School of Information Technology

2021 Honours Projects

DEAKIN UNIVERSITY

Published: October 2020
Deakin University CRICOS Provider Code: 00113B

PROJECTS

Use of AI and chatbots for helping people with depression and mindfulness

Supervisor: Dr Alessio Bonti, a.bonti@deakin.edu.au **Associate Supervisor:** A/Prof Mohamed Abdelrazek

Campus: Melbourne Burwood

Start: January or July

Project Description:

DWL : Deakin Wide Lab is an initiative that aims at creating novel and innovative solutions that will use the University as a test bed for experiments in order to solve real life problems that can scale up to the world.

Mental disorders, including depression, create difficult environments for people to live in. The stigmata associated with them also pushes people to hide having such problems. COVID-19 has shown that tools are now becoming imperative, during and past COVID-19 itself. Our chatbot, based on a past successful engagement with a leading organization, will further explore how AI can help to reduce the burden for people and for society.

The student will make use of the existing resources, including:

- Leveraging existing infrastructure and relationships
- Exploring how to train and enhance chatbots
- Identifying key metrics to be used in conversation design

Necessary Skills:

- Nodejs or alternative programming language (will require to learn nodejs), learn basic Hyperledger composer

Digital Twins - Study and Design of an IOT system for improving energy usage and decrease carbon footprint

Supervisor: Dr Alessio Bonti, a.bonti@deakin.edu.au **Associate Supervisor:** A/Prof Mohamed Abdelrazek

Campus: Melbourne Burwood

Start: January or July

Project Description:

DWL : Deakin Wide Lab is an initiative that aims at creating novel and innovative solutions that will use the University as a test bed for experiments in order to solve real life problems that can scale up to the world.

Energy efficiency has now become an imperative for most companies and governments, the term Digital Twin represents how our daily life can be simulated in a digital environment. This knowledge can help us monitor, predict and improve our daily lives by improving the world around us. Our system is based on Indoor tracking using bluetooth technology. Indoor tracking, or high resolution geopositioning can be very useful to create new services based on the tracking data of users.

We have developed a prototype infrastructure to track users inside Greenwood Park, using Estimote beacons. We currently use this data for temperature control and for other projects which leverage human activity.

The student will make use of the existing resources, including:

- Leverage existing infrastructure and relationships
- Explore the use of Beacons technologies
- Create new ways of using the data

Necessary Skills:

- Nodejs or alternative programming language (will require to learn nodejs)

DWL : Identity preservation using blockchain for real world uses (Blockchain and security)

Supervisor: Dr Alessio Bonti, a.bonti@deakin.edu.au **Associate Supervisor**: A/Prof Mohamed Abdelrazek

Campus: Melbourne Burwood

Start: January or July

Project Description:

DWL : Deakin Wide Lab is an initiative that aims at creating novel and innovative solutions that will use the University as a test bed for experiments in order to solve real life problems that can scale up to the world.

Blockchain technologies have allowed for creation of new services, but also for changes in our current ones. The promise of traceable immutable system of records based on decentralized trust have changed the way we design and envision our future social interactions and business relationships.

This project aims at identifying the benefits and costs of implementing a system that will use blockchain to allow users, groups and companies to safely share information either without revealing their identity, or by allowing easy to track audited documents.

This will greatly increase the value of data and enhance its protection, allowing the user to fully assess the current state of his DWL and own his data, may he want to freely disclose it, or sell it

The student will make use of the existing resources, including:

- Use and write Smart contracts
- Leverage existing infrastructure and relationships

Necessary Skills:

- Nodejs or alternative programming language (will require to learn nodejs), learn basic Hyperledger composer

Secure by design: A possibility using digital twins and blockchain

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

Campus: Melbourne Burwood

Start: January or July

Project Description:

A digital twin is a virtual representation of any real-world counterpart that allows its management (monitoring, maintenance, and autonomy). It also allows for testing and simulation of a real-world counterpart before production, thereby reducing the trial and error cost of production during a product's lifecycle. Numerous systems consider security as a later part of the product lifecycle, which introduces various vulnerabilities into the product. DT can incorporate every lifecycle phase originating at planning and design, which allows a focus on security before the operation and can be subject to security checks at each stage of the lifecycle. DTs are positioned to gain significant attention in the foreseeable future while playing a key in Industry 4.0, but current systems used to create DTs are mostly centralized and fall short of providing trusted data provenance, audit, and traceability. Also, data related to transactions, logs, and history are not secure or tamper-proof. Research has indicated a blockchain-based creation process of DTs to secure these shortfalls and ensure the data integrity of a DT. This project will further investigate how blockchain provides data integrity within a DT and vulnerabilities within that approach which can negate the value provided by blockchain. The project will include a critical analysis of literature, proof-of-concept implementation, and empirical evaluation results with in-depth discussion.

In this project, the student will investigate the use of DTs for cybersecurity and its application in providing security by design and using blockchain to ensure the data integrity and authenticity of a DT. Mechanisms to detect privacy anomalies in the smart automotive ecosystem and research into a proposed security-aware framework for digital twins currently exists. A proposed solution to ensure data integrity of digital twins has also been published recently which uses smart contracts to govern and track transactions initiated by participants involved in the creation of DTs thereby integrating blockchain into them.

Necessary Skills:

- Knowledge in industry 4.0, digital twin and blockchain is ideal

Developing an Innovative Privacy Enhancing Tool for Data After Death

Supervisor: Dr Arash Shaghaghi, a.shaghaghi@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

Throughout our lifetimes we consume, collate, curate, host and produce a staggering quantity of data – some by our own hand, some by others on our behalf, and some without our knowledge or consent. Collectively, our "digital footprints" represent who we are and who we were. Our digital legacies are immortal and can impact those we leave behind. Many of us take steps to secure our privacy while we're alive, but there's mounting evidence that we should be equally concerned about the privacy and security risks of our "data after death".

In collaboration with the Australian Information Security Association (AISA), we surveyed about 200 AISA members to assess their awareness of digital wills and associated Australian regulations that protect users' security and privacy. Our survey results confirmed that even key decision makers in the field and cybersecurity thought leaders had not considered or prepared for posthumous data risks.

Technological solutions for data after death proposed thus far fall into the category known as privacy-enhancing technologies - tools meant to protect users' privacy. Users have been reluctant and slow to adopt privacy enhancing technologies. In part, this is because they don't allow individuals the ability to control how they manage their privacy risks.

In this project, the student will work with the supervisor to develop an innovative, usable, and reliable solution to enable users manage the data that they leave behind across different services and platforms. The student is expected to be passionate to learn about blockchain technology as part of this project. A student failing to implement a proof of concept of the innovative tool will not be able to meet the minimum requirements for completion.

Data After Death project is led by Dr. Arash Shaghaghi and housed in Protective Security and Information Warfare Lab of CSRI at Dakin University.

Related Reading:

- The Conversation, article Digging your own digital grave: how should you manage the data you leave behind?
- AISA Cyber Today, Edition 2, article From the cradle to the grave, page 54

Necessary Skills:

- The student must be hands-on with solid knowledge and experience of programming

Data Analysis with Fuzzy Integrals

Supervisor: Dr Simon James, simon.james@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

The theory of fuzzy integrals has been developed both from the mathematical perspective in terms of generalising the kind of integration you would be familiar with in calculus, as well as from the perspective of data analysis, where integrals are used to replace the mean or median function in order to summarise data.

The key thing that distinguishes fuzzy integrals is that the aggregation can be non-additive, so on the data analysis side we are able to model interaction between variables and uncover complex relationships.

As theory and applications of fuzzy integrals are still in their infancy, there is potential to develop new methodologies for fitting models to data as well as investigating useful and interesting properties.

This project would suit those interested in both mathematics and computer science, allowing you to explore either depending on your capabilities and interest.

Necessary Skills:

- Completion of at least 2 mathematics units at 2nd year level
- Some basic programming will be beneficial, particularly in R

Classification-based Sensor Tuning

Supervisor: A/Prof Professor Tim Wilkin, tim.wilkin@deakin.edu.au

Campus: Melbourne Burwood

Start: January

Project Description:

Data-driven intelligent sensor adaption has many immediate applications in IoT and robotics contexts, such as smart satellites and drone-based surveillance and reconnaissance. Extending sensors with high performance embedded computing systems – such as Nvidia's TX2 – provides an opportunity to develop and apply techniques for adaptive sensing based on what the sensor is currently detecting (or believes it is sensing). For example, in multi- and hyperspectral imaging where objects may radiate in narrow frequency bands, filtering of input data to match the specific band containing the objects signal removes noise from the classifier input and improves classification accuracy. However, how does the sensor know which bandpass filter to apply? Furthermore, if the wrong filter is applied, this will almost certainly degrade classifier performance.

This project will investigate classification-based sensor tuning to propose an architecture and an algorithm for adaptive sensing based on sensed data and classifiers trained on this data. The project will be undertaken as part of the Cyber-Physical Systems Lab, within the Centre for IoT Ecosystems Research and Experimentation (CITECORE). This project will involve hands-on work and experience developing software and algorithms for embedded systems, and the student will have the opportunity to work on advanced hardware such as the TX2.

The learning outcomes from this project would directly underpin both further research studies (Masters or PhD), as well as prepare the student for working in emerging and growing industries, such as space technologies, defence technologies, precision agriculture, and the like.

