# IoT Garage

## 2016–2026

### The project book

Ten years of the research group, project by project.

**Charith Perera** • Cardiff University
iotgarage.net







00

WHO WE ARE

# A group that builds what it studies

The IoT Garage works across the whole Internet of Things stack, from the sensor to the person who lives with it.

4 **The people** How people live with connected systems

3 **The data** Privacy, data semantics and observatories

2 **The edge** Embedded AI and edge computing

1 **The sensor** Sensors and sensing infrastructure



**124**
publications, 2016 to 2026

**24**
doctoral researchers, current and past

**170+**
devices in the Smart Home Lab

Counted in November 2026 from the iotgarage.net publication list and team page.

01 **Privacy Fluid**
Privacy by design, consent, privacy education and tools for developers
PAGE 05

02 **Data Observatory**
Linked data, observatories, wildlife monitoring and data markets
PAGE 06

03 **Resilient Sensing**
Security, anomaly detection and trustworthy data
PAGE 07

04 **Edge Intelligence**
Small, low-power AI next to the sensor
PAGE 08

05 **Sustainable Environments**
Buildings, energy and the people inside them
PAGE 09

ALSO FROM THE GROUP: IOTCLASS.ORG AND IOT GARAGE TV

00

WHO LEADS THE GROUP

# About Charith Perera



**Reader**

School of Computer Science and Informatics, Cardiff University

**Visiting Faculty**

University of Illinois Urbana-Champaign

**Founder and Head**

IoT Garage and the Cardiff IoT Research Group

**Creative Director**

IOTClass CIC, the community interest company behind IoTClass.org

CARDIFF UNIVERSITY · UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN · Cardiff Internet of Things Group · National Edge AI Hub

## Awards and fellowships

**Google Research Scholar Award**
2023

**OECD Co-operative Research Programme Fellowship**
2025

**GCHQ National Resilience Fellowship**
2021

## Secondments

bre — Building Research Establishment, supported by PETRAS

CATAPULT Digital — Digital Catapult, Researcher in Residence

## Memberships and roles

**IEEE**
Senior Member

**ACM**
Senior Member • Associate Editor, ACM Transactions on Internet of Things

**BCS, The Chartered Institute for IT**
Fellow

**Royal Society of Arts**
Fellow

**Advance HE**
Senior Fellow of the Higher Education Academy

**UKYoung Academy**
Member

**World Wide Web Consortium**
Invited Expert, Web of Things Interest Group

**IEEE Smart Cities**
Member, with technical and DEI committee roles

**Association for Learning Technology**
Conference committee member

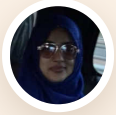
00

WHO WE ARE

# The people

Current doctoral researchers, and the doctoral and research staff alumni of the group, as listed on **iotgarage.net**.

## CURRENT TEAM



**Asma Irfan**
Influence through Data Driven Pervasive Interactions
PhD Student (2020-2026)

**Mark Butterworth**
Low Power IoT Infrastructure for Harsh Environments
PhD Student (2020-2027)

**Fatmah Alqarni**
Learning Privacy and Laws Through AI-Mediated Exploration and Design
PhD Student (2022-2026)



**Siyuan Li**
Adaptive Mobile Sensing within Buildings
PhD Student (2022-2026)



**Rayan Binlajdam**
Forest Health Index
PhD Student (2022-2026)



**Kira Nurse**
Assisting Young People with Neurodiversity
PhD Student (2023-2027)



**Maya Lhoste**
eDNA and Pollutant Monitoring in Rivers
PhD Student (2024-2028)

## DOCTORAL AND RESEARCH STAFF ALUMNI



**Suhas Devmane**
PhD Student (2021-2026)



**Mohamed Alosaimi**
PhD Student (2021-2026)



**Hakan Kayan**
Postdoctoral Researcher (2025-2026)



**Reem Aldhafiri**
PhD Student (2020-2025)



**Abdulaziz Aljohani**
PhD Student (2021-2025)

AA **Azhar Alsufyani**
PhD Student (2021-2026)

NH **Naeima Hamed**
Research Staff (2025)



**Yasar Majib**
PhD Student (2020-2025)



**Omar Mousa**
PhD Student (2021-2025)

NA **Norah Albazzai**
PhD Student (2021-2025)

WA **Wael Alsafery**
PhD Student (2021-2025)

AJ **Atheer Jeraisy**
PhD Graduate (passed 2026)

BA **Bayan Almuhander**
PhD Student (2019-2025)

LA **Lamya Alkhariji**
PhD Student (2018-2022)

NA **Nada Alhirabi**
PhD Student (2018-2022)

YA **Yaser Abu Awwad**
MPhil Graduate (passed 2022)

AA **Areej Alabbas**
PhD Student (2019-2024)

DF **Dominic Fonseca**
MPhil Graduate (passed 2022)

OM **Osian Morgan**
Research Staff (2021-2022)

MZ **Mary Zacharias**
Research Staff (2021-2022)

AK **Akin Kaki**
Research Staff (2021-2022)

LN **Luiz Nunes**
PhD Student (2014-2018)

00

WHAT IS INSIDE

# Contents

## 01 • Privacy Fluid


Ten years of privacy by design 08
Privacy for IoT builders 09
Privacy along the data flow 10
Protecting data and trust 11
PrivacyPulz 12
Privacy Assistant and EchoEase 13
PrivacyCube 14
PriviFy 15
Canella 16
Privacy Captain 17
Privacy Parrot (PARROT) 18
Assisting Young People with Neurodiversity 19
mySafeHome 20


## 02 • Data Observatory


Sensing as a Service: the idea 22
Sensing as a Service: making it real 23
Finding the right sensor 24
ForestQB 25
FooDS and PoachNet 26
Forest Health Index 27
BearWave 28
Talking Buildings 29
STREAM 30
WoT-AI Explorer 31
Forest Observatory 32
Listening to the forest 33
Reading number plates at the edge 34
Following a poacher's vehicle through the jungle 35
Pan-Borneo Elephants 36
EventCam.AI 37
CamTrap.AI 38
Smart City Data Markets 39
Reading a city's air 40
Talking Aquifer 41


## 03 • Resilient Sensing


InSituHome 43
Trusting synthetic home data 44
Context Aware Security for Smart Homes 45
Industrial security foundations 46
CASPER 47
Integrity Checking at the Edge 48
Knowledge-driven Security at the Edge 49
Anomaly Detection with Tiny Cameras 50
In-Vehicle Edge Security 51
Adaptive Mobile Sensing 52
Patterns of life in buildings 53
When building context changes 54
Resilient Built Environments 55
CASPER Shield 56
Early Signs of Domestic Violence 57




## 04 • Edge Intelligence


Edge-centric analytics platforms 59
Doing more with less data at the edge 60
Seeing in the dark at the edge 61
Making sensor AI explain itself 62
National Edge AI Hub 63
Edgy Organism: the data 64
Edgy Organism: the models 65
ARCADE and ScrewSet 66
FedBio-IoT 67
Secure Service Placement for IoT 68


## 05 • Sustainable Environments


SpaceSense & EcoCube 70
D-FACT 71
Knowing what a material is 72
Trusting where it came from 73


## 06 • Labs and datasets


Smart Home Lab 75
Living Edge Laboratory 76
Smart City Lego Lab 77
Smart Home Anomaly Dataset 78
IoT Products Dataset 79


## 07 • Teaching and learning


IoTClass.org 81
Internet of Things Education 82
Looking inside the smart home 83
Edge Analytics Lab Book 84
Objects you play with 85
IoT Kids Books 86
Design Ideas for Inclusive Smart Cities 87


## 08 • Engagement and impact


PETRAS Regional Networking Events 89
Sustainable IoT for Wildlife 90
Digital Twin Cardiovascular Care 91
Smart City EDI Atlas 92
SensaForge 93
TraceLoom 94


## And finally


The decade, 2016 to 2026 95
Where the work happens 96
Ten years in numbers 97
Tools and products 98
Who backs the work 99
Work with us 100




PART 01

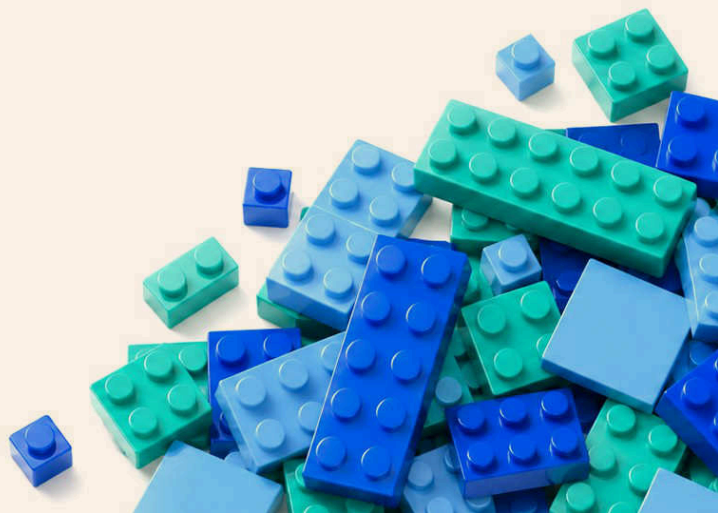
# 01



# Privacy Fluid

Privacy that people can see and hold, and that developers can build in from the first sketch.


Ten years of privacy by design ..... 08
Privacy for IoT builders ..... 09
Privacy along the data flow ..... 10
Protecting data and trust ..... 11
PrivacyPulz ..... 12
Privacy Assistant and EchoEase ..... 13
PrivacyCube ..... 14
PriviFy ..... 15
Canella ..... 16
Privacy Captain ..... 17
Privacy Parrot (PARROT) ..... 18
Assisting Young People with Neurodiversity ..... 19
mySafeHome ..... 20

01

PRIVACY FLUID

# Ten years of privacy by design

From design guidance to tools, accessible controls and learning

**2016** **Make principles practical**
Link privacy guidance to the stages of an IoT application's data life cycle.

**2017** **Guidance at a glance**
A cheat sheet makes privacy questions easier to bring into everyday design work.

**2018** **Put the person first**
Connect changing circumstances, privacy risks and useful services through user-centred engineering.

**2020** **Test design support**
Study how software engineers use privacy guidance to identify protective design measures.

**2021** **Atheer: Canella**
Turn privacy-law knowledge into components and feedback within visual IoT programming tools.

**2021** **Nada: Privacy Parrot**
Help developers explore privacy-aware application designs with interactive guidance.

**2021** **Lamya: explainable knowledge**
Organise privacy schemes and patterns into knowledge that software can use to explain design choices.

**2023** **Bayan: tangible privacy**
Make privacy awareness and control more visible through physical interfaces.

**2023** **Reem: accessible assistants**
Use conversational and multimodal interfaces to make smart-home privacy controls more accessible.

**2026** **Fatmah: learning through AI**
Connect educational mechanisms, privacy-design exploration and the evaluation of AI-supported privacy reasoning.

The story starts in 2016 with a practical question: how can privacy principles guide a connected system's design? Assessment guidelines and a cheat sheet translated abstract advice into questions engineers could use. Work on user-centred engineering then considered risks as circumstances change. By 2020, a controlled study had tested whether guidance helped engineers identify ways to protect personal data.

