framework to answer these two questions. We investigate graph-theoretical topics such as connectivity, colourings, linkedness of graphs of polytopes. These are well-established topics within graph theory, with dedicated books, and chapters in most textbooks (Diestel, 2017), but not yet in polytope theory.

Explainable Intentionality with Multi-objective Reinforcement Learning

Principal Supervisor: A/Prof Richard Dazeley, richard.dazeley@deakin.edu.au

Project description:

Researchers have long understood that an AI-based system's ability to explain its decision is critical to human acceptance, understanding and trust. Recently, with the growth of machine learning based systems there has been a significant increase in work in this domain. Explaining the behaviour of Goal-Driven agents however is currently mostly limited to local decisions rather than explaining the intentionality and temporal nature of the decision. Intentionality, however, is limited in single objective domains. Reward decomposition can provide some degree of justification provision around action preferences but is limited due to the correlation of reward signals.

Project aim:

In this project we will use a multi-objective framework to extract action preferences that allow a comparison of the possible actions against each of the objectives. This will be combined with our approach for transition probability prediction to explain to the user that the selected behaviour increases the opportunity of achieving a particular objective over other actions that lead to alternative and unwanted objectives. For instance, this will allow us to provide the explanation:

I did X instead of Y because X will still allow (with some probability) me to achieve my primary objective but is unlikely (with some probability) of causing Z (some undesirable outcome).

The natural extension to this will provide both counterfactual and contrastive explanations and this study will show to what degree human users can develop a mental model learnt from such explanations, allowing them to accurately predict the agent's behaviour in future environments.

Optimising self-organising mobile agents

Principal Supervisor: A/Prof Vicky Mak-Hau, vicky.mak@deakin.edu.au

Project description:

Given a task or a set of tasks, finding the optimal number of mobile agents required to complete the task(s) and the optimal sequence of procedures to carry out for each of the agents, is a highly complex optimisation problem. We consider the case for a set of self-organising mobile agents where the complete nature of the task(s) is not known in advance, and the agents are required to process the information acquired about the task(s) "on the fly" and derive an optimised plan to carry out the task(s). The outcome of the research can be applied to the construction, mining, and many other sectors where using mobile agents can significantly improve the safety of human workers.

Project aim:

The research that the student will be conducting is 1) to derive a generic scenario of application and working with industry (construction, mining, etc.) to identify three use cases, 2) a framework for solving the two optimisation problems: the optimal number of mobile agents required to complete the task(s) and the optimal sequence of procedures to carry out for each of the agents, and 3) implement the new techniques for solving problem instances from the three industry use cases.

EV fast-charging network optimisation

Principal Supervisor: A/Prof Vicky Mak-Hau, vicky.mak@deakin.edu.au

Project description:

Building a national electric vehicle fast-charging network is one of the national high priority infrastructure initiatives. By 2040, electric vehicles (EVs) are projected to account for 70% to 100% of new vehicle sales and at least 30% of the vehicle fleet in Australia. According to the Electric Vehicle Council, lack of access to charging stations has been identified by around two-thirds of motorists as a key barrier to the adoption of EVs. Australia currently has less than 2,000 public charging stations, of which approximately 250 are fast-charging. This research is to derive techniques for decision makers to optimise the national electric vehicle fast-charging network.

Project aim:

The research the student will be completing include: 1) analysing the current network use pattern of existing EV users, 2) predicting the network use pattern of EV users by 2040 and beyond, 3) deriving mathematical models and algorithms for finding the optimal locations of EV fast-charging stations based on a given set of parameters, 4) using simulation to generate parameter sets for the optimisation problems in 3) and run a comprehensive set of numerical experiments, and 5) using explainable AI to analyse the relations between the parameters and solutions and derive a decision tool for recommending a small number of decision plans for users.

Multi-Orbit Satellite Constellation Resource Optimization

Principal Supervisor: A/Prof Vicky Mak-Hau, vicky.mak@deakin.edu.au

Project description:

Multi-orbit satellite constellations, in low, medium, and geosynchronous earth, i.e., LEO, MEO and GEO provide exciting and unparalleled opportunities in the satellite communications domain. The multi-orbit constellations will provide unparalleled advantages, including among others the ubiquitous coverage to polar regions, maritime and aerospace with ultra-low latency, edge-processing for 5G and IoT networks, quantum key distribution, and effective disaster management. An important prerequisite for realizing these promises of multi-orbit constellations is to optimally manage the space and ground resources and the communications schedules among orbits and ground. This research project will devise techniques for dynamic resource management in multi-orbit satellite constellations.

Project aim:

The research student will investigate the issues and constraints in the multi-orbit constellations. The students will be responsible for (1) deriving mathematical models and algorithms for the dynamic management of ground stations and inter-orbit communications; (2) using explainable AI to analyze and establish relations between (i) the data traffic patterns based on weather conditions, geographical locations and demographics; and (ii) space and ground resources; (3) help devise decision-making tools for satellite operators based on steps 1 and 2; (4) develop visualization tools for dynamic resource management; (5) run a comprehensive set of experiments.