Internet of Things Research and Teaching: Vision and Mission

Annual Report (2021)

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 systems, 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 name ***'IoT Laboratory'***. We are not alone, see.

History: Established in December 2018 (within School of Computer Science and Informatics, Cardiff University). Previous Annual Reports: 2019, 2020

Principal Investigator: Charith Perera

As of December 2021, the research group comprises 17 PhD students, 3 MPhil students (and 2 affiliated PhD students), and 4 research assistants (and several affiliated PDRAs).

Research Assistants:

Mary Zacharias
Smart Home Testbeds [2021-2022]

Osian Morgan
Sensor-driven Anomaly Detection [2021-2022]

Akin Kaki
Forest Observatory [2021-2022]

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
[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
Low-Cost Reliable Multi-Sensor People Counting
[Since OCT 2020]

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

● **Wael Alsafery** 🇸🇦
Layered Framework Towards Resilient Smart Buildings
[Since JAN 2021]

● **Yaser Awwad** 🇮🇹
Video Analytics for Anomaly Detection
[Since JUL 2021]

● **Norah Albazzai** 🇸🇦
Augmenting Anomaly Detection with Tiny Cameras
[Since JUL 2021]

● **Suhas Devmane** 🇮🇳
Talking Buildings: Smart Building Pattern of life
[Since OCT 2021]

● **Omar Mousa** 🇸🇦
End-User Development for Linked-Data Observatories
[Since JAN 2021]

● **David Winter** (PT) 🇬🇧
AI-Assisted Personalised Blended Learning for IoT
[Since JUL 2021]

● **Abdulaziz Aljohani** 🇸🇦
Self-Configuring Anomaly Detection IoT Architecture
[Since JUL 2021]

● **Azhar Alsufyani** 🇸🇦
Context-Aware Knowledge-driven Cyber-Physical Security
[Since OCT 2021]

● **Mohammed Alosaimi** 🇸🇦
Evaluation Framework for Anomaly Detection
[Since OCT 2021]

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

Annual Summary for 2021

- The research group is continued to grow 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 methods: (1) *Privacy Fluid,* (2) *Data Observatories,* (3) *ResilientSensing.AI,* (4) *Learning Technologies For Internet of Things*.
- Eight PhD students and an MPhil student have started projects across these themes this year.
- Create a brand-new Smart Home lab with over 100 smart devices.

- Launched the Forest Observatory Interdisciplinary Research program (forest-observatory.org) to bring researchers across the universities and abroad to tackle challenges ranging from poaching, climate change, deforestation, biodiversity and more (Seed-funded through GCRF and EPSRC).
- Started a year-long secondment with Buildings Research Establishment (BRE) funded by PETRAS.
- Received funding from British Council to develop a new MSc module on ‘*Edge Analytics*’ in collaboration with IIT Ropar and IIIT Kottayam.
- Created an IoT Products Library for research and teaching purposes (YouTube Playlist)
- For the latest publications, visit Google Scholar Research Outputs

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:

Privacy Fluid
Data Observatories
ResilientSensing.AI
Learning Technologies For Internet Of Things

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 captures 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. 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)

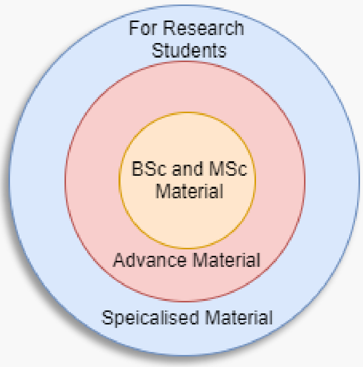
Learning Technologies For the Internet of Things: This theme aims to enhance teaching activities. We aim to understand how to teach IoT for different audiences (from high school to university students and beyond) with different skill levels and innovative tools and techniques. We aim to incorporate conversational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

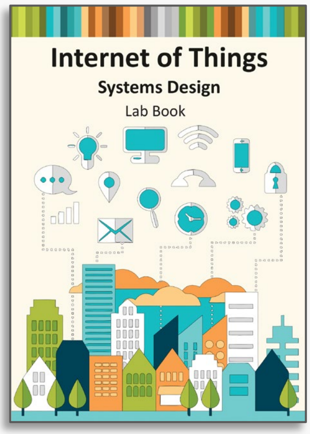
Content: The IoT content is structured under eight themes, namely, (1) *Applications and Use cases*, (2) *Architectures*, (3) *Sensing and Actuation*, (4) *Networking and Communications*, (5) *Data management and analytics*, (6) *Privacy and Security*, (7) *Human Factors and Interactions*, and (8) *Design Strategies and Prototyping*. Each section 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 advanced 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).



Internet of Things: Systems Design
Applications and Use Cases
Internet of Things: Systems Design
Architectures
Internet of Things: Systems Design
Sensing and Actuation
Internet of Things: Systems Design
Networking and Communications
Internet of Things: Systems Design
Data Management and Analytics
Internet of Things: Systems Design
Privacy and Security
Internet of Things: Systems Design
Human Factors and Interaction
Internet of Things: Systems Design
Design Strategies and Prototyping

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 so 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, including research updates, student successes, public engagement, etc.

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 organising and sharing their code through Gitlab (or similar). We actively maintain code repositories produced by each student related to each project.

Group Website (iotgarage.net)

We maintain a group website to disseminate the outcomes of different types of projects to a 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, links to publications, links to code repositories.

Funding Support (On-Going / Completed within 2021)

Going Global India – Exploratory Grants – Edge Analytics

(Co-Investigator)

877673574
Total: 20,000 GBP
Cardiff: 20,000 GBP

This project aims to create a postgraduate module focusing on *Edge Analytics*. The course content will be co-created between the UK & India (including engagement of students & industry) based on world-class course assessment frameworks. Course delivery will follow a hybrid offline/online model. Non-credit bearing content will be trialled with students at the three participating institutions. The proposing team has complementary expertise in - complex systems and IoT (Cardiff), edge computing and sensor networks (IIT Ropar) and IoT analytics (IIIT Kottayam).

EPSRC PETRAS 2 – Internal Strategic Projects and Engagement Fund (ISPEF)

(Co-Investigator)

EP/S035362/1
Total: 74,282 GBP
Cardiff: 74,282 GBP

This project will integrate the outcomes of the PETRAS-funded *Integrity Checking at the Edge (ICE)* project into a prototype operational decision support mechanism at Thales UK. Thales offers an end-to-end Autonomous Logistics Supply that combines an intuitive digital twin interface, unmanned command and control system, and an autonomous, all-terrain Unmanned Ground Vehicle (UGV) system with its own networked communications systems. UGVs are vital for supporting humanitarian rescue and relief efforts in unsafe environments – for example, in regions of natural disaster or conflict settings.

Institutional Sponsorship-International Partnerships

(Principle-Investigator)

(Internal)
Cardiff: 34,349 GBP

EPSRC funds this Institutional Sponsorship award for international partnerships in order to support the pursuit and development of global research partnerships. The primary objective of this project is to develop a better understanding of how to design and deploy a sustainable IoT network in a remote jungle environment with harsh conditions. We want to understand what kind of IoT network would ideally be suited to establish a forest observatory to enable sustainable sensors data collection and wireless communication. We would like to understand potential network design and topology, estimated costs, energy requirements, and other constraining factors that may need to consider when deploying an IoT network in a jungle.