## FROM GUIDANCE TO TOOLS

**Canella**
Privacy components inside visual IoT programming

**Privacy Parrot**
Interactive guidance on application designs



**Privacy Captain**
Explains which protections a design needs



**PrivacyCube**
Shows a home what its devices collect



**PriviFy**
Set privacy preferences with physical controls

**PrivacyPulz**
Helps new developers reason about privacy harms

**Scan for the project page**
iotgarage.net/go/privacy-by-design

## ALL PAPERS

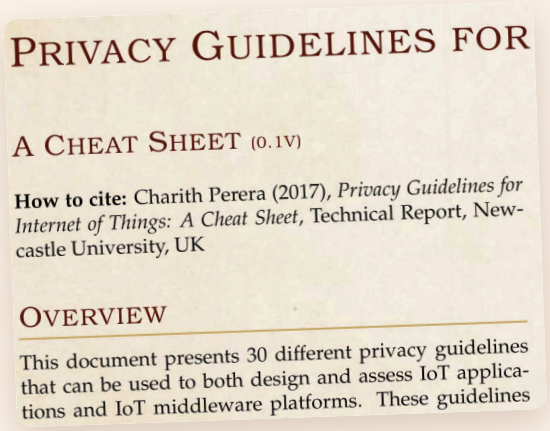

**Explicit and Implicit Learning Mechanisms in AI Educational Assistants**…
**Voice-Enabled Privacy Assistant Towards Facilitating Successful Agein**…
**Security and Privacy Requirements for the Internet of Things** Alhirabi, …
**Designing privacy-aware internet of things applications** Perera, Barha…
**Privacy Guidelines for Internet of Things** Perera • Technical Report, Newc…
**Interactive Privacy Management** Al Muhander, Wiese, Rana and Perera • AC…
**Privacy Laws and Privacy by Design Schemes for the Internet of Things**…
**Synthesising Privacy by Design Knowledge Towards Explainable Inter**…
**User-centric Privacy Engineering for the Internet of Things** Barhamgi, …
**Privacy-by-Design Framework for Assessing Internet of Things Applica**…

01

PRIVACY FLUID

# Privacy for IoT builders

Privacy guidelines for people who build IoT



PRIVACY GUIDELINES FOR

A CHEAT SHEET (0.1V)

**How to cite:** Charith Perera (2017), *Privacy Guidelines for Internet of Things: A Cheat Sheet*, Technical Report, Newcastle University, UK

OVERVIEW

This document presents 30 different privacy guidelines that can be used to both design and assess IoT applications and IoT middleware platforms. These guidelines

The 2017 cheat sheet: 30 privacy guidelines for IoT, grouped into eight families.

Privacy principles help only when builders can turn them into design decisions. The 2016 assessment framework linked guidance to the stages through which data passes. A cheat sheet and a call for a privacy mindset followed in 2017. Together, they asked engineers to consider what they collect, where they process it and what people can control before an application is built.

The 2020 study tested whether this guidance helped software engineers identify protective measures. Later work described tools that could explain privacy choices while a design takes shape. The handbook and pattern mappings connect broad principles to reusable solutions, while the device review examines where controls actually appear. These are complementary resources: evidence about design support, proposals for tools and examples of existing controls.

### EIGHT FAMILIES OF GUIDELINES

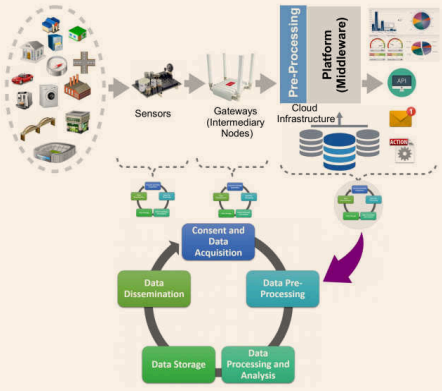
- **Minimise**
- **Hide**
- **Separate**
- **Aggregate**
- **Inform**
- **Control**
- **Enforce**
- **Demonstrate**

Each family becomes questions an architect can ask of a platform or an application, at every stage the data passes through.

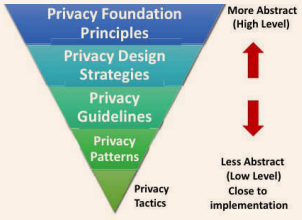
**75.12%**

of possible protective measures identified with the guidelines by ten software engineers across three IoT designs; a controlled design exercise, not evidence of legal compliance.

Information Sciences, 2020




Data moving from sensors to the cloud, and the life cycle each guideline is checked against.




From high-level principles down to tactics close to implementation.

- Guidance for assessing connected applications and platforms.
- Reusable patterns connect principles to practical design choices.

**Scan for the project page**

iotgarage.net/go/privacy-by-design

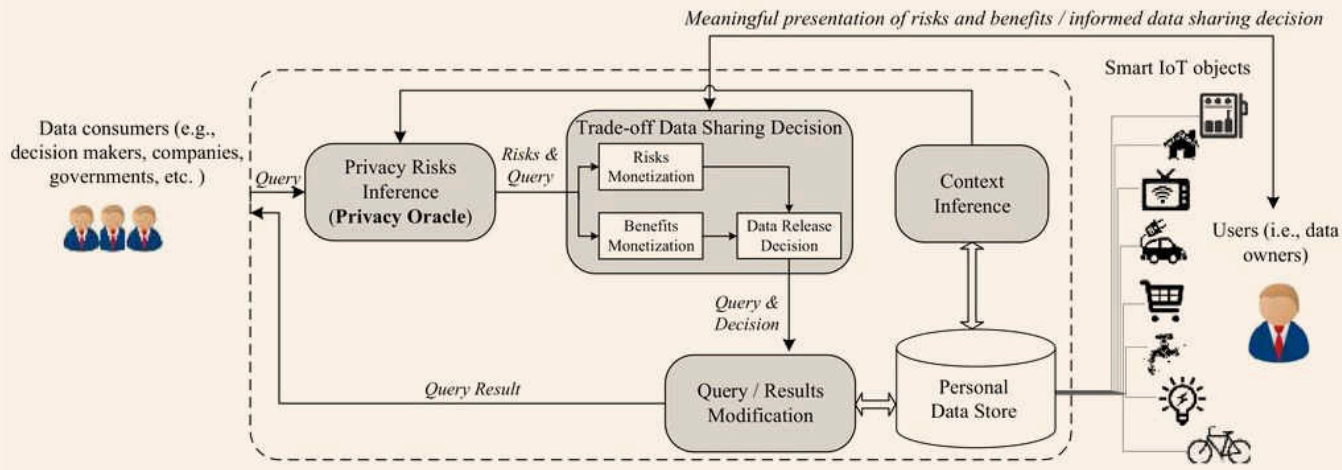
### ALL PAPERS

**IoT Device Privacy** 2026
**Designing privacy-aware internet of things applications** Perera, Barha…
**Examining the Interplay Between Privacy by Design (PbD) Schemes an…**
**Privacy Mindset for Developing Internet of Things Applications for Soci…**
**Envisioning Tool Support for Designing Privacy-Aware Internet of Thin…**
**Privacy Patterns for Internet of Things** 2020
**Privacy Guidelines for Internet of Things** Perera • Technical Report, Newc…
**Privacy-by-Design Framework for Assessing Internet of Things Applica…**

PRIVACY FLUID

# 01 Privacy along the data flow

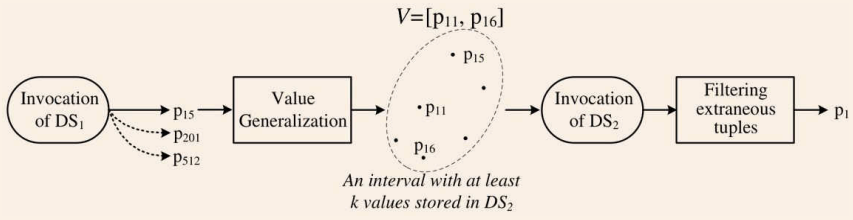
Helping people control what connected services can learn




Reference architecture connecting privacy risks, sharing decisions and modification of queries or results.

Privacy choices need to travel with data as services collect, combine and reuse it. The 2016 knowledge review asked how software could represent people's preferences without overwhelming them. Permission negotiation then explored whether an assistant could learn those preferences. The 2018 user-centred architecture connected this concern to changing circumstances: the same information can carry different risks in different situations.

The later methods address what happens when information crosses service boundaries. Privacy in Data Service Composition hides the particular value a service request concerns among alternatives. Delta-Risk instead calculates protection choices against a user's risk limit. Together with negotiation, these papers connect personal preferences to technical decisions. Their evaluations remain distinct: laboratory permission choices, service experiments and synthetic risk-management tests.




A service request is generalised to an interval of values before extraneous results are filtered.

**Scan for the project page**
iotgarage.net/go/privacy-by-design

**under 2 seconds**
to calculate protection strategies for up to 1,000 inferred risks in synthetic performance tests; no user study.
ACM Transactions on Internet Technology, 2021

**p = 0.013**
for more accurate agent defaults than random defaults in a laboratory study. Participants still checked the settings, so effort did not fall.
International Conference on Autonomous Agents and Multiagent Systems, 2017

- Represents privacy preferences in forms software can use.
- Protects the subject of requests between cooperating services.

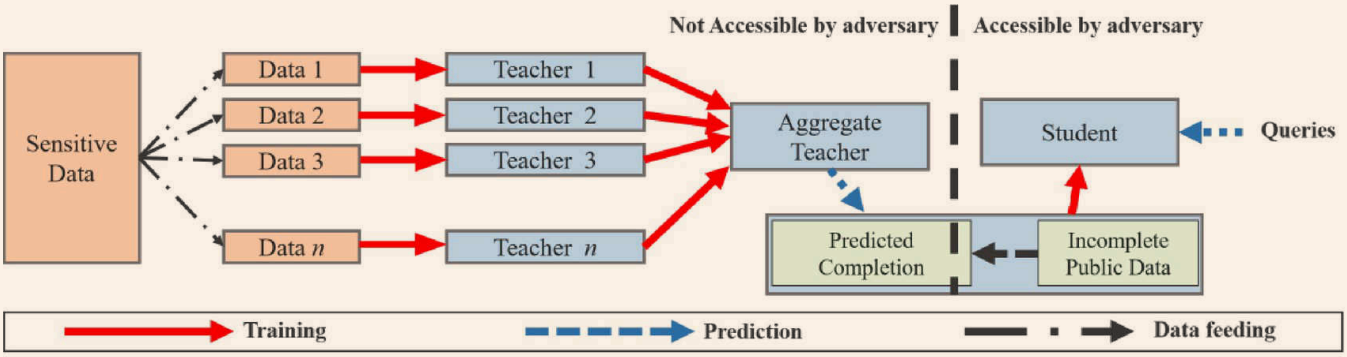
**ALL PAPERS**

**Delta-Risk: Towards Context-aware Multi-objective Privacy Managemen…**
**User-centric Privacy Engineering for the Internet of Things** Barhamgi, …
**Privacy-Knowledge Modeling for the Internet of Things** Perera, Liu, Ranj…
**Privacy in Data Service Composition** Barhamgi, Perera, Yu, Benslimane et …
**An Automated Negotiation Agent for Permission Management** Baarslag, …

PRIVACY FLUID

# 01 Protecting data and trust

Sharing useful information without exposing its contributors




Teacher models trained on sensitive data feed an aggregate teacher; a separate student model learns from it and answers queries.

