Cardiff Internet of Things Group

Internet of Things Garage

INTERNET OF THINGS GARAGE
Part of Cardiff IOT Group

Internet of Things Research and Teaching: Vision and Mission

Annual Report (2023)

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 focus less on giving theoretical guarantees. Our work aims 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, 2021, 2022

Principal Investigator: Charith Perera

As of 2023, the research group comprised 21 PhD students, 2 MPhil students (and 1 affiliated PhD students)

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]

Wael Alsafery
Layered Framework Towards Resilient Smart Buildings
[Since JAN 2021]

Yaser Awwad
Video Analytics for Anomaly Detection
[Since JUL 2021] [MPhil]

Norah Albazzai
Augmenting Anomaly Detection with Tiny Cameras
[Since JUL 2021]

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

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

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

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

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

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

Omar Mousa
End-User Development for Linked-Data Observatories
[Since JAN 2021]

Abdulaziz Aljohani
Self-Configuring Anomaly Detection IoT Architecture
[Since JUL 2021]

Azhar Alsufyani
Context-Aware Knowledge-driven Cyber-Physical Security
[Since OCT 2021]

Suhas Devmane
Talking Buildings: Smart Building Pattern of life
[Since OCT 2021]

Mohammed Alosaimi
Evaluation Framework for Anomaly Detection
[Since OCT 2021]

Fatmah Alqarni
Learning Privacy and Laws Through AI-Mediated Exploration and Design
[Since APR 2022]

Siyuan Li
Adaptive Mobile Sensing within Buildings
[Since OCT 2022]

Rayan Binlajdam
Forest Health Index
[Since OCT 2022]

Kira Nurse
Tangible Interfaces for Assisting Young People with Neurodiversity
[Since OCT 2024]

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

Annual Summary for 2023

- The research group has continued to grow around three research themes related to the Internet of Things (IoT), with a significant emphasis on build-driven research methods. One PhD student (Kira Nurse) has started projects across these themes this year.
- Nada Alhirabi passed her PhD and her work focused on *Designing Privacy-Aware Internet of Things Applications* (Project). Yaser Awwad passed his MPhil, and his work focused on *Anomaly Detection on the Edge using Smart Cameras under Low-Light Conditions* (Project).
- Several students attended and presented their work at a number of international and national conferences (e.g., Wales Tech Week, Health and Care Research Wales Conference, ACM Ubicomp, SOUPS, ESWC, PETRAS Health Care and Wellbeing, ACM/IEEE IoTDI, Percom2023)
- One BSc student went to DGFC (www.dgfc.life) to gain international experience (Vlog). Mark Butterworth (PhD student) also visited to gain domain understanding and conduct user duties related to their projects (Project).
- We organised the PETRAS Regional Showcase and Networking event. The event was thematically titled “Connected Spaces”. Its primary objective was to create a confluence of various PETRAS projects and interdisciplinary initiatives within the university (Event).
- Charith Perera visited The University of Wyoming-National Park Service (UW-NPS) Research Station as part of a Cardiff University delegation to explore potential research collaborations.
- We received funding from the Google Research Scholar Program to work on Tangible Interfaces for Assisting Young People with Neurodiversity Towards better Understanding Online Harms. Google provides unrestricted gifts to support research at institutions around the world and is focused on funding world-class research conducted by early-career professors.
- We received funding from Novel Computing for UK Defence and Security sandpit for Edgy Organism project to work on Modelling Patterns of Life with 100mW.
- Charith Perera, Yasar Majib, and Hakan Kayan completed the CyberASAP program, attended demo day and presented CASPER Shield (Demo)
- We have received funding from EPSRC PETRAS to develop an Augmented Reality Driven Smart City Demonstrator using Lego towards Public Engagement (Demo).
- For the latest publications, visit Google Scholar Research Outputs News

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), our surroundings (homes), our 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 to develop a shared Privacy Mindset through an AI-mediated assistive layer to reduce 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 during 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.

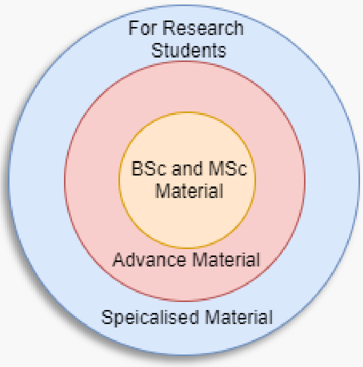
ResilientSensing.AI: This theme explores how we could add layers of resiliency to built environments (and beyond, such as smart city infrastructure) using IoT technologies (e.g., sensors). Smart environments bring both efficiency and convenience; however, they are also vulnerable to attacks and malicious 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 to 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.

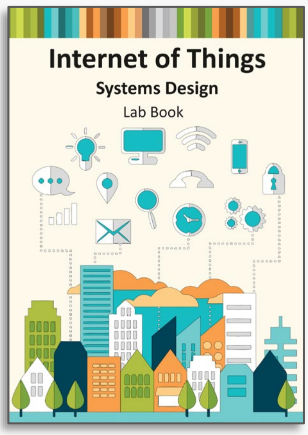
Teaching Vision

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 include 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). Advanced 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 an applied module, students are expected to complete at least six lab sessions. Students are provided with the lab book explaining each practical session step 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 time, through either PhD students or research associates. However, we also use these dissertation projects to initiate some high-risk projects or new research directions. Our students are encouraged (and supported) to produce research output (such as conference, workshop paper, and poster).

Dissemination and Community Engagement

IOT Garage TV (bit.ly/2Md8vJE)

YouTube (and similar platforms) has increasingly become a mainstream content distribution stream that provides large audience access. As a build-driven research group, demonstrations are a key part of our dissemination strategy and increase awareness. Therefore, we have created a dedicated YouTube channel to disseminate our work. We believe visual medium can efficiently and effectively motivate our students to complete their high-quality project work. YouTube videos on our channel also act as a gauge for prospective students. For example, video help students decide what kind of project they 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 other students can understand what has been done and how. This allows next year's 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 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, and PhD, to funded projects. We provide all the relevant information under each project, including team members, funder, partners, project demos, publications links, and code repositories.

Funding Support (On-Going / Completed within 2023)

(Co-Investigator)

EP/Y030133/1
Total: 1,409,560 GBP
Cardiff: 337,393 GBP

EPSRC Edgy Organism

The Edgy Organism project aims to develop electronic surveillance systems capable of detecting and alerting anomalous behaviour or identifying individuals who pose a threat in crowded public spaces. The challenge lies in creating systems that are minimally intrusive, operate with limited supervision and power, and can adapt in remote or unknown locations for extended periods. To achieve these goals, the project proposes integrating spiking neural network (SNN) technology into low-power neuromorphic hardware. Overall, the Edgy Organism project aims to revolutionise surveillance systems by leveraging spiking neural network technology and neuromorphic hardware to create autonomous, low-power, and efficient monitoring systems capable of detecting and reacting to anomalous behaviour in various real-world scenarios.

(Principle-Investigator)

EP/S035362/1
Total:: 15,000 GBP

EPSRC PETRAS 2 Event Support Grant (PESG)

We received funding from PETRAS Center to hold an event with the primary purpose of enhancing Knowledge Exchange (KE) and bolstering the impact of research within the PETRAS community. This initiative is key to promoting dialogue, encouraging networking, and building a community that extends beyond academia. By bringing together academics, industry experts, and local community members, the event seeks to catalyse new partnerships and potential grant applications, aligning with the Centre's goals of enhancing dissemination, impact, and engagement in PETRAS-funded projects. This gathering represents a significant step in advancing collaborative research and expanding the reach of impactful studies.

(Principle-Investigator)

EP/S035362/1
Total:: 5,000 GBP

EPSRC PETRAS Demonstrator

Our project combines LEGO and augmented reality (AR) to create an interactive showcase for PETRAS projects. Users can explore these projects through an AR interface linked to a LEGO Smart City Demonstrator. Evolving from earlier concepts, our accessible technology invites everyday software engineers to engage in this immersive experience. With a long-term goal of enhancing educational tools in smart city learning, we collaborate with architectural experts to ensure a realistic and engaging cityscape.

(Principle-Investigator)

Total:: 60,000 USD

Google Research Scholar Program

This project focus on Tangible Interfaces for Assisting Young People with Neurodiversity Towards better Understanding Online Harms. The project addresses the vulnerability of individuals, particularly the young and those with special educational needs, in the ungoverned internet landscape. It aims to develop specialised tools to enhance their online safety. Utilising visual supports proven effective in education and online safety, the project proposes a tangible user interface with visual indicators to help these groups better understand and navigate online risks. The focus is on co-designing and evaluating this interface to protect these vulnerable users.

(Principle-Investigator)
Total: 91,279 GBP

CASPER Shield (CyberASAP Program)

A smart home study carried out by NCC Group and the Global Cyber Alliance recorded more than 12,000 attack attempts in a week, including 2,435 specific attempts to maliciously log into the devices. Once they gain control, they can manipulate the device's capabilities, including network communication, actuation, and sensing. Our project aims to develop and commercialise a resilient cyber-physical anomaly detection framework to detect cyber-physical malicious activities within built environments (i.e., smart homes and buildings). We aim to achieve this by combining heterogeneous data streams, such as external sensor data observations and energy consumption data, with traditional Network Traffic Analysis (NTA) techniques. This commercialisation project aims to explore market potential and develop a proof of concept for the proposed approach.

