Internet of Things Research and Teaching: Vision and Mission

Annual Report (2020)

Charith Perera (MBA, PhD)

Introducing the Internet of Things Garage

We ❤ building connected things that work...also secure, safer, and sustainable

Most of our research is ***build-driven*** and somewhat ***experimental*** and mostly ***applied***. This means that we build things, systems, and techniques and evaluate them in real-world settings. We aim to demonstrate how they work but less focus on giving theoretical guarantees. In our work, the objective is to produce artefacts (software system, things) that are useful in the real world. Therefore, we felt that the name ***'IoT Garage'*** is more appropriate and describes our work well than the more traditional or common name ***'IoT Laboratory'***. We are not alone, see.

History: Established in December 2018 (within School of Computer Science and Informatics, Cardiff University).

Principal Investigator: Charith Perera

Research Associates:

Matthew Nunes
Integrity Checking at the Edge [PETRAS Catalyst Fund]

PhD Students: As of December 2020, the research group comprises of ten PhD students and one MPhil student (and two affiliated PhD students).

Nada Alhirabi
Designing Privacy by Design IoT Applications [Since OCT 2018]

Areej Alabbas*
Secure Service Placement for IoT [Since JAN 2019]

Atheer Jeraisy
Reusable Privacy Components for IoT [Since APR 2019]

Asma Irfan (PT)
Adapting to Discomfort Towards Sustainable Built Environments [Since JAN 2020]

Naeima Hamed
Semantic Data Integration For Forest Observatory [Since JAN 2020]

Reem Aldhafiri
Cyber-Physical Privacy for Ageing & Learning Disabilities [Since OCT 2020]

Mark Butterworth (PT)
Low Power IoT Infrastructure for Harsh Environments [Since OCT 2020]

Lamya Alkhariji
Knowledge-Driven Privacy by Design for IoT [Since DEC 2018]

Emad Aliwa*
In-Vehicle Edge Security [Since APR 2019]

Bayan Almuhander
Privacy-Aware Smart Home Data Management [Since OCT 2019]

Hakan Kayan
Context-Aware Security for Cyber-Physical Systems [Since JAN 2020]

Yasar Majib
Context-Aware Security for Smart Homes [Since OCT 2020]

Dominic Fonseca
Edge Analytics for Sanitary Facility Monitoring [Since OCT 2020]

* Affiliate PhD students: Omer Rana is the primary supervisor for Areej Alabbas and Emad Aliwa.

Alumni (Hall of Fame): Every year, a number of BSc and MSc students undertake their final year projects within the group.

Muhammad Usman
MSc (2020)
Quarriable Smart City Data Markets

Mengdi Li
MSc (2020)
Synthesising Privacy by Design Schemes

Matthew Potter
BSc (2020)
Privacy Cube

Sean Savitz
BSc (2020)
Living Edge Laboratory

Benjamin Thornton
BSc (2020)
IoT Data Trading

Jamie Galvin
BSc (2020)
IoT Lab Book

Oliver Copleston
BSc (2020)
Mesh Networking for Audio-Visual Art

Tanveer Ahmed
BSc (2020)
Remote Animal Trap Monitoring

Dervla O'Brien
BSc (2020)
Object-based Interactive Nutrition Education

Annual Summary for 2020

- The research group is now restructured around three research themes (and an additional theme dedicated to enhancing teaching and learning experience) related to the Internet of Things (IoT) with a significant emphasis on build-driven research method: (1) *Privacy Fluid,* (2) *Data Observatories,* (3) *ResilientSensing.AI,* (4) *Learning Technologies For Internet of Things*.
- Six PhD students and an MPhil student have started working on these themes this year.
- Seven BSc students completed their final projects
  - Luke Jone (2019) published a poster paper in Ubicomp 2020
  - Sean Savitz (2020) got a paper accepted based on his BSc work
  - Majority of the projects were affected by COVID-19 as we were unable to do evaluations.
- Two MSc students completed their dissertations.
- Designed, developed, and published an IoT module (online) to be delivered at both undergraduate and postgraduate level (link).
- A collaboration with iPoint Ltd kicked started with KESS2 Knowledge Economy Skills Scholarship funding support.
- GCHQ has awarded Charith Perera a National Resilience Fellowship. Projects will start in January 2021.

Looking forward to 2021…

Research Vision

Research Interests: Our research primarily focuses on three research questions:

1. How can we build an efficient and effective sensing infrastructure to acquire and use sensor data to better understand and improve ourselves (individuals), surroundings (homes), communities, and the world?
2. How can we encourage sensor data sharing in order to achieve (1)?
3. How can we achieve (1) and (2) without compromising safety, privacy or security?

The research group is formulated around research themes as follows:

Figure 1: Primary Research Themes

Privacy Fluid: This theme aims at developing a shared *Privacy Mindset* through AI mediated assistive layer towards reducing stakeholder breakdown. The objective is to develop a unified framework and methodology that allows capturing privacy-related information throughout the software development life cycle (i.e., from concept to implementation) and the product life cycle (i.e., from onboarding to disposal). For example, Privacy Fluid will support Privacy by Design (PbD) activities by assisting designers through design tools at the design phase. It will then interact with the developers through development tools to support implementing these privacy-protecting measures. Subsequently, privacy fluid will interact with end-users by assisting them in configuring privacy settings. We believe such a unified approach can significantly enhance privacy protection due to shared knowledge and provenance.

Data Observatories: This theme aims at developing open data observatories across different domains ranging from smart cities to wildlife conservation to understand how we can make data available for citizen scientists and other end users. We use knowledge-based AI techniques such as Linked-data and semantic web to support end-users to extract knowledge without significant technical expertise while supporting interoperability and provenance.

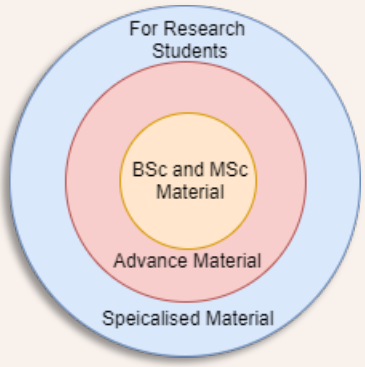
ResilientSensing.AI: This theme explores how we could add layers of resiliency to built environments (and beyond, such as smart city infrastructure) using IoT technologies (e.g., sensors). Smart environments bring both efficiency and convenience; however, they are also vulnerable to attacks and malicious activities due to connectedness. Resilience means the ability and the capacity to recover from cyber-physical attacks (detect, mitigate and recover)

Learning Technologies For Internet of Things: This theme aims to enhance teaching activities. We aim to understand how to teach IoT for different audiences (from high school to university students and beyond) with different skill levels and innovative tools and techniques. We aim to incorporate conversational AI, and personalised learning into teaching and learning experience to facilitate large student cohorts.

Teaching Vision

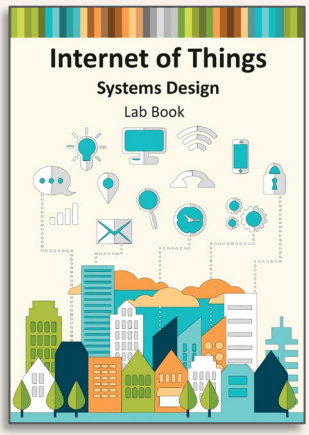
At the undergraduate level, the Internet of Things related content is delivered (to second-year students) through a module titled ***CM2306 Communication Networks***. IoT is delivered through a dedicated module titled ***CMT223 Internet of Things: Systems Design*** at the postgraduate level. Both modules are (mostly) identical in terms of delivery and content. However, expectations (from an assessment perspective) are higher at the postgraduate level (link).

Content: The IoT content is structured under eight theme, namely, (1) *Applications and Use cases*, (2) *Architectures*, (3) *Sensing and Actuation*, (4) *Networking and Communications*, (5) *Data management and analytics*, (6) *Privacy and Security*, (7) *Human Factors and Interactions*, and (8) *Design Strategies and Prototyping*. Each of these sections gets delivered through one or more lectures (which includes dedicated slide decks).



Modularity and Complexity: The content under each theme is developed in a modular and layered fashion based on the complexity of the content. This means that each topic has a certain amount of content that delivers the basic information to the students, sufficient to complete both undergraduate and postgraduate modules. However, if a student interested in learning more, they can follow advance material and learn by themselves. *Advanced materials* are structured and delivered in a similar fashion to the basic material (at times embedded within basic material but are clearly marked) and provide close guidance on following up and self-studying the material. *Specialist materials* are less structured and less organised. they are delivered through either seminars or tutorials (pre-recorded or in-class). Advance and specialised material may help the students complete the assignments in a much higher quality but not mandatory. Specialised material may be useful for new research students to advance their knowledge.

Labs and Practical: As a result of being an applied module, students are expected to complete at least six lab sessions. Students are provided with the lab book that explains each practical session steps by step.