Scalable Circular Supply Chains for the Built Environment

(Co-Investigator)

EP/V042017/1
Total: 368,095 GBP
Cardiff: 424,033 GBP

This project will demonstrate how one of the largest industries in the UK can utilise a digital platform to harness the benefits of a sustainable circular supply chain to reduce waste, increase safety, and promote greater fiscal responsibility. The Architecture, Engineering & Construction (AEC) sector plays a crucial role in the UK economy by employing over 2 million people to deliver civil engineering projects that underpin our economic growth. One of the biggest contributors to GDP, the ACE sector represents commercial activity spanning individual contractors through to multi-national corporations collaborating through complex asset distribution networks that account for over £10 billion of trade. This project is a collaboration between Cardiff University and Newcastle University.

EPSRC PETRAS 2 - Opportunity Fund

(Principle-Investigator)

EP/S035362/1
Cardiff: 133,833 GBP

This secondment aims to explore how to add layers of resilience to built environments in the Internet of Things (IoT) context. Smart built environments such as smart homes and office buildings heavily depend on IoT systems to reliably sense and monitor their surroundings. Such dependencies also create high risk. Malicious parties could tamper these IoT devices and systems to report incorrect data to control systems. Such unreliability could create a significant risk (even be catastrophic and fatal) to build environments. Therefore, we need to develop a resilient built environment by creating multiple layers of resiliency. This means that even a malicious party may manipulate some IoT devices (or some part of the IoT system), the rest of the IoT system will be able to get together and protect and maintain its functionality with minimum impact on the built environment.

GCHQ National Resilience Fellowship

GCHQ

(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)

Department for Digital, Culture, Media & Sport

(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 future factories and water treatment systems, 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 consumers 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.

Altifio

Altifio is an innovation hub. It aims to discover or create innovative technology solutions for companies to help them in a variety of ways, such as competing in a new market, acquiring customers at lower costs, or developing new tools to do work more efficiently.

Airbus Group

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

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.

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.

Danu Gurang Field Center

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

Exalens

Exalens protects digital manufacturing against downtime and safety incidents through early warning of both system malfunctions and cyber security breaches. With ground-breaking cyber-physical security analyst AI, manufacturers enhance their operational resilience with automated incident detection and response.

Government Communications Headquarters

GCHQ is an intelligence and security organisation responsible for providing signals intelligence and information assurance to the government and armed forces of the United Kingdom.

Innovate Trust

Innovate Trust provides support and guidance to disabled people. In addition, Innovate Trust provides support to elderly, young, disadvantaged, and vulnerable members of the local community through our Student Volunteer projects.

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.

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.

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.

Thales

Thales has established a new National Digital Exploitation Centre (NDEC) in Blaenau Gwent. The £20 million site will be used for digital and cyber security training and research facilities, providing lab space for, SMEs and microbusinesses to test and develop digital concepts.

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.

PRIVACY FLUID

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

Researcher: Nada Alhirabi (PhD Student-2018-2023)

Internet of Things (IoT) applications development and design process is more complicated than others, such as 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 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 efficiently, effectively, and collaboratively develop an interactive design method (facilitate through a tool) that incorporates privacy-preserving techniques into the early phases of the software development life cycle. 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. This project is 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 engineers' capabilities and enhancing privacy knowledge.

PRIVACY PARROT

Partners and Relevant Projects

PETRAS MY DATA FIX

Outcomes

- **[Journal]** Nada Alhirabi, Omer Rana, and Charith Perera. 2021. **Security and Privacy Requirements for the Internet of Things: A Survey**. ACM Trans. Internet Things 2, 1, Article 6 (February 2021), 37 pages. PDF BIB
- **[Demo] PRIVACY PARROT:** Interactive Privacy-Aware IoT Application Design Tool (*Work-in-progress*) VIDEO

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 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 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 is 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 enhancing privacy knowledge. PRIVACY CAPTAIN uses a knowledge-based AI technique to review a given IoT system design and assist on how optimally applying privacy patterns.

Partners and Relevant Projects

PETRAS

Outcomes

- **[Journal]** Lamya Alkhariji, Nada Alhirabi, Mansour Naser Alraja, Mahmoud Barhamgi, Omer Rana, and Charith Perera. 2021. **Synthesising Privacy by Design Knowledge Toward Explainable Internet of Things Application Designing in Healthcare**. ACM Trans. Multimedia Comput. Commun. Appl. 17, 2s, Article 62 (June 2021), 29 pages. 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 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 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 is 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.
- We aim to develop a series of reusable privacy-preserving components that can be easily adapted into the IoT application development process based on the above findings.
- Develop a framework to examine and operationalise each privacy-preserving component in order to quantify them towards developing a gamification-based education method.

Partners and Relevant Projects

PETRAS

Outcomes

- **[Journal]** Atheer Aljeraisy, Masoud Barati, Omer Rana, and Charith Perera. 2021. **Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective**. ACM Comput. Surv. 54, 5, Article 102 (June 2022), 38 pages. PDF BIB DATA SET

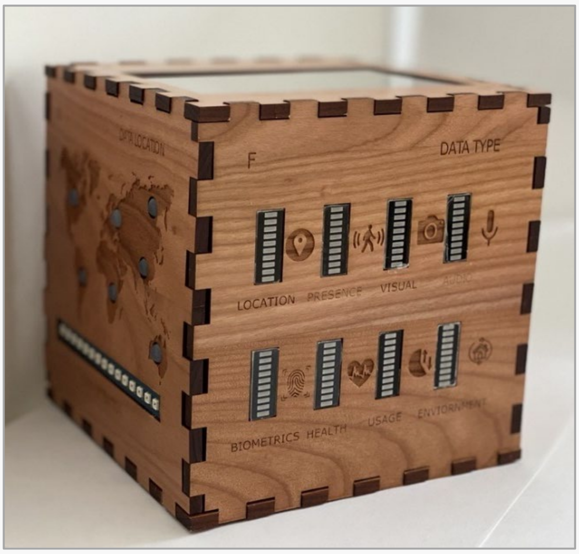
PRIVACY FLUID

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 functional and usable devices is a key challenge in the Internet of Things (IoT) industry. The primary user interface in traditional desktop and mobile contexts 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 increasing 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, **Privacy-Aware Internet of Things Notices In Shared Spaces: A Survey**, Technical Report, 2020 PDF BIB
- **[Demo]** **PrivacyCube:** Interactive Privacy-Aware IoT Application Design Tool (*Work-in-progress*) VIDEO

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 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 convenient and efficient 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 share 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 adults 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 with 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

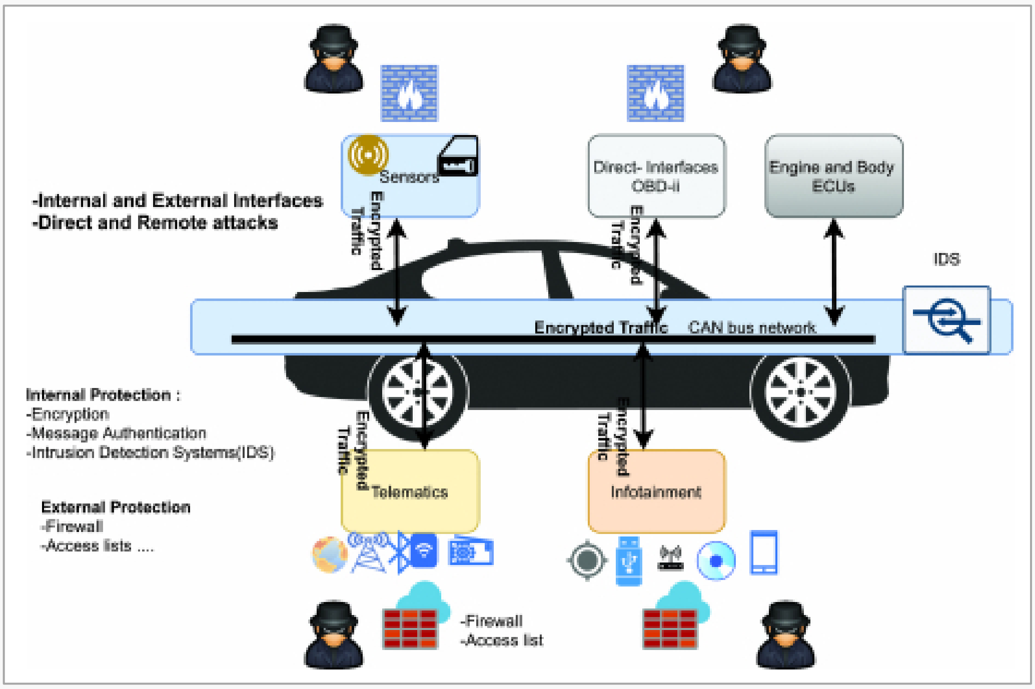
Partners and Relevant Projects

Innovate Trust PETRAS

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 aim 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