(Co-Investigator)
Total: 29,989 GBP

UK – Egypt Trans-National Education (TNE) Grant: Edge Analytics 2.0

Due to the popularity of edge computing and IoT, there is a huge interest and demand in the market for skilled professionals. The "Edge Computing and Analytics 2.0" module was chosen to fulfil the demand raised by both industry and academia. We will develop course content based on world-class course frameworks between the UK and Egyptian universities. Joint students and researchers will collaborate to face climate change by building edge applications on smart cities, smart grids, and water and energy management to achieve SDG goals. This project extend the module developed previously.

(Co-Investigator)

EP/V042017/1
Total: 792,128 GBP
Cardiff: 424,033 GBP

Scalable Circular Supply Chains for the Built Environment

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.

(Co-Investigator)

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

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

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.

Partners

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.

Connected Places Catapult

The Connected Places Catapult in the UK fosters innovation in transport and cities. It collaborates with businesses and academia to develop smart technologies, enhancing urban living and creating more efficient, sustainable transportation systems.

Danu Gurang Field Center

Danau Girang is a collaborative research and training facility managed by Sabah Wildlife Department and Cardiff University. Situated in a rich, biodiverse region, it conducts vital research, conservation efforts, and educational programs on local ecosystems and species.

Defence Science and Technology Laboratory

The Defence Science and Technology Laboratory (DSTL) in the UK is a key part of the Ministry of Defence. It focuses on scientific research and technology, enhancing national security and military effectiveness through innovations.

Digital Communities Wales

Digital Communities Wales champions digital inclusion, empowering people and organisations across Wales. They offer training, support, and resources, fostering digital skills and literacy, ensuring everyone can benefit from and participate in the digital world

Exalens

Exalens protects digital manufacturing against downtime and safety incidents through early warning of both system malfunctions and cyber security breaches. Manufacturers enhance their operational resilience with ground-breaking cyber-physical security analyst AI 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.

Google

Google LLC is an American multinational technology company focusing on artificial intelligence online advertising, search engine technology, cloud computing, computer software, quantum computing, e-commerce, and consumer electronics.

His Majesty's Government Communications Centre

His Majesty's Government Communications Centre (HMGCC) in the UK specialises in communication and information systems. It provides secure technology solutions, ensuring government communication integrity and supporting national security with cutting-edge technical expertise.

Innovate Trust

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

Metropolitan Police

The Metropolitan Police Service, based in London, UK, is a crucial law enforcement agency. It maintains public safety, prevents crime, and upholds law and order across the capital, ensuring a secure and peaceful community.

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.

Office of Communications

The Office of Communications, commonly known as Ofcom, is the government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the United Kingdom.

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.

Safehouse Technology

Safehouse Technology Ltd is an End-to-end IoT service provider. Our services are used by councils, health organisations and housing associations to remotely monitor both people who wish to remain independent, and housing stock owned by Councils or Housing Associations.

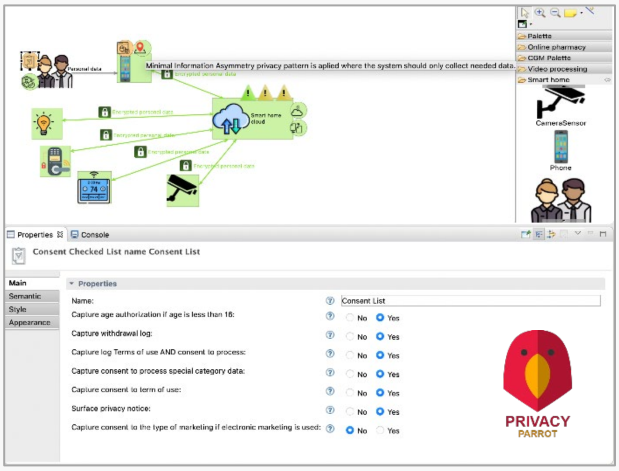
Vortex IoT

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. Due to the above complications, non-functional requirements like privacy tend to be overlooked. Thus far, privacy concerns have not been explicitly considered (i.e., in a 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 (facilitated 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 while creating PbD IoT application designs.

Partners and Relevant Projects

PETRAS MY DATA FIX

Outcomes

- **[Journal]** Nada Alhirabi, Stephanie Beaumont, Dulani Meedeniya, Omer Rana, and Charith Perera, **Designing Privacy-Aware IoT Applications for Unregulated Domains**, ACM Trans. Internet Things, 2024 (in Print) PDF
- **[Journal]** Nada Alhirabi, Stephanie Beaumont, Jose Tomas Llanos, Dulani Meedeniya, Omer Rana, and Charith Perera, **PARROT: Interactive Privacy-Aware Internet of Things Application Design Tool**, ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), Volume 7, Issue 1(1), pp 1–37, March, 2023 PDF BIB SOURCE VIDEO
- **[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), pp 1-37. PDF BIB
- **[Demo]** Nada Alhirabi, Omer Rana, and Charith Perera, **Demo Abstract: PARROT: Privacy by Design Tool for Internet of Things**, In Proceedings of the 2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI) 2022, 107-108 PDF BIB SOURCE VIDEO VIDEO
- **[Poster]** Nada Alhirabi, Stephanie Beaumont, Omer Rana, and Charith Perera, **Privacy-Patterns for IoT Application Developers**, In Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp/ISWC '22), 7-9 PDF BIB SOURCE POSTER

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

Researcher: Lamya Alkhariji (PhD Student-2018-2024)

Internet of Things (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 like privacy tend to be overlooked. 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 engineers' capabilities and enhancing privacy knowledge.

Partners and Relevant Projects

PETRAS

Outcomes

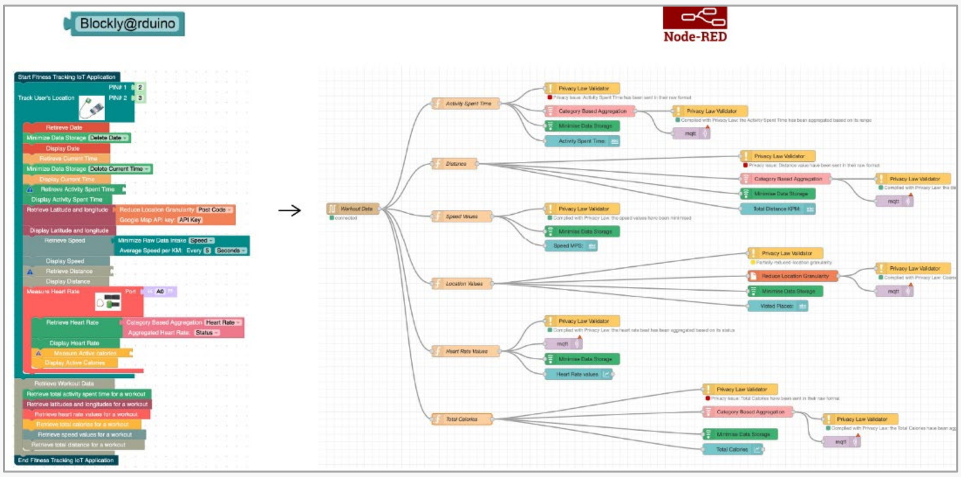
- **[Journal]** Lamya Alkhariji, Nada Alhirabi, Mansour Naser Alraja, Mahmoud Barhamgi, Omer Rana, and Charith Perera. 2021. **Synthesising Privacy by Design Knowledge Toward Explainable Internet of Things Application Designing in Healthcare**. ACM Trans. Multimedia Comput. Commun. Appl. 17, 2s, Article 62 (June 2021), 29 pages. PDF BIB RESOURCES SOURCE
- **[Journal]** Lamya Alkhariji, Suparna De, Omer Rana, Charith Perera, **Semantics-based Privacy by Design for Internet of Things Applications**, Future Generation Computer Systems (FGCS), Volume 138, January 2023 PDF BIB RESOURCES SOURCE
- **[Poster]** Lamya Alkhariji, Suparna De, Omer Rana, and Charith Perera, **Ontology Enabled Chatbot for Applying Privacy by Design in IoT Systems**, In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). Association for Computing Machinery, New York, NY, USA, 3323–3325 PDF BIB SOURCE POSTER

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-2019-2024)

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 software and hardware to cooperate across multiple nodes with different capabilities. Due to the above complications, non-functional requirements like 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 use gamification techniques to motivate software developers to incorporate more and more reusable privacy-preserving components within their IoT applications. This gamification framework is integrated into popular IoT development tools.



Partners and Relevant Projects

PETRAS

Outcomes

- **[Technical Report]** Atheer Aljeraisy, Omer Rana, Charith Perera, Canella: Privacy-Compliant End-to-End IoT Development Ecosystem, Technical Report, 2024 (Under Review) PDF
- **[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 RESOURCES SOURCE
- **[Demo]** Atheer Aljeraisy, Omer Rana, Charith Perera, **Canella: Privacy-Aware End-to-End Integrated IoT Development Ecosystem**, Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp 279-281, 2023 PDF BIB SOURCE VIDEO

PRIVACY FLUID

Interaction Methods for Privacy Preferences Management in Shared Spaces

Researcher: Bayan Almuhander (PhD Student-2019-2024)

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 devices 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.