Necessary Skills:

- Python or C++ programming skills essential (must be a competent programmer)
- Experience working with single-board computers (e.g., Raspberry Pi, ODroid C+) and linux operating system
- Basic knowledge of imaging technologies (such as RGB cameras)
- Experience with using libraries such as TensorFlow or CaffeNet a plus (but not essential)
- Demonstrated capacity for self-directed learning; willingness to learn and work in a collaborative research team

Visually Mediated Control in Robotics

Supervisor: A/Prof Tim Wilkin, tim.wilkin@deakin.edu.au

Campus: Melbourne Burwood

Start: January

Project Description:

For most humans' vision is our primary sense, and our world is structured and organised to permit visually mediated behaviour. Within robotics, vision is an extremely useful passive sensing technology, and many decades of research into computer vision and robotic vision has taken us to the point where vision is now a meaningful source of information for robots and their control systems. Of specific interest to the Supervisor is the problem of visually mediated flight control for drones (multirotor and small fixed wing aircraft).

This is not a single project proposal, but rather a call for students interested in computer vision and robotics to undertake a project in the space of visually mediated control in robotics. Some suggested projects are:

- Visually mediated landing behaviour for multirotor drones
- Visual pursuit and evasion in robotics (airborne or ground)
- Biological models for visually mediated control

Alternatively, the student may propose their own project related to robotic vision and negotiate the scope and objectives of this project with the Supervisor.

These projects will be undertaken as part of the Cyber-Physical Systems Lab, within the Centre for IoT Ecosystems Research and Experimentation (CITECORE). Students will have access to a range of specialised hardware, including drones, open source flight controllers, embedded computers, etc., should these be needed for the project. The learning outcomes from this project would directly underpin both further research studies (Masters or PhD), as well as prepare the student for working in emerging and growing industries, particularly those focused on developing or applying robotics technology.

Necessary Skills:

- Python or C++ programming skills essential (must be a competent programmer)
- Experience working with single-board computers (e.g., Raspberry Pi, ODroid C+) and linux operating system a plus
- Basic knowledge of robotics, and of imaging technologieS
- Demonstrated capacity for self-directed learning; willingness to learn and work in a collaborative research team

Backdooring Federated Learning and Mitigations

Supervisor: Dr Leo Zhang, leo.zhang@deakin.edu.au **Associate Supervisor**: Dr Xinguin Ma

Campus: Geelong Waurn Ponds

Start: January or July

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 backdooring. In particular, backdooring aims to control the model's behaviour on specific attacker-chosen inputs via implanting a backdoor to the model during training/fine-tuning.

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 backdooring 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 backdooring 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.

Necessary Skills:

- Familiar with Python, Good Math background, and preferably (but not required) know Machine Learning and Deep Learning

Designing a Trust Management Framework for the Internet of Things

Supervisor: Dr Anuroop Gaddam, anuroop.gaddam@deakin.edu.au **Associate Supervisor**: Dr Keshav Sood

Campus: Melbourne Burwood or Geelong Waurn Ponds

Start: January or July

Project Description:

The Internet of Things (IoT) consists of a huge number of entities like the users, various sensors other devices and applications connected through a communication infrastructure. In many scenarios (e.g. Industrial, agricultural and health monitoring) the IoT's are deployed in large-scale often communicating external entities or working together to collect, process the data from physical environments. As IoT is a dynamic system, there raises a new fundamental issue of knowing whether an individual IoT entity can securely communicate with another and if so, then to what extent. In the IoT, entities must interact with one another often in unknown and uncertain circumstances. Therefore, in such systems, it is important to include mechanisms that can help in such interactions by overcoming this uncertainty. There is a significant need to develop a trust model for the IoT, considering the highly dynamic nature and other distinct characteristics of such systems using Machine Learning (ML) techniques. Trust mechanisms allow entities to decide whether or not to interact with other entities. The student needs to research on the metrics and methods for establishing trust in dynamic IoT systems and develop a trust management framework that can improve access control mechanisms easing the decision-making process under uncertainty in large-scale IoT systems.

Necessary Skills:

- Machine Learning, IoT, Data Mining, R or Python

Design of a Multi-sensor IoT-enabled Device for Discrete and Outdoor Deployable Gait Monitoring

Supervisor: Dr Anuroop Gaddam, anuroop.gaddam@deakin.edu.au **Associate Supervisor**: Prof Maia Angelova

Campus: Melbourne Burwood / Geelong Waurn Ponds

Start: January or July

Project Description:

Walking is crucial to maintaining health and wellbeing in older age. A decline in community ambulation (walking for transport or recreation) is associated with loss of independence for community-dwelling older people and is a predictor of residential care admission and mortality. Key components of ambulation are gait speed, the ability to walk while performing concurrent cognitive and motor tasks and the ability to negotiate unpredictable terrain. The decline in mobility increases risks of frailty via reductions in strength, power and muscle mass with major negative implications on psychological health. As Gait is the sixth vital sign, it can be used to estimate the survival rate of the elderly and also can be used to predict some undiagnosed ailments. Unfortunately, gait is usually measured on a specially designed walk path, which has to be done at clinics or health institutes. Wearable tracking services using an accelerometer, or an inertial measurement unit can measure the gain for a certain time interval, but not all the time, due to the lack of a sustainable energy source, and inconvenience to the elderly user. Using image analysis to identify the Gait have many shortcomings like accuracy, the sensing errors caused by thermal noise and overlapping sensing regions. To tackle the shortcomings of the above discussed, this research develops an IoT framework and a prototype to measure gait using a newly developed innovative sensor. By developing an unobtrusive IoT system that can be embedded in outdoor landscapes to monitor individuals' gait and identify patterns of gait change. The sensorized landscape would be positioned in an area frequented by target users to improve data collection opportunities. To create a gait profile for the individual and estimate the individual's fall risk from the spatial-temporal data collected by the sensors, the research also needs to be focused on developing machine learning / AI techniques. This project involves collaborating with external multi-disciplinary research team in New Zealand.

Necessary Skills:

- Machine Learning, IoT, Data Mining, R or Python
- Desirable electronics and signal processing

Developing Anomaly Detection Models for Detecting Sensor Faults in Internet of Things

Supervisor: Dr Anuroop Gaddam, anuroop.gaddam@deakin.edu.au **Associate Supervisor**: Prof Maia Angelova

Campus: Melbourne Burwood / Geelong Waurn Ponds

Start: January or July

Project Description:

Over the past few years, the Internet of Things (IoT) has gained significant recognition to become a novel sensing paradigm to interact with the physical world. The sensors within the Internet of Things are indispensable parts and are the first port to capture the raw data. As the sensors within IoT are usually deployed in environments which are harsh, which inevitably make the sensors venerable to failure and malfunction. Beside sensor faults and malfunctions, the inherent environment where the sensors are usually installed could also make the sensor to fail prematurely. These conditions will make the sensors within the IoT to generate unusual and erroneous data, often known as outliers. Outliers' detection is very crucial in IoT to detect the high probability of erroneous reading or data corruption, thereby ensuring the quality of the data collected by sensors. Data anomalies, abnormal data or outliers are considered to be the sensor data streams that are significantly distinct from the normal behavioural data.

As the Internet of Things are very different from the Wireless sensor networks there is a huge necessity for developing adequate protocols and techniques to address unique challenges and constraints of IoT. The scope of project includes developing models to provide the highest accuracy in detecting sensor faults and outliers in IoT context.

Necessary Skills:

- Data Mining, R or Python

Context Provider/Service Annotation for Context-as-a-Service IoT Platform

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alireza Hassani

Campus: Melbourne Burwood

Start: January or July

Project Description:

During the last several years, we have witnessed a huge rise of the IoT market. More and more ordinary objects are converted into smart things and are connected to the internet. These smart connected objects are capable of providing real-time information about entities and their environment through internet-based services, which is refer to as Context Service. Internet of Things is set to dominate every aspect of our life and bring about transformation in nearly every industry (private and public). An important aspect of IoT is the data and, in particular, the ability to understand and contextualize such data in order to use it effectively. However, the metadata required to make sense of this data is mostly inaccurate, incomplete and, in many situations, only human interpretable. To address this challenge, it is required to classify, annotate and semantically enrich IoT data-streams/services. Context-as-a-Service (CoaaS) IoT platform has been developed under Prof A Zaslavsky leadership as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS.

The students will have to investigate, design, and implement an algorithm to accurately classify IoT data-streams/services and enrich the IoT data-stream/services with domain specific metadata extracted from domain ontologies and semantic sensors ontologies (SOSA). The student will build the prototype tool for PoC.

Necessary Skills:

- Distributed computing, Java, Python, software engineering and computer science literacy

Context Provider/Service Selection for Context-as-a-Service IoT Platform

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alireza Hassani

Campus: Melbourne Burwood

Start: January or July

Project Description:

During the last several years, we have witnessed a huge rise of the IoT market. More and more ordinary objects are converted into smart things and are connected to the internet. These smart connected objects are capable of providing real-time information about entities and their environment through internet-based services, which is refer to as Context Service. Internet of Things is set to dominate every aspect of our life and bring about transformation in nearly every industry (private and public). An important aspect of IoT is the data and, in particular, the ability to understand and contextualize such data in order to use it effectively. However, the metadata required to make sense of this data is mostly inaccurate, incomplete and, in many situations, only human interpretable. To address this challenge, it is required to classify, annotate and semantically enrich IoT data-streams/services. Context-as-a-Service (CoaaS) IoT platform has been developed under Prof A Zaslavsky leadership as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS.

The students will have to investigate, design, and implement an automatic approach to select the best possible context service among all the available & relevant services in a way that the total cost be minimised while the requirements of the requests are fully fulfilled. The student will build the prototype tool for PoC and integrate with CoaaS.