Research with BSc and MSc students: Most of the dissertation projects we offer are research-oriented. These projects are usually aligned with existing projects we are working on, at a given point of time, through either PhD students or research associates. However, we use these dissertation projects to initiate some high-risk projects or new research directions as well. All of our students are encouraged (and supported) to produce research output (such as conference, workshop paper, poster).

Dissemination and Community Engagement

IOT Garage TV (bit.ly/2Md8vJE)

YouTube (and similar platforms) has increasingly become a mainstream content distribution stream that provides large audience access. As a build-driven research group, demonstrations are a key part of our dissemination strategy and increase awareness. Therefore, we have created a dedicated YouTube channel to disseminate our work. We believe visual medium can efficiently and effectively motivate our students to complete their high-quality project work. YouTube videos on our channel also act as a gauge for prospective students. For example, video help students to decide what kind of project they would want to do and the quality of the output they may want to produce. We also use the YouTube channel as a part of our reproducibility and knowledge transfer strategy. We strongly encourage students to create screencasts in such a way that another student could understand what has been done and how. This allows next year students to take the projects forward. Screencasts also help students provide valuable insights about their projects to their fellow students, which might not be feasible in traditional documentation approaches.

IOT Garage News (@IOTGarageNews)

As a complementary to the YouTube channel, Twitter has increasingly become one of the primary ways people consume news updates. We maintain a Twitter account to broadcast updates about our group activities. This includes research updates, students successes, public engagement, and so on.

IOT Garage Code (@IOTGarage)

We take reproducibility and '*building on top of previous work*' very seriously. As a supplement to the screencast, we also encourage to organise and share their code through Gitlab (or similar). We actively maintain code repositories produce by each student related to each project.

Group Website (iotgarage.net)

We maintain a group website to disseminate outcomes of different type of projects to the wider audience. Projects can be varied from BSC, MSc, PhD, to funded projects. We provide all the relevant information under each project, including team members, funder, partners, project demos, linked to publications, links to code repositories.

Funding Support

GCHQ National Resilience Fellowship

(Principle-Investigator)

Total: 55,342 GBP
Cardiff: 55,342 GBP

The Research Fellowships Programme for National Resilience is part of the agency's efforts to pioneer a new kind of security by harnessing academia and industry's collective power to provide fresh perspectives on ways to address national security priorities. The academics could be called upon in the future to help understand a technical challenge in their area of expertise. This fellowship aims to explore how we can use low-cost multi-sensors (e.g., temperature, vibration, motion, etc.) to detect anomalies in a given environment to detect potential cyberattacks against smart buildings.

Connected Communities in the Rural Economy (CoCoRE)

(Co-Investigator)

TS/T016558/1
Total: 5,000,000 GBP
Cardiff: 588,734 GBP

Connected Communities in the Rural Economy (CoCoRE) will bring together experts across the University along with Monmouthshire and Blaenau Gwent County Councils, Cisco, Utterberry, Cardiff City Deal, Innovation Point and Bristol University. Its focus is centred upon the south-east Wales rural region of Monmouthshire and its neighbour Blaenau Gwent. They will innovate in areas such as 'immersive tourism' and 'farming security' as key parts of the rural economy, whilst leveraging related technologies such as Artificial Intelligence, the Internet of Things and Cyber Security as part of an 'innovation platform'.

EPSRC PETRAS 2 (National Centre of Excellence for IoT Systems Cybersecurity)

(Co-Investigator)

EP/S035362/1
Total: 13,850,000 GBP
Cardiff: 290,920 GBP

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity is a consortium that connects 12 research institutions with outstanding expertise in securing the connected world. This Research program has funded Integrity *Checking at the Edge* project. ICE project studies the factories and water treatment systems of the future, undertaking composite vulnerability analysis of interactions between edge devices, cloud and legacy systems.

RCUK Catapult Researchers in Residence award (Digital) - Quarriable Smart City Data Markets

(Principle-Investigator)

EP/T517203/1
Total: 50,000 GBP
Cardiff: 50,000 GBP

The funding was given to initiate a project affiliated with the H2020 funded *SynchroniCity* project. *SynchroniCity* project aims to create a data marketplace that facilitates businesses to develop IoT- and AI-enabled services to improve citizens' lives and grow local economies. However, at the moment, the data offers are searched, modelled, and sold syntactically. This project aims to enrich data with semantic capabilities using ontologies and reasoning techniques by allowing data consumers to query data semantically. Such semantic technology-driven data marketplaces allow data consumer to acquire very specific data instead of asking for large volumes of less relevant data.

Partners

Awen Collective
Awen Collective develops software for critical infrastructure (water, energy, transport, etc.) and manufacturers to reduce cyber-attacks and cyber-threat.

Airbus Group
Airbus Group Innovations are industry leaders in industrial control system (SCADA) security and have a well-equipped testbed at their Newport site.

Digital Catapult
Digital Catapult drives the early adoption of artificial intelligence, immersive and future networks technologies to make UK businesses more competitive and productive and grow their economy.

Building Research Establishment
The Building Research Establishment (BRE) is a centre of building science in the United Kingdom, owned by a charitable organisation, the BRE Trust. BRE provides research, advice, training, testing, certification and standards for public and private sector organisations in the UK and abroad.

PETRAS National Centre for Cyber Security
The PETRAS National Centre of Excellence for IoT Systems Cybersecurity is a consortium that connects twelve research institutions with outstanding expertise in securing the connected world.

Vortex IoT
Vortex IoT builds sensors and networks for harsh environments where conditions are hostile, and power supply is limited, AI is needed & data security is critical.

iPoint
iPoint aims to simplify fleet and data management across the transport industry by unlocking and correlating information from multiple platforms and networks by developing a single transport management platform.

CloudTexo
Cloudtexo is the leading Distribution Service Provider for IIoT, Mobility & Cloud. We deliver disruptive technologies consumed by enterprises.

Danu Gurang Field Center
Danau Girang is a collaborative research and training facility managed by Sabah Wildlife Department and Cardiff University.

My Data Fix
UK qualified corporate and finance lawyer with regulatory expertise gained from an international career. My Data Fix specialises in all aspects of data privacy, having worked as the Global Data Protection Officer for an international organisation whose business is personal data.

PRIVACY FLUID

Interactive Design Method for Augmenting Software Design Process Toward Privacy-Aware Internet of Things Application Designs

Researcher: Nada Alhirabi (PhD Student-2018-2022)

Internet of Things (IoT) applications development and design process is more complicated than others, such as the one for desktop, web, or mobile. That's because IoT applications need both software and hardware to cooperate across multiple nodes with different capabilities. Moreover, it requires different software engineers with different expertise to cooperate (e.g., frontend, backend, and database). Due to the above complications, non-functional requirements, such as security and privacy, tend to be overlooked.

Yearly, a significant number of devices and applications are connecting to the Internet, which raises potential privacy risks. Typically, IoT applications collect and analyse personal data that can be used to derive sensitive information about individuals. However, thus far, privacy concerns have not been explicitly considered (i.e., as unified manner), despite isolated solutions (i.e., a specific technique that address specific privacy challenge) in software engineering processes when designing and developing IoT applications, partly due to a lack of Privacy-by-Design (PbD) methods for the IoT.

This project's primary objective is to develop an interactive design method (facilitate through a tool) that incorporate privacy-preserving techniques into the early phases of the software development life cycle efficiently, effectively, and collaboratively. We envision our tool to be collaboratively used by business analysts, requirement engineers, user experience designers, and software engineers together during the process of creating privacy by design IoT application designs. Our secondary objective is to explore whether such a tool could also enhance novice engineers' privacy knowledge (e.g., university students). This project composed of three main objectives:

- Review the existing design notations, models, languages and tools that facilitate capturing and integrating non-functional requirements (i.e., security and privacy).
- Co-Design an interactive privacy-aware Internet of Things application design methodology towards reducing breakdowns
- Evaluate the efficiency and effectiveness of PRIVACY PARROT (Privacy by Design for the Internet of Things) as a tool for augmenting software engineer's capabilities and enhance privacy knowledge.

PRIVACY PARROT

Partners and Relevant Projects

PETRAS MY DATA FIX

Outcomes

- **[Journal]** Nada Alhirabi, Omer Rana, Charith Perera, **Security and Privacy Requirements for the Internet of Things: A Survey**, *ACM Transactions on Internet Things (TIOT)*, 2(1):6, 2021
  PDF BIB

PRIVACY FLUID

Augmenting Software Design Processes by Developing Knowledge-based AI Technique Towards Assisted Privacy-aware Internet of Things Application Designing

Researcher: Lamya Alkhariji (PhD Student-2018-2023)

Internet of Things (IoT) applications development and design process is more complicated than others, such as the one for desktop, web, or mobile. That's because IoT applications need both software and hardware to cooperate across multiple nodes with different capabilities. Moreover, it requires different software engineers with different expertise to cooperate (e.g., frontend, backend, database). Due to the above complications, non-functional requirements, such as security and privacy, tend to be overlooked.