Partners and Relevant Projects

PETRAS

Outcomes

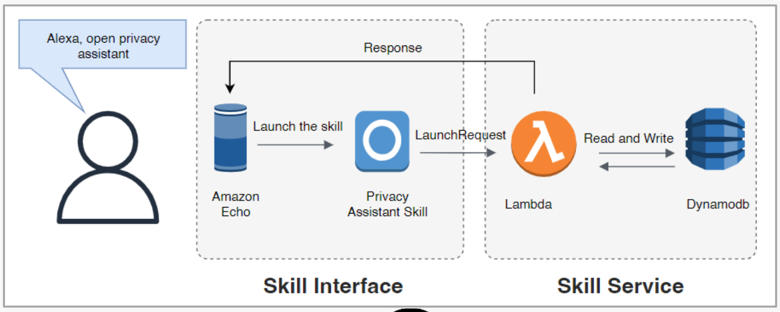
- **[Technical Report]** Bayan Al Muhander, Omer Rana, Nalin Arachchilage, and Charith Perera, **PrivacyCube: Tangible Privacy Interface for Improving Privacy Awareness in IoT** PDF
- **[Journal]** Bayan Al Muhander, Jason Wiese, Omer Rana, Charith Perera, **Interactive Privacy Management: Toward Enhancing Privacy Awareness and Control in the Internet of Things**, ACM Trans. Internet Things, Volume 4, Issue 3, Article No.: 18, pp 1–34 PDF BIB SOURCE
- **[Demo]** Bayan Al Muhander, Omer Rana, Charith Perera, **PriviFy: Configuring Privacy Preferences of IoT Devices using Tangible Interfaces**, 2024 VIDEO
- **[Demo]** Bayan Al Muhander, Omer Rana, Nalin Arachchilage, and Charith Perera, **Demo Abstract: PrivacyCube: A Tangible Device for Improving Privacy Awareness in IoT**, In Proceedings of the 2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI) 2022, 109-110 PDF BIB SOURCE VIDEO 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 are typically convenient and efficient to the environments in which 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 consider that some 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 smart devices to monitor them. Privacy concerns are one of the most significant barriers to using the monitoring device in a smart home. Older adults, especially those with mild cognitive impairment, are vulnerable to privacy violations 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 better configure their privacy and data protection requirements.



Partners and Relevant Projects

Innovate Trust PETRAS

Outcomes

- **[Technical Report]** Reem Aldhafiri, Georgina Powell, Elizabeth Smith, Charith Perera, **Understanding the Privacy Needs of Older Adults Using IoT Devices**, 2024 (Under Review)
- **[Technical Report]** Reem Aldhafiri, Georgina Powell, Elizabeth Smith, Charith Perera, **Voice-Enabled Privacy Assistant Towards Facilitating Successful Ageing in Smart Homes**, 2024 (Under Review)
- **[Conference]** Reem Aldhafiri, Georgina Powell, Elizabeth Smith, and Charith Perera, **Enhancing Privacy Awareness and Digital Skills in Smart Home Device Users with Privacy Assistant: A Conversational Interface for Older Adults,** Cyberpsychology Section Annual Conference, 24-25 July North East 2023
- **[Demo]** Reem Aldhafiri, Georgina Powell, Elizabeth Smith, Charith Perera, **Voice-Enabled Privacy Assistant Towards Facilitating Successful Ageing in Smart Homes,** IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp 343-345, 2023 PDF BIB SOURCE VIDEO

PRIVACY FLUID

Facilitating Novice Software Engineers to Learn Privacy by Design and Privacy Laws through AI-Mediated Exploration and Design

Researcher: Fatmah Alqarni (PhD Student-2022-2026)

Internet of Things (IoT) applications development and design process is more complicated than others, such as desktop, web, or mobile. IoT applications need software and hardware to cooperate across multiple nodes with different capabilities. Due to the above complications, non-functional requirements like privacy tend to be overlooked. One way to address this problem is to better educate novice software engineers about applying privacy-preserving measures in their IoT systems design process. Currently, universities are mostly focusing on teaching cyber security than privacy. Therefore, novice software engineers have very limited knowledge of designing a privacy-aware system, especially when collecting sensitive information using sensors in IoT applications.

In this project, our focus is to develop a technique (formulate as a tool) driven by AI to help novice software engineers to learn privacy and privacy laws by using design activities. The novice engineers will use our tool to implicitly and explicitly help them understand how to incorporate privacy-preserving design features into their IoT system. It is important to note that our focus is on enhancing novice engineers' teaching and learning experience. We do not aim for the proposed technique to be used in the context of industrial software engineering. However, we believe that the knowledge that noise of ranging is gained from interacting with our tool will enable them to apply privacy-preserving measures in an industrial setting. As a community, privacy researchers have developed a large number of privacy-preserving measures identified by various names, such as privacy principles, guidelines, strategies, goals, and patterns (which add up to 168 privacy-preserving measures in total).

Each of these privacy-preserving measures is varied in granularity; some are very high level, and others are low level (close to implementation). Despite investing a significant amount of resources over many years (e.g., privacypatterns.org, privacypatterns.eu), there aren't any unified mechanisms at the moment to help novice software engineers learn how to apply those privacy-preserving measures in their designs in a meaningful way. One of our key objectives is to encapsulate all this knowledge into a tool where novice engineers will incrementally learn how these heterogeneous sets of privacy-preserving measures could be potentially used to preserve privacy and comply with privacy laws. This project has three main objectives:

- Conduct literature review on intelligent design tools and how they implicitly and explicitly contribute to enhancing the understanding of the domain knowledge of the end users.
- Develop a technique that highlights privacy risks and explains what kind of privacy preserving meassure could be applied in a given context (i.e., IoT system Design) while allowing novice software engineers to learn more about privacy and legal compliance better.
- Evaluate the efficiency and effectiveness of the proposed techniques as well as scalability, extendibility, usability and so on.

Partners and Relevant Projects

PETRAS

Outcomes

- **[Technical Report]** Fatmah Alqarni, Omer Rana, Charith Perera, **Intelligent Design Techniques Towards Implicit and Explicit Learning: A Systematic Review**, 2024 PDF (Under Review)

Tangible Interfaces for Assisting Young People with Neurodiversity Towards better Understanding Online Harms

Researcher: Kira Nurse (PhD Student-2023-2026)

The Internet has become ubiquitous – most people are now connected to it via many different types of devices to consume the various services it offers. However, the Internet is not governed by any authority and continues to operate with very limited mechanisms to police, govern or control either service providers or consumers. Such environments allow malicious entities to thrive and take advantage of vulnerable people. According to the UK Government Online Harm White Paper, nearly nine in ten UK adults and 99% of 12 to 15-year-olds are online. Out of all the groups, older (65+) and younger people are the most vulnerable on the Internet. Young people with special educational needs (for example, autism, dyslexia, and attention deficit hyperactivity disorder, ADHD), are particularly vulnerable. Young people with these conditions can find it more challenging to understand information and intent, remember essential information such as passwords, and attend to and monitor risks. Current tools and techniques developed in the context of protecting individuals from online harm are not designed with these vulnerable groups, such as young people with special educational needs, in mind. We believe that more specialised tools/techniques must be developed in collaboration with stakeholders to better inform and protect these vulnerable groups from online harm. Our project is one step towards this aim.

There is evidence that young people with special educational needs benefit from visual supports. They can help young people with conditions such as autism, ADHD, and dyslexia to break down barriers related to verbal communication, attention, monitoring, and working memory. They are often used in educational settings to help support learning, understanding, and retention of information. They are also beginning to emerge in the context of online safety. For example, Ambitious About Autism and the National Society for the Protection of Cruelty Against Children (NSPCC) recently published a visual handbook for young people with special educational needs about interacting with friends and strangers online. Based on the above evidence, we hypothesise that a tangible user interface with visual indicators could help young people with special educational needs to better understand how the Internet works and how online services use their data and to be mindful of common online harms. In this project, we aim to co-design, develop and evaluate the effectiveness of a tangible user interface that could help young people with special educational needs (focusing initially on autism, dyslexia and ADHD) and their family members. This project has three main objectives:

- Can a tangible user interface with visual indicators help young people with autism, dyslexia or ADHD to better understand how the Internet works, how online services use their data, what online harm and privacy risks are, and develop a better understanding towards protecting themselves?
- Can a tangible user interface with visual indicators be used by young people with autism, dyslexia or ADHD and their family members to explore, learn and improve their privacy and online harm awareness together? How effective would such an approach be?
- What experiences can a tangible user interface offer that traditional web/mobile computing screen-based interfaces cannot? What are the pros and cons of tangible user interfaces for young people with autism, dyslexia or ADHD and their families?

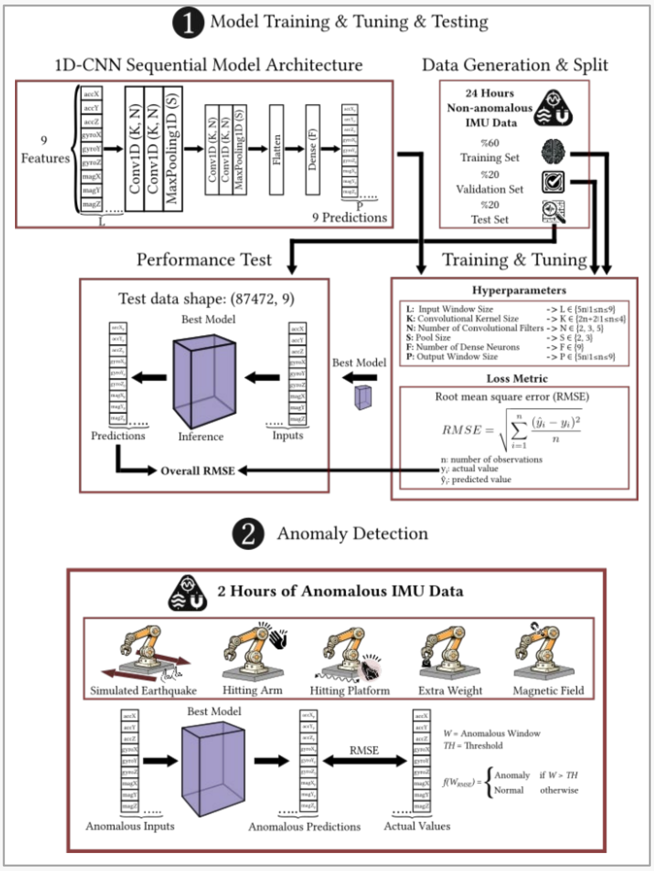
Partners and Relevant Projects

Google Research · Ofcom · Cymunedau Digidol Cymru / Digital Communities Wales

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 interconnectivity 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 the 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.