ipoint PETRAS

Outcomes

- **[Journal]** Emad Aliwa, Omer Rana, Charith Perera, and Peter Burnap. 2021. **Cyberattacks and Countermeasures for In-Vehicle Networks**. ACM Comput. Surv. 54, 1, Article 21 (January 2022), 37 pages. PDF BIB

*Lead by Omer Rana

RESILIENTSENSING.AI

Low-Cost Reliable Multi-Sensor People Counting Tool Kit For Remote Sanitary Facility Monitoring

Researcher: Dom Fonseca (MPhil Student-2020-2022)

This project focuses on developing a low-cost multi-sensor people counting 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). All the sensor data collected by all the sensors are currently 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 faced 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.

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.

RESILIENTSENSING.AI

Integrity Checking at the Edge

Team: Matthew Nunes, Pete Burnap, Charith Perera (2019-2022)

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. In contrast, 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. 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. 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.

- 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

PETRAS

Outcomes

- [Demo] **ICS-ViZ:** Integrity Checking at the Edge: Visualising cyber Attacks towards enhanced Decision-Making Experience (*Work-in-progress*) VIDEO

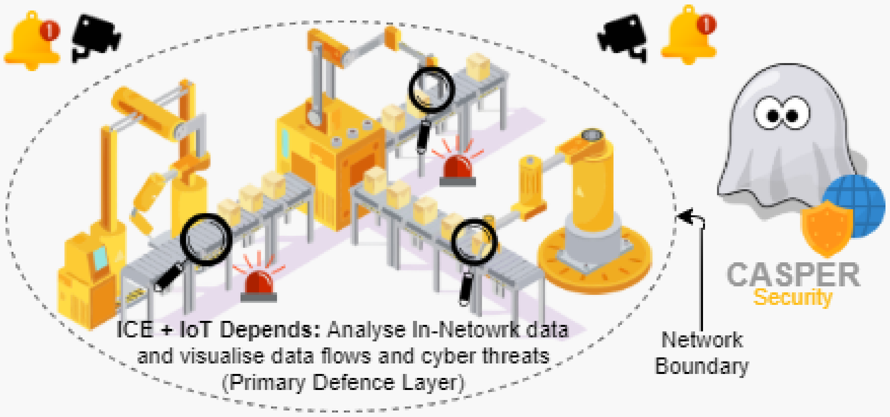
RESILIENTSENSING.AI

Context-Aware Security 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 have shown that a variety of new vulnerabilities have occurred due to this transition, leading to an increase in the targeting of ICPSs. Key findings from Verizon's 2020 data breach report show that 381 data breaches (10% of total) are against industrial systems, not all 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:


ICE + IoT Depends: Analyse In-Netowrk data
and visualise data flows and cyber threats
(Primary Defence Layer)
Network
Boundary
CASPER
Security

- 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 experimental evaluations.

Partners and Relevant Projects

PETRAS GCHQ EXALENS®

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

RESILIENTSENSING.AI

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 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. Even if a temperature sensor transmits a high value, it can trigger an open window. Currently, available solutions 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 at midnight while spoofing the smart plug and preventing 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 cyber-physical anomaly detection techniques in 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 from an independent IoT sensor network.

Partners and Relevant Projects

PETRAS bre GCHQ

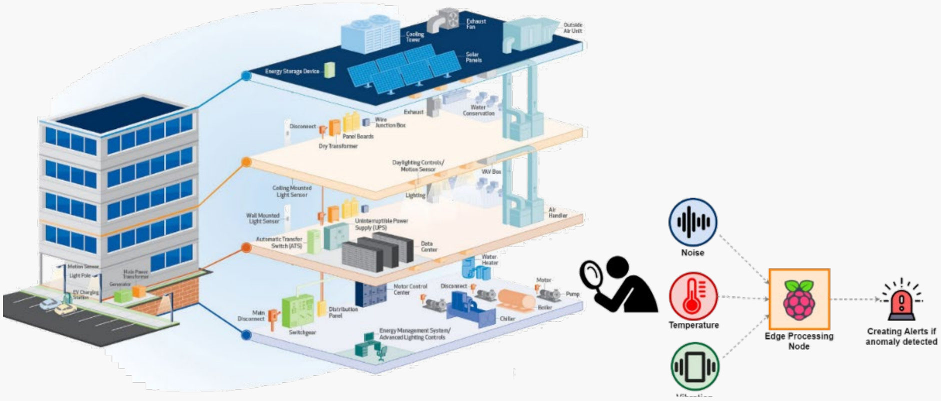
Outcomes

- **[Technical Report]** Yasar Majib, Omer Rana Charith Perera, **Cyber-Physical Behavior of Smart Home: Survey**, Technical Report, 2022 PDF

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, these secondary IoT sensors would use a secondary network (e.g., Bluetooth, ZigBee) and stay as an air-gapped system to reduce 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.

Partners and Relevant Projects

PETRAS

Outcomes

- [Journal] Hakan Kayan, Yasar Majib, Wael Alsafery, Mahmoud Barhamgi, Charith Perera, **AnoML-IoT: An End To End Re-Configurable Multi-Protocol Anomaly Detection Pipeline for Internet of Things**, Elsevier Internet of Things, Volume 16, 2021. PDF BIB CODE CODE
- [Technical Report] Yasar Majib, Yuhua Li, Behzad Momahed Heravi, Sharadha Kariyawasam, Charith Perera, **Detecting Anomalies within Smart Buildings using Do-It-Yourself Internet of Things**, Technical Report, 2021 PDF CODE

RESILIENTSENSING.AI

Video Analytics towards Anomaly Detection on Edge for Smart Cities

Researcher: Yaser Abu Awwad (MPhil Student-2021-2022)

Camera’s are widely used in the smart city domain to monitor and supervise environments such as road traffic, office buildings, smart homes, etc. However, most commercial (off-the-shelf) camera systems can only detect a few sets of predefined objects (e.g., person and vehicles) and behaviours. Most of these camera systems are designed for streaming the video to the cloud. In a limited number of systems, cameras themselves may do minor edge processing tasks such as detecting people and vehicles. Such primitive capabilities are not sufficient to facilitate more complex use-cases below. Further sending video streams to the cloud without processing may not be useful and require significant network bandwidth, especially when the systems need to be scaled for thousands of cameras. Further, not all video frames are worth processing in-depth.

Farms in Monmouthshire want to prevent/detect crime and safeguard lone workers. The objective is to prevent thefts of machinery and livestock and monitor farmers to ensure their safety, particularly whilst working alone at remote locations on the farm. Raglan Castle in Monmouthshire wants to detect vandalism and ensure children's safety from monitoring any children climbing walls or performing any dangerous activities so that the local staff can intervene in a timely manner. Blaenau Gwent wants to monitor their car parks to understand how they are being used as well as how to better incentify the use of public transport (e.g., monitor how many people get off from a vehicle). Another important aspect is to detect anti-social behaviour using bus stop cameras. All the use cases require some level of anomaly detection capabilities beyond what off the shelf systems can provide.