Yearly, a significant number of devices and applications are connecting to the Internet, which raises potential privacy risks. Typically, IoT applications collect and analyse personal data that can be used to derive sensitive information about individuals. However, thus far, privacy concerns have not been explicitly considered (i.e., as unified manner), despite isolated solutions (i.e., a specific technique that address specific privacy challenge) in software engineering processes when designing and developing IoT applications, partly due to a lack of Privacy-by-Design (PbD) methods for the IoT.
This project's primary objective is to develop a Knowledge-based AI technique that assists software engineers by automatically incorporating Privacy by Design (PbD) techniques into a given IoT application design. This project composed of three main objectives:

- Review and synthesise privacy by design schemes through curating and systematically analysing existing privacy strategies, guidelines, principles, and patterns in the context of IoT.
- Semantically model privacy patterns and IoT systems using knowledge-based AI techniques towards the automated assignment.
- Develop and Evaluate the efficiency and effectiveness of PRIVACY CAPTAIN (Context-Aware Privacy Assistant for the Internet of Things) as a tool for augmenting software engineer's capabilities and enhance privacy knowledge. PRIVACY CAPTAIN uses a knowledge-based AI technique to review a given IoT system design and assist on how optimally apply privacy patterns.

Partners and Relevant Projects

PETRAS

Outcomes

- **[Journal]** Lamya Alkhariji, Nada Alhirabi, Mansour Naser Alraja, Mahmoud Barhamgi, Omer Rana, Charith Perera, **Synthesising Privacy by Design Knowledge Towards Explainable Internet of Things Application Designing in Healthcare,** *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 2021 (in Print) PDF BIB DATA SET

PRIVACY FLUID

Augmenting Software Engineers' Capabilities Towards Developing Privacy Law-Friendly Internet of Things Applications using End-User Development Paradigm.

Researcher: Atheer Jeraisy (PhD Student-2019-2023)

Internet of Things (IoT) applications development and design process is more complicated than others, such as the one for desktop, web, or mobile. That's because IoT applications need both software and hardware to cooperate across multiple nodes with different capabilities. Moreover, it requires different software engineers with different expertise to cooperate (e.g., frontend, backend, database). Due to the above complications, non-functional requirements, such as security and privacy, tend to be overlooked.

In order to address this issue, we need to find a way to support and motivate software developers. In this project, we primarily focus on privacy. We aim to address this problem using two methods. First, we need to develop easy to use privacy-preserving software components (some form of modules) that developers can incorporate into their IoT application development process. These privacy-preserving components should be reusable and generic enough to be used across multiple domains and applications. Furthermore, these privacy-preserving techniques should be integrated into existing IoT software development tools (i.e., popular IDEs and software frameworks). Secondly, we will use gamification techniques to motivate the software developers to incorporate more and more reusable privacy-preserving components within their IoT applications. This gamification framework will also be integrated into popular IoT software development tools. This project composed of three main objectives:

- Systematically analyse privacy by design schemes to find out how they can be used to satisfy and comply with privacy laws around the world in the context of IoT.
- Explore how different types of privacy by design schemes and elements within them (such as privacy strategies, principles, guidelines, and patterns) can be transformed into reusable privacy-preserving components.
- Based on the above findings, we aim to develop a series of reusable privacy-preserving components that can be easily adapted into the IoT application development process.
- Develop a framework to examine and operationalise each privacy-preserving components in order to quantify them towards developing a gamification-based education method.

Partners and Relevant Projects

Outcomes

- **[Journal]** Atheer Aljeraisy, Masoud Barati, Omer Rana, Charith Perera, **Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective**, *ACM Computing Surveys (CSUR)*, 2021 (in Print) PDF BIB DATA SET

PRIVACY FLUID

Interaction Methods for Privacy Preferences Management in Shared Spaces

Researcher: Bayan Almuhander (PhD Student-2019-2023)

The balance between protecting users' privacy while providing cost-effective devices that are functional and usable is a key challenge in the Internet of Things (IoT) industry. In traditional desktop and mobile contexts, the primary user interface is a screen. However, in IoT, screens are rare or very small, which invalidate most traditional interaction approaches (i.e., popup notifications).

We examine how end-users interact with IoT products and how the IoT devices convey information back to the users, particularly regarding their data (i.e., How IoT devices manage data about end-users). We explore how individuals with a non-technical background can be notified about the privacy-related information of the spaces they inhabit in an easily understandable way.

This project's primary objective is to develop a tangible device that facilitates interactive privacy preferences management of IoT devices in shared spaces such as smart homes. We envision our 'PrivacyCube' as an enhanced privacy notice for the IoT devices and assist people in making informed privacy decisions and increase privacy awareness. 'PrivacyCube' is expected to act as a centralised hub that visualises how various smart home devices manage data. This project has three objectives:

- Review the various methods available to notify the end-users while considering the factors that should be involved in the notification alerts within the physical domain.
- Develop a tangible interactive device that serves as a privacy notice and visualises how IoT devices manage data in shared spaces such as smart homes.
- Evaluate the effectiveness of the PrivacyCube towards increasing privacy awareness and privacy preference management in shared spaces such as smart homes.

Partners and Relevant Projects

PETRAS

Outcomes

- **[Technical Report]** Bayan Al Muhander, Jason Wiese, Omer Rana, Charith Perera, **Interactive Privacy Preferences Management for Shared Spaces in the Internet of Things**, Technical Report, 2020 PDF BIB

PRIVACY FLUID

Privacy Considerations when Designing Smart Home Systems to Facilitate Independent Living for Ageing

Researcher: Reem Aldhafiri (PhD Student-2020-2024)

We live in the revolution of smart home devices such as smart speakers, lighting and thermostats, which are being rapidly developed and adopted by different people. Those devices collect, process, and disseminate end-user data to facilitate different functionalities, such as recommendations and automation. These functionalities typically being convenience and efficiency to the environments they are being deployed. For example, a smart lighting system may automatically configure its setting to reduce energy consumption while providing optimal service to the end-users. However, such functionalities require them to monitor end-user behaviour and track their whereabouts, moods, preference, etc.

Smart devices are connected and sharing data to achieve a common goal. We can be considerate that some of the devices have sensitive data such as the house's location that can negatively affect the household's life. People (especially older adult and vulnerable people) face violating their privacy if data collection practices deviate. Some studies show that the elderly have privacy concerns and avoid using any smart devices that monitor them. Privacy concerns are one of the most significant barriers in using the monitoring device in a smart home. Older adults, especially those who have a mild cognitive impairment, are vulnerable to the risk of privacy being violated as they may not configure their privacy preferences.

This project focuses on privacy and data protection in smart homes and users of vulnerable communities by using physical artefacts. We focus on augmenting existing smart home systems and their privacy configuration mechanisms to improve privacy and data protection among vulnerable groups and help them configure their privacy and data protection requirements better. The main objectives of the project are:

- Review existing work of designing privacy-aware Internet of Things for vulnerable groups
- Co-Designing privacy needs of Internet of Things systems to support successful ageing and learning disabilities
- Rethinking Privacy-Awareness in Connected Homes: Design and Evaluation of a Privacy Toolkit Towards Augmenting Older People and Learning Disabilities

Partners and Relevant Projects

Innovate Trust PETRAS

PRIVACY FLUID

Optimal Placement and Scheduling of Service Function Chaining (SFCs) under Security Constraints*

Researcher: Areej Alabbas (PhD Student-2019-2023)

Virtualized Network Functions (VNFs) is a technique used to replace hardware-based functions by a set of software-based functions. These functions are dynamically deployed across multiple clouds based on the cost of deployment, availability of required resources and proximate to the end-user. The process of chaining these VNFs to form end to end service is called Service Function Chaining (SFC). SFC is a set of service functions (SFs) that are ordered to provide a specific service. This study aims to propose an algorithm used to optimal placement of SFCs in multi-cloud architecture based on security constraints. This study will also build an analytics model, taking into account two factors: security constraints and performance.

RESILIENTSENSING.AI

Detecting In-Vehicle Cyber Attacks through Controller Area Network (CAN) Bus Data Analytics on-the-Edge*

Researcher: Emad Aliwa (PhD Student-2019-2023)

In this project, we investigate Controller Area Networks (CAN) bus and its security vulnerabilities and countermeasures in the context of different vehicle networks (e.g., (i) In-vehicle network, (ii) vehicle-to-vehicle and (iii) vehicle-to-infrastructure. Today, vehicles are fitted with a large number of sensors and actuators. These sensors and actuators produce and consume large volumes of data. These data items are managed through a system called CAN bus. At the same time, more and more vehicles are getting connected to the Internet. Furthermore, vehicles also provide a wide range of interfaces that can be used to connect external devices to them, such as mobile phones. Both Internet connectivity and external interfaces create more vulnerabilities. These external connections could be manipulated to conduct cyber-attacks against vehicles. In this project, we are aiming to develop algorithms that can be used to detect malicious activities and cyberattacks by analysing the CAN Bus data. Further, we will explore how the CAN Controller can be improved to be more secure from cyberattacks from the inside out and vice versa.