Partners and Relevant Projects

PETRAS GCHQ EXALENS

Outcomes

- **[Technical Report]** Hakan Kayan, Ryan Heartfield, Omer Rana, Pete Burnap, and Charith Perera, **Real-time Anomaly Detection in Industrial Robotic Arms via TinyML**, 2024 PDF
- **[Technical Report]** Hakan Kayan, Ryan Heartfield, Omer Rana, Pete Burnap, Charith Perera, **CASPER: Context-Aware IoT Anomaly Detection System for Industrial Robotic Arms**. 2024 PDF
- **[Journal]** Hakan Kayan, Yasar Majib, Wael Alsafery, Mahmoud Barhamgi, Charith Perera, **AnoML-IoT: An End-To-End Reconfigurable Multi-Protocol Anomaly Detection Pipeline for Internet of Things**, Elsevier Internet of Things (Elsevier IOT), Volume 16, 100437, December 2021 PDF BIB SOURCE CODE CODE CODE
- **[Journal]** Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, Charith Perera, **Cybersecurity of Industrial Cyber-Physical Systems: A Review**, ACM Computing Surveys (ACM CSUR), Volume 54, Issue 11s, January 2022, Article No.: 229, pp 1–35 PDF BIB SOURCE
- **[Demo]** Hakan Kayan, Omer Rana, Pete Burnap, Charith Perera, **CASPER: Context-Aware Anomaly Detection System for Industrial Robotic Arms**, IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp 282-284, 2023 PDF BIB SOURCE VIDEO CODE DATA SET DATA SET

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

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

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 exploiting a cyber vulnerability or a physical channel(s). 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 insufficient in the IoT scenario. This project focuses on cyber-physical behaviour, where we aim to detect cyber attacks by detecting anomalies in smart homes through cyber-physical behavioural data analysis. 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 can detect such anomaly events by physically observing temperature, vibration, light, or sound even though the malicious party may have compromised the smart plug and the smart home hub preventing it from generating NTA-based anomaly.

Partners and Relevant Projects

PETRAS bre GCHQ

Outcomes

- **[Technical Report]** Yasar Majib, Omer Rana, Andre Asaturyan, Sharadha Kariyawasam, Behzad Momahed Heravi, Charith Perera, **Cyber Physical Anomaly Detection for Smart Homes: A Survey** PDF (Under Review)
- **[Journal]** Yasar Majib, Mohammed Alosaimi, Andre Asaturyan, and Charith Perera, **Dataset for Cyber-Physical Anomaly Detection in Smart Homes**, Frontiers in the Internet of Things, Volume 2, 2023, pp, 1–15 PDF BIB SOURCE CODE DATA SET DATA SET
- **[Journal]** Yasar Majib, Mahmoud Barhamgi, Behzad Momahed Heravi, Sharadha Kariyawasam, Charith Perera **Detecting Anomalies within Smart Buildings using Do-It-Yourself Internet of Things**, Journal of Ambient Intelligence and Humanized Computing (JAIHC), September 2022 PDF BIB DATA SET SOURCE CODE

RESILIENTSENSING.AI

Video Analytics towards Anomaly Detection on Edge for Smart Cities

Researcher: Yaser Abu Awwad (MPhil Student-2021-2023)

Cameras 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., persons and vehicles) and behaviours. Most of these camera systems are designed for streaming video to the cloud. In a limited number of systems, cameras may do minor edge processing tasks such as detecting people and vehicles. Such primitive capabilities are insufficient to facilitate the 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 by 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 and how to better incentivise 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.

(a) High-Light, "Farm". (b) Rainy Weather, "Car Parking". (c) Low-Light and Noise, "Farm". (d) Low-Light and Noise, "Castle".

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, extracting information and actions to be incorporated 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 an in-depth analysis using their full capabilities by feeding the selected frames into several different pre-trained computer vision models.

Partners and Relevant Projects

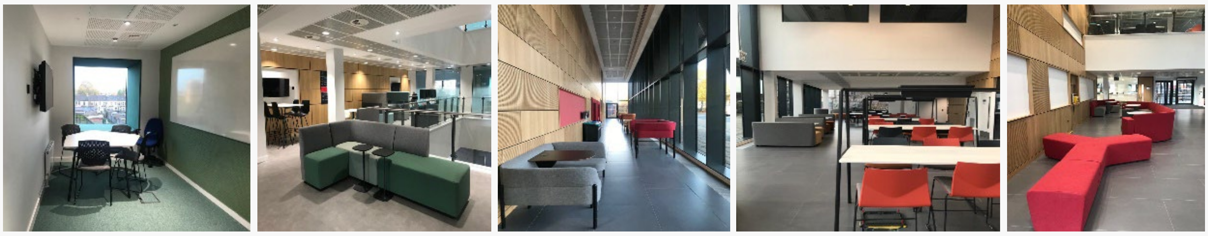
Outcomes

- **[Technical Report]** Yaser Abu Awwad, Omer Rana, Charith Perera, **Anomaly Detection on the Edge Using Smart Cameras Under Low-Light Conditions** PDF (Under Review)

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. 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 used within indoor environments to monitor occupancy and usage of spaces to improve 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

Outcomes

- **[Journal]** Wael Alsafery, Omer Rana, Charith Perera, **Sensing within Smart Buildings: Survey,** ACM Computing Surveys (CSUR), Volume 55, Issue 13(297), 2023, pp 1–35. PDF BIB SOURCE

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

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

Anomaly detection is identifying unexpected items or events in data sets that differ from the norm. It is a well-investigated area within research communities; however, anomaly detection using IoT sensor data is comparatively unexplored. In order to develop IoT sensor-based anomaly detection solutions, 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, competing requirements such as privacy vs performance could need to be managed. We believe that the best way to handle these challenges is to develop a self-configurable anomaly detection system configuring the above-mentioned parameters at runtime and adapting to the given context. In this project, we propose FedBio-IoT, a federated self-configuring IoT architecture for context-aware anomaly detection. 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 the 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.

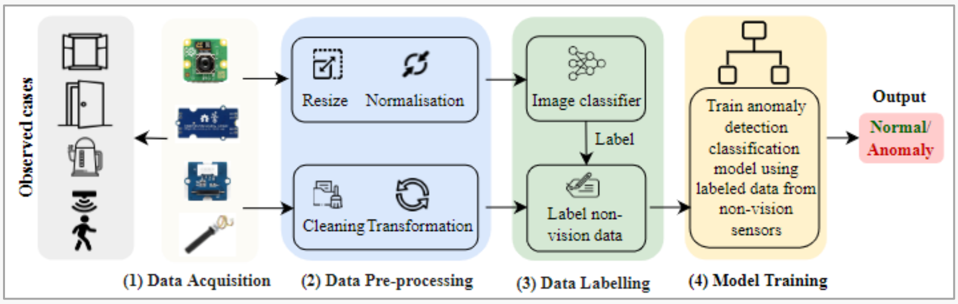
Partners and Relevant Projects

PETRAS GCHQ

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

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

In the cyber world, anomalies are detected by 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 sensors 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.



Partners and Relevant Projects

Outcomes

- **[Technical Report]** Norah Albazzai, Omer Rana, Charith Perera, **Camera as a Trainer for Anomaly Detection,** 2024 (Under Review) PDF
- **[Technical Report]** Norah Albazzai, Omer Rana, Charith Perera, **Camera as a Sensor Towards Augmenting Anomaly Detection in the Internet of Things Systems: A Survey,** Technical Report, 2024 PDF BIB
- **[Conference]** Norah Albazzai, Omer Rana, and Charith Perera, **Camera-Assisted Training of Non-Vision Sensors for Anomaly Detection**, IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI) 2023, pp. 452–453. PDF BIB SOURCE POSTER

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

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

Smart devices are heterogeneous, and each has a different set of capabilities in 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 evolve automatically, depending on users' needs, and adapt to 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 where ordinary tasks are impossible. Therefore, securing smart spaces can be challenging due to device heterogeneity, continuous changes in 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 and 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, environmental conditions, calendar information). Some updates could be simple as downloading a calendar, whereas others require data analytics (e.g., detecting 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. Currently, smart home security solutions focus on network traffic analysis to detect cyber-physical threats using ML/DL techniques. This project aims to demonstrate knowledge-based systems' utility in 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 for 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

Outcomes

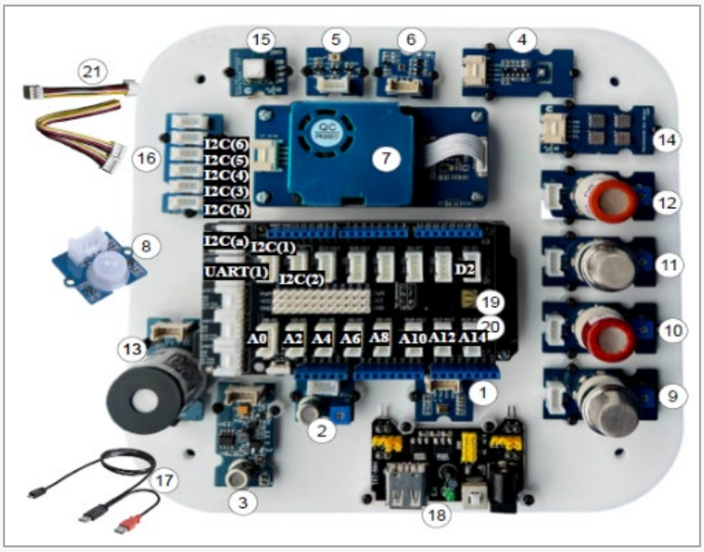
- [Technical Report] Azhar A. Alsufyani, Omer Rana, Charith Perera, **Knowledge-based Cyber Physical Security at Smart Home: A Review,** 2024 (Under Review) PDF

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 maintenance 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.