**Group similar records**
Microaggregation keeps confidential values varied inside each group.

**Share a protected model**
Hand over a privately trained model instead of artificial examples.

**Prove who is calling**
Authentic Caller checks identity without a certificate authority.

**Combine feedback secretly**
Encrypted ratings build a shared reputation without exposing anyone.

**Deter insiders**
Sanctions, effort, risk and reward shape what employees do.

Protecting data involves more than hiding a name. The microaggregation work groups similar records while keeping confidential values varied, exposing a trade between privacy and useful detail. Authentic Caller addresses another boundary: proving who is communicating without relying on a certificate authority. The crowd-sensed trust protocol then combines encrypted feedback so that a shared reputation need not expose each person's contribution.

These technical protections sit alongside questions about behaviour and the usefulness of shared data. The insider-security survey examines employees' attitudes towards sanctions, effort and reward. The private-data synthesis study compares handing over artificial examples with sharing a protected trained model. Across the papers, trust depends on choosing what to reveal, to whom and for what purpose, with separate evidence for each setting.

**0.31% to 7.66%**
reported accuracy advantage for a private trained model over training on private synthetic data at the same privacy level. Tests used MNIST and FASHION-MNIST images, not factory data.
IEEE Transactions on Industrial Informatics, 2023

**9 of 11**
hypotheses supported in a survey of 444 UK employees. These are self-reported attitudes, not observed reductions in security incidents.
Future Generation Computer Systems, 2019

**Scan for the project page**
iotgarage.net/go/privacy-by-design

ALL PAPERS

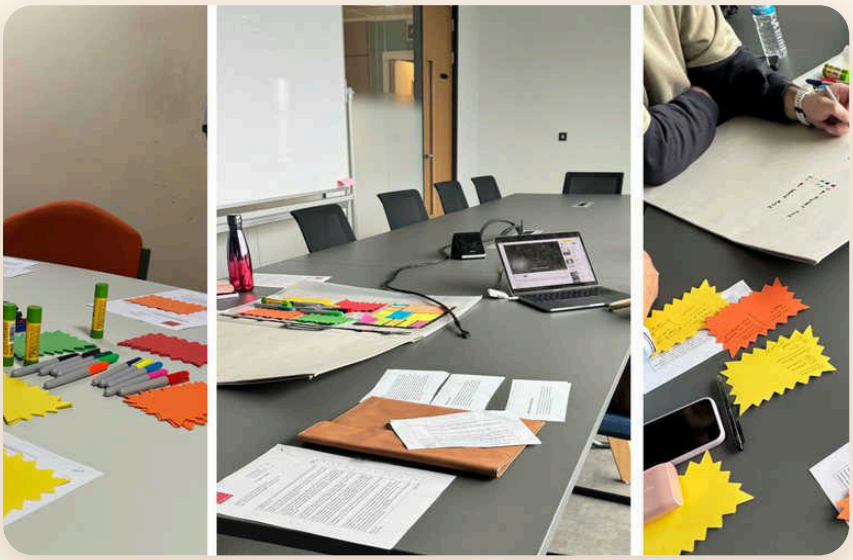
**On the Private Data Synthesis Through Deep Generative Models for Data…**
**Hybrid Microaggregation for Privacy-Preserving Data Mining** Abidi, Ben …
**Deterrence and prevention-based model to mitigate information securit…**
**Privacy-preserving Crowd-sensed Trust Aggregation in the User-centri…**
**Authentic Caller** Azad, Bag, Perera, Barhamgi et al. • IEEE Transactions on In…

01

PRIVACY FLUID

# PrivacyPulz

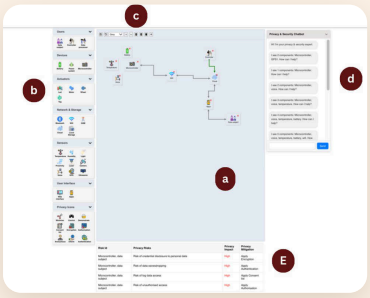
Teaching privacy while students design smart products



Three photographs of a co-design workshop table: sticky notes, marker pens, printed sheets and a participant writing on a large sheet.

People who build connected products, the Internet of Things (IoT), often overlook privacy because the systems are complex. University courses tend to teach cybersecurity more than privacy. New software engineers can finish their studies without knowing how to spot privacy risks in a design, or which data protection laws apply to it.

The project began with a review of how AI educational assistants teach through instruction and learning by doing. PrivacyPulz lets students draw a connected product and consider privacy as they design. Workshops helped shape the tool. Related work explores how generative AI can support privacy risk assessment and help developers reason about potential harms.




The PrivacyPulz design screen: canvas, icons palette and toolbar where students assemble an IoT product.

**WHO**
Fatmah Alqarni

**WHEN**
2022 to 2026

**Scan for the project page**
iotgarage.net/go/privacypulz

**38**
studies of AI educational assistants, published from 2000 to 2024, were reviewed. They were selected from 16,335 records.
AI (MDPI), 2026

- PrivacyPulz is a learning tool: students assemble an IoT product on a canvas and answer privacy questions as they design.
- It is aimed at university computer science students and new developers.
- The design was shaped in co-design workshops with computer science students.



**ALL PAPERS**

**Evaluating Generative AI Support for Privacy-by-Design in IoT Develop…**
**Explicit and Implicit Learning Mechanisms in AI Educational Assistants…**
**From Sensors to Privacy Harms** 2026

01

PRIVACY FLUID

# Privacy Assistant and EchoEase

Smart speaker privacy settings anyone can manage




A study room set up with an Echo Show playing a video of a presenter, and answer paddles on the tables: thumbs up and down, faces, and the numbers 1 to 3.

Smart speakers can help older adults and people with learning disabilities live independently, but they also collect personal information. Privacy settings can be difficult to find and understand in a phone app. The project examines the barriers older adults encounter and explores ways to make privacy controls more accessible in everyday use.

The project builds privacy assistants that explain and change these settings in conversation. It began with a voice-only Privacy Assistant on Amazon Alexa, published as a demo in 2023. Later work added matching on-screen visuals for older adults, and EchoEase, which uses video with Makaton signing and simple symbols on an Echo Show. The systems were co-designed with community partners including Innovate Trust.

**WHO**
Reem Aldhafiri

**WHEN**
2020 to 2026

**Scan for the project page**
iotgarage.net/go/privacy-assistant

**3**

older people aged 65 to 72 tried the first voice-only Privacy Assistant. This is early evidence from a small sample. It shows the idea is feasible, not that awareness lasts.

IEEE PerCom Workshops, 2023

- A voice assistant that talks people through three privacy areas: voice recording, location and voice purchasing.
- Designed for older adults and for adults with learning disabilities, groups that standard privacy settings often exclude.
- Runs on Amazon Alexa devices, including the Echo Show screen.



**ALL PAPERS**

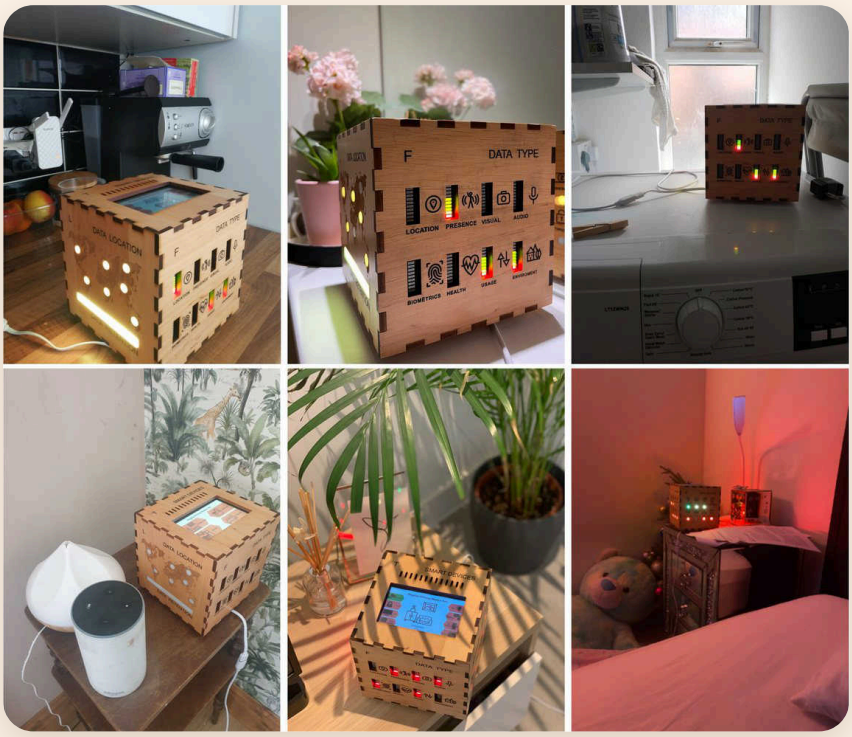
**Privacy Concerns, Barriers, and Solutions for Older Adults Using Intern…**
**Enhancing Privacy Management for Older Adults** 2025
**Enhancing Privacy Awareness and Digital Skills in Smart Home Device U…**
**EchoEase: Multimodal Privacy Controls for People with an Intellectual D…**
**Voice-Enabled Privacy Assistant Towards Facilitating Successful Ageing…**

01

PRIVACY FLUID

# PrivacyCube

Making smart-home privacy practices visible in everyday life




Six photographs of PrivacyCube in home settings, with its lights and touch screen on.

Smart-home devices collect information without always giving people an understandable account of what happens to it. Long privacy policies are difficult to navigate, and many devices offer little space for a notice. The survey behind PrivacyCube organises the questions a notice should answer and the choices designers can make about how that information is presented and explored.

PrivacyCube turns those questions into a physical object with lights and a touch screen. Its faces show aspects of data collection, use, access, storage and retention. Evaluations examine how people understand it in a focus group, in homes and at a public event. The findings concern small samples and self-reported awareness; the cube displays policy information rather than analysing device traffic.

**WHO**
Bayan Al Muhander

**WHEN**
2019 to 2025

**Scan for the project page**
iotgarage.net/go/privacycube

**p = 0.00041**
increase in self-reported privacy awareness in eight households after two weeks with the cube. The small sample limits generalisation.
ACM Transactions on Internet of Things, 2025

**42**
articles surveyed to develop the privacy-management toolkit. The toolkit itself was not tested with users in this paper.
ACM Transactions on Internet of Things, 2023

- The survey provides a design toolkit for privacy notices.
- PrivacyCube makes policy information visible through a physical interface.



**ALL PAPERS**

**PrivacyCube: Data Physicalization for Enhancing Privacy Awareness in…**

**Interactive Privacy Management** Al Muhander, Wiese, Rana, Perera • ACM Tr…

PRIVACY FLUID

# 01 PriviFy

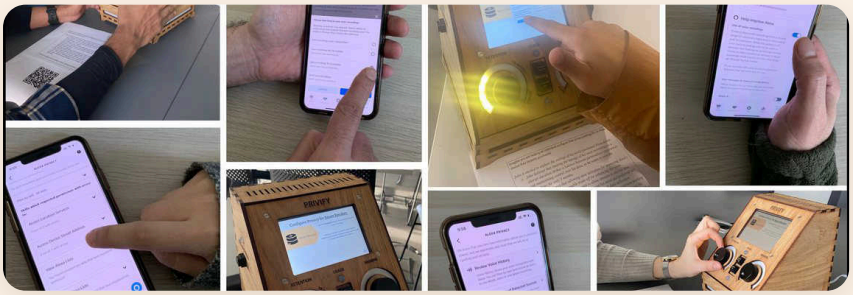
Physical controls for changing smart-device privacy preferences




Side and front views of PriviFy, with a touch screen, rotary controls and buttons.