Partners and Relevant Projects

PETRAS

ipoint

Outcomes

- **[Journal]** Emad Aliwa, Omer Rana, Charith Perera, Peter Burnap, **Cyberattacks and Countermeasures For In-Vehicle Networks**, *ACM Computing Surveys (CSUR)*, 2021 (in Print)
  PDF BIB

*Lead by Omer Rana

RESILIENTSENSING.AI

Edge Analytics for Sanitary Facility Monitoring

Researcher: Dom Fonseca (MPhil Student-2020-2021)

This project focuses on developing a novel distributed predictive analytics technique that can efficiently be used in edge computing scenarios. Our partner iPoint is focused on developing sensor data based intelligent services to monitor and maintain hygiene facilities in remote locations (e.g., remote sanitary facilities). Currently, all the sensor data collected by all the sensors are directly sent to the cloud. All the required processing happens within the cloud, and relevant commands are sent back to each hygiene facility. This approach is inefficient from many aspects and could also impact service quality and customer satisfaction in certain scenarios.

To address the challenges face by iPoint, we aim to develop a novel data processing architecture capable of moving analytics across different nodes (within the architecture). This means that iPoint will no longer be required to send all the sensor data to the cloud all the time. The onboard computer will conduct most of the data analytics local and will only send the summarised/aggregated data to the cloud. However, our proposed algorithms will consider context information when deciding where the data analysis should happen.

- Design and develop distributed algorithms that can dynamically orchestrate IoT resources on edge to satisfy a given sensing requirement without continuous connectivity to the cloud.
- Design and develop a self-organising and reconfigurable IoT infrastructure that integrates resources from multiple layers (i.e., edge, fog, cloud) on demand.

Partners and Relevant Projects

RESILIENTSENSING.AI

Adapting to Discomfort Towards Sustainable Built Environments

Researcher: Asma Irfan (PhD Student-2020-2026) [PT]

The buildings and buildings' construction sectors are responsible for over one-third of global final energy consumption and nearly 40% of total direct and indirect CO2 emissions. Many approaches have been proposed in the literature to tackle the challenge of reducing energy consumption in built environments. For example, some approaches focus on automation and predictive behaviour modelling to optimise energy consumption. In contrast, in our project, we chose to use 'adapting to discomfort' as our approach to reduce energy consumption. This project aims at developing a design framework to facilitate adaptation to discomfort. By doing this, we aim to reduce energy consumption within built environments. We aim to develop a series of prototypes, conduct co-design workshops, and validate the proposed framework through in-the-wild studies.

Integrity Checking at the Edge

Researcher: Matthew Nunes (Research Associate-2019-2021)

Industrial Control Systems (ICS) is the all-encompassing term to describe Distributed Control Systems (DCS) and Supervisory Control And Data Acquisition (SCADA). DCS tend to refer to the systems connecting sensors actuators and controlled locally at a plant. Whereas SCADA refers to systems used to control and manage communication geographically remote systems. Security has not traditionally been given much attention within ICS environments since they have not faced many threats because they have not been connected to the Internet in the past. Besides, there is a wide range of proprietary protocols used in ICS environments that are not as well known, thereby giving the illusion of security. Despite the challenges associated with designing security solutions for ICS environments, it is still a very relevant topic as attacks against ICS environments increased by 110% as of 2016.

When designing an IDS for an ICS environment, the most important factor to consider is its impact on the overall performance. As ICS environments tend to be hard real-time environments, even the smallest delay introduced by an IDS can have catastrophic effects. Therefore, particular care must be taken when determining how the IDS should intercept data as any delays render the solution unusable. Additionally, despite their widespread use within regular IT environments, Signature-based IDS are largely obsolete within environments. This is due to the wide range of devices and protocols used within ICS. Digital Bond provides the most well-known set of IDS rules for SCADA. However, its support is limited by the type of devices and protocols it recognises far from exhaustive.

To help with the uptake of IDS solutions within an ICS environment, it is important that operators can trust the system. To gain their trust and make actionable decisions, it is essential that they clearly understand the IDS solution operates and what informs its decisions. To this end, we review visualisation solutions of both network traffic and ML algorithms to understand the best way to communicate information about them. This will allow us to create a holistic solution that can (i) recognise malicious behaviour and pass on the information to an administrator in a manner that will give the administrator confidence in its conclusions, and (ii) provide relevant detail about the malicious activity so the administrator can determine the most appropriate course of action for remediation. These objectives relate to the goals of the PETRAS Integrity Checking at the Edge (ICE) project:

- Develop an explainable IDS for ICS in an OT context that would enable security operations teams to drill into an alert and identify security concerns and suitable mitigation solutions.
- Develop a method that is dynamic and allows an analyst to interrogate it in real-time. The method is chosen will be open-source.
- Develop an explainable solution that is complementary with the leading algorithm(s) for ML-based attack detection in OT.

Partners and Relevant Projects

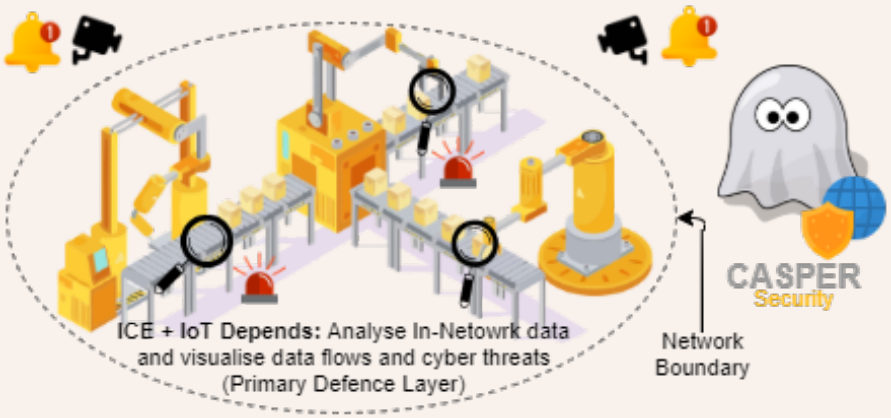
RESILIENTSENSING.AI

Context-Aware Security System for Industrial Cyber-Physical Edge Resources

Researcher: Hakan Kayan (PhD Student 2020-2024)

Industrial cyber-physical systems (ICPSs) manage critical infrastructures by controlling the processes based on the "physics" data gathered by edge sensor networks. Recent innovations in ubiquitous computing and communication technologies have prompted the rapid integration of highly interconnected systems to ICPSs. Hence, the "security by obscurity" principle provided by air-gapping is no longer followed. As the inter-connectivity in ICPSs increases, so does the attack surface. Industrial vulnerability assessment reports (see Figure 1) have shown that a variety of new vulnerabilities have occurred due to this transition, led to an increase in the targeting of ICPSs. Key findings from Verizon's 2020 data breach report shows 381 data breaches (10% of total) are against industrial systems where not all of them target OT equipment.

We aim to develop a context-aware anomaly detection mechanism/model that physically observes ICPS edge devices to detect cyberattacks. The proposed approach aims to answer the question of "Can we accurately detect cyberattacks in an industrial environment with a low-cost IoT network by observing physical behaviours?". The followings are the main objectives of the project:



- Review the current ICPSs from a cybersecurity perspective.
- Develop end-to-end reconfigurable IoT sensing infrastructure for training and deploying analytics at scale.
- Augment cyberattack detection through physical behavioural monitoring in ICPSs.
- Evaluate the efficiency of a Context-aware Dynamically Adaptive IoT Edge Network for Cyber Attack Detection in Industrial Control Systems (CASPER) through extensive experimental evaluations.

Partners and Relevant Projects

PETRAS GCHQ AIRBUS GROUP

Outcomes

- **[Technical Report]** Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, Charith Perera, **Cybersecurity of Industrial Cyber-Physical Systems: A Review**, Technical Report, 2020 PDF

Context-Aware Security for Smart Homes using Cyber-Physical Behavioural Data Analysis

Researcher: Yasar Majib (PhD Student-2020-2024)

The rapid growth of the Internet of Things (IoT) requires a deep look into security and privacy challenges. This growth is changing our contemporary world, which is now connected in novel ways and poses new challenges. Nowadays, these tiny little devices (IoTs) routinely communicate with each other on behalf of humans. As we move further into this AI era, the world needs assurance that this fabric of interconnected things is not vulnerable to any traditional or cyber-physical security threats. The entire spectrum of IoT fabric includes; devices/things, connectivity, storage, and applications – all of which are potentially vulnerable. In addition to traditional connectivity channels, IoTs are exposed to physical channels such as temperature, humidity, air quality, illumination, sound, and many more. A single vulnerable IoT can be a gateway to break into a secure smart home system by being exploited by a cyber vulnerability or by a physical channel[s].