This project combines pre-trained object detection and computer vision models to detect complex anomaly behaviours using cameras. Each pre-trained model plays a crucial role in a particular scene to extract information and actions to be incorporated together to detect different types of anomalies. Moreover, this project is not focused on processing a full video in real-time. It aims to pick up signals of potential anomalies through lightweight edge processing (e.g., a farm animal moving towards an unusual area). Once the signals are detected, systems will conduct in-depth analysis using their full capabilities by feeding the selected frames into several different pre-trained computer vision models. The objective of this project is as follows:

- Conduct a literature review on anomaly detection from camera feeds image/video and explore the types of anomalies.
- Measure trade-offs of processing videos fully and partially on edge and in the cloud.
- Explore the factors that impact anomaly detection performance in terms of environment and in-the-wild challenges, such as lighting, angle, camera resolution and other factors.
- Develop a system that can automatically adapt and decide which anomalies should be monitored on edge to pick the early signals related to a given use-case (i.e., deployment) to improve overall performance and accuracy.
- Develop a technique to detect anomalies using off-the-shelf cameras by applying existing deep learning and computer vision techniques.

Partners and Relevant Projects

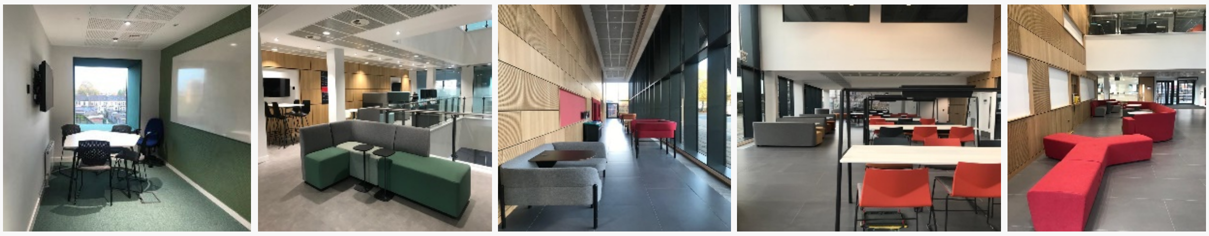
UtterBerry® CISCO BT

RESILIENTSENSING.AI

Sensing as a Service within Buildings Towards Data-Driven Collaborative Service Design

Researcher: Wael Alsafery (PhD Student-2021-2025)

University buildings are unique given they partly act as office buildings and partly as semi-public buildings. There are permanent office spaces for staff members (academic, research students, technical staff, etc.). On the other hand, there are a large number of taught students maybe visiting and temporarily occupying the building. They may use the building for a variety of different activities such as individual work, group work, meetings, socialising, and so on. Modern university buildings are built having these requirements in mind at the design stage by incorporating different types of spaces to facilitate these students and their needs. However, there aren't any follow-ups being carried out to measure these spaces' actual utilisation after the building is commissioned and handed over to the University.



This project is conducted within the Abacws, the newly built home for Computer Science and Mathematics students at Cardiff University. It contains a number of different types of spaces that are dedicated to facilitating taught students, research students, and staff members. Not all modern buildings, including Abacws, are augmented with sensors due to additional costs and lack of perceived value and understanding. First, we aim to develop, deploy, and understand which IoT technology is best suited to measure occupant behaviour and usage patterns related to different types of study spaces. Secondly, we aim to understand how to utilise IoT technology to facilitate occupants and the building service design team to communicate better and make collaborative and informed decisions using data-driven approaches to study space utilisation. Even though this project primarily focuses on Abacws, the technology we develop could apply to any building with similar characteristics and requirements (e.g., multi-purpose heterogenous open spaces to facilitate temporary occupants). This project is composed of several objectives:

- Conduct a literature review on how sensor technologies are being used within indoor environments to monitor occupancy and usage of spaces towards improving service delivery.
- Design, develop and deploy IoT sensing technologies to monitor a variety of heterogeneous study spaces and investigate which technologies work best for each space by measuring their performances and trade-offs.
- Develop data-driven approaches to facilitate/mediate informed communication between occupants and the building's service design team towards improving the overall quality of service

Partners and Relevant Projects

RESILIENTSENSING.AI

Self-Configuring Internet of Things Architecture for Context-Aware Anomaly Detection

Researcher: Abdulaziz Aljohani (PhD Student-2021-2025)

Anomaly detection is the process of identifying unexpected items or events in data sets, which differ from the norm. It is a well-investigated area within research communities, and however, anomaly detection using IoT sensor data is comparatively unexplored. In order to develop, IoT sensor-based anomaly detection solution, engineers require significant technical knowledge (e.g., which algorithms to use, how to set parameters, etc.) and domain knowledge (e.g., agriculture, built environments, usual patterns within a given context, etc.). Recently, some commercial solutions (e.g., Microsoft Anomaly Detector) are being developed to simplify the development process by allowing engineers to use black-boxed anomaly detection algorithms with few configurable parameters (i.e., sensitivity, max window size, max anomaly ratio).

We believe that much more complicated contributing factors need to be considered when deploying anomaly detection systems. Further, even though we may know some of the contributing factors during design time, we may not know how to configure a system until we deploy the anomy detection system in a given context. For example, IoT devices have limited resources (e.g., energy, memory, computing resources) and may have shared responsibilities (i.e., not dedicated to anomaly detection). As a result, which devices would be available to perform anomaly detection may not be known beforehand. Further, the heterogeneity of IoT application scenarios makes it infeasible to find one generalised anomaly detection technique that works for every possible IoT architecture. Additionally, the could be competing requirements such as privacy vs performances that need to be managed. We believe that the best way to handle these challenges is to develop a self-configurable anomaly detection system that can configure the above-mentioned configurable parameters at runtime and adapt to the given context. We propose FedBio-IoT, a federated self-configuring IoT architecture for context-aware anomaly detection in this project. FedBio-IoT is based on nature-inspired algorithms that use the concept of evolutionary algorithms and swarm intelligence to monitor, configure, adapt, and change the federated IoT architecture according to the population's behaviour and biological evolution from one generation to the next. We aim to investigate how to reduce the technical and domain expertise engineers require and reduce trial-and-error guesswork required during the development stage. This project is composed of several objectives:

- Conduct a literature review on anomaly-detection techniques, their characteristics and configurable properties.
- Study the capabilities of a wide range of swarm-intelligence algorithms that can be used in self-configuring IoT architecture and examine their strengths and weaknesses.
- Evaluate the performance of self-configuring IoT architecture for context-aware anomaly detection based on swarm intelligence through experimental evaluations in different IoT application scenarios.

Partners and Relevant Projects

PETRAS GCHQ EXALENS

RESILIENTSENSING.AI

Explore the Role of Tiny Cameras Towards Augmenting Anomaly Detection within Built Environments

Researcher: Norah Albazzai (PhD Student-2021-2025)

Modern smart built environments are Cyber-Physical Systems (CPS) in nature. CPSs are composed of physical systems (hardware), software systems and potentially other systems (e.g., human systems). In the cyber world, anomalies are detected through analysing network packets. However, the cyber-physical world requires a different approach to monitor both network and physical worlds. An anomaly is an observation that does not conform to a normal pattern. Anomalies within built environments include intrusion, fire, variation in power consumption, unusual activation of smart devices, abnormal living patterns and so on. Traditional physical anomaly detection systems (e.g. temperature sensor monitoring afire through temperature variations) use simple sensors (temperature, humidity, vibration, motion). For example, an open window has been detected using a temperature sensor. However, as the complexity of the anomalies increases, the achieved results become less accurate. In addition, traditional sensors can be affected by noises produced by the surrounding environment. Another limitation of traditional sensors is that they can only detect measurable properties, and simple sensors cannot detect some parameters. Cameras are an advanced type of sensor that has been used mainly in surveillance tasks. Historically, in anomaly detection, the utilisation of camera sensors is limited due to multiple factors such as increased costs, comparatively larger, and privacy issues. However, tiny cameras are becoming cheaper and less than 1 inch in length.