Necessary Skills:

Distributed computing, Java, Python, software engineering and computer science literacy

Context Service discovery, composition, and chaining for IoT platform CoaaS

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alireza Hassani

Campus: Melbourne Burwood

Start: January or July

Project Description:

During the last several years, we have witnessed a huge rise of the IoT market. More and more ordinary objects are converted into smart things and are connected to the internet. These smart connected objects are capable of providing real-time information about entities and their environment through internet-based services, which is refer to as Context Service. Internet of Things is set to dominate every aspect of our life and bring about transformation in nearly every industry (private and public). An important aspect of IoT is the data and, in particular, the ability to understand and contextualize such data in order to use it effectively. However, the metadata required to make sense of this data is mostly inaccurate, incomplete and, in many situations, only human interpretable. To address this challenge, it is required to classify, annotate and semantically enrich IoT data-streams/services. Context-as-a-Service (CoaaS) IoT platform has been developed under Prof A Zaslavsky leadership as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS.

The student will have to investigate, design, and implement an automatic approach to discover available context services based on incoming requests from users written in CDQL. An important aspect of Service discovery is service composition and chaining, which means sometimes it is required to combine several services in order to respond to an incoming request. The student will build the prototype tool for PoC and integrate with CoaaS.

Necessary Skills:

- Distributed computing, Java, Python, software engineering and computer science literacy

User-centric interface for smart context provider registration in Context-as-a-Service IoT platform

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alireza Hassani / Dr Alexey Medvedev

Campus: Melbourne Burwood

Start: January or July

Project Description:

Context-as-a-Service (CoaaS) has been developed under Prof A Zaslavsky as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS and it requires registration of context providers/consumers in the CoaaS platform.

The students will have to explore and analyse existing GUI tools for service registration, write a detailed critical literature review, followed by proposing, designing, implementing and demonstrating the prototype that will also be integrated with CoaaS IoT platform. Students would be asked to consider using open-source software. Considerations should be given to automatic discovery of relevant context providers and context-based automatic registration in CoaaS. The student will build the prototype tool for PoC and integrate with CoaaS.

Necessary Skills:

- Distributed computing, Java, Python, visualisation, software engineering and computer science literacy

CASE tool for developing SLAs between context providers and Context-as-a-Service IoT platform

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alexey Medvedev

Campus: Melbourne Burwood

Start: January or July

Project Description:

Context-as-a-Service (CoaaS) has been developed under Prof A Zaslavsky as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS and in many cases it requires a Service Level Agreement (SLA) between context providers/consumers and the CoaaS platform. The issues that need to be addressed include:

- Complex SLA definition. How to bill for complex queries?
- SLA representation. How to model SLAs?
- Create a visual tool for SLA development
- When the caching policy tells to use more or less resources, allocate/deallocate these resources in cloud and make sure that CoaaS uses the resources and meets the SLA requirements

The students will have to explore and analyse existing CASE tools for service level agreements (SLA), write a detailed critical literature review, followed by proposing, designing, implementing the algorithm and demonstrating the prototype that will also be integrated with CoaaS IoT platform. Students would be asked to consider using open-source software. The student will build the prototype tool for PoC and integrate with CoaaS.

Necessary Skills:

- Distributed computing, Java, Python, visualisation, software engineering and computer science literacy

Context-as-a-Service IoT platform performance dashboard

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alexey Medvedev

Campus: Melbourne Burwood

Start: January or July

Project Description:

Context-as-a-Service (CoaaS) has been developed under Prof A Zaslavsky as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries serving various IoT applications, which will enrich observed and sensed data to provide more accurate validated data for decision support. CoaaS prototype is running in the SIT research cloud. Context provisioning is a critical component of CoaaS and in many cases it requires a Service Level Agreement (SLA) between context providers/consumers and the CoaaS platform. The performance dashboard will have to address the following features:

- Measuring and visualising performance and resource consumption in CoaaS
- Resource planning
- Optimization hints
- Applying ML/deep learning to performance logs

The students will have to explore and analyse existing performance dashboards, write a detailed critical literature review, followed by proposing, designing, implementing the performance dashboard software component and demonstrating the prototype that will also be integrated with CoaaS IoT platform. Students would be asked to consider using open-source software.

Necessary Skills:

- Distributed computing, Java, Python, visualisation, software engineering and computer science literacy

Smart Context Definition Query Language Editor V2

Supervisor: Prof Arkady Zaslavsky, arkady.zaslavsky@deakin.edu.au **Associate Supervisor**: Dr Alireza Hassani

Campus: Melbourne Burwood

Start: January or July

Project Description:

Context-as-a-Service (CoaaS) has been developed under Prof A Zaslavsky as part of EU Horizon-2020 project bIoTope. It allows near real-time processing of incoming and historical context for serving multiple concurrent context queries written in CDQL – language developed as part of CoaaS. CDQL Editor V1 allows interactive formulation of context queries and IDE-like execution of these queries. We see the need for more complex and sophisticated context queries development and hence the project proposal which will address such issues as:

- Support of packages
- Support of cross-referencing
- Debugging
- Schema exploration
- Other functionality typical to query IDEs

The students will have to explore analyse and compare existing context query languages and IDEs and write a detailed critical literature review, followed by proposing, designing, implementing and demonstrating the prototype of CDQL V2. Smartness should be expressed as on-the-fly hints, predictive query formulation and user personalisation.

Necessary Skills:

- Distributed computing, Java, Python, visualisation, software engineering and computer science literacy

Goal Reasoning for Robotic Swarms

Supervisor: Dr Jan Carlo Barca, jan.barca@deakin.edu.au **Associate Supervisor**: Dr Kevin Lee

Campus: Melbourne Burwood

Start: January

Project Description:

At present robotic swarms must be told what goals to achieve and how goals can be decomposed into sub-goals. This constraint is limiting for swarms that perform missions in complex environments when it is not feasible to manually engineer/encode complete knowledge of what goal(s) should be pursued for every conceivable state. This is also a major drawback in situations where actions fail, new opportunities arise or events take place that strongly motivate changing the goals.

This exciting project will address the above issue by investigating how intelligent robotic swarms can reason about, formulate, select and manage their goals/objectives autonomously.

Algorithms will be developed using Gazebo, the preferred simulator in DARPAs virtual robotics challenge. Depending on time and progress, the work can be evaluated using the Crazyflie drone platform.

The selected student will be given an opportunity to publish his/her work internationally if the output is of high quality.

Necessary Skills:

- C++ programming skills are required

Herding Light Armoured Patrol Vehicles with a Swarm of UAVs

Supervisor: Dr Jan Carlo Barca, jan.barca@deakin.deu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

In this project the student will build on swarm robotics technology which has been developed in collaboration with Australian defence. The student will seek inspiration from biological shepherding dogs to herd a team of armoured patrol vehicles through an urban cityscape and into a capture location using a swarm of fixed wing UAVs.

All the work will be done in the SCRIMMAGE simulator (http://www.scrimmagesim.org/) and the project is likely to result in a high impact publication at an international conference given that a large portion of the work already has been completed.

A scholarship will be offered to the student who undertakes the project, if the student has a WAM of 80 or above.

Students who have a desire to progress into a PhD program are preferred.

Necessary Skills:

- C++

Advanced Decomposition Techniques for Multi-Component Optimisation Problems

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

Campus: Melbourne Burwood

Start: January or July

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.

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 approaches to measure the search performance itself. Finding such techniques is a part of this research.

Necessary Skills:

- Advanced programming skills in Java, C#, or C++ (Essential)
- Knowledge of combinatorial optimisation techniques, e.g. meta-heuristics (Desired)
- Knowledge of integer programming and experience with IBM ILOG CPLEX Optimisation Studio (Desired)

Studying the Efficacy of Discretization for Non-linear Models in Machine Learning

Supervisor: Dr Nayyar Zaidi, nayyar.zaidi@deakin.edu.au

Campus: Melbourne Burwood

Start: January

Project Description:

Feature handling is the key to training effective classification models. Data pre-processing techniques such as feature scaling, standardization, discretization, embeddings, etc. can dramatically impact the modelling results.

In earlier works, we showed the effectiveness of feature discretization on linear parametric models such as Logistic Regression, Support Vector Classifier. In this work, we study the effect of discretization on non-linear parametric models such as Deep Artificial Neural Networks and Generalized Linear Models. Our hypothesis is that discretization (either un-supervised equal frequency or supervised entropy-based) will result in improving the classification performance but also will result in faster convergence, leading to faster training times.

We will undertake a study on over 100 datasets from UCI repository in this project. The outcome of the study will be a detailed analysis of the models with or without discretization, in terms of bias, variance, training and classification time, speed of convergence, 0-1 loss and mean-square-error.

Necessary Skills:

- Machine Learning, Deep Learning, Tensorflow, Python, Linear Algebra, Probability

Adversarial attacks on medical machine learning

Supervisor: Dr Lei Pan, l.pan@deakin.edu.au **Associate Supervisors**: Dr Sutharshan Rajasegarar, Dr Daniel Ma, Dr Chandan Karmakar

Campus: Melbourne Burwood

Start: January or July

Project Description:

Medical practitioners and researchers are developing and even deploying many AI-driven systems to aid medical diagnosis, treatment, and even insurance claims. But adversarial attacks, as a new form of attacks against machine learning and deep learning models, become an emerging threat to the medical field. There are several papers with high impact, for example:

- Science Vol 363, Issue 6433, article Adversarial attacks on medical machine learning
- arXiv.org, article Understanding Adversarial Attacks on Deep Learning Based Medical Image Analysis Systems
- Nature Machine Intelligence Vol 2, article Secure, privacy-preserving and federated machine learning in medical imaging
- Nature Medicine Vol 26, article Deep learning models for electrocardiograms are susceptible to adversarial attack

In this project, students will evaluate the performance of adversarial attacks against medical machine learning systems. The attacks are made under different settings with respect to attackers' knowledge (zero knowledge, limited knowledge, or perfect knowledge), attackers' capability (poisoning attacks, or evasion attacks), and alike.