Assume a temperature sensor in a smart home network is vulnerable and exploited by an adversary. It can trigger an open window event if a temperature sensor is transmitting a high value. The solutions currently available are mostly focused on traditional Network Traffic Analysis (NTA) for detecting anomalies in cyber systems (Intrusion Detection or Intrusion Prevention), which is not sufficient in the IoT scenario.

This project is focused on cyber-physical behaviour, where we aim to detect cyber attacks by detecting anomalies by cyber-physical behavioural data analysis in smart homes. We aim to develop low-cost multi-purpose sensor nodes which can detect anomalies in a smart home by analysing cyber-physical data. In another scenario, imagine a malicious party switch on a toaster add midnight while spoofing the smart plug and prevent it from reporting to the smart home hub. The multi-purpose sensor network we propose can be used to detect such anomaly events by physically observing temperature vibration, light or sound even though the malicious party may have compromised the smart plug as well the smart home hub preventing it from generating NTA-based anomaly. The project has the following objectives:

- Review the existing anomaly and cyber-attack detection techniques in the landscape of smart homes.
- Predict smart home automation rules as well as behavioural patterns using a distributed multi-purpose sensors network.
- Detect anomalies by observing behavioural patterns by combining network traffic analysis and observational data gathered through an independent IoT sensor network.

Possible Partners and Relevant Projects

PETRAS bre GCHQ

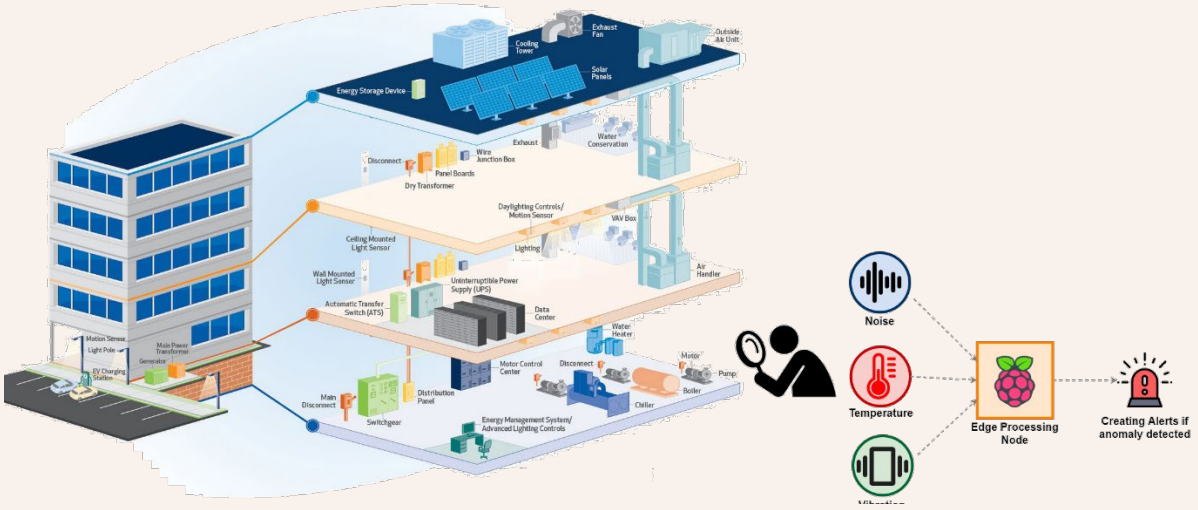
RESILIENTSENSING.AI

Detecting Cyber Attacks Using Secondary IoT Sensors in Buildings

Researcher: Charith Perera (Principle Investigator-2021-2021)

Cyber-attacks on Industrial Control Systems (ICS) are monitored through traditional techniques such as Network Traffic Analysis (NTA). While we acknowledge the merit of NTA, more sophisticated attacks (example below) will evade NTA approaches by spoofing the readings from the sensors making ICS significantly vulnerable. Let us consider a scenario: if an attacker intends to overheat a system, they could alter the fan behaviour (e.g., speed). Simultaneously, the attacker may also maliciously control the connected temperature sensors to prevent reporting increased temperatures back to the control system, leading to overheating.

To detect such sophisticated attacks, we propose to develop a secondary low-cost IoT sensor network that combines sensors data and state-of-the-art deep learning techniques to detect anomalies. Further, this secondary IoT sensors would use a secondary network (e.g., Bluetooth, ZigBee) and stay as an air-gapped system to reduced potential parallel attacks. For example, an unexpected fan shutdown might be detected through changes in temperature or the absence of noise where all parameters can be captured through sensors (i.e., physical observations).



This fellowship aims to explore how can we use low-cost multi-sensors (e.g., temperature, vibration, motion, etc.) to detect anomalies in a given environment to detect potential cyber attacks against ICS. Malicious actors always try to find sophisticated ways to carry-out attacks (e.g.Stuxnet, Ukraine, power-grid cyberattack). To prevent attacks that evade NTA, we aim to develop a secondary layer of protection based on physical behaviour to mitigate the weaknesses of NTA. It is important to note that our intention is not to ignore NTA based techniques. Instead, our objective is to add more resilient to the BMS network by adding a secondary protection layer of security.

Partners and Relevant Projects

Semantic Knowledge-Driven On-demand Data Offerings for Quarriable Smart City Data Marketplaces

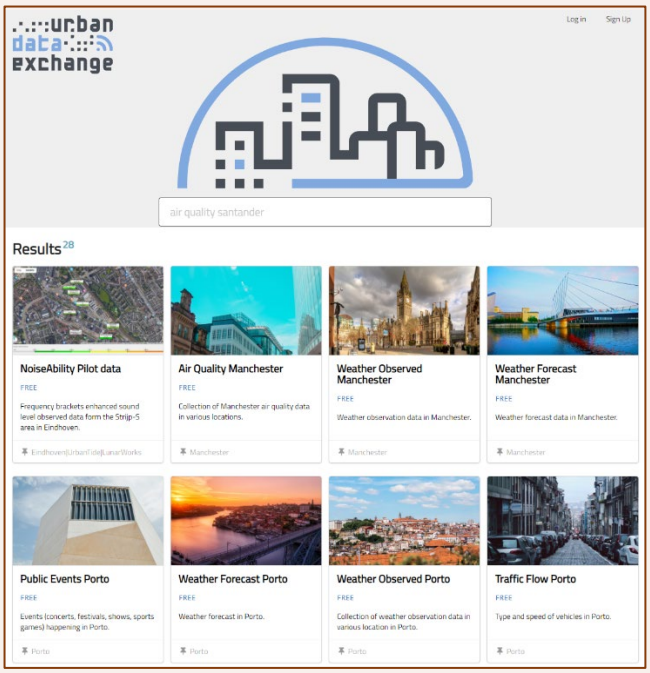
Researcher: Charith Perera (Principle Investigator-2019-2021)

Cities are increasingly get augmented with sensors through both public, private, academic sector initiatives. Most of the time, these sensors are deployed by having a primary reason in mind (e.g., noise sensors) by a sensor owner (e.g., city council). However, over the last few years, the community has understood the importance of making the data captured by these sensors available for a wider community beyond their primary usage. Different business models have been proposed to achieve this, including the creation of data marketplaces(e.g., iot-data-marketplace.com). The vision is to encourage new start-up and small businesses to create novel products and services by utilising the datasets to generate additional value to the economy. At the moment, in data marketplaces, data are sold as predefined independent datasets (e.g., noise level and car park status datasets may be sold separately). This approach creates a number of challenges such as;

(i) Difficulties in pricing which leads to higher prices (per dataset),
(ii) Higher network communication and bandwidth requirement and
(iii) Information overload for data consumers (i.e., parties who buy data).

In this project, we propose a semantic-driven technique to create on-demand data offering for data marketplaces. Our approach goes beyond predefined data offering to on-demand custom data offering. More importantly, we solve the three challenges mentioned above. The project composed of serval objectives:

- Develop an ontology by combining a few different well-known ontologies that can model any type of sensor data in the context of IoT data marketplaces.
- Propose a unique on-demand data offer creation technique. Buyers are given the opportunity to create their own custom data request (data order) by considering four different aspects, namely location, data type, date/time, and service level agreement.
- Through a series of use cases, demonstrate the utility of knowledge engineering (including reasoning/inferencing) in data marketplaces.
- Evaluate the performance of the proposed approach in three different distributed data marketplace setups.