This project investigates how to augment sensor-based anomaly detection systems with tiny cameras in a privacy-aware manner. For example, to reduce privacy invasion, camera sensors will only be activated to observe a scene if another sensor (e.g. temperature, motion) produces an abnormal result. Further, we believe tiny cameras can be used to train other senors over time to improve their anomaly detection capabilities and reduce the involvement of tiny cameras in decision-making, therefore reducing privacy concerns. This project use pre-trained object detection and computer vision models to detect anomalies and correlate them with other sensor data to improve the overall performance of the anomaly detection system. The project has the following main objectives:

- Conduct a literature review on camera systems to explore the role of the camera as a sensor in the context of anomaly detection in built environments.
- Investigate how integrating sensor-based anomaly detection with low-cost cameras can affect the overall performance.
- Identify the capabilities and limitations of the tiny camera sensor and the deployment challenges.
- Investigate how the tiny camera can be used to (re)train other sensors over time and enhance their performance.
- Measure the trade-offs between privacy and the utility of the proposed anomaly detection system within built environments.

Partners and Relevant Projects

PETRAS bre

Context-Aware Knowledge-Driven Cyber-Physical Security at the Edge for Smart Homes

Researcher: Azhar Alsufyani (PhD Student-2021-2025)

Smart devices are heterogeneous where each of them has a different set of capabilities in terms of sensing and actuation. To unlock the true potential of self-adaptive smart spaces, these devices should work and collaborate by sharing their capabilities to achieve a given goal. These smart IoT devices should automatically evolve, depending on the needs of users, and adapt to the new contexts/conditions. While smart spaces are advantageous and desirable in many ways, they may be hacked, exposing privacy and security, or rendering the entire area a hostile environment in which ordinary tasks are impossible to do. Therefore, securing smart spaces can be challenging due to device heterogeneity, continuous changes of context, and limited device resources.

This project aims to develop techniques that can dynamically configure a given smart space (i.e., self-adapting) to achieve a goal (i.e., ensuring security and safety of the cyber-physical system) without needing of cloud services (i.e., edge computing). To achieve this, we adopt Monitor-Analyze-Plan-Execute-Knowledge (MAPE-k) method. Some of the investigations we need to carry out are as follows. First, we need to capture information that MAPE-k requires. Some key pieces of static information are smart device capabilities, limitations. For example, devices such as smart vacuum cleaners can move. Another example is webcams which have the capability of taking images. Other important information needs to be continuously updated (e.g., device locations, weather, environment conditions, calendar information). Some updates could be simple as downloading a calendar, whereas others require data analytics (e.g., detect a window open by analysing temperature variations near the window). We expect this knowledge base to be modelled around well-known ontologies (e.g., W3C SSN, W3C BOT). Next, we aim to assess and select open-source frameworks that can analyse a given context and plan the right course of action to achieve the given goal. We aim to combine rule-based systems, e.g., Drools/OpenHAB-Rules and AI planning techniques, e.g., Optaplanner, to implement parts of MAPE-k. We aim to build the demonstrators using OpenHAB. Currently, smart home security solutions focus on network traffic analysis to detect cyber-physical threats using ML/DL technique. This project aims to demonstrate the utility of knowledge-bases systems towards smart home security.

- Conduct a literature review on knowledge-based techniques that are being developed and deployed within the smart home domain with a special focus on cyber-physical security
- Develop a knowledge model to capture all the relevant information required by Monitor-Analyze-Plan-Execute-Knowledge (MAPE-k) loop to enable self-adaptive cyber-physical security.
- Investigate, select and implement the best techniques for each phase within MAPE-k while utilising open-source APIs/frameworks as much as possible.
- Measure the trade-offs of competing techniques and make recommendations of their use
- Develop a series of demonstrators to showcase how knowledge-based self-adaptive systems work in-the-wild in the context of smart homes.

Partners and Relevant Projects

PETRAS bre

RESILIENTSENSING.AI

Talking Buildings: Making Buildings Talk using Adaptable Data Analytics

Researcher: Suhas Devmane (PhD Student-2021-2025)

Modern smart buildings are equipped with IoT sensors to facilitate efficient and effective maintains of buildings. These IoT sensors can be used to measure quite valuable aspects of buildings such as structural health, occupant behaviours, occupant health, and many more towards increasing functionality, comfort, safety, and reducing running costs. Even though much academic work has been done to generate these insights from sensor data, deploying them in the real world is quite challenging due to the simplistic assumption made within academic work. A more viable option is to buy very expensive off-the-shelf solutions from companies specialising in Buildings Management Systems (BMS) or Buildings AI solutions providers. The downside is that these solutions are often highly restrictive in terms of capabilities, extendability and adaptability. For example, we will be required to deploy their sensors exactly as prescribed and require a lot of manual labour to adapt them to new building types and layouts. Further, most of these BMS and AI solutions are designed to be used by domain experts (e.g., estate people who have specialised knowledge on energy standards, sustainability standards and so on).

In this project, we aim to address two key issues highlighted above. First, we will investigate how we could develop a semantic interoperability layer between IoT sensors and data analytics so the analytics could be adaptable for a given building's configuration and layout. We aim to embed the domain knowledge into the system we are building so non-domain experts can use the system to understand better how the buildings are performing. To make the system more accessible, we aim to utilise conversational AI techniques to mediate the communication between the building and the non-experts. By doing this, we aim to give a voice to the buildings so they can communicate with humans in natural language and express how it feels. We envision a future that the buildings will be able to answer its performance-related questions (e.g., Building Research Establishment Environmental Assessment Method (BREEAM)) with the help of IoT sensors. This project has the following objectives:

- Conduct a literature review on the relationship between useful insights and what data types and analytics are required to generate such insights in the context of built environments.
- Extend (or combine) existing building ontologies to develop a semantic interoperability layer between IoT sensors and data analytics so the analytics could be adaptable for a given building's configuration and layout, which can also handle the heterogeneity of IoT sensors.
- Develop a library of adaptable analytics that can generate insights using IoT sensor data while handling heterogeneity in terms of accuracy, reliability, sampling rates, etc.
- Extend the knowledge models further to capture the information related performance-related standards such as BREEAM
- Implement conversational AI-driven chatbot that can facilitate natural language communication between the non-experts and the building itself about buildings performance.

Partners and Relevant Projects

bre

RESILIENTSENSING.AI

Developing an Evaluation Framework for Anomaly Detection within Built Environments

Researcher: Mohammed Alosaimi (PhD Student-2021-2025)

Smart Built Environments are composed of physical and digital infrastructure and aims to improve data-driven decision-making and provide faster and cheaper operation and maintenance (e.g., better whole-life value). They are increasingly more vulnerable to cyber-physical attacks. Anomaly detection techniques are traditionally used to detect any abnormal behaviours. Anomaly detection is a broad field with a rich history where many different techniques have been developed. Out of those, a subset of techniques is focused on real-time anomaly detection. Another subset of techniques focuses on sensor data based on real-time anomaly detection. A key challenge of anomaly detections in the context of built environments is that they are heterogeneous in nature produced by different sensing devices in an unorderly fashion. Some data types are sensor values (e.g. temperature 23C). Other data types could be status or commands (e.g., ON/OFF, 0-1). Some data types could be energy consumption. There are also encrypted data where the actual content is unknown but the metadata available (e.g., packet destination, packet size, frequency co communication). Developing anomaly detection techniques within such context require comprehensive testbeds (or at least datasets collected from a comprehensive testbed). However, currently, no significant emphasis has been put on developing testbeds that can be used to develop, evaluate and compare anomaly detection techniques.