Understanding a privacy policy is only part of managing a connected home. People also need to find and change the settings that govern their devices. PriviFy explores a dedicated physical interface for that task, bringing controls for retention, use and sharing into a wooden tabletop object rather than leaving them scattered through an application's settings menus.

The prototype combines a touch screen, knobs, buttons and lights, and a demonstration paper introduces the tangible interface. The fuller evaluation compares it with a commercial smart-speaker application in a controlled task. Participants used both interfaces, allowing a direct comparison. The study does not separate the effect of physical controls from the advantage of having a specialised interface designed for that task.



Hands using PriviFy and a smartphone privacy interface during study tasks.

**WHO**
Bayan Al Muhander

**WHEN**
2019 to 2025

**Scan for the project page**
iotgarage.net/go/privacycube

**82.8 vs 45.7**
mean usability scores for PriviFy and the Alexa application in a counterbalanced study with 20 participants. One smart-speaker scenario; the comparison does not isolate tangibility from interface specialisation.

- Knobs and buttons provide direct access to privacy settings.
- The demonstration and fuller evaluation are separate outputs in the same KB paper lineage.

**ALL PAPERS**

**PriviFy: Designing Tangible Interfaces for Configuring IoT Privacy Pref…**

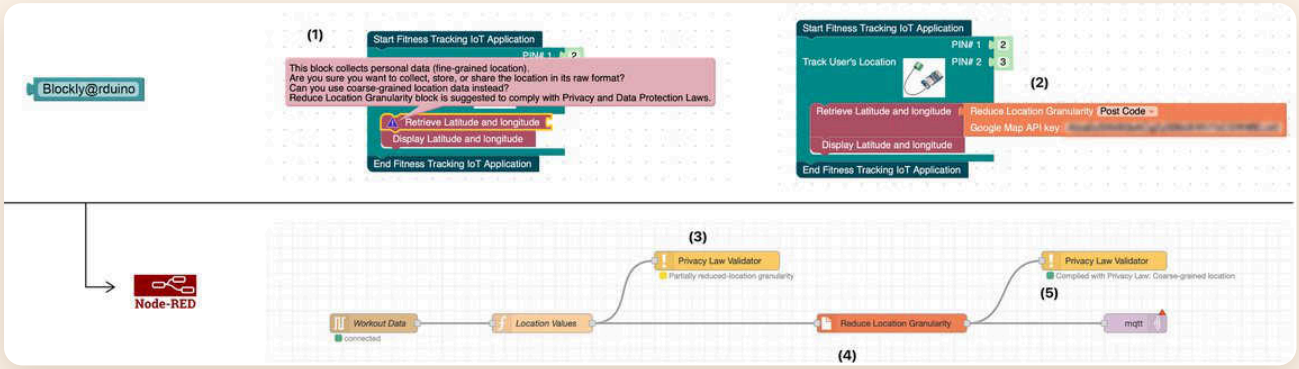
**PriviFy: Designing Tangible Interfaces for IoT Privacy Configuration** Al …

01

PRIVACY FLUID

# Canella

Privacy building blocks inside the tools developers already use




A warning appears when a block collects precise location, and a Reduce Location Granularity block and node are added in Blockly@rduino and Node-RED.

Developers of connected products, the Internet of Things (IoT), are expected to follow privacy laws such as GDPR from the start. Most are not privacy experts. The laws are written for lawyers, and a product sold in several countries faces several laws at once. Common development tools give little help with building privacy protection into an application.

The project compared privacy laws and mapped them to established design patterns. Canella turned this knowledge into privacy blocks and nodes for visual programming tools, warning developers about personal data and suggesting safer options. Focus groups and a lab study shaped and tested the prototype. Further work adds privacy education to these tools.

**WHO**
Atheer Aljeraisy

**WHEN**
2019 to 2026

**Scan for the project page**
iotgarage.net/go/canella

## 5 laws

on privacy and data protection were merged into one combined framework and mapped to 73 privacy patterns. This is the authors' analysis and is not legal advice.

ACM Computing Surveys, 2021

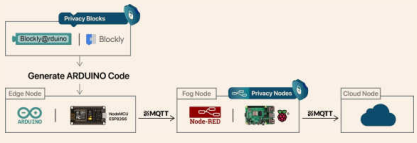
## 100

focus-group participants in 25 groups helped shape the design of Canella.

Proceedings of the ACM on IMWUT, 2024




NASA-TLX workload ratings, lower is better: the group using Canella (experimental) against the control group.




Canella architecture: privacy blocks in Blockly@rduino on the device, and privacy nodes in Node-RED, linked through to the cloud.

- Canella adds privacy blocks to Blockly@rduino and privacy nodes to Node-RED, two visual programming tools.

**ALL PAPERS**

**Privacy Education and Compliance** 2026
**Canella: Privacy-Aware End-to-End Integrated IoT Development Ecosys…**
**Empowering IoT Developers with Privacy-Preserving End-User Develop…**
**Privacy Laws and Privacy by Design Schemes for the Internet of Things…**

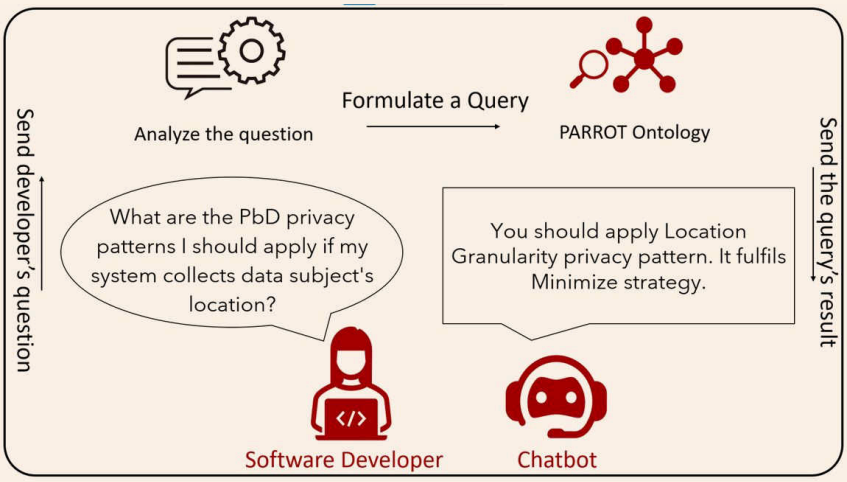
01

PRIVACY FLUID

# Privacy Captain

A knowledge base that answers developers' privacy design questions

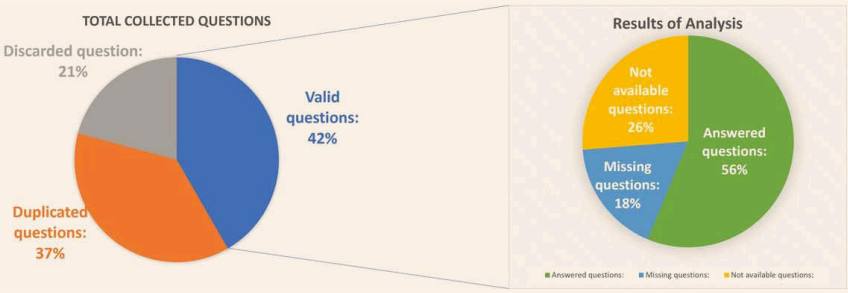



A developer asks which privacy pattern applies when a system collects location. The chatbot, using the PARROT ontology, suggests Location Granularity.

A developer who wants to build privacy into a connected product finds principles, strategies, guidelines and dozens of design patterns, with no map between them. Internet of Things (IoT) systems make this harder, because data moves across many devices. Developers also want to know why a privacy measure helps, and not only be told to use it.

The project first examined 74 privacy patterns against ten Privacy by Design schemes and applied them to three IoT use cases. It then built PARROT, an ontology: a structured knowledge base a computer can query. PARROT was shaped by questions that software developers asked in workshops. It was tested in a study where a researcher answered developers' questions using only the ontology.




Pie charts from the user study: 56% of valid questions answered, 18% missing from the ontology, 26% with no available answer.

**WHO**
Lamya Alkhariji

**WHEN**
2018 to 2022

**Scan for the project page**
iotgarage.net/go/privacy-captain

**74**
privacy patterns were examined against ten Privacy by Design schemes by two independent researchers.

ACM Transactions on Multimedia Computing, Communications, and Applications, 2021

**56%**
of the valid privacy questions developers asked were answered by the PARROT ontology. Answers were delivered by a person (Wizard of Oz) with 10 participants, not by a working chatbot.

Future Generation Computer Systems, 2023

- Privacy Captain is the project's assistant concept. PARROT is the ontology, or knowledge base, behind it.
- It is for software developers designing IoT applications.

**ALL PAPERS**

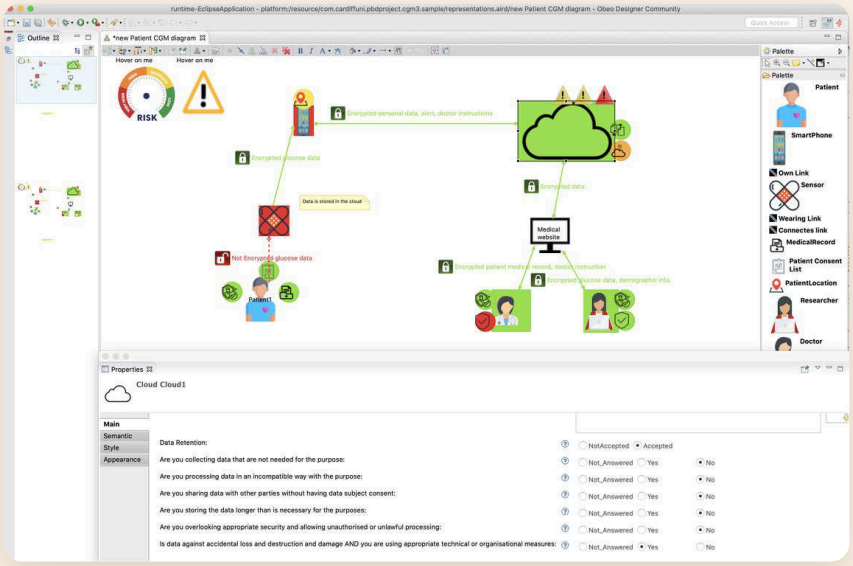
**Semantics-based Privacy by Design for Internet of Things Applications...**
**Synthesising Privacy by Design Knowledge Towards Explainable Inter...**
**Ontology Enabled Chatbot for Applying Privacy by Design in IoT Syste...**

01

PRIVACY FLUID

# Privacy Parrot (PARROT)

A design tool that prompts developers to build privacy in early



The PARROT interface: design area, palette and privacy feedback.

Connected devices such as health monitors and smart home sensors collect sensitive personal data. The law expects privacy to be built in from the start, an idea called Privacy by Design. In practice developers rarely follow it. Developers and privacy lawyers use different terms, so designs often reach the lawyer with gaps that are costly to fix late.

PARROT is an interactive design tool. As a developer draws a system, it asks simple Yes or No questions, colours each part by privacy risk and suggests privacy patterns (proven ways to solve common privacy problems). It was built with a privacy lawyer and tested in controlled lab studies against Mural, a plain online whiteboard tool, first on a health scenario and later on smart homes and online pharmacies.




A researcher stands beside a conference poster titled 'Privacy-Patterns for IoT Application Developers'.