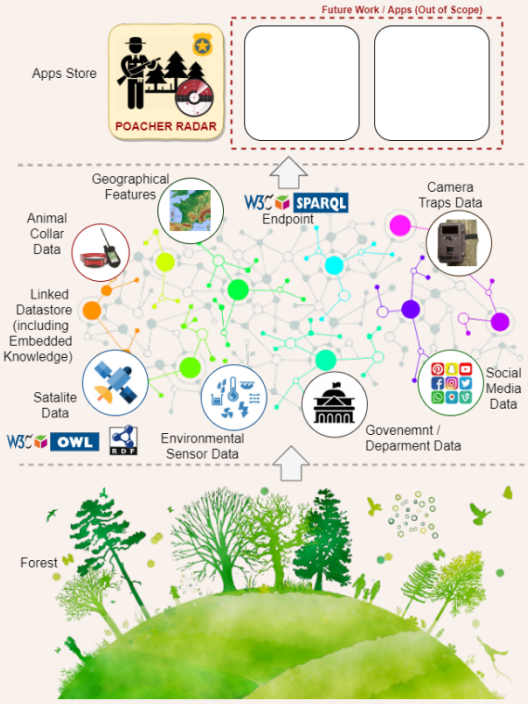
Partners and Relevant Projects

SYNCHRONICITY CATAPULT Digital

Semantic Data Integration Towards Forest Observatory based App Ecosystem

Researcher: Naeima Hamed (PhD Student-2020-2024)

Poaching and animal trafficking are significant challenges around the world. Anti-poaching efforts are always underfunded and under-resourced. Law enforcement officers cannot keep up with the large number of poachers who are trying to kill and capture animals. Due to limited manpower, they cannot patrol and protect vast areas of land. We will semantically integrate data gathered by Bio-science researchers and environmental scientists to predict where the poaching activities would occur in the future. Our data-driven prediction models will tell areas and time frames that have a high likelihood of having poaching incidents. Therefore, law enforcement agencies can deploy their limited resources into those areas. This project will focus on the Lower Kinabatangan Wildlife Sanctuary, Sabah, Malaysia. This project is a collaboration between the School of Computer Science and the School of Biosciences (and its Danau Girang Field Centre; DGFC) at Cardiff University.



Our approach is to develop a Forest Observatory and develop data-driven predictive analytics to predict poaching incidents. Forest Observatory is a Linked Datastore that integrates heterogeneous data. We consider Forest Observatory as an extension of Urban Observatories which aim at gathering real-time urban data across cities. Collecting data in forests is much more challenging than in cities due to the lack of infrastructure. However, while we expect to deploy an Internet of Things (IoT) infrastructure to enable poaching monitoring, we should be able to utilise already collected data sets to develop predictive poaching models. For example, DGFC has data sets collected by researchers for wildlife species monitoring over the last decade, such as animal collar data, camera traps, satellite imagery, LiDAR and environmental data, with each data set generated using different time frames durations, geographic areas etc. In order to develop a Forest Observatory, we aim to integrate data sets collected by the bioscience researchers at DGFC into a unified linked data store using semantic data integration techniques (computer science methods) while conforming to the data modelling standards (e.g., ontologies) and needs of bioscience research (Bioscience methods) within the context of developing a model and novel tools that are exportable to other areas of the world where poaching is a threat to wildlife conservation.

Partners and Relevant Projects

Dynamically Orchestrate-able Low Power Internet of Things Infrastructure for Sustainable Wildlife Conservation

Researcher: Mark Butterworth (PhD Student-2020-2026) [PT]

This project aims to develop a reliable communications technique to monitor animal traps remotely. Low power digital transmission techniques encounter many hurdles when operating in harsh / dense junsgle environments. Traditionally the problem can be overcome using higher power transmissions; however, in this case, it is not possible as devices need to operate for long periods autonomously and cannot afford the increased burden of regular battery changes. This research project aims to examine frequencies and develop protocols that will allow secure, reliable communication across dense jungle environments using low power digital transmission protocols.

The research aims to deliver a fully functional concept demonstrator based upon communications theory; the key objective is to be able to monitor sensing infrastructure in the Kinabatangan wildlife sanctuary without the need to visit each sensor.




Trap activation detection – Most traps operate using weight-based or bait based activation triggers. Smaller animals could accidentally become ensnared, meaning cages must be visited regularly to ensure animal safety. Any sensor monitoring system must be very reliable and fail-safe to ensure wildlife welfare.

Poacher tracking – While poachers and vehicles' accurate pursuit is not practical without deployed sensors on the person or vehicle, it would be possible to monitor poachers activities and their movements. Sensors could monitor people passing through pinch points and congregating at meeting points. The data from these sensors could provide information to other data science projects to help elicit information on poacher behaviour and help predict everyday activities.

Poacher detection – Vehicles are not allowed in the sanctuary after 19:00 so sensors deployed to detect these vehicles could use vibration sensors, Automatic Number Plate Recognition (ANPR), or sound as it is reasonable to assume that vehicle in the wildlife reserve after 19:00 are unauthorised.

Remote camera trap battery monitoring – Messages for monitoring and reporting battery life can be tiny and not time-critical. Message updates can be provided on a predetermined cycle, such as hourly or daily. This tradecraft would reduce the number of messages sent and enhance battery life. User-definable heartbeats would allow the user to define a refresh timeframe with which they are comfortable.

Partners and Relevant Projects

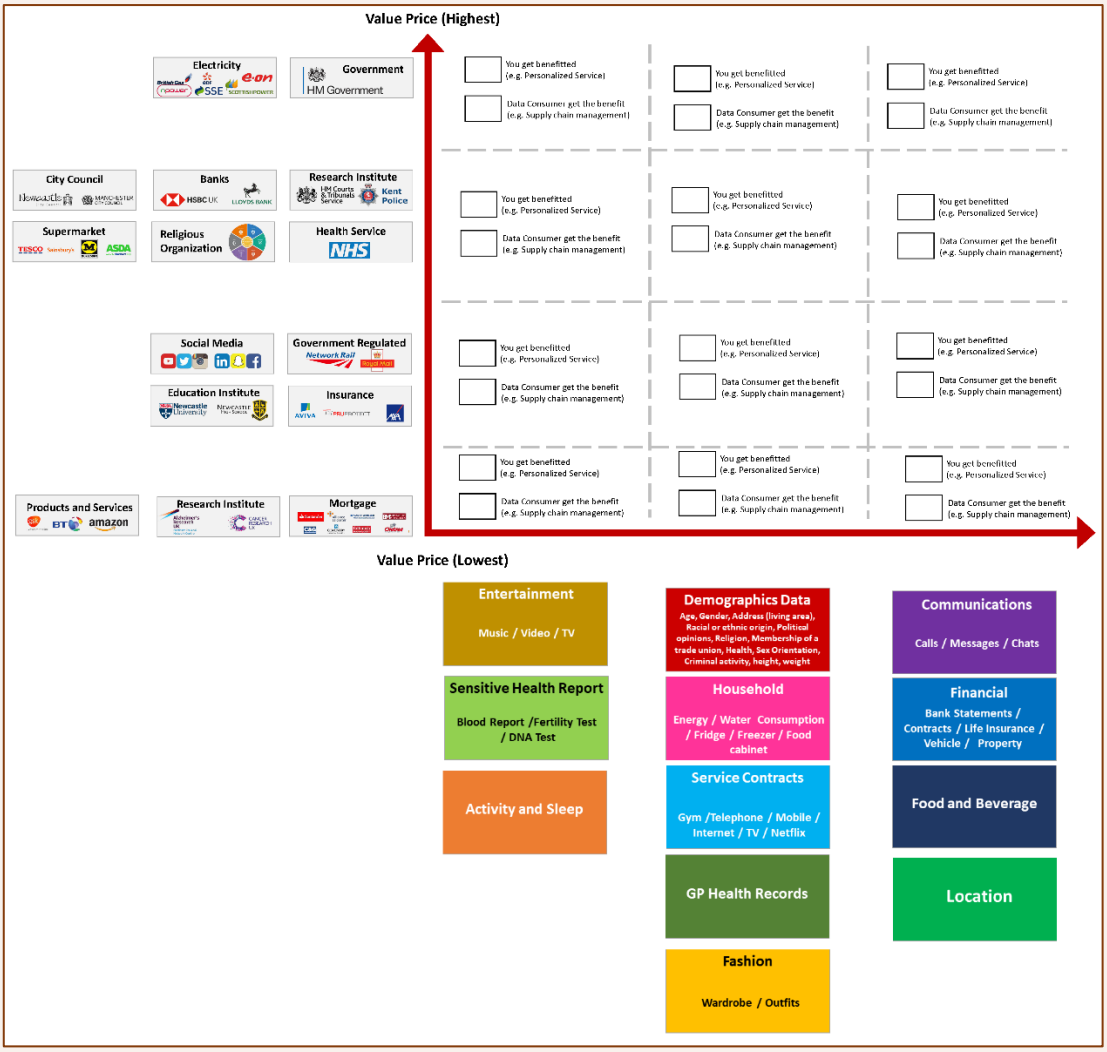
Incubator Projects

Developing a User Study Platform Towards Understanding IoT Data Trading Preferences

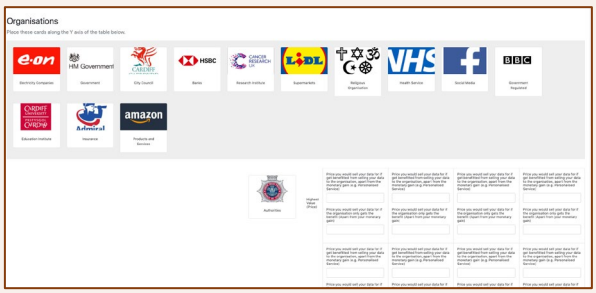
BSc

Researcher: Benjamin Thornton (BSc Student-2020)

This project develops a web application that takes the user-centric approach of investigating the problem of people's willingness to trade different types of IoT data to different organisations by creating a platform where people can create user studies, participate, and analyse responses to them. The platform can manage different types of user studies that can utilise the matrix-based of user preferences measurements. It also has built-in email-based survey distribution support as well as automated generation of heatmaps and analytics. VIDEO



This project was affected by COVID-19, and we could not evaluate the artefacts we built in a real-world setting.