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 analytic s 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 in which the buildings can answer performance-related questions (e.g., Building Research Establishment Environmental Assessment Method (BREEAM)) with the help of IoT sensors. This project has the following objectives:



Partners and Relevant Projects

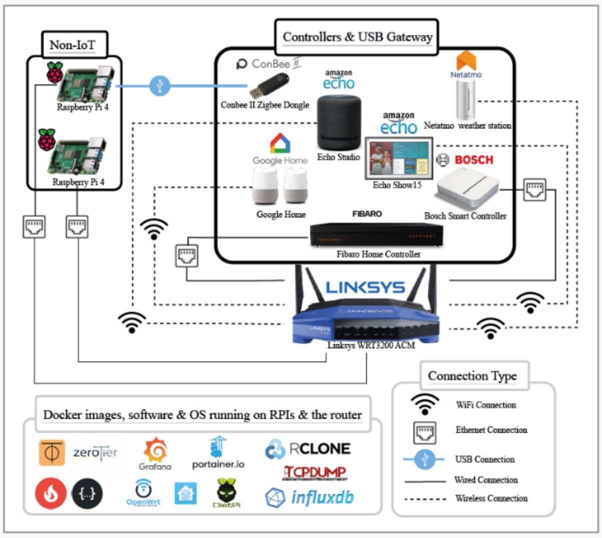
Outcomes

- **[Technical Report]** Devmane Suhas, Omer Rana, Charith Perera, **Human–Building Interaction Towards A Sustainable Built Environment: A Review,** Technical Report, 2023 PDF
- **[Technical Report]** Suhas Devmane, Pete Burnap and Charith Perera, **Dataset for Anomaly Detection in Smart Buildings Using IoT Sensors**, Technical Report, 2023

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 aim 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 detection in the context of built environments is that they are heterogeneous in nature and 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 of communication). Developing anomaly detection techniques within such a context requires comprehensive testbeds (or at least datasets collected from a comprehensive testbed). However, 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.

Partners and Relevant Projects

PETRAS bre GCHQ

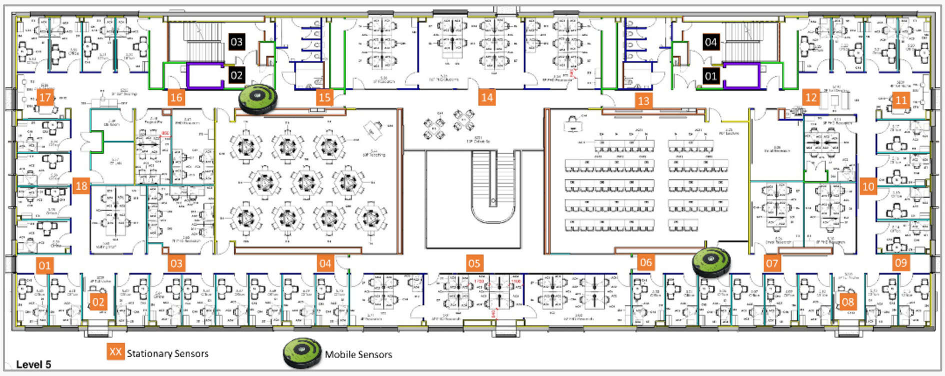
- **[Technical Report]** Mohammed Alosaimi, Omer Rana, and Charith Perera, **Testbeds and Evaluation Frameworks for Anomaly Detection within Built Environments: A Systematic Review,** Technical Report, 2023 PDF

Low-Cost Adaptive Mobile Sensing within Buildings towards Augmenting Smart Buildings

Researcher: Siyuan Li (Cecilia) (PhD Student-2022-2026)

Nowadays, people spend most of their time in indoor environments. The indoor environment has become a key factor in people's health and productivity. At the same time, smart building systems have emerged and are playing a role in building management to improve the health and productivity of occupants. Sensors are placed in the building to collect data to generate insights. Smart building systems use AI to understand the occupants' habits from the data and use actuators to improve occupant experience and overall building efficiency. There are several sub-systems in the smart building system, for example, the air quality system, the lighting system, the thermal comfort system, and the HVAC system (heating, ventilation, and air conditioning). Depending on the size and use of the building, the number of different sub-systems and sensors varies. The number of sensors and the way they are placed becomes a challenge. A large number of sensors need to be deployed throughout the building to generate useful results and insights. Such deployments, especially if retrofitting, would lead to increased deployment costs/effort/time and maintenance costs.

This project aims to design a smart building system for an existing building that reduces the complexity and consumption of the system without compromising accuracy and functionality by using mobile sensors instead of static sensors. The system has four sub-systems, an air quality system, a lighting system, a thermal system, and an activity recognition system. There is an additional control centre to integrate the various systems and make them interoperable. The activity recognition system is also the only subsystem that collects human data. It will detect the number of people in the design area and send it to the control centre. Except for the activity recognition system, all other systems collect environmental data. The main objectives of this project are:



- Conduct a literature review of autonomous/mobile systems used in smart building systems and smart environments and classify and compare their utility, characteristics, and capabilities.
- Design a mobile sensor system based on IoT technology to reduce the number of sensors used in a smart building system and try to achieve equal or (close enough results).
- Evaluate the performance of the mobile sensors system and examine the trade-offs between static/stationary sensor systems and hybrid systems in the context of various anomaly detection tasks (e.g., violation of sustainability standards, comfort and wellbeing preferences, etc.)

Partners and Relevant Projects

RESILIENTSENSING.AI

Resilient Build Environments (CASPER Shield)

Team: Charith Perera, Hakan Kayan, Yasar Majib (2022-2023)

Motivation and Business Need: NCC Group and the Global Cyber Alliance recorded more than 12,000 attacks to maliciously log into smart home devices. Recent statistics show that over 200 million smart homes can be subjected to these attacks. Conventional security systems are either focused on network traffic monitoring (e.g., firewalls) or physical environment monitoring (e.g., CCTV or sensors), but not both. These systems fail to detect sophisticated attacks/intrusions (e.g., advanced persistent threats, zero-day) that can cause physically behavioural changes (e.g., an increase in room temperature due to hacked smart air conditioner). Thus, there is a need for an advanced Cyber-Physical security system for homes that can detect those abnormalities. You can think of our product as 'anti-virus software for smart homes' that protect you and your connected things from cyber criminals and physical intrusion, making the connected living spaces more secure and safer.

Technical Challenge: To secure smart homes, we promise a Cyber-Physical anomaly detection system that uses AI/ML technology to identify the 'normal' of the home and detect the 'abnormal'. We look for abnormal occurrences in a smart home using cyber and physical data rather than relying only on insecurely transmitted, manipulable cyber/network data. Our techniques will discover real-time anomalies based on the behaviours of devices and occupants. A key technical challenge is to figure out how to integrate cyber and physical data best to detect anomalies in smart homes.

Market Opportunity and Competition: The smart home market is worth £87.61 billion, expected to grow to £136.34 billion in 5 years. The smart home security market is £0.69 billion and is expected to reach £1.08 billion in 2026. The smart home security market could be our target market. Initially, we will focus on the independent living and remote healthcare market, where smart devices are increasingly being adopted. This project is part of the CyberASAP programme.