**WHO**
Nada Alhirabi, Stephanie Beaumont, Omer Rana, Charith Perera

**WHEN**
2018 to 2022

**Scan for the project page**
iotgarage.net/go/privacy-parrot

## 14 developers

scored significantly higher on privacy when they designed with PARROT than when the same developers used a plain whiteboard tool (Wilcoxon p = 0.0005). Controlled lab study on set use cases, not real projects.

Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 2023

## 3 of 47

design notations published between 1999 and 2019 cover privacy, while 33 support security. This survey shows the gap that PARROT targets; it does not evaluate PARROT.

ACM Transactions on Internet of Things, 2021

- A design-time tool for software developers who build Internet of Things applications.
- Turns privacy law and Privacy by Design ideas into prompts, colour-coded feedback and privacy-pattern suggestions.

**ALL PAPERS**

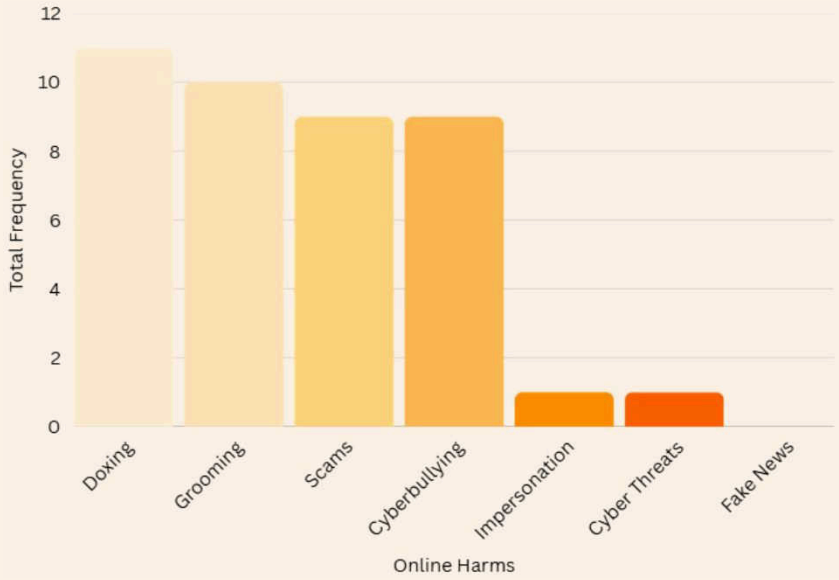
**Designing Privacy-Aware IoT Applications for Unregulated Domains** Al...
**Privacy-Patterns for IoT Application Developers** Alhirabi, Beaumont, Ran...
**Security and Privacy Requirements for the Internet of Things** Alhirabi, ...
**PARROT: Interactive Privacy-Aware Internet of Things Application Desi...**
**PARROT: Privacy by Design Tool for Internet of Things** Alhirabi, Rana, Pe...

01

PRIVACY FLUID

# Assisting Young People with Neurodiversity

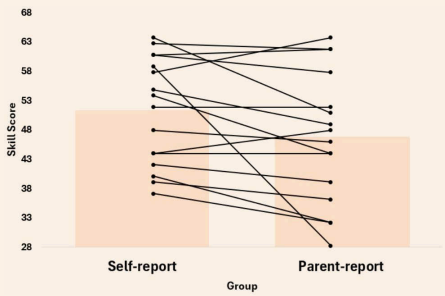
Helping neurodivergent young people stay safe online




How often each online harm was ranked number one.

Neurodivergent young people, for example those with autism, dyslexia or ADHD, use the internet every day. Yet their own views are under-represented in research, and most existing work focuses on vulnerability. Online safety resources are seldom designed with these learners in mind, which leaves a gap in accessible safety information and support.

The team ran four weekly workshops in each of seven secondary schools in South Wales. The workshops combined creative activities, questionnaires, a privacy-policy review and scam scenarios, and parents answered parallel questionnaires. The published study describes the internet as a social space, a personal space and a risky space. The project is also developing Safety Cube, a tangible device for online safety education.




Self-reported against parent-reported digital skills; lines join each pair.

**WHO**

Charith Perera, Georgina Powell, Kira Nurse

**PROGRAMME**

Google Research Scholar • 2024 to 2026

**Scan for the project page**

iotgarage.net/go/neurodiversity

**57 + 39**

neurodivergent young people aged 11 to 13 and parents took part, through 28 one-hour school workshops

ACM ASSETS, 2026

- A Google Research Scholar project with partners Innovate Trust, Digital Communities Wales and Ofcom.
- Asks neurodivergent young people themselves about being online, alongside their parents.
- Doxing (publishing someone's private details) and scams were prominent worries; these are worries, not measured incidents.



**ALL PAPERS**

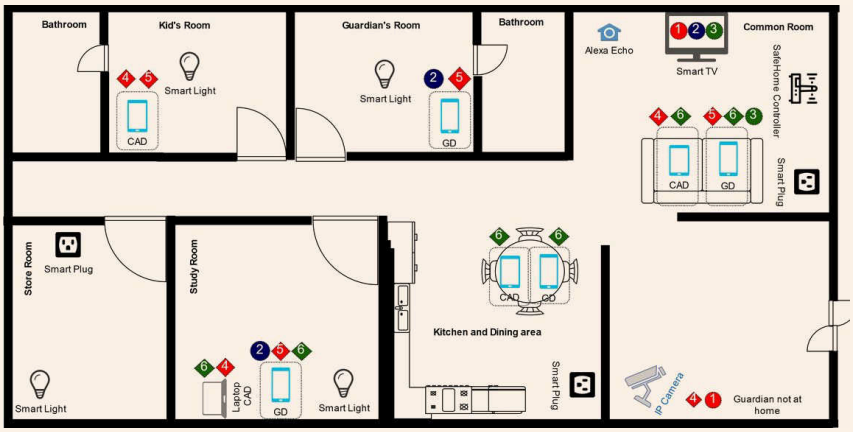
**Online Experiences and Safety of Neurodivergent Young People** Nurse, ...

01

PRIVACY FLUID

# mySafeHome

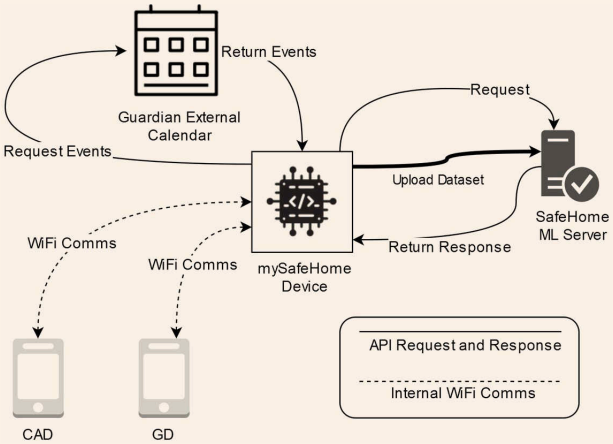
Smart-home access for children that adapts to where a parent is




The six demonstration scenarios on the home floor plan.

Children reach the internet through more and more devices, including connected televisions and fridges. Parents who are less confident with technology find it hard to protect children from harmful content and services. Existing parental controls usually just allow or block. They do not adapt to whether a parent is actually present with the child.

mySafeHome is a prototype home gateway built on a Raspberry Pi, a small low-cost computer. It uses Wi-Fi signal strength to judge how close a guardian is, together with a schedule and the guardian's calendar. It then limits or opens up a child's internet access. The system does not judge content itself. It was shown on six scripted scenarios.




Dynamic access control from RSSI (Wi-Fi signal strength) readings.

**WHO**
Yasar Majib, Charith Perera

**WHEN**
2019

**Scan for the project page**
iotgarage.net/go/mysafehome

**6**

scripted use-case scenarios demonstrated: three with a smart TV and three with a child's mobile or tablet. A prototype demonstration, with no user study or deployment with real families.

IEEE World Forum on Internet of Things (WF-IoT), 2020

- A home-level firewall that controls internet access for all device types.
- Gives granular levels of access, not only allow or block.
- Keeps the parent as the decision maker instead of relying on automated content filtering.



**ALL PAPERS**
**Context Aware Family Dynamics based Internet of Things Access Contr...**

PART 02

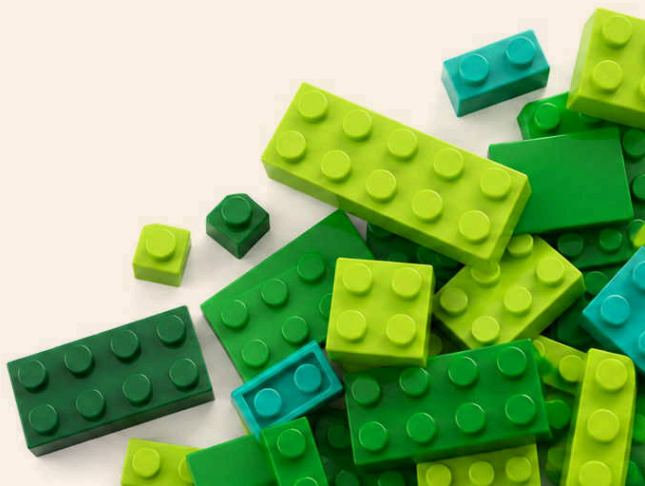
# 02



# Data Observatory

Data from many places, joined up so that people can ask it questions.


Sensing as a Service: the idea 22
Sensing as a Service: making it real 23
Finding the right sensor 24
ForestQB 25
FooDS and PoachNet 26
Forest Health Index 27
BearWave 28
Talking Buildings 29
STREAM 30
WoT-AI Explorer 31
Forest Observatory 32
Listening to the forest 33
Reading number plates at the edge 34
Following a poacher's vehicle through the jungle 35
Pan-Borneo Elephants 36
EventCam.AI 37
CamTrap.AI 38
Smart City Data Markets 39
Reading a city's air 40
Talking Aquifer 41

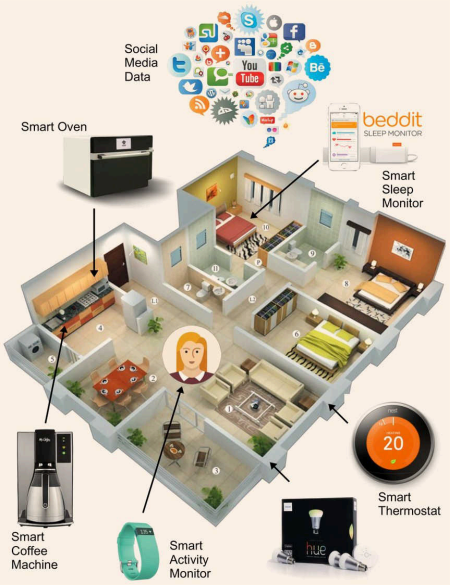



02

DATA OBSERVATORY

# Sensing as a Service: the idea

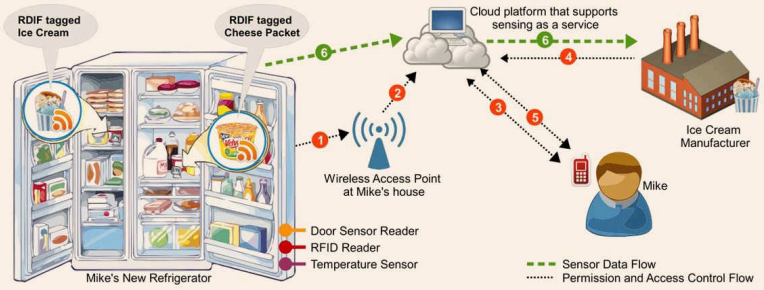
Giving people a say in how their device data is shared




The roadmap illustrates connected appliances and personal devices around a home.