The thesis consists of three major parts: The first part of this project is to conduct a critical literature review on the currently published literature. Then the students are expected to implement the algorithms mentioned in some papers. The final part is the benchmark results of running these algorithms with respect to a few datasets.

Necessary Skills:

- Machine learning algorithms, python, scikit-learn

Quantifying Uncertainty in Machine Learning Predictions

Supervisor: Dr Nayyar Zaidi, nayyar.zaidi@deakin.edu.au

Campus: Melbourne Burwood

Start: January

Project Description:

Quantifying uncertainties in prediction of machine learning model is an area of active research. For example, if we predict, Hawks will win against Cats in tomorrow's game or patient has a cancer, etc. --- how certain or uncertain we are in our prediction. Several strategies are generally applied such as confidence intervals, prediction intervals, conformal prediction, deep learning based.

The aim of this project is to study these approaches systematically by first identifying the relevant techniques -- secondly, identifying the datasets – thirdly, identify the metrics that quantifies the effectiveness of the quantification, and finally, detailed experiments to understand the relative merit of each approach.

This initial study will lead to a much bigger study for developing new models or modifying existing one -- with much better ability to quantify their predictions.

Necessary Skills:

- Machine Learning, Deep Learning, Tensorflow, Python, Linear Algebra, Probability

Resource Management with Deep Reinforcement Learning

Supervisor: Dr Nayyar Zaidi, nayyar.zaidi@deakin.edu.au

Campus: Melbourne Burwood

Start: January

Project Description:

Resource management problems are ubiquitous in computer system's applications. For example, job scheduling in Operating System, machine placement in cloud, etc. Solutions to such problems are generally based on constrained optimization based algorithms. With the proliferation of machine learning, there is a wide interest in reinforcement learning for resource management problems.

In this project, we will investigate the effectiveness of deep reinforcement learning algorithm known as deepRM for resource management. The project involves converting the existing Theano code to Tensorflow, and then modifying the methodology to incorporate different set of constraints, which will make it more general, versatile and powerful.

The project will study competing constrained optimization algorithms, and will critically establish the effectiveness of deepRM and also modifications of deepRM as well.

Necessary Skills:

- Machine Learning, Deep Learning, Tensorflow, Python, Optimization, Linear Algebra, Probability

Applications of Adversarial Machine Learning in Medical AI

Supervisor: Dr Daniel Ma, daniel.ma@deakin.edu.au **Associate Supervisors**: Dr Lei Pan, Dr Sutharshan Rajasegarar, Dr Chandan Karmakar

Campus: Melbourne Burwood

Start: January or July

Project Description:

Medical practitioners and researchers are developing and even deploying many AI-driven systems to aid medical diagnosis, treatment, and even insurance claims. Medical AI studies medical images and signals to aid medical experts to make better decisions regarding diagnosis, screening and treatments. But adversarial attacks, as a new form of attacks against machine learning and deep learning models, have become an emerging threat to the medical field. In computer vision tasks such as image classification and object detection, adversarial attacks have been demonstrated can easily fool state-of-the-art deep learning models with tiny, human-imperceptible adversarial manipulations of the input data. In medical AI, adversarial attacks can cause severe consequences such as misdiagnosis of a disease, fake medical conditions and insurance fraud, undermining their reliability and trustworthiness.

In this project, student will investigate the vulnerability of current deep learning-based medical AI models and develop effective defence methods against adversarial attacks. Student will also learn the knowledge of adversarial machine learning, an emerging subfield of machine learning that aims to identify vulnerability and weakness of current machine learning models. Possible research directions, including, but not restricted to:

- Adversarial attack medical AI systems based on retinal images, skin images, chest-x-ray, CT scans and ECG time series.
- Develop effective defence methods against adversarial attacks based on robust optimization and adversarial machine learning techniques.
- The positive use of adversarial noise to protect private medical records from being exploited by unauthorized deep learning models.

Necessary Skills:

- Basic concepts of machine learning, deep learning and computer vision; familiar with deep learning frameworks like TensorFlow and PyTorch

Robot control using deep interactive reinforcement learning

Supervisor: Dr Francisco Cruz, francisco.cruz@deakin.edu.au **Associate Supervisor**: A/Prof Richard Dazeley

Campus: Geelong Waurn Ponds

Start: January or July

Project Description:

Intelligent robots have recently taken their first steps into domestic scenarios. It is thus expected that robots learn to perform tasks, which are often considered rather simple for humans. However, for a robot to reach human-like performance diverse subtasks need to be accomplished in order to satisfactorily complete a given task. These subtasks include perception, understanding of the environment, learning strategies, knowledge representation, awareness of its own state, and manipulation of the environment.

Reinforcement Learning (RL) [1] is a learning approach supported by behavioural psychology where an agent, e.g., a person or a robot, interacts with its environment trying to find an optimal policy to perform a particular task. In every time step, the agent performs an action reaching a new state and, sometimes, may obtain either a reward or a punishment. The agent tries to maximize the obtained reward by choosing the best action in a given state [2].

On the other hand, deep learning [3] is composed of many processing layers and has been successfully tested, among others, in image classification by representing different levels of abstraction [4]. Moreover, deep reinforcement learning [5] has combined the two aforementioned approaches to learning a motor policy mapping from a set of states to a set of actions. Deep reinforcement learning uses a neural network to learn the sum of direct rewards and expected future rewards for each action-state either in discrete or continuous domains [6].

In this project, the student will work with the deep reinforcement learning approach with interactive feedback applied to a domestic robot scenario. In this context, it is expected to develop a simulated human-robot scenario where the robot observes the environment states by using deep learning approaches and decide actions to perform by means of interactive reinforcement learning.

Necessary Skills:

- Good programming skills

1 R. S. Sutton and A. G. Barto. Reinforcement Learning: An Introduction. Cambridge, MA, USA: Bradford Book, 1998.
2 Francisco Cruz, Sven Magg, Yukie Nagai, and Stefan Wermter. Improving interactive reinforcement learning: What makes a good teacher? Connection Science, In Press, 2018.
3 Goodfellow, Y. Bengio, and A. Courville. Deep learning. Cambridge: MIT press, 2015.
4 Y. LeCun, Y. Bengio, and G. Hinton. Deep learning. Nature, Vol. 521, Nr. 7553, pp. 436-444, 2015.
5 V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller. Playing atari with deep reinforcement learning. arXiv preprint arXiv:1312.5602, 2013.
6 M. Kerzel, H. Beik-Mohammadi, M. A. Zamani, S. Wermter. Accelerating Deep Continuous Reinforcement Learning through Task Simplification. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), pp. 139-144, 2018.

Autonomous and Intelligent IoT Access Control Model using Deep Learning

Supervisor: Dr Keshav Sood, keshav.sood@deakin.edu.au **Associate Supervisors**: Dr Morshed Chowdhury, Dr Frank Jiang

Campus: Melbourne Burwood

Start: January or July

Project Description:

The Internet of Things (IoT) Access Control system allows an entity to securely access the network and resources and ensures the confidentiality of information by guiding the network to share information with authorized entities only. Doubtlessly, an exponential rise in the growth of IoT networks have been seen, almost in every sector. In IoT domain, companies are developing new technologies, protocols, etc., this make IoT networks extremely heterogeneous which will impact the decision making ability of autonomous and Intelligent IoT access control security systems. Eventually the access control models can be compromised. The conventional solutions to strengthen the access control model's abilities cannot be applicable in complex future heterogeneous scenarios (such as 5G and 6G). We observe that the heterogeneous IoT data streams analysis will promisingly help to address this issue. In this project we aim to design an autonomous-intelligent IoT access control architecture for next-generation heterogeneous networks for Australians.

In this early work, deep learning based approaches will be used to analyse complex heterogeneous IoT data streams. Following this analyses, a novel autonomous and intelligent IoT security architecture for the next generation heterogeneous networking will be proposed. Significantly, the framework will be capable to early alarm the risk of cyber-attacks in real-time, timely detection of anomaly connections, and will help to avoid any unplanned network maintenance. This will enable IoT network providers to offer more secure network services and efficiently prioritise their resources on higher value-adding services. Eventually this would also save significant operational and capital expenditure or costs.

Necessary Skills:

- Moderate to good understanding of network design
- Minimal understanding of cyber security issues
- Good knowledge of machine learning or Python language
- A willingness to learn new technical concepts in 5G

Distributed Goal Reasoning for the Dynamic Internet of Things (IoT)

Supervisor: Dr Kevin lee, kevin.lee@deakin.edu.au **Associate Supervisor**: Dr Jan Carlo Barca

Campus: Melbourne Burwood

Start: January or July

Project Description:

Internet of things (IoT) devices are being deployed in Increasingly large numbers, supporting applications such as smart transport, smart energy, logistics management and smart cities. They are also being heavy used in critical applications such as health monitoring and emergency management. With increasingly complex and dynamic application requirements, and therefore deployments, IoT devices and networks are increasingly having to make decisions about different priorities. Such priorities include, the need to conserve battery, demand to transfer data wirelessly, performing computation, maintaining a mesh network, and performing sensor and actuator actions.