Developing a testbed has always been treated as a secondary task as the development of anomaly detection takes priority. The impact of a testbed's characteristics and properties towards the anomaly detection techniques developed using them is largely unknown and less studied. The fundamental problem with generating synthetic environments is that in order to be realistic, a large amount of data must be generated in order to provide a convincing pattern of life for the simulated network, as well as give the appearance of longevity (the network must not appear to have been recently generated). Further, anomaly detection techniques are challenging to evaluate, especially when developed using different testbeds and conditions. This project aims to develop a comprehensive framework to evaluate the capabilities of a given anomaly detection technique. The project objectives are:

- Conduct a literature review to determine how testbeds are built to evaluate IoT-based anomaly detection techniques.
- Identify characteristics and properties of smart home testbeds that impact the quality of the anomaly detection techniques developed using them.
- Develop techniques to capture, annotate and model data from smart home testbeds to support comparable anomaly detection techniques development.
- Develop techniques to generate synthetics datasets realistic enough compared to real-time live anomaly detection and measure the trade-offs of both approaches.

Partners and Relevant Projects

RESILIENTSENSING.AI

Integrity Checking at the Edge (ICE) for Operational Decision Support (ICE-ODS)

Team: Matthew Nunes, Pete Burnap, Charith Perera, Neetesh Saxena (2021-2022)

This project will integrate the outcomes of the PETRAS-funded “Integrity Checking at the Edge (ICE)” project into a prototype operational decision support mechanism at Thales UK. Thales offers an end-to-end Autonomous Logistics Supply that combines an intuitive digital twin interface, unmanned command and control system, and an autonomous, all-terrain Unmanned Ground Vehicle (UGV) system with its own networked communications systems. UGVs are vital for supporting humanitarian rescue and relief efforts in unsafe environments – for example, in regions of natural disaster or conflict settings.

However, UGVs and their communication systems are vulnerable to cyber-attacks which could disrupt such missions. Most existing cyber attack detection systems only flag the presence of an attack. The current ICE project is working with Thales to understand when and how an attack is occurring and support making decisions such as when and how to act to ensure the continuity of the mission. This is vital as such missions are not as simple as stopping communication or turning the devices off during attack – everything must keep operating, and human interaction in the most strategic and minimal impact way is key. A key outcome of the current ICE project is a visual and interactive method to “dig into” data collected from edge networks – to flag anomalies and potential cyber-attacks – and to enable security operations analysts to collaborate with business continuity teams in a way that enables cyberattacks to be responded to while taking into account the impact of any incident response decisions on the wider system. This is unusual, especially in operational technology settings where the focus is on the safety of the system. The aims of this project are:

- To co-create a practical and impactful toolkit with Thales that translates the outcomes of the ICE project into a living, breathing context that has major life-critical safety and cybersecurity implications. Thales are supporting integration through access to real UGV testbeds and leading workshops with CU to capture insider knowledge on possible responses to cyber threats.
- To validate the outcomes of the ICE project in a real-world setting and gain end-user feedback in a real-world scenario.
- To create a permanent showcase demonstrator of the outcomes of PETRAS-funded research at a major private sector R&I investment location – Thales Ebbw Vale. This is a £25m+ facility that aims to transform the region around into a hotbed of economic activity.
- To identify and mitigate vulnerabilities to cyber-attacks within the showcase demonstrator, thereby ensuring that the demonstrator represents a benchmark testbed for cyber risk visualisation and assessment.

Partners and Relevant Projects

THALES PETRAS

Data Observatories

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

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

Cities are increasingly augmented with sensors through public, private, and 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-ups and small businesses to create novel products and services by utilising the datasets to generate additional economic value. Currently, 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;

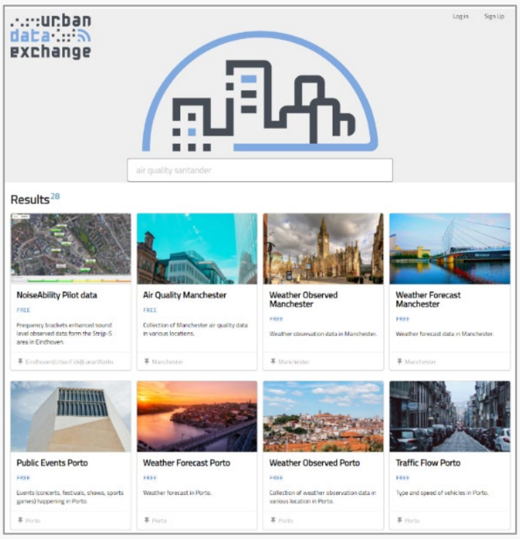
(i) Difficulties in pricing which leads to higher prices (per dataset),

(ii) Higher network communication and bandwidth requirement and

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

This project proposes 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 is 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 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.



Results 28

NoiseAbility Pilot data
FREE
Frequency brackets enhanced sound level observed data form the Strijp-S area in Eindhoven.
Eindhoven|UrbanTide|LunarWorks

Air Quality Manchester
FREE
Collection of Manchester air quality data in various locations.
Manchester

Weather Observed Manchester
FREE
Weather observation data in Manchester.
Manchester

Weather Forecast Manchester
FREE
Weather forecast data in Manchester.
Manchester

Public Events Porto
FREE
Events (concerts, festivals, shows, sports games) happening in Porto.
Porto

Weather Forecast Porto
FREE
Weather forecast in Porto.
Porto

Weather Observed Porto
FREE
Collection of weather observation data in various location in Porto.
Porto

Traffic Flow Porto
FREE
Type and speed of vehicles in Porto.
Porto

Partners and Relevant Projects

SYNCHRONICITY

CATAPULT Digital

Outcomes

- **[Technical Report]** Naeima Hamed, Andrea Gaglione, Luca Iadema, Alex Gluhak, Omer Rana, Charith Perera, **Quarriable Smart City Internet of Things Data Marketplaces: A Case Study**, Technical Report, 2021 PDF CODE CODE CODE VIDEO

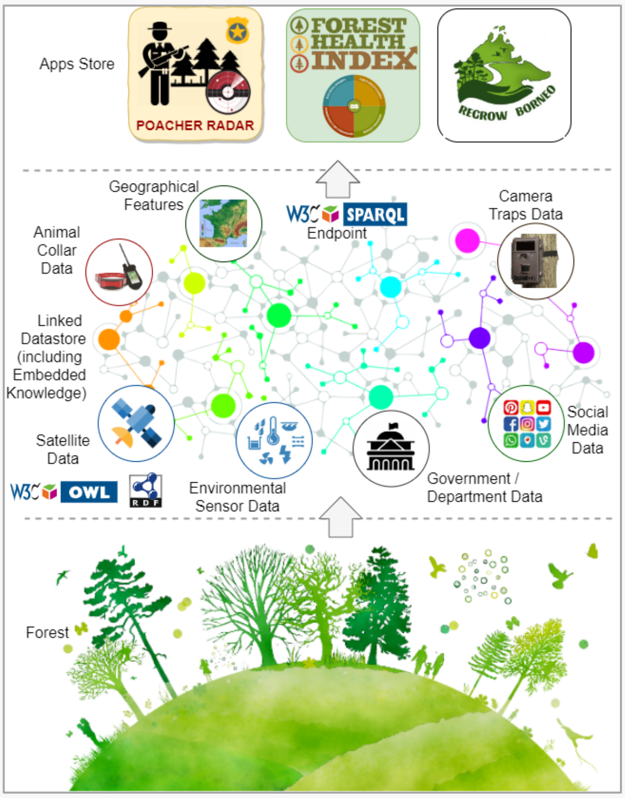
Data Observatories

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 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 will occur in the future. Our data-driven prediction models will tell areas and time frames that are highly likely to have 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 collaborates 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. 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 aim 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.