Smart devices collect information about daily life, but it often stays inside separate services. People may have little control over sharing it, while organisations cannot easily find information that could help them. Sensing as a Service explores a market where device owners choose to share data and receive rewards or useful advice in return.

The buying and selling article introduces the idea, the roadmap develops its research questions, and the ecosystem paper sketches the services needed to support it. Together they describe how owners, markets and analysts could work together. These are proposals for a future system, with privacy, negotiation and ease of use still needing practical solutions.




A refrigerator scenario links household sensors, an owner and a manufacturer through a cloud service.

**WHO**

Charith Perera, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos and colleagues

**Scan for the project page**

iotgarage.net/go/s2aas

- Owners would choose which data to share.
- Rewards could include money, vouchers or useful advice.
- The ecosystem includes personal data storage, trading and analysis.

**ALL PAPERS**

**Designing the Sensing as a Service Ecosystem for the Internet of Thing…** **Sensing as a Service for Internet of Things** Perera • Leanpub Publishers, 2…

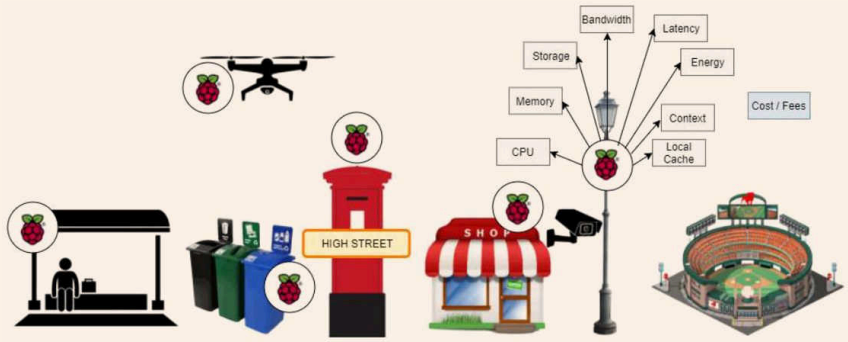
**Sensing as a Service (S2aaS)** Perera • IEEE Internet of Things eNewsletters, …

02

DATA OBSERVATORY

# Sensing as a Service: making it real

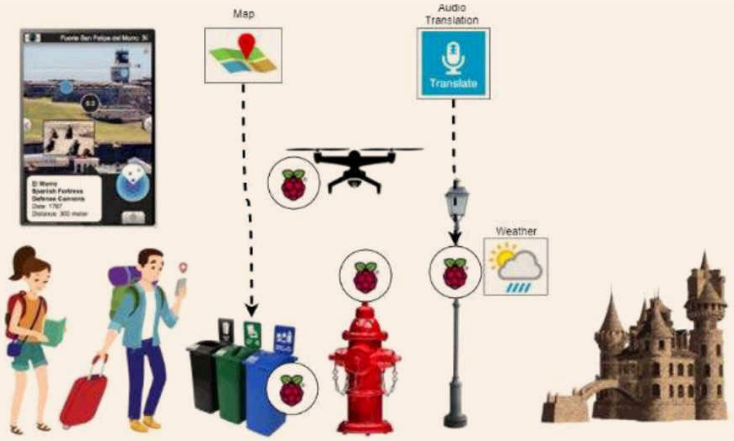
Renting nearby devices and keeping household data under control




A high-street scenario places computing nodes on street furniture and other infrastructure.

A business may need sensor readings for a short period without wanting to buy and install equipment. A household may be willing to share information but want a say in what leaves the home. These papers explore the practical arrangements that could make shared sensing useful while keeping control with the people providing the data.

The rentable infrastructure article imagines borrowing sensing and computing resources already installed nearby. The Databox paper describes a personal data container that checks sharing requests against household preferences. Both identify work needed on finding resources, arranging tasks, negotiating access and judging privacy risks. They set out designs and research challenges without reporting a working deployment or measured benefits.




A tourism scenario shows nearby devices offering maps, translation and weather services.

**WHO**

Charith Perera, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos and colleagues

**Scan for the project page**

iotgarage.net/go/s2aas

- Existing infrastructure could serve additional users for a fee.
- A Databox would act as a gatekeeper for personal data.
- Access requests need to respect household privacy preferences.

**ALL PAPERS**

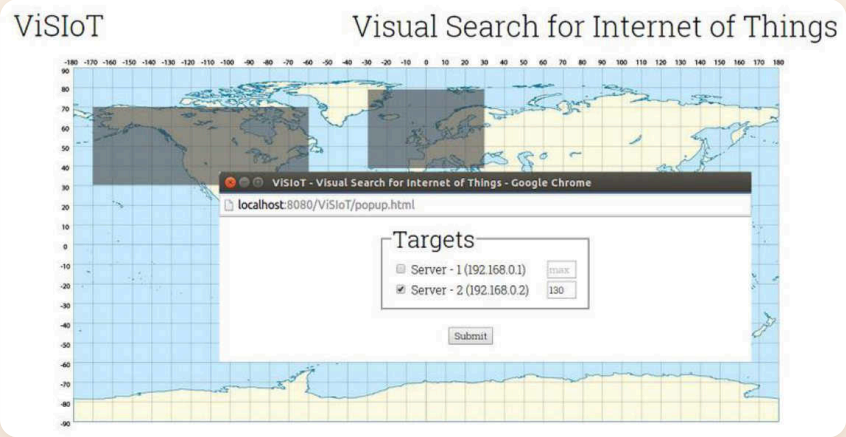
**Rentable Internet of Things Infrastructure for Sensing as a Service (S2…**

**Valorising the IoT Databox** Perera, Wakenshaw, Baarslag, Haddadi et al. • Tra…

DATA OBSERVATORY

# 02 Finding the right sensor

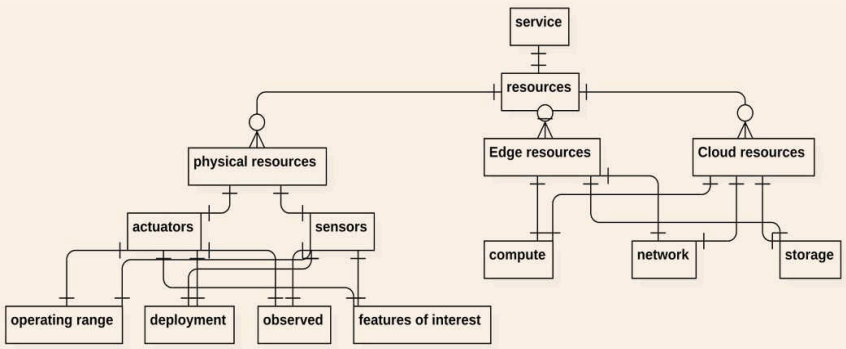
Choosing useful devices and services from a crowded network




The ViSIoT interface combines a world map with a target-server selection window.

Finding a sensor is only the start. Its location, cost and other properties must suit the task, and the surrounding computing services must work together. These studies ask how to choose useful resources from large collections, how to judge the quality of those choices, and how to help people configure a connected application.

ViSIoT offers a map interface for searching sensor repositories and preparing resources for use. Related studies compare selection methods, examine the effect of user preferences and add a filtering step to improve choices. IoT-CANE brings knowledge about devices and services into a shared model and recommends configurations. The evidence combines software benchmarks with a small expert questionnaire.




The IoT-CANE model links sensors and physical devices with computing, network and storage resources.

**WHO**

Luiz H. Nunes, Julio C. Estrella, Alexandre Cladio Botazzo Delbem, Stephan Reiff-Marganiec, Charith Perera

**Scan for the project page**

iotgarage.net/go/resource-discovery

**4× to 8.5×**

the running time of TOPSIS for the added Elimination-Selection step in this case study, trading speed for better selection quality.

IEEE Consumer Communications & Networking Conference, 2018

**< 2 minutes**

to deploy 100,000 virtual sensors in the ViSIoT performance test. Ranking properties were generated; this was not a usability study.

International Journal of Services Computing, 2016

- Selection quality matters alongside search speed.
- Several comparisons use generated sensor properties.

**ALL PAPERS**

**IoT-CANE: A unified knowledge management system for data-centric Int…**
**Multi-criteria IoT resource discovery** Nunes, Estrella, Perera, Reiff-Margani…
**A Distributed Sensor Data Search Platform for Internet of Things Enviro…**
**The Elimination-Selection Based Algorithm for Efficient Resource Disco…**
**The Effects of Relative Importance of User Constraints in Cloud of Thin…**

02

DATA OBSERVATORY

# ForestQB

Asking a wildlife database questions without writing code



A researcher on a forest path holds up a hand-held tracking antenna.

Wildlife researchers at the Danau Girang Field Centre in Borneo hold long-running sensor and field-survey records. Linked data connects records, but getting answers normally means writing queries in a specialist language called SPARQL. The project reviews ways to make linked data easier to explore and works with ecologists who need access to it.

ForestQB puts two tools side by side: a form-and-map query builder and a chatbot called ForestBot. A researcher can ask a question in plain words, see the filters it produces, adjust them and get results. The design drew on a field study at the centre. It was tested with 18 bioscience participants, and later work added large language models to handle harder questions.

**WHO**
Omar Mussa

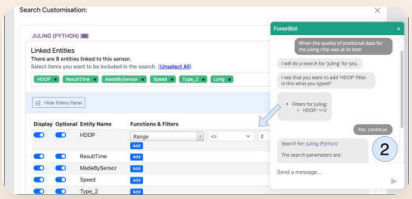
**WHEN**
2021 to 2024

**Scan for the project page**
iotgarage.net/go/forestqb

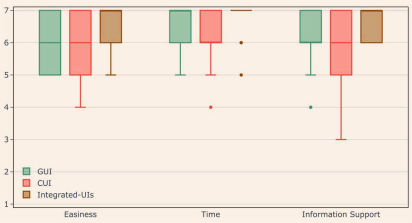
**100% vs 39%**
first-attempt correct completion on the hardest task: chatbot and query builder together, against the chatbot alone (18 participants from one school, set tasks, one dataset)
ACM Journal on Computing and Sustainable Societies, 2024

**89.2%**
GPT-4o accuracy turning complex filter questions into search settings, given a few examples (the authors' own 40-question test set, one observatory's data)
ACM Transactions on the Web, 2026

- A query builder and a chatbot that work together, so users never write SPARQL.
- Built for bioscience researchers working with Danau Girang Field Centre data.




ForestBot chat beside the ForestQB filter panel, turning a typed question into search filters.




Post-task satisfaction for the graphical, chatbot and integrated interfaces (7 is best).