The Cyber Security Academic Startup Accelerator Programme is a 1-year programme (FEB-2022-2023) separated into three stages; only the best teams progress to the next stage after an evaluation by a panel of senior academics, investors, industry experts and startup advisors. CyberASAP (funded by DCMS) is a national competition to identify the most promising commercial opportunities VIDEO

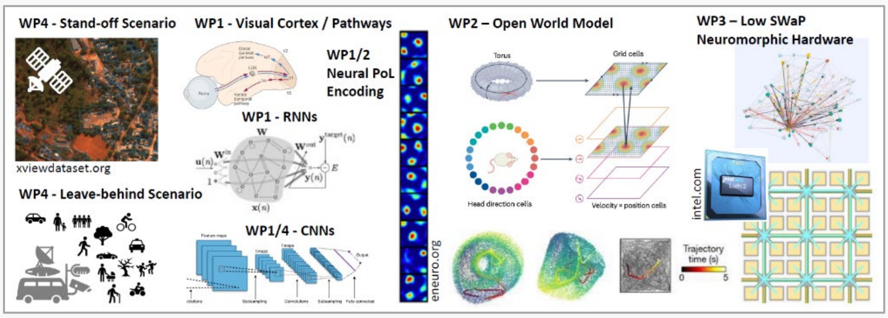
RESILIENTSENSING.AI

Edgy Organism: Modelling Patterns of Life with 100mW

Team: Martin Trefzer(York), Elena Gheorghiu (Stirling), Charith Perera (Cardiff), Oliver Rhodes (Manchester), Konstantinos Gatsis (Oxford) (2024-2027)

The Edgy Organism project aims to develop electronic surveillance systems capable of detecting and alerting anomalous behavior or identifying individuals who pose a threat in crowded public spaces. The challenge lies in creating systems that are minimally intrusive, operate with limited supervision and power, and can adapt in remote or unknown locations for extended periods. The project proposes integrating spiking neural network (SNN) technology into low-power neuromorphic hardware to achieve these goals. SNN hardware, such as Intel Loihi and True North, has reached a stage of maturity where scalable building blocks of synapses and neurons are available. These devices can process data using sophisticated bio-inspired models. The goal of Edgy Organism is to combine and push the boundaries of these technologies to create a system that can detect, classify, and potentially predict anomalous patterns of life (PoL) by drawing analogies with the nervous system of biological organisms. The project will demonstrate the capabilities of the Edgy Organism system through two real-world scenarios: Stand-off, which involves observing and processing patterns of life from a satellite, and Leave-behind, which entails covert surveillance in close proximity. The concept of Edgy Organism is based on leveraging the unique information processing capabilities of the human brain to make fast decisions with minimal computing power.

This concept, known as neuromorphic engineering, combines neuroscience and neural network research to create adaptable systems that can operate effectively in dynamic environments while meeting low size, weight, and power requirements. Despite the availability of low SWaP-capable neuromorphic devices like Intel Loihi, the field is still in its early stages and lacks scalability and adaptability for task-driven applications. The Edgy Organism project aims to fill this gap by developing a design methodology, neural network architecture, and low SWaP neuromorphic hardware implementation for autonomous monitoring and decision-making in uncertain environments. The project will draw inspiration from the brain's processing and representation of data, targeting the Intel Loihi device for its efficiency in running complex SNNs. Principles from the visual cortex and the hippocampal-entorhinal grid-cell system will be used to create efficient neural encodings of PoL and build a high-dimensional cognitive map capable of representing and detecting anomalies. The efficiency, resilience, and security of these neural encodings will be evaluated in the Stand-off and Leave-behind scenarios. Overall, the Edgy Organism project aims to revolutionise surveillance systems by leveraging spiking neural network technology and neuromorphic hardware to create autonomous, low-power, and efficient monitoring systems capable of detecting and reacting to anomalous behavior in various real-world scenarios.



Partners and Relevant Projects

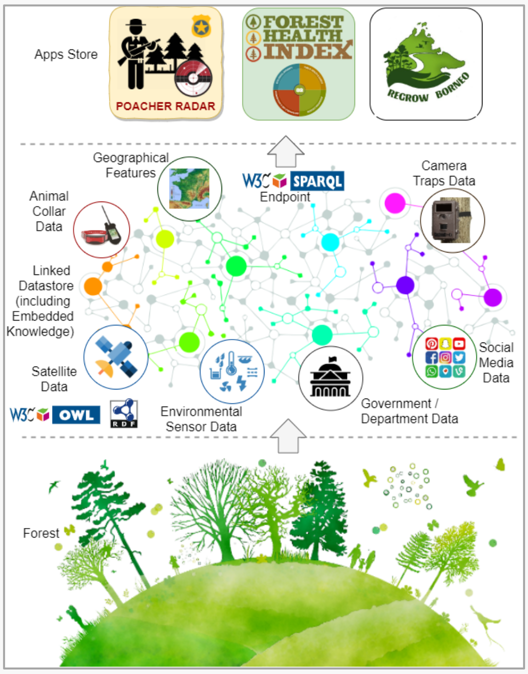
[dstl] HMGCC GCHQ

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, **A Comparison of Open Data Observatories**, 2024 PDF
- **[Technical Report]** Naeima Hamed, Omer Rana, Pablo Orozco-terWengel, Benoît Goossens, Charith Perera, **Forest Observatory: A Resource Of Integrated Wildlife Data**, 2024 PDF BIB RESOURCES VIDEO
- **[Conference]** Naeima Hamed, Omer Rana, Benoît Goossens, Pablo Orozco-terWengel, and Charith Perera, **FOO: An Upper-Level Ontology for the Forest Observatory,** European Semantic Web Conference (ESWC), 2023, vol 13998. Springer, pp154-158 PDF BIB SOURCE RESOURCES
- **[Journal]** Naeima Hamed, Andrea Gaglione, Alex Gluhak, Omer Rana, and Charith Perera, **Query Interface for Smart City Internet of Things Data Marketplaces: A Case Study**, ACM Transactions on Internet of Things (TIOT), Volume 4, Issue 3, No: 19, pp, 1–39 PDF BIB SOURCE VIDEO

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 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.

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.

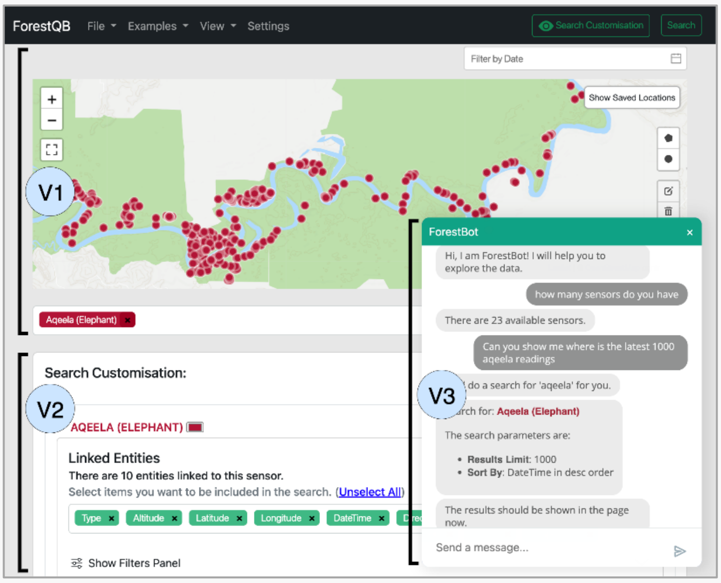
Partners and Relevant Projects

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 end-users will unlikely use it.

This project makes the Linked-Data more accessible and allows the non-technical end-user (e.g., Bioscience Researchers, and 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.



Partners and Relevant Projects

DANAU GIRANG • FIELD CENTRE •

Outcomes

- **[Technical Report]** Omer Mussa, Omer Rana, Pablo Orozco-terWengel, Benoît Goossens, Charith Perera, **ForestQB: Enhancing Linked Data Exploration through Graphical and Conversational UIs Integration,** Technical Report, 2024 PDF
- **[Technical Report]** Omer Mussa, Omer Rana, Pablo Orozco-terWengel, Benoît Goossens, Charith Perera, **Making Linked-Data Accessible: A Review**, Technical Report, 2024 PDF
- **[Demo]** Omar Mussa, Omer Rana, Benoît Goossens, Pablo Orozco-terWengel and Charith Perera, **ForestQB: An Adaptive Query Builder to Support Wildlife Research**, In Proceedings of the 12th International Semantic Web Conference (Posters & Demonstrations Track), Hangzhou, China, October 23-27, 2022 PDF BIB SOURCE VIDEO

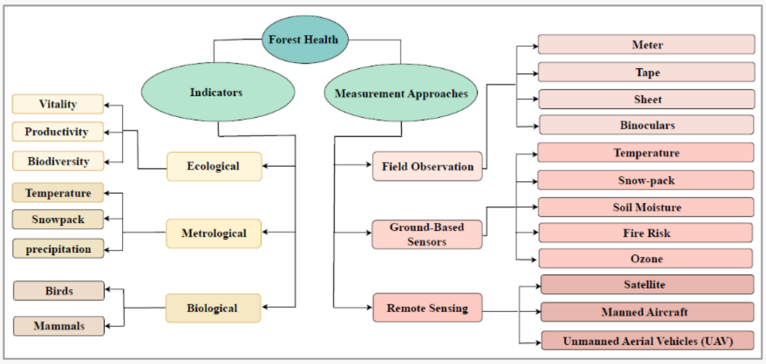
DATA OBSERVATORIES

Integrate a Heterogeneous set of Data towards Developing a Forest Health Index

Researcher: Rayan Binlajdam (PhD Student-2022-2026)

Internet of Things technologies has been used in the context of Wildlife Conservation in various ways. One such area of interest is forest health. Forest health has been defined from many different perspectives. Forest health can be defined by the production of forest conditions which directly satisfy human needs and by resilience, recurrence, persistence, and biophysical processes which lead to sustainable ecological conditions. Forest health is a qualitative term that refers to the general condition of a forest. A healthy forest is relatively free of insect infestations, diseases, exotic weeds, and air pollution. A healthy forest can resist damage from catastrophic events like acute insect and disease attacks, fire, wind, and flooding and fully recover from these perturbations to continue its life history functions over decades, centuries, or millennia. However, there aren't any well-accepted methodologies to measure forest health. Some frameworks highlight (foresthealthindex.org) so that need to consider when measuring forest health. These are high-level frameworks without any specific formula to operationalise and measure a given forest area.