Partners and Relevant Projects

DANAU GIRANG • FIELD CENTRE •

Outcomes

- **[Technical Report]** Naeima Hamed, Omer Rana, Pablo Orozco-terWengel, Benoît Goossens, Charith Perera, **Open Data Observatories**, Technical Report, 2021 PDF

Data Observatories

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 jungle 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 examines frequencies and develops protocols that 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 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 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 vehicles in the wildlife reserve after 19:00 are unauthorised.

Remote camera trap battery monitoring – Messages for monitoring 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 users to define a refresh timeframe with which they are comfortable.

Partners and Relevant Projects

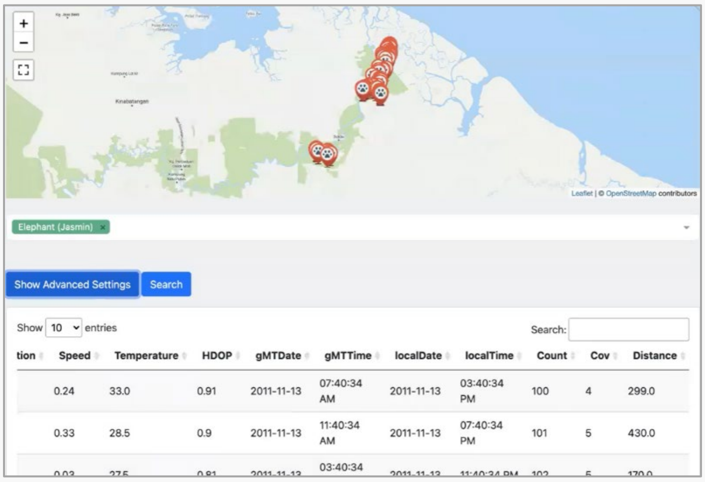
DANAU GIRANG • FIELD CENTRE

Making Linked Data Accessible through End-User Development for Bioscience Researchers in the Context of Micro Observatories

Researcher: Omar Mussa (PhD Student-2021-2025)

Linked-Data is a set of design principles to structuring data in an interconnected system to make them accessible and machine-readable. When the data gets linked, it becomes traversable, and nodes will be linked through relationships. Linked Data breaks down the information silos that exist between various formats and brings down the fences between various sources. It facilitates the extension of the data models and allows easy updates. As a result, data integration and browsing through complex data become easier and more efficient. In addition, Linked-Data follows a specific schema that makes it easily understood by machines and humans alike. Unfortunately, even though the data is human-readable, it is challenging for non-expert users to retrieve it because Linked-Data will need a good understanding of Semantic queries. Learning Semantic query (i.e., SPARQL Query Language) is not easy for non-expert users, and it is unlikely end-users will use it.

This project makes the Linked-Data more accessible and allows the non-technical end-user (e.g., Bioscience Researchers, wildlife conservationists) to perform their job more efficiently through developing novel interfaces. More specifically, we aim to combine GUIs with conversational AI techniques to facilitate efficient and effective linked data retrieval for non-technical users. The naive user will not need to have any experience using SPARQL or any other query language to retrieve the data. Besides, expert users will perform their job easier in less time. This project composes three main objectives:



Show 10 entries   Search:

tion	Speed	Temperature	HDOP	gMTDate	gMTTime	localDate	localTime	Count	Cov	Distance
	0.24	33.0	0.91	2011-11-13	07:40:34 AM	2011-11-13	03:40:34 PM	100	4	299.0
	0.33	28.5	0.9	2011-11-13	11:40:34 AM	2011-11-13	07:40:34 PM	101	5	430.0
	0.03	27.5	0.81	2011-11-13	03:40:34	2011-11-13	11:40:34 PM	102	5	170.0

- Review existing end-user development techniques on how to make Linked-Data accessible.
- Design and develop a hybrid interface that combines traditional WebGUI with a conversational chatbot to allow non-technical users to efficiently and effectively express data requirements.
- Enhance the user experience by developing novel data visualisations techniques and context-aware predictions that enable end-users to explore data more efficiently and effectively.

Partners and Relevant Projects

Outcomes

- **[Technical Report]** Omer Mussa, Omer Rana, Pablo Orozco-terWengel, Benoît Goossens, Charith Perera, **Making Linked-Data Accessible: A Review**, Technical Report, 2022 PDF

Scalable Circular Supply Chains for the Built Environment

Team: Yingli Wang (PI), Jon Gosling, Omer Rana, Pete Burnap, Charith Perera, Yacine Rezui, Qian Li, Rajiv Ranjan, Aad van Moorsel, Graham Morgan, Ellis Solaiman (2021-2024)

The outcome of this multi-disciplinary industry/academic co-development effort will be to create a scalable, decentralised blockchain environment to enable tracking of reusable materials, parts/components or services to support a circular supply chain for the Architecture, Engineering and Construction (AEC) sector. The academic team in the project will create a digital (software) platform (supporting supply chain tracking and data analytics) to facilitate 5 "R" features, which are: (i) Reuse and Redistribute (ii) Refurbish and Remanufacture; and (iii) Recycle. The outcome will be validated with sector-leaders in AEC, such as HS2, Arup, Celsa Steel and with an SME (SeroHomes). The key transformational contribution of this project is an establishment and assessment of a highly connected circular supply chain that contributes to radical whole lifecycle decarbonisation and waste reduction within an AEC project. We believe the digital (software) platform will also have the potential for commercialisation and possible integration with systems from other AEC suppliers – such as the "Pathway to Zero" tool from SeroHomes (to achieve zero carbon outcomes within a retrofit context). Our strategy to improve impact and usage will involve close consultation and co-development with our industry partners – who will provide use cases and actively work with us to design and realise the software platform and new digitally enabled supply chain models.

We explore four research questions (RQs):

- RQ1: How do we design, execute and govern a circular supply chain (CSC) that is environmentally sustainable and economically viable for the AEC sector?
- RQ2: How do we incentivise organisational actors to participate in a CSC, particularly by increasing transparency of operations within a CSC?
- RQ3: How do we automatically label and subsequently track the whole life-cycle activities of materials/ components/ assets and services to a) provide better insights into their composition and effectiveness at end-of-use, and b) sustain and preserve existing building stock?
- RQ4: How can economic models be developed to support the digital infrastructure that is essential to drive a CSC and sustain it over the lifecycle of an AEC asset?

The main outcomes of the research will be: a) a digital (software) platform that harnesses the potential of multi-layered blockchain (often referred to as "parachain", e.g. in Ethereum Plasma and Polkadot.Network) and the concept of 'material & service passport' to show the circularity potential of materials/components/ assets/ services and enable stakeholders (designers, main contractors, manufacturers and clients) to assess the likelihood for 5R. b) a road map based on the co-developed (with industry) digital platform, to incentivise repeated use and integration of "circularity" within industry-based systems – aimed at influencing a behaviour change in the way that the 5R are considered in the AEC sector and to enable collaborative partnerships to support CSC.