**ALL PAPERS**

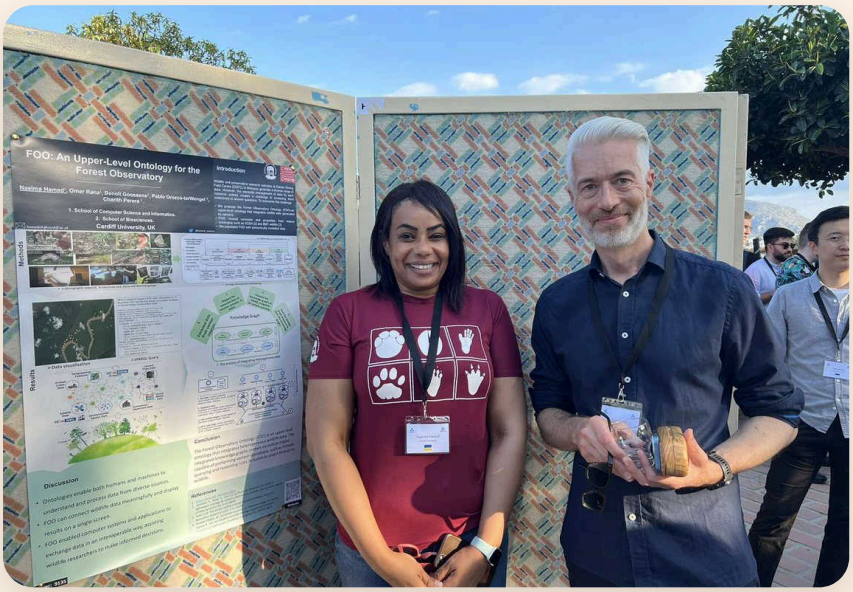
**Towards Usable Linked Data Retrieval** 2026
**ForestQB: Enhancing Linked Data Exploration through Graphical and Co…**
**ForestQB: An Adaptive Query Builder to Support Wildlife Research** Muss…
**Dialogue Meets Data** Mussa, Rana, Goossens, Orozco ter Wengel, et al. • ACM …
**Towards Enhancing Linked Data Retrieval in Conversational UIs using L…**

02

DATA OBSERVATORY

# FooDS and PoachNet

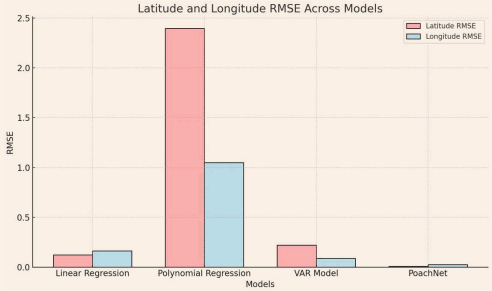
Joining up forest wildlife data to help predict poaching risk




Naeima Hamed at ESWC 2023, standing with a second person in front of the FOO poster.

A forest research station collects many kinds of data: GPS collars, soil measurements, vegetation surveys, camera-trap images and field notes. Each sits in its own format, so questions that cut across them are hard to answer. A review of 13 Open Data Observatories identified four recurring challenges: integrating data, keeping its quality, recording where it came from, and protecting privacy.

The project built FOO, a shared vocabulary (an ontology) for forest observatories, and used it to turn four wildlife datasets from the Danau Girang Field Centre into linked knowledge graphs called FooDS. PoachNet then uses such a graph to predict an elephant's next GPS position and flags risk near oil-palm plantations. It was trained on one elephant and tested offline.




RMSE comparison between PoachNet and baseline models.

**WHO**
Naeima Hamed

**PROGRAMME**
EPSRC, Global Challenges Research Fund (GCRF) • 2020 to 2024

**Scan for the project page**
iotgarage.net/go/foods-poachnet

**94% vs 72%**
FOOPS! FAIR score for the FOO ontology, against the SOSA ontology (shows FAIR compliance, not semantic quality or adoption)
ACM Journal on Computing and Sustainable Societies, 2025

**0.0166**
average RMSE (prediction error) for PoachNet's next-position forecast; linear regression scored 0.144 (one elephant, offline test)
Sensors, 2024

**13**
Open Data Observatories compared, all facing the same four data-management challenges
ACM Journal of Data and Information Quality, 2025

- FOO is an ontology (a shared vocabulary) for forest observatory data.
- FooDS links four wildlife datasets from one field centre so they can be queried together.

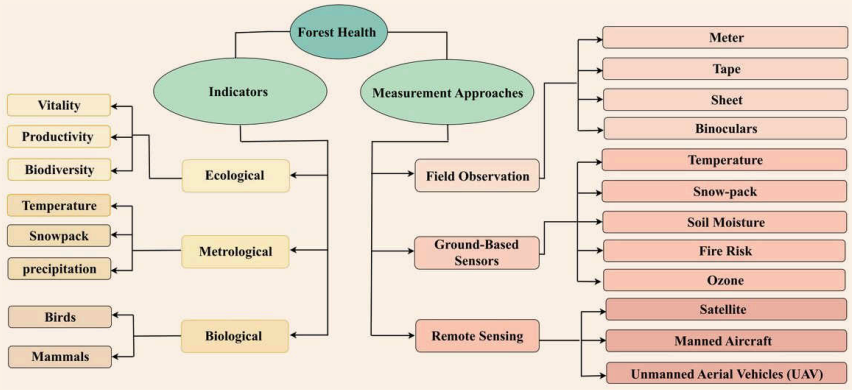
**ALL PAPERS**

**A Comparison of Open Data Observatories** Hamed, Rana, Orozco-terWenge…
**PoachNet: Predicting Poaching Using an Ontology-Based Knowledge Gr…**
**FooDS: Ontology-based Knowledge Graphs for Forest Observatories** Ha…
**FOO: An Upper-Level Ontology for the Forest Observatory** Hamed, Rana, …

DATA OBSERVATORY

# 02 Forest Health Index

Combining sensors, drones and satellites to judge forest health




Forest health measurement approaches and indicators.

Is a forest healthy? There is no single measurement that answers this. Foresters look at many signs, such as vitality, biodiversity, temperature and soil moisture, and they gather them in different ways: by walking the site, with sensors on the ground, and from drones, aircraft and satellites. Bringing these sources together into one picture is hard, and each forest has its own priorities.

The project began with a systematic review that links forest health indicators, sensing technologies and artificial intelligence to sustainable forest management. Its main message is that forest health assessment needs several data sources together. The follow-on work is ForestPulse, a web tool that lets forest managers choose and weight their own indicators and view the results.

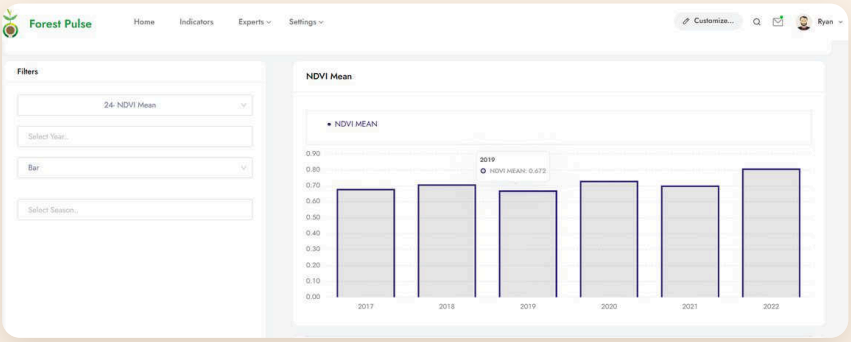
**WHO**
Rayan Binlajdam

**WHEN**
2022 to 2026

**Scan for the project page**
iotgarage.net/go/forest-health

**215**
studies from 2015 to 2025 covered in a PRISMA (structured) literature review
ACM Journal on Computing and Sustainable Societies, 2025

- A published review of how sensing and AI are used to assess forest health.
- The review does not propose or validate a universal forest health index.
- Partner: Danau Girang Field Centre.




The ForestPulse interface, with controls for choosing an indicator and a chart of the selected indicator over time.



**ALL PAPERS**

**ForestPulse: Designing and Evaluating a Configurable Framework for C…**

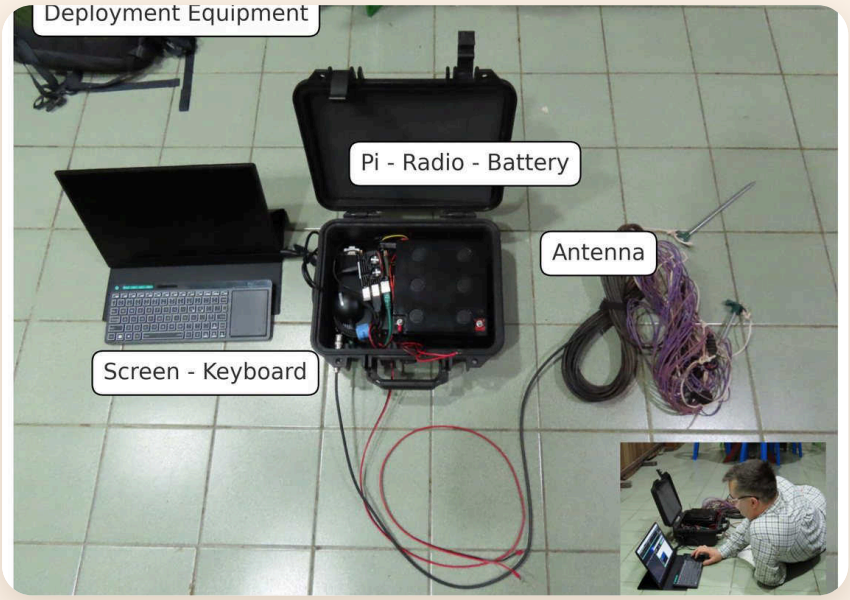
**Sustainable Forestry with Artificial Intelligence** Binlajdam, Meedeniya, J…

02

DATA OBSERVATORY

# BearWave

Low-power radio alerts from deep forest, bounced off the sky




Deployment equipment laid out on a tiled floor: a case holding the Pi, radio and battery, a screen and keyboard, and a coiled antenna.

In Borneo, sun bears are caught in humane traps for research. Staff must check each trap every day, moving through dense and risky rainforest. A simple radio alert would save those trips, but common options struggle: LoRaWAN and Sigfox signals are blocked by the canopy, satellite links need clear sky and a subscription, and there is no mobile coverage.

BearWave sends a small alert almost straight up on shortwave radio. The upper atmosphere reflects it back down over the trees, a technique called NVIS. Initial trials took place in UK woodland as a stand-in for rainforest. Subsequent field work examines the system in the Borneo rainforest, where terrain and forest cover make communication difficult.




IoT Garage researchers at ACM COMPASS 2025 in Toronto.

**WHO**
Mark Butterworth

**WHEN**
2020 to 2025

**Scan for the project page**
iotgarage.net/go/bearwave

**97% • 93% • 94%**
of messages delivered in three one-week UK woodland trials: Belpha Farm, Clydach and Brockweir Wood (not tested in Borneo in this paper)
ACM COMPASS, 2025

- Sends trap and sensor status alerts where there is no mobile or network coverage.
- Uses NVIS: a shortwave signal sent upward and reflected back down by the ionosphere.
- Transmits at 1 W on a 5 MHz single-band antenna.