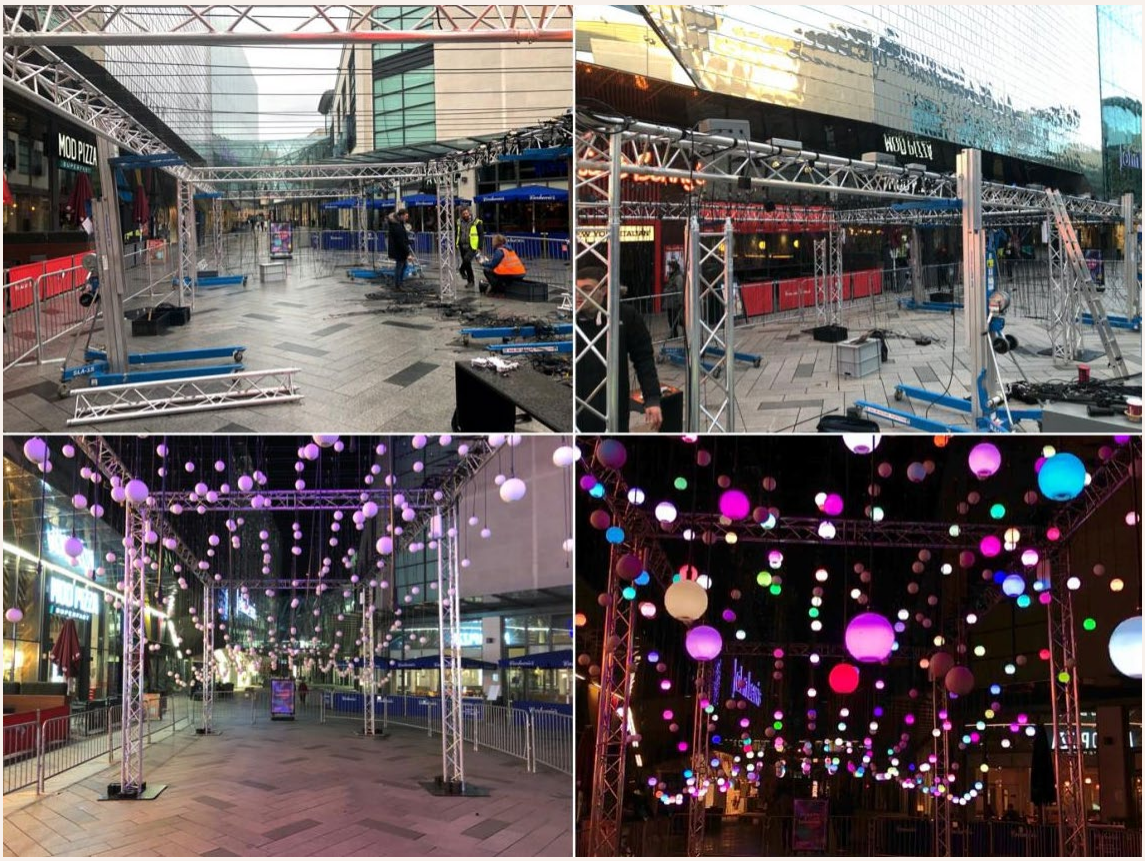


Mesh Networking for Audio-Visual Art

Researcher: Oliver Copleston (BSc Student-2020)

BSc

This project presents a novel mesh networking solution that enables conventional WiFi hardware to host tens of thousands of wireless devices, far beyond their normal capacity. This dramatically changes how and who can create an art installation as there is no longer a need for expensive and complicated networking hardware. Most home WiFi routers struggle to support upwards of 30 wireless clients. The aim of this project is to create a proof of concept system that can demonstrate the feasibility of a mesh network to support real-time audio and light artworks, which can be used to support the future development of the product. By leveraging existing WiFi infrastructure, the possibility emerges for clients to design and install their own art pieces. This has opened the opportunity for SquidSoup to develop a rich software toolkit for Bloom, providing users of varied ability the means of producing spectacular audio and light experiences. This project was done in collaboration with the renowned artist collective SquidSoup VIDEO



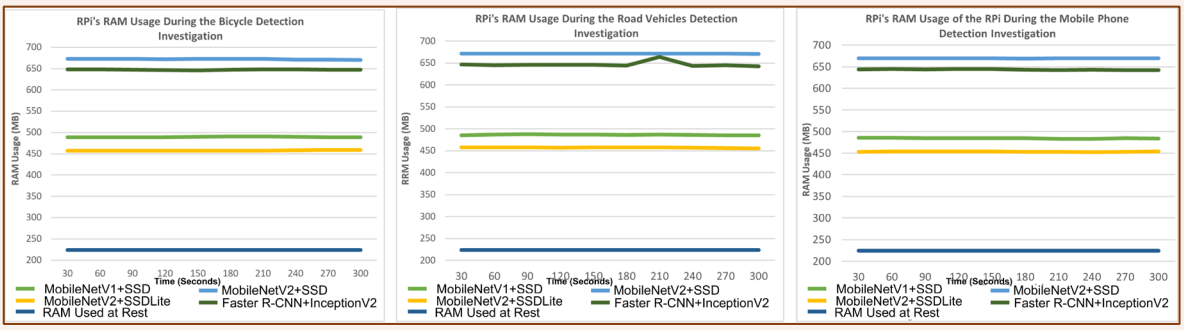
This project was partially affected by COVID-19.

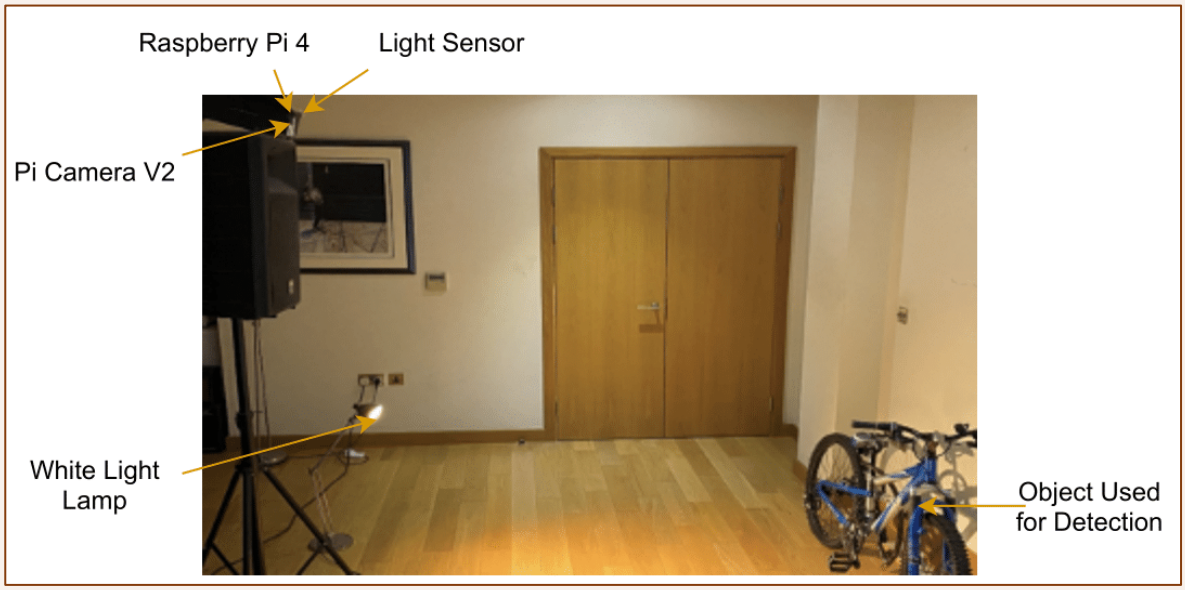
Edge Analytics on Resource-Constrained Devices

Researcher: Sean Savitz (BSc Student-2020)

BSc

Video and image cameras have become an important type of sensor within the Internet of Things (IoT) sensing ecosystem. Camera sensors can measure our environment at high precision, providing the basis for detecting more complex phenomenon in comparison to other sensors, e.g. temperature or humidity. This comes at a high computational cost on the CPU, memory and storage resources and requires consideration of various deployment constraints such as lighting and height of camera placement. Using benchmarks, this work evaluates object classification on resource-constrained devices, focusing on IoT cameras' video feeds. The models that have been used in this research include MobileNetV1, MobileNetV2 and Faster R-CNN that can be combined with regression models for precise object localisation. We compare the models by using their accuracy for classifying objects and the demand they impose on a Raspberry Pi's computational resources. Various IoT deployments are investigated by comparing the probability scores of classifying chosen objects using different camera placement. We conclude that the Faster R-CNN model that is configured with the InceptionV2 regression model has the highest accuracy. However, this is at the cost of additional computational resources. We found that the best model to use for object detection functionality on the Raspberry Pi is the MobileNetV2 model that is paired with the SSDLite regression model. This results in the highest accuracy and probability score for object classification, in comparison to other mobile-friendly models used in this work, whilst using the least amount of computational resources.