This project will investigate the use of distributed goal reasoning to optimize the decisions made by individual IoT nodes and the network as a whole. The focus of the project will be the development and use of optimization algorithms, utility functions, heuristics and other techniques to support the goals of IoT applications.

Deep Learning Based Crop Identification in Precision Agriculture

Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au **Associate Supervisor**: Dr Mumtaz Ali

Campus: Melbourne Burwood

Start: January or July

Project Description:

The strategic management of farming requires crop field monitoring. Crop differentiation through remote sensing is a complicated and difficult task, particularly if different crops have identical spectral responses and patterns. In such scenarios, crop identification could be improved by combining object-based image analysis and advanced deep learning methods. In this project, novel deep learning models will be designed to combine in a hierarchical classification framework to map major crops utilizing images captured by satellites. Then these deep learning models will be built with different combinations of spectral and textural features obtained after the segmentation of the remote images in an object-based framework. Experiments will be carried out to demonstrate the effectiveness and advantages of the proposed deep learning models over the state-of-the-art schemes used for crop identification in precision agriculture.

Necessary Skills:

- Programming skill in Python; Basic knowledge in machine learning and deep learning

A data analytics-based crop yield prediction system using advance deep learning models

Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au **Associate Supervisor**: Dr Mumtaz Ali

Campus: Melbourne Burwood

Start: January or July

Project Description:

The deep learning methodologies are the leading tool in agricultural sector to provide support for farmers in examining crop yields under different climate conditions. In this project, the recurrent neural network (RNN) and convolutional neural network (CNN) will be utilized to predict crop yields based on the observed environmental conditions from the field, and to provide recommendations about the desired crops that can be grown in that field or not. The environmental factors such as humidity, temperature, rain, and moisture will be used as inputs into RNN and CNN models to identify the suitable crops by classifying them based on the climatic conditions. This project can provide yield prediction and efficient crop detection for farmers by providing a complete early monitoring system.

Necessary Skills:

- Programming skill in Python; Basic knowledge in machine learning and deep learning

Effective Federated Machine Learning Approach for Privacy-sensitive Application

Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au **Associate Supervisor**: Md. Palash Uddin

Campus: Melbourne Burwood

Start: January or July

Project Description:

Federated Learning (FL), introduced by Google in 2017, is a privacy-preserving machine learning paradigm that enables multiple local participants (devices) to train a common Deep Neural Network (DNN) in parallel using their own private datasets. The locally trained models are then aggregated (combined) through a central server to generate a new global model, which is subsequently sent back to the local participants for retraining. This process of training and aggregation is repeated until reaching the learning convergence. In this manner, individual participant's data privacy is preserved as the participants do not need to share their private data with each other, and even not with the server. Therefore, FL has a great potential to be deployed for many real-world privacy-sensitive machine learning applications, such as image recognition, sentiment analysis, clinical care activities, burglary analysis and user activity analysis.

This project aims to develop a new effective FL approach and evaluate its performance thoroughly. The Honours student may engage for:

- Literature review on different types of existing FL algorithms
- Implementation and performance evaluation of the potential existing FL algorithms
- Designing and developing a new effective FL algorithm (possibly based on the evaluated existing algorithms)
- Evaluating the performance of the proposed algorithm and comparing it with other state-of-the-art algorithms

Necessary Skills:

- Programming skill in Python; Basic knowledge in machine learning and deep learning

Blockchain Interoperability

Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au **Associate Supervisor**: Dr Dimaz Wijaya, Dr Longxiang Gao

Campus: Melbourne Burwood

Start: January or July

Project Description:

Information exchange or asset transfer is enabled between users within the same blockchain environment. However, with the wide array of blockchain products now available in the market, blockchain interoperability becomes an emerging issue. A user in one blockchain may want to exchange information with other users in other blockchains that have completely different sets of protocols; blockchain interoperability is necessary to execute the operation.

This project explores existing challenges in blockchain interoperability. Research in the project may focus on one or two of the following subjects:

- Blockchain-DBMS interoperability
- Public-to-public, private-to-public, and private-to-private blockchain interoperability
- Cross-chain communication, cross-chain protocols (notarisation, relay, atomic swaps)
- Blockchain interoperability protocol standards such as Interchain and Interledger
- Blockchain extensions (sidechains, child chains)
- Multi-blockchain systems (such as Polkadot, Cosmos, Kadena)
- Consensus methods in cross-chain protocols (such as Tendermint, Strong Federation)

Necessary Skills:

- Programming skill in Python or JavaScript; Basic knowledge in blockchain (Bitcoin, Ethereum)

Robust Digital Audio Watermarking Using Deep Learning

Supervisor: Prof Yong Xiang, yong.xiang@deakin.edu.au **Associate Supervisor**: Dr Tianrui Zong

Campus: Melbourne Burwood

Start: January or July

Project Description:

Digital watermarking is a promising technology to tackle copyright infringement. In audio watermarking, the copyright information, such as signatures, logos, and IDs, is embedded directly into the audio signals without degrading the quality of the signals. When the violation of copyright happens, the watermark can be extracted for copyright protection.

One challenging task for audio watermarking is to correctly extract the embedded imperceptible watermark from a manipulated audio signal. The manipulations of audio signals include noise addition, filtering, compression, re-sampling, re-quantization, cropping, jittering, amplitude scaling, time scaling, pitch scaling, and recapturing.

This project aims to design a watermarking embedding and detecting system using deep learning technology to achieve the robustness against the above-mentioned operations. The following goals should be achieved in this project:

- Build a dual-input deep learning model to embed the copyright information into the host audio signal to generate the watermarked audio signal
- Simulate attacks on the watermarked signal to generate the attacked audio signals for training
- Design a deep learning model to extract the copyright information from the attacked audio signals

Necessary Skills:

- Programming skill (Python preferred); Basic knowledge in machine learning and deep learning; Basic knowledge in audio signals

Investigation of physical activity patterns with data analytics and wearable devices

Supervisor: Dr Sutharshan Rajasegarar, sutharshan.rajasegarar@deakin.edu.au **Associate Supervisor**: Prof Maia Angelova

Campus: Melbourne Burwood

Start: January or July

Project Description:

Monitoring physical activities with wearable devices, such as wrist worn or body worn accelerometer devices, is increasingly popular and cost-effective way to study performance, training and well-being of athletes. The research challenge is to analyse sensor data, alone or in combination with other data, and to investigate for patterns of movement activities. Identification and classification of patterns of different movements is central to monitoring and analysing athlete's performance and athlete's fatigue.

The aim of this project is to investigate patterns of physical activities using GPS and accelerometry data. The project will study the associations between different time series signals/data measured with accelerometer from the human movements. Physical activities such as running, walking, jumping, specific movements of arms and legs, etc will be investigated using physical/physiological time series. Features will be extracted from the signals and modelled using tools and methods from data analytics and machine learning algorithms. The objectives of the project are to identify specific movements from the analysis of data and classify such movements.

Necessary Skills:

- Programming skills: ability to program in Python
- Machine learning learning knowledge

Anomaly detection with deep learning

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

Campus: Melbourne Burwood

Start: January or July

Project Description:

Detecting anomalous measurements from data is important for finding interesting events or security purposes. Deep learning methods can be used to model the normal patterns in the data and find the anomalies. The aim of the project includes, performing literature survey on existing anomaly detection methods that use deep learning techniques. Implementing and comparing some of the latest methods for detecting anomalies using publicly available data. Propose improvements to the existing methods and evaluate them.

Necessary Skills:

- Programming skills: ability to program in Python
- Machine learning knowledge

Deep learning based Non-intrusive load monitoring from smart meter data

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

Campus: Melbourne Burwood

Start: January or July

Project Description:

Energy consumption monitoring has been widely used in households due to widespread deployment of smart meters across the nations, including Australia. The process of identifying the individual devices and their usage patterns from the aggregated energy consumption data from smart meter is called the Non-intrusive load monitoring (NILM). The aim of the project include surveying the state-of the-art deep learning based NILM methodologies, and proposing novel deep learning based algorithms for accurately detecting the individual devices and anomalous energy usage patterns from the aggregated data.

Necessary Skills:

- Programming skills: ability to program in Python
- Machine learning knowledge

Detecting shapes from hand gestures using wearable devices and machine learning

Supervisor: Dr Sutharshan Rajasegarar, sutharshan.rajasegarar@deakin.edu.au **Associate Supervisor**: Dr Chandan Karmakar

Campus: Melbourne Burwood

Start: January or July

Project Description:

Wearable devices based on accelerometer sensors are becoming popular, and mostly used for detecting physical activities. Many of our daily gadgets e.g. smart phone also include this sensor. Recently, accelerometer sensors have been using for many applications, including medical condition diagnostic, etc. In this project we aim to use off-the-shelf accelerometer device to detect different shapes drawn by the user. The project involves a complete cycle of data analytic activities i.e., from data collection to train deep learning models and detecting the activities accurately from the data.