IoT sensors are useful due to their ability to accurately measure environmental parameters on the ground level. However, deploying large-scale IoT networks in forest environments are quite challenging as sensors can only monitor a small geographical area. Therefore, the only way to scale up is to deploy a large number of sensor nodes, which is difficult due to hardware costs, deployment costs, difficulty in providing energy and developing network communication in harsh environments with high humidity and a lot of physical obstacles and so on. Another alternative mechanism is to use drones to observe a forest area. However, drones have limitations where they only see first from the top and cannot directly sense what is happening deep inside the jungles at the soil level. If we were to use drones, we would need to use proxy measurements to determine what is happening on the ground by looking at the quality of the trees and other characteristics that can be remotely measured through cameras. In this project, our objective is to combine both IoT and drone imaging data. Drones bring the scalability aspect, and IoT technologies bring the accuracy aspect. To combine, we will deploy both IoT and drones in a test forest environment to train a model capable of using drone images to predict the outcomes of IoT sensors and, subsequently, the forest health index. We might also use satellite images to complement drone imaging and IoT data.



Partners and Relevant Projects

Outcomes

- **[Technical Report]** Rayan Binlajdam, Oktay Karakus, Omer Rana, Pablo Orozco-terWengel, Benoit Goossens, Adisorn Lertsinsrubtavee, Preechai Mekbungwan, Deepak Mishra, Aruna Seneviratne, and Charith Perera, **Integrate a Heterogeneous Set of Data Toward Developing a Forest Health,** Technical Report, 2024 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

- **[Conference]** Stanly Wilson, Kwabena Adu-Duodu, Yinhao Li, Ringo Sham, Yingli Wang, Ellis Solaiman, Charith Perera, Rajiv Ranjan, Omer Rana, **Tracking Material Reuse Across Construction Supply Chains,** IEEE 19th International Conference on e-Science (e-Science), Limassol, Cyprus, 2023, pp. 1-4 PDF BIB SOURCE

DATA OBSERVATORIES

Forest Observatory

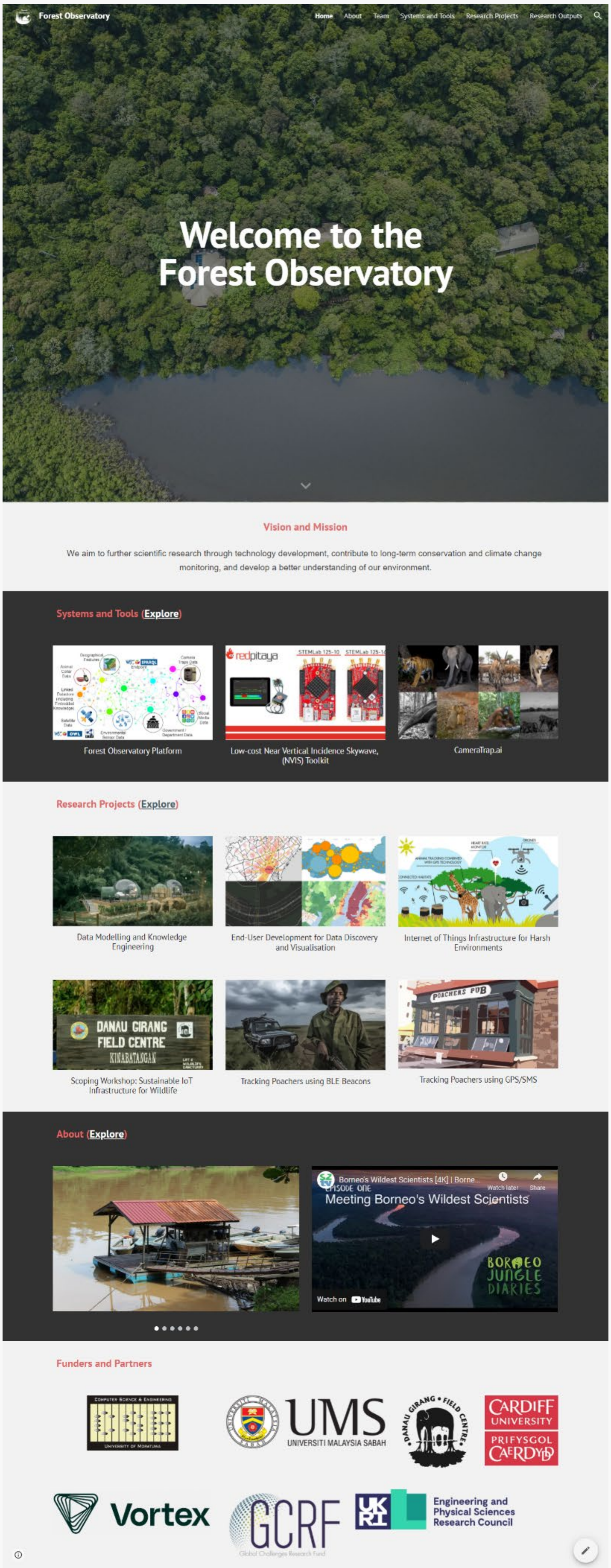
Team: Charith Perera, Omer Rana, Benoit Goossens, Pablo Orozco-TerWengel, Oktay Karakus (2021-Present)

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 program focuses on fundamental and applied research, resulting 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, aiming to gather 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



DATA OBSERVATORIES

Internet of Things Network for Forest Observatory

Team: Charith Perera, Omer Rana, Benoit Goossens, Pablo Orozco-TerWengel, (2022-2023)

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 deployed an IoT network with three sensors and three network extension mesh routers supported by a gateway to push data to the cloud. We wanted 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. Our long-term plan is to develop a forest observatory that has the capability to observe animals and the environment through heterogeneous sensors at scale to facilitate bioscience research and wildlife conservation activities. This project aims to collect data over 24 months period of time.

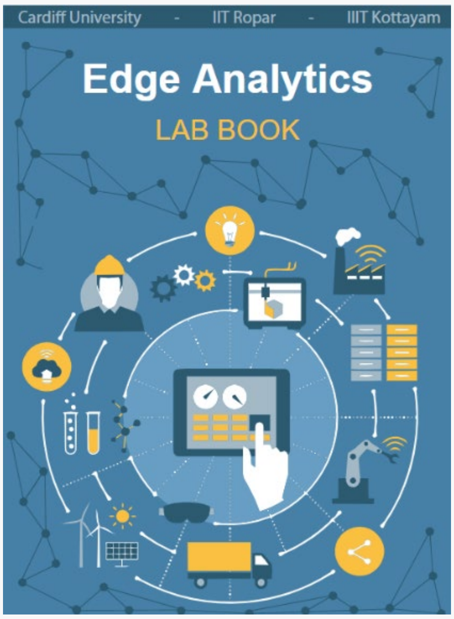
Danau Girang Field Centre (DGFC) and surrounded area. Researchers conduct research usually 2-4 miles from the river bank and 20 miles each side along the river (5.430443299150367, 118.0396091749387)

(From Left to Right) both the rechargeable battery pack and the sensor attached to a tree, rechargeable battery pack, sensor installed on top of the DGFC main building roof

UK – Egypt Trans-National Education (TNE) (Edge Analytics 2.0)

Team: Omer Rana, Charith Perera, Anish Jindal, Mohamed Taher Alrefaie, Mohamed Medhat Gaber, Khaled Elgeneidy, Sahar Hamed (2023)

Edge analytics focus on using AI on user-owned devices. We focus on developing course content between UK and Egyptian universities based on world-class course frameworks. Joint students and researchers collaborated by building edge applications on smart cities, smart grids, water and energy management to achieve SDG goals. As millions of Internet of Things (IoT) devices generated vast amounts of data, the we recognised the limitations due to the propagation delay in uploading this data to the cloud. This realisation underscored the need for data analysis at the edge of the network, where the data was generated, especially for real-time applications. Therefore, edge analytics emerged as a critical field of study within the project. The rising popularity of edge computing and IoT spurred a significant market demand for skilled professionals. In response, the "Edge Computing and Analytics 2.0" module was introduced to meet the needs of both industry and academia.



This new course was built upon the outcomes of a previously funded project between Cardiff University and IIIT India. To address the evolving market demands, the consortium implemented two fundamental enhancements: firstly, adding hardware training to teach students how to build edge devices; secondly, incorporating several industrial case studies and applications in smart cities, drawing on the deep expertise of the consortium. Additionally, we extended the edge analytics work that had been conducted previously.

- Joint curriculum development that aims to graduate engineers qualified to work on modern edge computing applications in the UK and Egypt.
- Faculty and researchers exchange of knowledge via physical and virtual mobility between the consortium.
- Development of industrial projects that serves Egypt 2030 Vision through smart cities applications in New Administrative Capital, Galala City, and the new industrial zone near Ain Sokhna and Suez Canal.
- Offer a professional diploma at Galala University based on the extended content developed by the consortium.
- Research collaboration and exchange between participating institutes, using research-based course content, industrial projects and use of dedicated labs to run projects across UK and Egypt's universities.