This project was affected by COVID-19, and we could not evaluate the artefacts we built in a real-world setting.

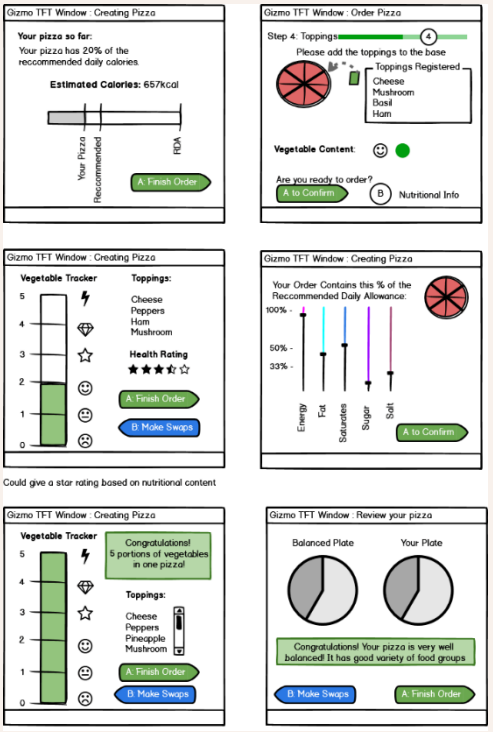
- **[Journal]** Sean Savitz, Charith Perera, Omer Rana **Edge Analytics on Resource-Constrained Devices**, *Int. J. Computational Science and Engineering*, (In Print) PDF BIB VIDEO VIDEO

Educating Primary School Kids about Nutrition using Object-based Interactions

BSc

Researcher: Dervla O'Brien (BSc Student-2020)

Children worldwide have poor diets and poor understanding of nutrition, confining food into dichotomous "healthy" and "not-healthy" groups rather than grasping deeper, more realistic concepts of variety and balance. Child nutrition is of vital importance to health, longevity and lifelong good eating habits. Adequate nutrition is vital for brain development and learning[96]. However, nutrition is quite a complex topic. Dietary information can often become reduced to crude messages regarding "healthy" versus "unhealthy" food choices. Yet, the issue is clearly more complex than this. Foods labelled "healthy" can become quite the opposite if eaten in very large quantities and demonising "unhealthy" foods can lead to problematic feelings of guilt and shame around eating. Instead, nutrition advice seems to agree that eating a variety of foods in a balanced way is a better message to convey. Can we encourage children to develop these more nuanced ideas of food? By specifically tailoring the design to children as the target audience for these messages, we can help them develop healthier eating habits earlier in life and intervene before early adolescence when eating disorders will be developed. We need to combat some of the more extreme (and often dangerous) dietary messages such as 'clean eating', which is often promoted via social media like Youtube and Instagram.



This project explores how an interactive food ordering system could help enable children to learn to make healthier dietary choices for themselves. The project extends a previous study on the PizzaBox system and explores how it can be applied to an audience of 9-11-year-old children, with the additional aim of being an innovative and engaging way to educate in nutrition and dietary choices. Several designs are explored and discussed, and a final design is produced, incorporating the advice of a community dietitian. Further research should extend the functionality, perhaps with a focus on how this project could be used within a program of education in schools. It would be beneficial to measure how effective this intervention is at changing dietary habits and educating it's users. The demo video is here VIDEO.

This project was affected by COVID-19, and we could not evaluate the artefacts we built in a real-world setting.

Next-Generation User Interfaces for the Internet of Things Data Marketplaces

MSc

Researcher: Muhammad Usman (MSc Student-2020)

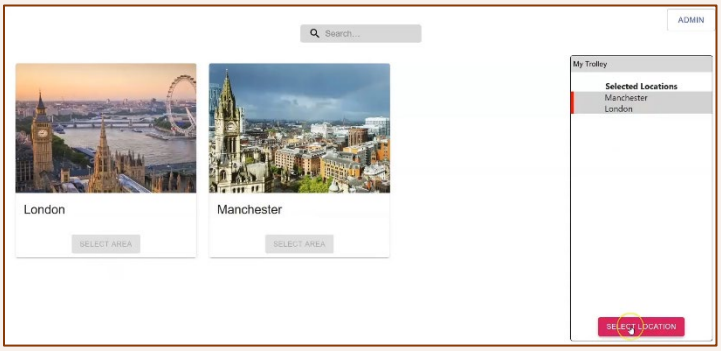
Cities are increasingly get augmented with sensors through both public, private, academic sector initiatives. Most of the time, these sensors are deployed by having a primary reason in mind (e.g., noise sensors) by a sensor owner (e.g., city council). However, over the last few years, the community has understood the importance of making the data captured by these sensors available for a wider community beyond their primary usage. Different business models have been proposed to achieve this, including the creation of data marketplaces(e.g., iot-data-marketplace.com). The vision is to encourage new start-up and small businesses to create novel products and services by utilising the datasets to generate additional value to the economy. At the moment, in data marketplaces, data are sold as predefined independent datasets (e.g., noise level and car park status datasets may be sold separately). This approach creates a number of challenges such as;

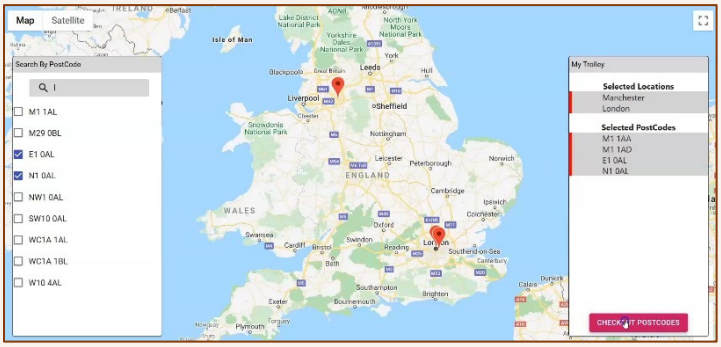
(i) Difficulties in pricing which leads to higher prices (per dataset),

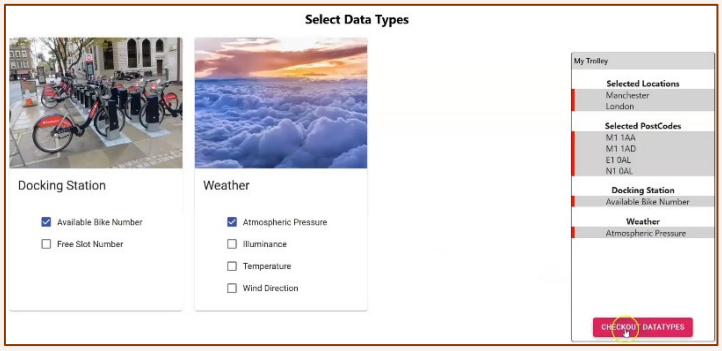
(ii) Higher network communication and bandwidth requirement and

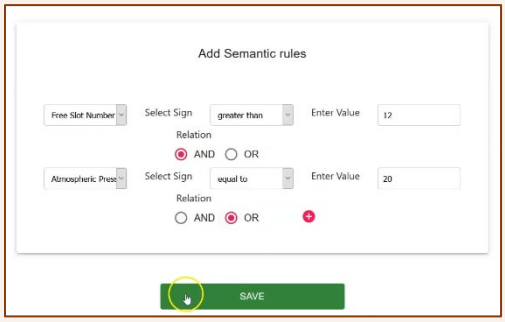
(iii) Information overload for data consumers (i.e., parties who buy data).

This project focused on developing a next-generation UI that allows data consumers to pick and choose and buy the exact dataset they need. VIDEO









This project was affected by COVID-19, and we could not evaluate the artefacts we built in a real-world setting.

iotgarage.net

gitlab.com/IOTGarage

bit.ly/2JMoSd4

@IOTGarageNews