Necessary Skills:

- Programming knowledge, such as Python, R or Matlab
- Knowledge about Machine learning/deep learning algorithms

Animal Embodiment for Conservation using Virtual Reality

Supervisor: Dr Thuong Hoang, thuong.hoang@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

The disconnection between people and natural landscapes ('nature deficit disorder') is well-documented and of concern to educationalists and to governments given its impact on mental health and well-being, especially with the increasing rate of urbanisation. This second stage investigates, design, and evaluate the impact of augmented and virtual reality experiences on promoting individual and community behavioural changes for biodiversity/nature conservation as well as increasing wellbeing through connection with nature. The focus of this stage is to investigate the extent of emotional connection enabled by mixed reality technology via embodiment of endangered animals. The innovative approach of the project creates virtual reality experiences that immerses the users in a virtual natural landscape, not as human, but embodied as one of the endangered Corroboree Frog or Orange-bellied Parrot. This approach creates a powerful connection with nature by seeing through the eyes of an endangered species, which is not possible using other medium or technologies.

Necessary Skills:

- Experience with virtual or augmented reality development

Avatar Decoder Pipeline for Multiple Simultaneous Avatar Appearances based on Trusted Relationships

Supervisor: Dr Thuong Hoang, thuong.hoang@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

Avatars are virtual representations of users in the virtual world. Prior work has demonstrated the importance of visual representation towards user's identity, privacy, and interactions with others, in terms of self-confidence, trust and privacy.

This project explores a novel technique for avatar mesh decoder, to enable simultaneous multiple virtual representations of the same user to individual online participants, based on an established trust relationship. The focus area is a new concept in terms of identity, authentication, and privacy relating to VR devices and technologies, as well as a novel perspective on societal consideration of multiple identities and virtual representation of our avatars in virtual worlds.

Necessary Skills

- Experience with virtual or augmented reality development

Device-centric Smart Neuralmorphic Computing

Supervisor: Dr Frank Jiang, frank.Jiang@deakin.edu.au **Associate Supervisor**: Prof Robin Doss

Campus: Melbourne Burwood

Start: January or July

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 heterogenous 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 Neuralmorphic computing algorithms, Spiking Neural Network (SNN) and new protocols will be further developed, validated for smart anomaly detection/diagnosis in low-powered IoT devices.

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 Neuralmorphic 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

Necessary Skills:

- Moderate to good understanding of network design
- Minimal understanding of cyber security issues
- Good knowledge of machine learning or Python language
- A willingness to learn new technical concepts in 5G

Blockchain-Based Authentication and Privacy Preserved Learning Scheme for Autonomous Vehicular Fog Infrastructure

Supervisors: Prof Robin Doss, robin.doss@deakin.edu.au and Dr Frank Jiang, frank.jiang@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

Interconnected vehicles are one of the key nodes in the fog infrastructure as the extension of cloud computing. It is a distributed computing infrastructure oriented and can extend computing power and data analytics to the "edge" of the network. It enables customers to analyse and manage data locally, thus obtaining instant insights through links. Fog computing has certain mobility integrating network, computing, storage and application core competencies on the edge side of the network near the object or data source. We aim to establish an edge fog computing infrastructure to provide a real-time and safe computing platform with the blockchain as the core technique to interconnect the vehicle network.

To achieve the secured interconnected vehicular edge system, this project proposes an advanced blockchain-based authentication scheme for autonomous vehicular within the fog infrastructure. As an emerging technology that attracts extensive attentions in both industries and academia recently, the blockchain technology suits a decentralized application environment that possesses the characteristic of the distributed consensus.

The expected outcome of this research includes:

- A new classification method for connected users and information in vehicle network meets the needs of blockchain analysis
- An intelligent system for discovering connected vehicles and information based on block chaining technology
- An algorithm for information chain authentication and reconstruction based on blockchain technology

Research Activities:

- Be part of the SPYRIT IoT team, fortnightly project meetings closely, development of new blockchain-based Scheme for VANETs authentication with privacy-preservation considerations
- Literature review on Blockchain and malware detections and privacy preservation techniques
- Launch attacks: Use of Veins Simulation Platform with attacks, such as Miral attacks, Man-in-the-middle attacks, etc
- Explore the learning schemes, such as Federated Learning scheme

Preferred Knowledge/Skills (at least 2 of them):

- Computer Networks and Cyber Security
- VANET Simulators

Necessary Skills:

- Moderate to good understanding of network design
- Minimal understanding of cyber security issues
- Good knowledge of machine learning or Python language
- A willingness to learn new technical concepts in Security/Privacy

Opening the Secret of Deep Learning

Supervisor: Dr Daniel Ma, daniel.ma@deakin.edu.au **Associate Supervisor**: Dr Leo Zhang

Campus: Melbourne Burwood

Start: January or July

Project Description:

Deep learning models, deep neural networks (DNNs) in particular, have been the main driving force of the great success of modern artificial intelligence. In parallel to their superior representation learning capabilities, DNNs have been found also extremely vulnerable to small adversarial manipulations. In the case of images, tiny, human-invisible perturbations can easily fool state-of-the-art DNNs into making incorrect predictions. These perturbed examples are known as adversarial examples (or attacks). This phenomenon has been widely observed in many computer vision and natural language processing applications. Although many works have been proposed to create new attacks, or defence methods, it is still unclear why such a family of powerful models are so sensitive to small noise.

In this project, student will start from simple networks and image classification tasks to uncover this dark channel of DNNs and provide deeper understanding of deep learning. This project aims to answer the following questions:

- Why small perturbation is important in DNNs. In other words, why DNNs cannot ignore small noise like humans?
- Is it possible to design a dataset that one can learn robust DNNs from it? Or is it possible to design a dataset where DNNs can learn nothing useful from it but vulnerability?
- Where does this vulnerability of DNNs come from: model, data or training process?
- Is this vulnerability of DNNs a natural consequence of its superb performance?
- How can we use this vulnerability to protect your selfies and social medical data from being exploited by unauthorized deep learning models?

Necessary Skills:

- Basic concepts of machine learning, deep learning and computer vision
- Familiar with deep learning frameworks like TensorFlow and PyTorch

Analysis of Eye Fixation Data

Supervisor: Dr Atul Sajjanhar, atuls@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

The project is jointly supervised with Defence Science and Technology Group (DSTG).

Human operators can experience significant fluctuations in cognitive workload (CW) while performing cognitive tasks. Generally, high CW is considered to impact negatively on task performance. On the other hand, low CW can cause lapses of attention and poorer subsequent recall from long-term memory. The ultimate aim of the project is to monitor the CW and improve the efficacy of task performance by managing fluctuations in CW.

Measurement of CW is a significant challenge because it is subjective in nature. Physiological measures have been adopted by researchers for predicting CW. In this project, we propose to use eye-fixation data for non-intrusive computation of CW.

The project will develop insights into the relationship between eye-fixation and CW. We will define potential metrics to compute CW from eye-fixation data. Temporal visualisation will be used to display CW and highlight anomalous patterns in CW.

Necessary Skills:

- Programming skills are required

Deep Learning for Insider Threat Detection

Supervisor: Dr Atul Sajjanhar, atuls@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

The aim of the research is to improve the detection of insider threats. Malicious users can potentially exploit such threats leading to cybersecurity breaches. Detecting insider threats is particularly challenging because it is originated by insiders who have privileged access. Further, the ability to detect new threats is non-trivial.

Insider threat detection will be implemented using deep learning. Recently, deep learning has been used to identify correlated features from a large set of candidate features and has shown great potential for insider threat detection.

The end-product of the research will be a framework for the detection of insider threats. The proposed framework is motivated by deep learning because it has a proven ability to detect abnormal behaviour of the user more intelligently than traditional approaches for unsupervised learning.

Necessary Skills:

- Programming skills are required
- Knowledge of Python is preferred

Analysis of blockchain-based anomaly detection algorithms

Supervisor: Dr Lei Pan, l.pan@deakin.edu.au **Associate Supervisor**: Dr Sutharshan Rajasegarar

Campus: Melbourne Burwood

Start: January or July

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 more and more popular in blockchain-based systems. For example, there are research papers recently published on anomaly detection conducted on blockchain systems, such as the following papers:

- Prado-Romero, M.A., Doerr, C. and Gago-Alonso, A., 2017, November. Discovering bitcoin mixing using anomaly detection. In Iberoamerican Congress on Pattern Recognition (pp. 534-541). Springer, Cham
- Signorini, M., Pontecorvi, M., Kanoun, W. and Di Pietro, R., 2018. BAD: Blockchain anomaly detection. arXiv preprint arXiv:1807.03833
- Chen, T., Zhu, Y., Li, Z., Chen, J., Li, X., Luo, X., Lin, X. and Zhange, X., 2018, April. Understanding ethereum via graph analysis. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications (pp. 1484-1492). IEEE
- Chen, T., Li, Z., Zhu, Y., Chen, J., Luo, X., Lui, J.C.S., Lin, X. and Zhang, X., 2020. Understanding Ethereum via Graph Analysis. ACM Transactions on Internet Technology (TOIT), 20(2), pp.1-32

The project consists of three major parts:

The first part of this project is to conduct a critical literature review on the currently published literature. Then the students are expected to implement the algorithms mentioned in some papers. The final part is the benchmark results of running these algorithms with respect to standardized datasets, and propose improved algorithms.

Necessary Skills:

- Machine learning (python + scikit-learn preferred)

Avoiding Geographic Regions in Tor

Supervisor: Dr Frank Jiang, frank.Jiang@deakin.edu.au **Associate Supervisor**: Dr Morshed Chowdhury

Campus: Melbourne Burwood

Start: January or July

Project Description:

Traffic-analysis attacks are a persisting threat for Tor users. When censors or law enforcement agencies try to identify users, they conduct traffic-confirmation attacks and monitor encrypted transmissions to extract metadata—in combination with routing attacks, these attacks become sufficiently powerful to de-anonymize users. While traffic-analysis attacks are hard to detect and expensive to counter in practice, geographical avoidance provides an option to reject circuits that might be routed through an untrusted area. Unfortunately, recently proposed solutions introduce severe security issues by imprudent design decisions.