Partners and Relevant Projects

sero ARUP DIGITAL DISRUPTION DXC.technology HS2 RPL Digital KB KATE BAUCHEREL

Data Observatories

Forest Observatory

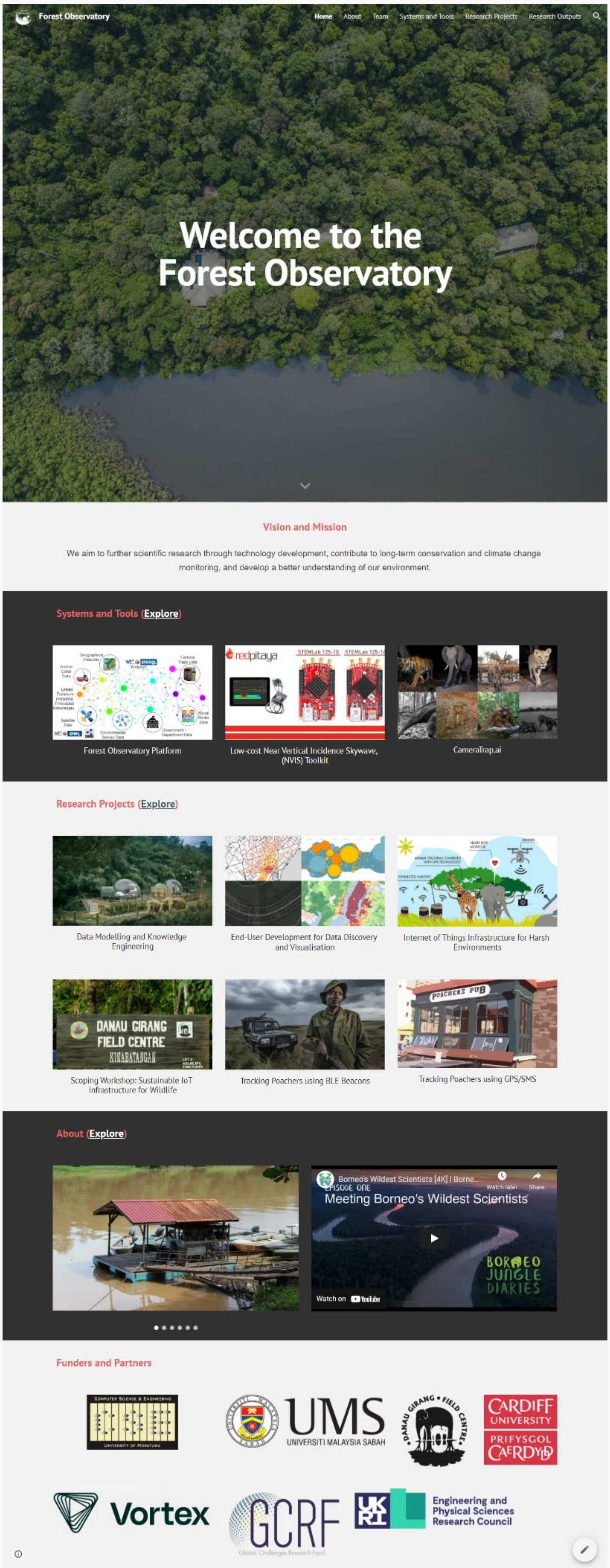
Team: Charith Perera, Omer Rana, Benoit Goossens, Pablo Orozco-TerWengel, Oktay Karakus (2021-Present)

This is a research program seed-funded through different sources over the last few years, such as GCRF Facilitation, EPSRC International Partnerships, and several Cardiff University summer student projects and travel funding. This research program aims to bring faculty and related projects and strategic recourses underutilised and scattered across the University under a coherent theme that would enhance collaborative interdisciplinary research. The research program focuses on fundamental and applied research, which results in usable tools and systems.

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 IoT infrastructure to enable poaching monitoring, we should utilise already collected data sets to develop predictive models to better track poaching activities.

To develop a Forest Observatory, we aim to integrate various data sets collected by the bioscience researchers at DGFC into a unified linked data store. We use semantic data integration techniques while conforming to the data modelling standards (e.g., ontologies) and needs of bioscience research --towards developing a model and novel tools that are exportable to other world areas where poaching is a threat to wildlife conservation.

Visit: forest-observatory.org



Welcome to the Forest Observatory

Vision and Mission

We aim to further scientific research through technology development, contribute to long-term conservation and climate change monitoring, and develop a better understanding of our environment.

Systems and Tools (Explore)

Forest Observatory Platform

Low-cost Near Vertical Incidence Skywave, (NVIS) Toolkit

CameraTrap.ai

Research Projects (Explore)

Data Modelling and Knowledge Engineering

End-User Development for Data Discovery and Visualisation

Internet of Things Infrastructure for Harsh Environments

Scoping Workshop: Sustainable IoT Infrastructure for Wildlife

Tracking Poachers using BLE Beacons

Tracking Poachers using GPS/SMS

About (Explore)

Borneo's Wildest Scientists [4K] | Borne...

EPISODE ONE Meeting Borneo's Wildest Scientists

Funders and Partners

Computer Science & Engineering
University of Moratuwa
UMS
UNIVERSITI MALAYSIA SABAH
DANAU GIRANG • FIELD CENTRE
CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD
Vortex
GCRF
Global Challenges Research Fund
UKRI
Engineering and Physical Sciences Research Council

Learning Technologies

Course Development in Edge Computing and Analytics

Team: Omer Rana, Charith Perera, Nitin Auluck, Sujata Pal, Shajulin Benedict (2021-2022)

Due to the increasing popularity of cloud and edge computing, edge analytics focuses on using machine learning & AI on user-owned devices. Short term benefits: engineers qualified to work on modern edge computing applications in the UK and India, economic benefit & student exchange, and micro-credentials offered online. Long-term benefits include research collaboration between participating institutes, research-based course content, and dedicated online labs. The course content will be co-created between the UK & India (including engagement of students & industry) based on world-class course assessment frameworks. Course delivery will follow a hybrid offline/online model. Non-credit bearing content will be trialled with students at the three participating institutions. The proposing team has complementary expertise in - complex systems and IoT (Cardiff), edge computing and sensor networks (IIT Ropar) and IoT analytics (IIIT Kottayam).

The course titled “Edge Analytics” was chosen to acknowledge the demand and requirements raised from the participating organisations of the proposal. In fact, the market analysis manifested the necessity of organising such a course due to the evolving demand from varied research domains such as healthcare, education, smart cities, governmental, social goodness, and so forth of the Indian/UK market. Before validating the statement, the potential students willing to travel to the UK/India were assessed for their preferences.

Based on the carefully identified partners for the proposal, we are self-assessed to deliver the best among the many other competitors for the proposed course. Due to the team's expertise proposing the course and the huge market demand, we are confident that the course will generate significant interest among students and working professionals.

- There will be faculty visits in which an Indian faculty will visit the UK and vice versa. During these visits, the faculty will observe the various state of the art infrastructure relevant to the proposed course, e.g. visiting the IoT and distributed systems labs. The faculty will have detailed discussions and brainstorming to create a relevant course plan. The discussion and collaboration will continue online after the visits are over.
- Focus on increasing the critical thinking capability of the students in the course plan. This will involve the administration of in-class discussions and take-home assignments.
- We aim to make this course very hands-on with a good amount of laboratory activity and projects. Some of these will involve designing and implementing edge analytics solutions for state of the art real-life applications.

Partners and Relevant Projects

INTERNET OF THINGS GARAGE

iotgarage.net

gitlab.com/IOTGarage

bit.ly/2JMoSd4

@IOTGarageNews