Partners and Relevant Projects

Durham University | جامعة الجلالة GALALA UNIVERSITY | BRITISH COUNCIL

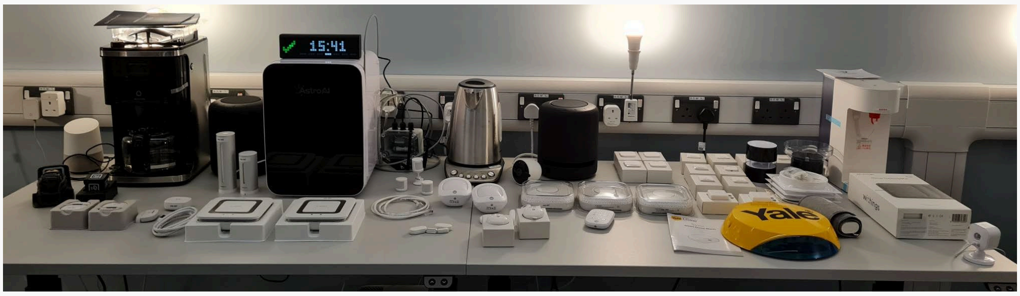
The Knowledge Hub Universities | partnered with Coventry University

RESEARCH INFRASTRUCTURE

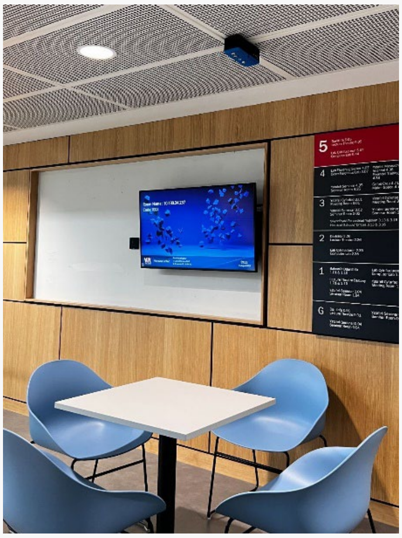
Smart Home Lab

Team: Charith Perera, Mary Zacharias, Mohamed Alosaimi, Yasar Majib (2021-)

The Smart Home Lab (SHL) is a key research facility designed, developed and managed by the IoT group. It is a physical space comprised of over 170 networked smart home devices. It has six hotdesk working areas where researchers (staff and students) can conduct research with smart home devices. It comprises a wide range of devices such as smart TV, environmental monitoring kettles, various smart speakers, robotic vacuum cleaners, smart metre bells, door locks and many more. We use OpenHab and Home Assistant to capture semantic data and Wireshark to capture network traffic and related network communications and behaviours. The smart home lab also comprises a video network connected to six different types of smart home and consumer CCTV cameras to a network video recorder that allows connecting video analysis research.



RESEARCH INFRASTRUCTURE



Abacws Smart Building Testbed

Team: Charith Perera, Suhas Devmane (2022-)

The Abacws Smart Building Testbed is one of our latest projects in the design and development phase. We are developing and deploying sensor nodes across two floors in the Abacws building at high density, which capture a wide range of sensor data and enable the researcher to contact various research. We collect over 16 different types of sensor parameters at a high frequency, enabling us to monitor the building at high resolution. The nodes will be deployed in shared spaces and do not capture any privacy-sensitive information

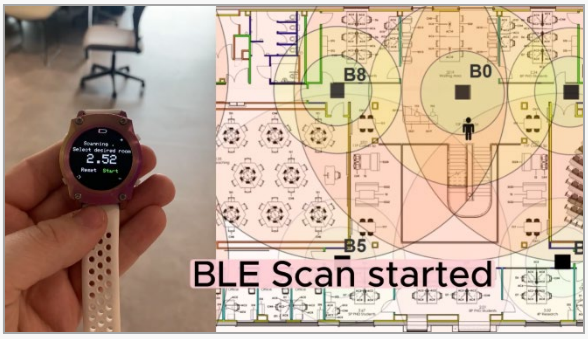
Incubator Projects

Indoor Navigation System using Smart watch and BLEs

BSc

Researcher: Craig Thompson (BSc Student-2023)

This project focused on aiding individuals with communication difficulties in navigating large, complex buildings like universities or museums using an indoor navigation device. Over five months, the device was developed using an open-smartwatch and BLE beacons, installed in the University's ABACWS building. It guides users via BLE signals and Dijkstra's algorithm, tested by students in real-world scenarios. After all trails were completed, it was found that 100% of the participants found their destination using this form of indoor navigation device, with an average recommendation rating of 6.9 out of 10. However, from technical evaluations, the reliability of BLE Signals decreased by 15.5% during busy periods, highlighting this project's potential limitations in scenarios with high Bluetooth interference VIDEO

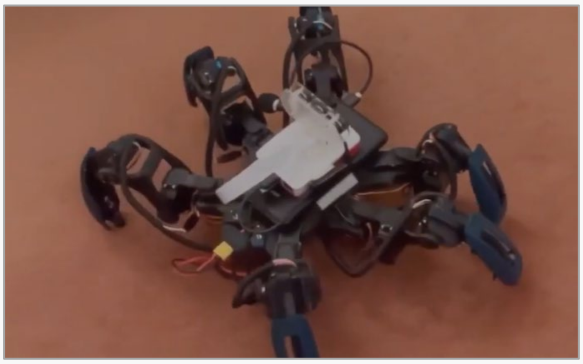


Robot Assistant to Prevent and Manage Falls

BSc

Researcher: Nafis Ahmed (BSc Student-2023)

This project developed a fall detection hexapod robot to aid fall management in the ageing population, integrating features like a guiding night light, AI for fall detection, a camera for person tracking, and Wi-Fi for emergency calls, all powered by a Raspberry Pi. The study emphasised practical implementation, showing the robot's social care and fall prevention potential. It demonstrated the use of accessible technology in creating effective care solutions evolving personalised care technology VIDEO

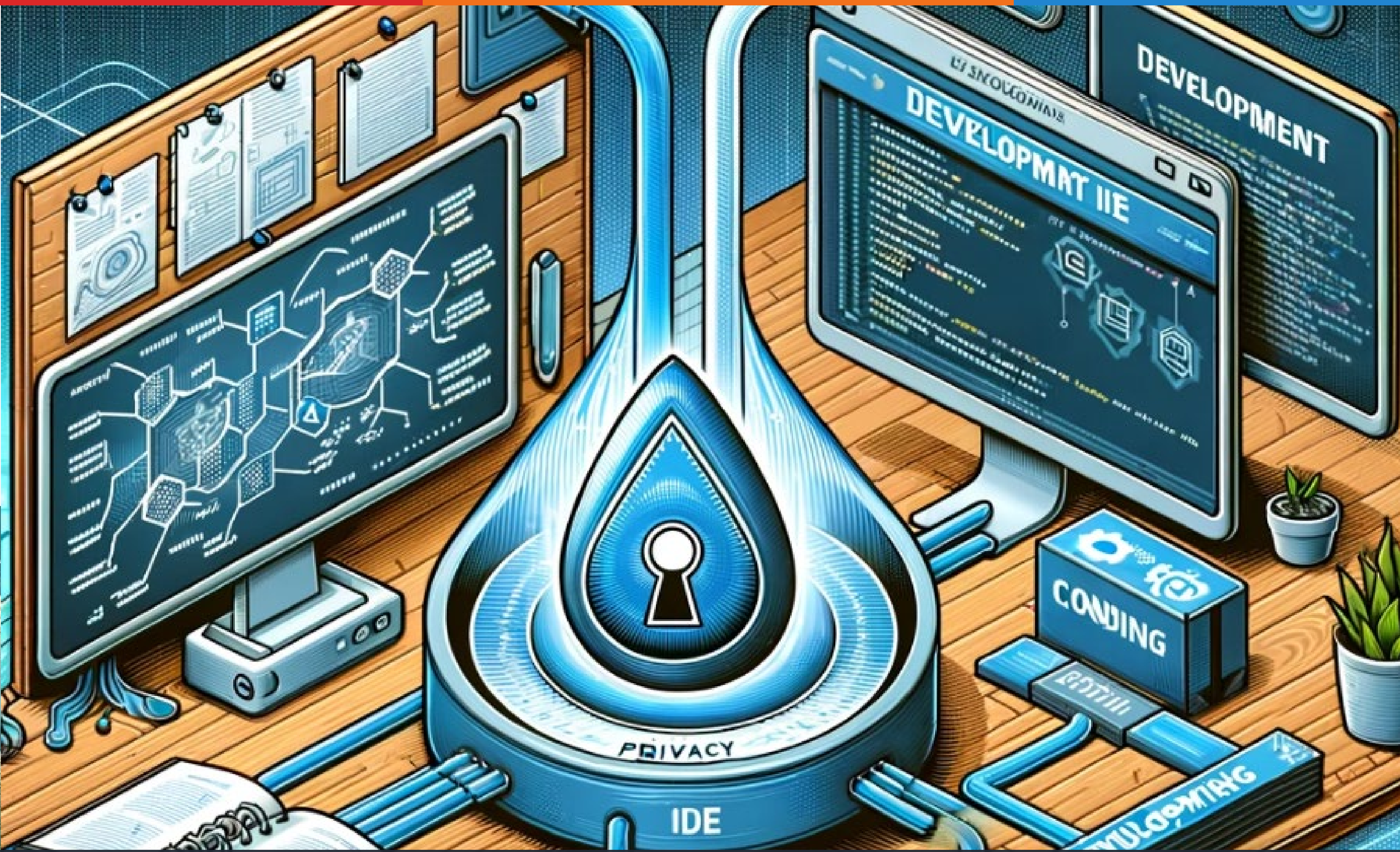


PETRAS in Lego Demonstrator

Funded

Team: Hakan Kayan, Jana Jhaveri, Semih Sarisoy (2023)

Our project combines LEGO and augmented reality (AR) to create an interactive showcase for PETRAS projects. Users can explore these projects through an AR interface linked to a LEGO Smart City Demonstrator. Evolving from earlier concepts, our accessible technology invites everyday software engineers to engage in this immersive experience. With a long-term goal of enhancing educational tools in smart city learning, we collaborate with architectural experts to ensure a realistic and engaging cityscape VIDEO



gitlab.com/IOTGarage

bit.ly/2JMoSd4

@IOTGarageNews