In this research, we approach geographical avoidance starting from a thorough assessment of its challenges. These challenges serve as the foundation for the design of an empirical avoidance concept that considers actual transmission characteristics for justified decisions. Furthermore, we address the problems of untrusted or intransparent ground truth information that hinder a reliable assessment of circuits. Taking these features into account, we conduct an empirical simulation study and compare the performance of our novel avoidance concept with existing approaches. Our results show that we outperform existing systems by 22% fewer rejected circuits, which reduces the collateral damage of overly restrictive avoidance decisions. In a second evaluation step, we extend our initial system concept and implement the prototype TrilateraTor.

Expectations: Producing a platform as the prototype which satisfies the requirements of a practical deployment, maintaining Tor's original level of security, provides reasonable performance, and overcomes the fundamental security flaws of existing systems. Students will work on the experiments and produce publishable results/research outcome.

Preferred Knowledge/Skills (at least 1 of them):

- Computer Networks and Cyber Security
- Probability theory

This work will be based on the former work we have done in 2019 as the fundamental basis.

Necessary Skills:

- Moderate to good understanding of network design
- Minimal understanding of cyber security issues
- Good knowledge of machine learning or Python language
- A willingness to learn new technical concepts in Security/Privacy

Software Dependency Graphs: Does Success Breed Success?

Supervisor: Dr habil. Marek Gagolewski, m.gagolewski@deakin.edu.au **Associate Supervisor**: Dr Grzegorz Siudem (Warsaw University of Technology)

Campus: Melbourne Burwood

Start: January or July

Project Description:

It is claimed that the distribution of the node degrees in many real-world graphs, e.g., social networks, follows a power law; it approximately holds that the fraction of vertices of degree k is equal to k-ß, 2<ß<3. We call such graphs scale-free. The universality of this property, however, has been recently called into question. The envisaged research project will study the characteristics of networks of Python and R packages and the dependencies between them. Various agent-based models describing the evolution of PyPI and CRAN repositories will be formulated and tested.

References:

- Holme P., Rare and everywhere: Perspectives on scale-free networks, Nature Communications 10, 2019, no. 1016
- Broido A.D., Clauset A., Scale-free networks are rare, Nature Communications 10, 2019, no. 1017
- Siudem G., Żogała-Siudem B., Cena A., Gagolewski M., Three dimensions of scientific impact, Proceedings of the National Academy of Sciences of the United States of America (PNAS) 117(25), 2020, pp. 13896-13900. doi:10.1073/pnas.2001064117
- Żogała-Siudem B., Siudem G., Cena A., Gagolewski M., Agent-based model for the h-index – Exact solution, European Physical Journal B 89:21, 2016. doi:10.1140/epjb/e2015-60757-1

Necessary Skills:

Very good working knowledge of and skills related to:

- probability and statistics
- graph theory
- programming in (Python or R) and (C, C++ or Java)
- algorithms and data structures

Network traffic analysis with deep learning

Supervisor: Dr Lei Pan, l.pan@deakin.edu.au **Associate Supervisor**: Dr Sutharshan Rajasegarar

Campus: Melbourne Burwood

Start: January or July

Project Description:

Industry control systems (ICSs) are the important for our daily lives because they control critical infrastructure like power grid, water treatment, gas pipes. However, security attacks like false data injection, reply attacks, and DoS attacks greatly endanger the safety and security of ICSs. Contemporary approaches employ machine learning and deep learning algorithms to detect these attacks at the next work level. For example, the link below contains a few datasets and several research papers:

- Industrial Control System (ICS) Cyber Attack Datasets

The project consists of three major parts:

The first part of this project is to conduct a critical literature review on the currently published literature. Then the students are expected to implement the algorithms in the reviewed papers. The final part is the benchmark results of running these algorithms with respect to one or two datasets, and propose improved algorithms.

Necessary Skills:

- Data mining algorithms with machine-learning project experiences (Python + scikit-learn preferred)

Deep learning based Learning Data Analysis in Online Education

Supervisor: A/Prof Jianxin Li, jianxin.li@deakin.edu.au **Associate Supervisor**: Xiangyu Song, PhD student

Campus: Melbourne Burwood

Start: January or July

Project Description:

With the rapid development of the Internet era, online education and its related technologies are being increasingly accepted and used by more and more educational institutions. How to make the best use of the advantages brought about by online education is being widely discussed.

This project is dedicated to using deep learning techniques to mine students' implicit learning patterns through the students' learning activities recorded online and explore the correlations between them and students' academic performance.

We will build some state-of-the-art neural network based models, such as GCNs based, to solve some challenging real-world problems in relevant scenarios, such as student performance prediction and automatic exam paper generation.

The proposed model will be implemented using the major Python frameworks, Pytorch or TensorFlow. The specific experiments will include reproducing the relevant baseline models and implementing the proposed model framework as well as optimizing it to achieve the desired results.

Necessary Skills:

- Must be familiar to Python
- Has completed at least one deep learning unit and can program the classic deep learning models

Carbon Tenements: Tokenisation of Carbon Credits

Supervisor: Prof Peter Eklund, peter.eklund@deakin.edu.au **Associate Supervisor/'Client'**: Mr Jesse Mcmeikan

Campus: Melbourne Burwood

Start: January or July

Project Description:

This project explores the idea of tokenisation of carbon credits using blockchain technology. The idea is to create a marketplace and ecosystem for the exchange of tokens between carbon tenement holders and greenhouse gas producers. Landholders of high-density carbon sinks (e.g. forests and mangroves) represent reserves of carbon offsets of significant value to the well-being of the global climate. The idea is to reward their conservation through effective land management by establishing a tokenomic model that utilises new advances in decentralised finance to tokenise the value of carbon sequestration as a new financial derivative. The positive network effect will be to financially incentivise all participants in the network, conserving valuable natural carbon sinks (our best asset to restoring balance to our biosphere), and speeding up the transition towards a green economy.

Necessary Skills:

- Interest in Blockchain and programming Smartcontracts

Support for children diagnosed with Amblyopia

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

Associate Supervisors: Dr Amanda Douglass (Optometry), Dr Geoff Sampson (Optometry), Dr Alexia Maddox (SCCA), Dr Lienors Torre (SCCA), Dr Rose Woodcock (SCCA)

Campus: Melbourne Burwood

Start: January or July

Project Description:

Amblyopia ('lazy eye') is a developmental eye condition which reduces vision in one eye. Traditional treatment involves patching or using eye drops to penalise the preferred eye to encourage strengthening of vision in the amblyopic eye. However, these current treatments have poor compliance with children as they temporarily reduce their ability to undertake normal tasks.

The condition is well understood from a clinical perspective, with visual improvement best in younger years when neural plasticity is greatest (8 years and younger). Novel treatments, including VR games, are beginning to be developed to address the compliance issue. However, very little is known about amblyopia as a day to day experience. Moreover, there is no qualitative data to explore how these treatments are experienced by children and their families.

Several ongoing research projects are assessing the effectivity of technology based amblyopia diagnostic tools, treatments and data collection mechanisms. This project will integrate with one of these, involving the development of virtual reality, augmented reality, game based or creative technology solutions, participating in deploying and collecting data using these, and in assessing their effectivity.

Necessary Skills:

- A background in game design and development, virtual and augmented reality, or creative technology product prototype would be an asset to this project.

3D Point Cloud Processing

Supervisor: Dr Xuequan Lu, xuequan.lu@deakin.edu.au **Associate Supervisor**: Dr Shang Gao

Campus: Geelong Waurn Ponds

Start: January

Project Description:

The computing of visual data like 3D point clouds has received remarkable attention nowadays. Recent smart techniques such as autonomous driving and robot navigation primarily rely on point cloud data. For instance, recognizing different objects is very critical for autonomous driving, and it can be achieved via point cloud segmentation (a task in point cloud processing).

With advanced visual capture devices, it is easy to capture millions of points (or more) for a single point cloud. How to efficiently handle such large amount of points is also a challenge. In this Honours project, students are expected to focus on a few typical tasks on point cloud processing, proposing or designing feasible techniques (algorithms) to address the involved tasks. The research work can be submitted to prestigious conferences or journals.

Necessary Skills:

- Programming languages (at least one, e.g. Python, C++, C#, etc)

Machine Learning for Energy Consumption Patterns and Behavior Analysis for End-users

Supervisor: Dr Adnan Anwar, adnan.anwar@deakin.edu.au **Associate Supervisor**: Dr Sutharshan Rajasegarar

Campus: Melbourne Burwood or Geelong Waurn Ponds

Start: January or July

Project Description:

Analysis of (electrical) energy consumption and supply are important for effective monitoring and management of the network assets. Customer profiling can help to perform this in an efficient and reliable way. Advanced machine learning is a key tool to identify customers' profiles which have similar energy consumption patterns, based on time series data. The aim of the project includes, performing literature survey on existing time series analysis methods used for energy analysis and customer profiling. Analysis of existing work on forecasting customer consumption using clustering, machine learning/deep learning methods. Implementing and comparing some of the existing methods using the publicly available datasets. Propose improvements to the existing methods. Possible use of customer profiles to investigate anomalies or misbehaviours based on the model.

This project will help the students to enhance their skills and experience in the area of machine learning and artificial intelligence. Outputs from this project will help to understand some industry practices on customer behaviour analysis. Students will also develop hands-on experience in advanced machine learning models and implementations.

Necessary Skills:

- Python (or similar) coding at least basic level (and interest to learn more), analytical mindset, passion in machine learning

Next Generation AI for Adverserial Networks

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

Campus: Melbourne Burwood or Geelong Waurn Ponds

Start: January or July

Project Description:

In the age of Internet-of-thing, the enormous amount of data attracts cyber attacker to launch various types of cross-site scripting, ransomware, SQL injections, email spoofing, audit-train-falsification not only through the traditional internet, but also based on weak security measures of the smart devices and IoT protocols. The amount of data and the velocity has made it challenging for the traditional security systems to detect an attack and cyber threat efficiently and accurately. Advanced Machine Learning (ML) based models and techniques can be a viable solution to mitigate security threats. ML algorithms can update the models in real-time as per the requirements; mine and process big data efficiently and effectively; and detect attack with veracity. Lightweight property is another key aspect. On top of that, a machine learning model itself could be vulnerable by new types of adversarial attacks. This domain is known as adversarial machine learning (AML). This project has two phases: i. Develop a lightweight but accurate ML model for cyber-threat detection, ii. Protect the model against adversarial attacks.

This project will help the students to enhance their skills and experience in the area of machine learning and artificial intelligence. Outputs from this project will help to understand some industry practices on cyber threat analysis. Students will also develop hands-on experience in advanced machine learning models and implementations.

Curious to know what AML is?

Necessary Skills:

- Python (or similar) coding at least basic level (and interest to learn more), analytical mindset, passion in machine learning

Co-simulator for Modeling Cyber-Physical Systems

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

Campus: Melbourne Burwood or Geelong Waurn Ponds

Start: January or July

Project Description:

The Smart Grid system is one of the key infrastructures to sustain our future society. It is a complex system that comprises two independent parts: PHYSICAL power grids and communication networks based CYBER layer. To understand the impact of a cyber-physical smart grid, it is important to develop a simulator that captures both cyber and physical phenomena. In this project, the aim is to develop a smart grid Co-simulation Framework.

The role of the student will be to focus on the integration of the network simulator with energy system simulator. Supervisor's previous work will be a starting point. The project has main aims from where students can choose one (or both) based on their experience and interest.

- Aim1: Backend modelling of the co-simulators and improve the simulator performances and usages
- Aim2: Display the simulation in a GUI based front-end.

The project will help students to build a good understanding of two emerging areas – energy system and communication system. It will enhance their skills on programming and analytics.

Necessary Skills:

- Programming skills in Java, C++, pythor or others.
- Passionate to do programming.

Reinforcement Learning for Walking Control of a Quadruped Robot in variable terrain

Supervisor: A/Prof Tim Wilkin, tim.wilkin@deakin.edu.au **Associate Supervisor**: Dr Alexey Medvedev

Campus: Melbourne Burwood

Start: January

Project Description:

In this project, a student will be working with a prototype of a robotic dog and the virtual model of a quadruped robot. The aim is to investigate the capability and limitations of reinforcement learning and, potentially, other ML techniques to teach the robot how to behave in complex situations, such as walking over inclined terrain, slippery terrain, walking using only three legs, recovering after falling and other possible situations. The obtained models will be transferred into the software of a robot dog prototype.

The project will be undertaken as part of the Cyber-Physical Systems Lab, within the Centre for IoT Ecosystems Research and Experimentation (CITECORE). This project will involve hands-on work and experience developing software and algorithms for embedded systems, and the student will have the opportunity to work on hardware such as the robotic dog above.

The learning outcomes from this project would directly underpin both further research studies (Masters or PhD), as well as prepare the student for working in emerging and growing industries, such as space technologies, defence technologies, precision agriculture, and the like.

Necessary Skills:

- ML, reinforcement learning
- C for Arduino programming skills; Python for ROS applications
- Experience working with single-board computers and Linux operating system
- Basic knowledge of robotic simulation and modelling (Gazebo, Open AI gym, 3D modelling software, etc)
- Demonstrated capacity for self-directed learning; willingness to learn and work in a collaborative research team

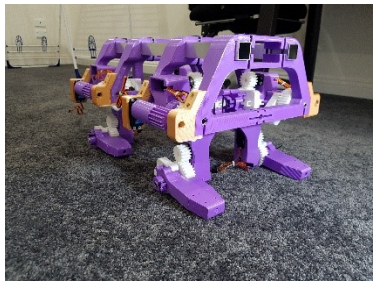
Develop a framework for software-in-the-loop and hardware-in-the-loop simulation and evaluation of controllers for a robotic dog

Supervisor: A/Prof Tim Wilkin, tim.wilkin@deakin.edu.au **Associate Supervisor**: Dr Alexey Medvedev

Campus: Melbourne Burwood

Start: January

Project Description:



In this project, a student will be working with a prototype of a robotic dog. To enable complex movements, it is essential to create a virtual model of the dog for using this model in simulations. The model should consider the weight of components, speed and torque of the servomotors, limits of joints, and other possible parameters.

The student will need to research and develop motor controllers for the robot, to enable basic behaviours such as walking, and evaluate these in the simulation. The obtained results can be transferred into the embedded software of the robot.

The project will be undertaken as part of the Cyber-Physical Systems Lab, within the Centre for IoT Ecosystems Research and Experimentation (CITECORE). This project will involve hands-on work and experience developing software and algorithms for embedded systems, and the student will have the opportunity to work on hardware such as the robotic dog above.

The learning outcomes from this project would directly underpin both further research studies (Masters or PhD), as well as prepare the student for working in emerging and growing industries, such as space technologies, defence technologies, precision agriculture, and the like.

Necessary Skills:

- C for Arduino programming skills; Python for ROS applications
- Experience working with single-board computers and Linux operating system
- Basic knowledge of robotic simulation and modelling (Gazebo, 3D modelling software, etc)
- Demonstrated capacity for self-directed learning; willingness to learn and work in a collaborative research team

Access Control for Internet of Things (IoT) through Zero Trust

Supervisors: Dr Arash Shaghaghi, a.shaghaghi@deakin.edu.au and Dr Adnan Anwar, adnan.anwar@deakin.edu.au

Campus: Melbourne Burwood or Geelong Waurn Ponds

Start: January or July

Project Description:

Traditional perimeter-based security architectures do not have sufficient design traits to foster security for critical infrastructures such as smart girds, industrial IoT (IIoT) and other cyber physical systems (CPS). In view of this, Zero Trust Architecture (ZTA), which is based upon the notion of least privilege is widely seen as an appropriate alternative. As referred to in the National Institute of Standards and Technology (NIST) report on ZTA, authentication and access control are two key tenets of ZTA for all CPS infrastructures.

Zero Trust necessitates a fine-grained and context-aware access control. The literature suggests that these access control requirements can be accomplished by attributes-based and usage-control access control. However, different IoT-enabled environments such as smart homes, smart grids, healthcare IoT, and smart buildings have entirely different access control requirements, requiring different arrangements of access control components. Most of the current frameworks for the aforementioned scenarios do not identify the appropriate requirements required by the corresponding scenarios, thereby leading to inadequate access control instantiations.

The proposed project extends a recent project funded by the Australian Department of Defence (DoD). The student will work with the wider project team including Dr. Zubair Baig and Prof. Robin Doss to design and implement an innovative access control system in the context of IoT ZTA. The student will be a member of SPYRIT Lab at the Centre for Cyber Security Research and Innovation (CSRI) of Deakin University during the time of the project.

Note: Australian Citizens or International students from NATO and Five Eye Countries may be eligible for a generous honours scholarship by The Cyber Security Cooperative Research Centre (CSCRC) when working on this project. However, this will be dependent on a separate successful application to CSCRC once a suitable candidate is identified.

Eligibility Criteria: WAM: Distinction, excellent grades in cybersecurity units including cryptography and network security

Further reading: NIST Computer Security Resource Centre, article Zero Trust Architecture

Necessary Skills:

- Good Programming background (Python or Java)

A Novel Multipath Data Scheduling for Future IoT Systems

Supervisor: Dr Shiva Pokhrel, shiva.pokhrel@deakin.edu.au

Campus: Melbourne Burwood

Start: January or July

Project Description:

With the growing presence of the Internet of Things and Cyber Physical Systems in industry, the use of WiGig or 5G for Industrial IoT (IIoT) is already evident. Automation with data exchange within and among manufacturing plants is undergoing a tremendous change along with IIoT, which is made possible by the gradual convergence of information technology (IT) with operational technology (OT). Such a convergence can be potentially benefitted by jointly using recent advances in communication technologies, e.g., coexisting WiGig and 5G. In this project, we first analyze the existing technical challenges for the coexistence of WiGig and 5G for IT/OT convergence, then develop and evaluate a robust multipath protocol (drawing on WiGig and 5G seamlessly) to create ultrareliable and smooth connectivity. The project will provide a dynamic architecture for the future industrial communications, connecting industrial robots timely, analyzing data precisely and delivering real-time insights reliably.

Industries may benefit greatly from adopting next-generation communication technologies for industry 4.0. The proposed project can help maximize industry' existing communication network's utility and has significant impact on how efficiently industry 4.0 landscape will be utilized by them. It will enable manufacturing plants to improve production efficiency and quality, leading to substantial cost savings and high degree of customer satisfaction.

Necessary Skills:

- Programming Python, Matlab, Distributed Machine Learning