**ALL PAPERS**

**HF Communication for Rainforest Wildlife Monitoring** 2026

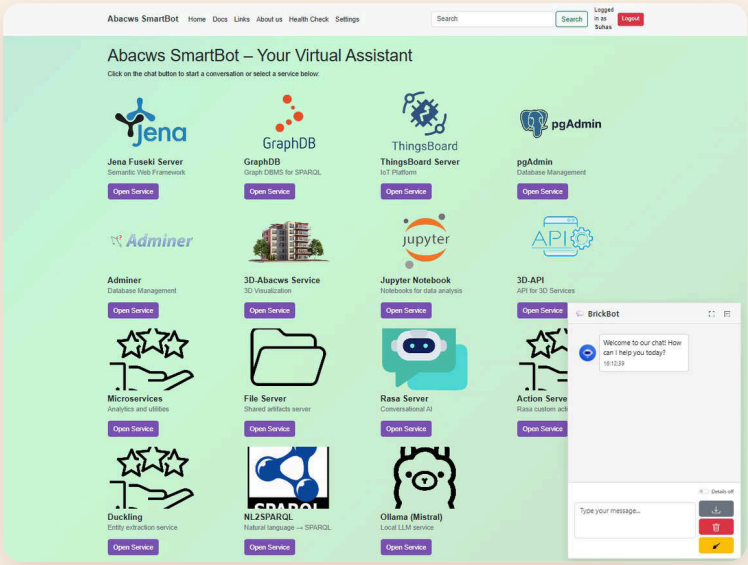
**Enhancing Remote Conservation in Borneo** Butterworth, Rana, Orozco-te…

02

DATA OBSERVATORY

# Talking Buildings

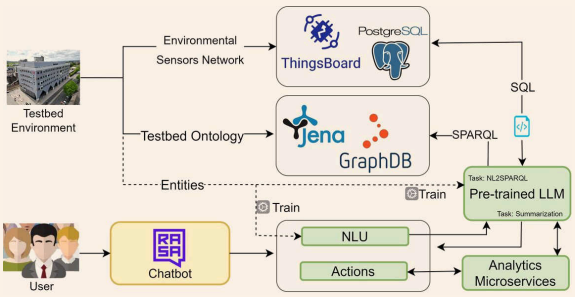
Ask a smart building questions in plain English




The Abacws SmartBot home screen, with tiles for its services and a chat window open.

Modern buildings carry a great many sensors for air quality, temperature and energy. The readings could help people run buildings in a healthier and greener way, but they sit in databases that only specialists can query. A facilities manager or an occupant who simply wants to know about the air in one room has no easy way to ask.

The project surveyed sensors and ways people engage with buildings, then built OntoSage, a chatbot that turns questions into database queries and replies in plain language. It uses a structured description of a building to find sensors and was tested in Abacws. Further work explores conversation when data is incomplete and ways to discover readings by time and place.




Testbed set-up: the building sensor network, the testbed ontology and the chatbot that links users to them.

**WHO**
Suhas Devmane

**WHEN**
2021 to 2025

**Scan for the project page**
iotgarage.net/go/talking-buildings

**85% • 88%**
exact match and execution accuracy when turning plain-language questions into database queries (held-out test set, one building)
World Wide Web, 2026

**219**
articles and 8 sustainability standards reviewed in the survey
ACM Computing Surveys, 2026

- OntoSage answers natural-language questions about a smart building.
- For people who are not data experts, such as building managers and occupants.



**ALL PAPERS**

**OntoSage+: Designing and Evaluating Human-Smart Building Conversa…**
**Utilizing Internet of Things in Human-Building Interaction to Support …**
**Spatio-Temporal Semantic Data Discovery for Sustainable Building Man…**
**OntoSage: Intelligent Human-Building Smartbot for Semantic Smart Bu…**
**Talking Buildings** Devmane, Rana, Lannon, Perera • WISE, 2024

02

DATA OBSERVATORY

# STREAM

How pollution relates to wildlife in the Rivers Taff and Ely



**WHO**
Maya Lhoste

**PROGRAMME**
Natural Environment Research Council (NERC) • 2024 to 2028

**Scan for the project page**
iotgarage.net/go/stream

- Runs from 2024 to 2028.
- Studies the Rivers Taff and Ely.
- Current work is water-quality analysis with a reproducible dashboard pipeline.

Brick model for illustration; no photograph is filed for this project yet.

Rivers carry traces of what people put into them. STREAM, short for Two Rivers' eDNA and Anthropogenic Pollutant Monitoring, studies how the spread of pollutants relates to river wildlife in the Taff and the Ely in South Wales. Environmental DNA, or eDNA, means the genetic traces that living things leave in water, which can show what lives there without catching anything.

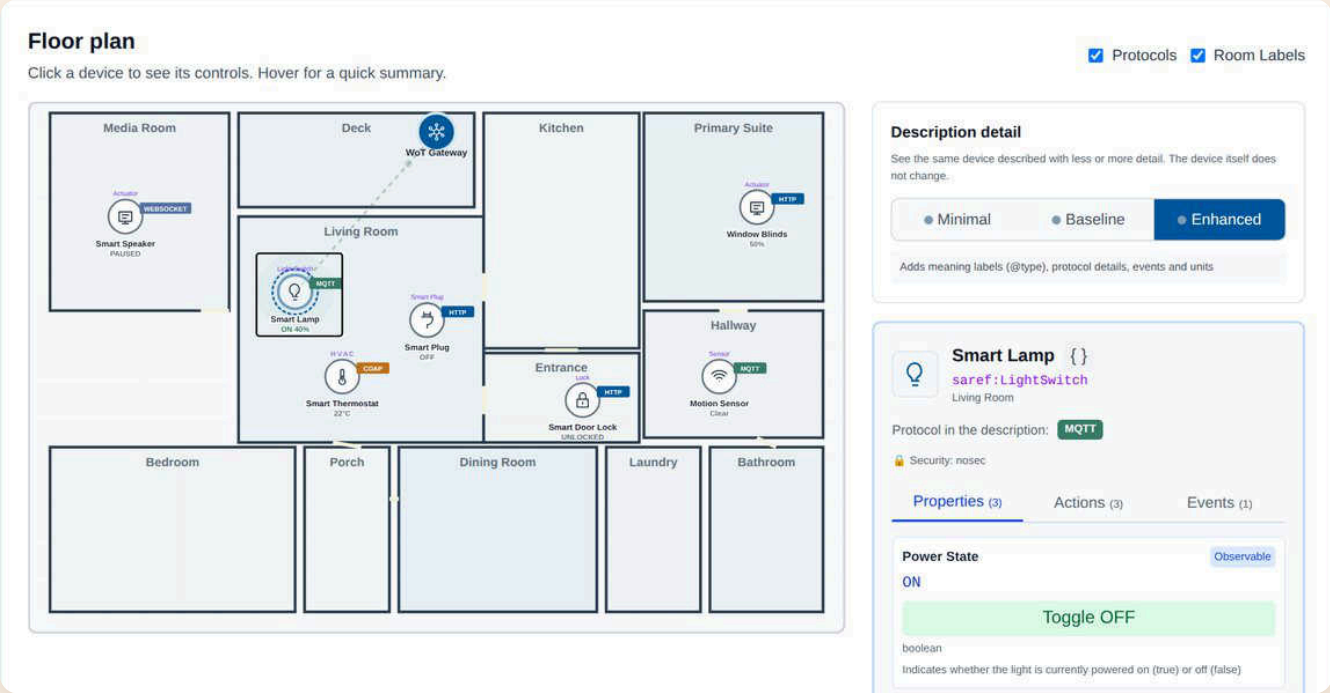
The project plans to combine eDNA analysis, chemical testing of pollutants, species tests and a dashboard for stakeholders. So far the filed work covers water-quality data: how pollutant levels vary along the River Ely and its tributaries, how temperature and acidity affect the readings, and how the Ely compares with other Welsh rivers. The eDNA part is future work.

02

DATA OBSERVATORY

# WoT-AI Explorer

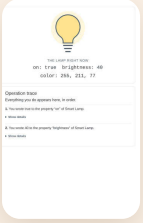
Learn how smart devices describe themselves, then see what AI adds




The virtual home floor plan in WoT-AI Explorer. The Smart Lamp is selected, and its controls and the protocol named in its description appear on the right.

Connected devices need a common way to explain what they can sense and control. Since 2024, WoT-AI has explored how the W3C Web of Things helps software understand those capabilities. A Thing Description is a machine-readable device fact sheet. The project asks how these descriptions can support clearer interaction, including requests made through AI language models.

The public WoT-AI Explorer brings that question into a browser-based learning journey. Visitors inspect a virtual lamp's description, operate it manually, add a language request and compare recorded model responses. Tutorials, narrated films and operation traces explain what happened. The simulated home needs no physical equipment or API key, letting learners explore the interface before considering real connected devices.



The simulated lamp's current state and the operation trace recording manual changes to its power and brightness.

**WHO**
Charith Perera

**PROGRAMME**
W3C Invited Expert • 2024 onwards

**Scan for the project page**
iotgarage.net/go/wot-ai

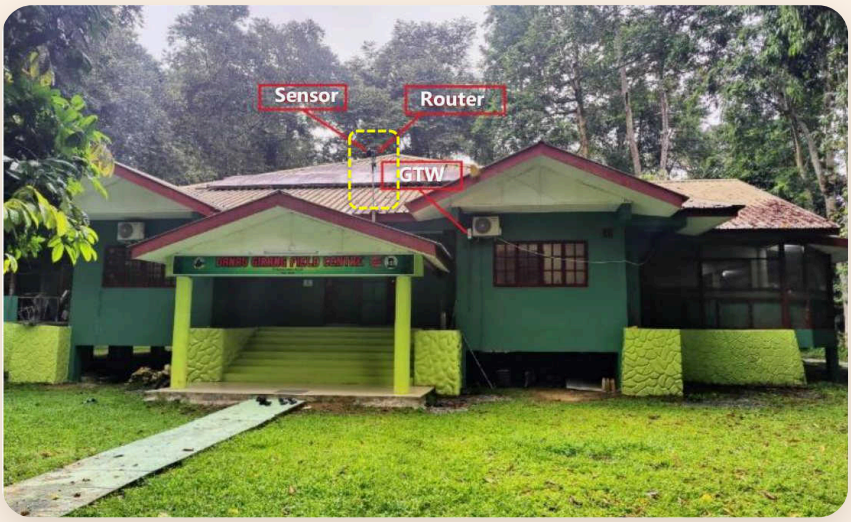
- Visit https://ngcharithperera.github.io/wot-ai/ to explore the simulated home and guided lamp activities.
- Recorded model responses are teaching examples; device states and timing belong to the simulator.
- Independently developed educational project with tutorials and narrated films; not an official W3C product.

02

DATA OBSERVATORY

# Forest Observatory

Connected research shaped by conservation work in Sabah




Installation location 1, the main building of the Danau Girang Field Centre, with labels marking the sensor, router and gateway.

In Sabah, Malaysian Borneo, conservation work at the Danau Girang Field Centre depends on reaching remote equipment and getting information through dense forest. The 2019 wildlife infrastructure report gathered practical challenges with field-centre staff. It set an agenda for sensing, communication and joined-up information. The later jungle network report describes a wireless mesh installation, turning part of that agenda into equipment at the site.

The hub connects projects with their own pages: Naeima Hamed's work gives forest records a shared vocabulary, Rayan Binlajdam's work examines forest health, and Mark Butterworth studies radio links through vegetation. Pan-Borneo elephants, EventCam and CamTrap address related monitoring questions, while poacher tracking explores threats to conservation. These linked efforts share a setting and motivation; each has its own methods, evidence and limits.



Rainforest on the bank of a muddy river.



Five people standing on steps outside a building during the 2019 field centre visit.

**PROGRAMME**
EPSRC International Partnerships
• 2021 to 2022

**Scan for the project page**
iotgarage.net/go/forest-observatory

- Works with Danau Girang Field Centre in Sabah, Malaysian Borneo.
- The infrastructure report identifies needs; the network report describes an installation.
- Linked projects develop different parts of the conservation research agenda.



**ALL PAPERS**

**Internet of Things Network for Forest Observatory (Sabah, Malaysia Bor…**

**Internet of Things for Efficient Wildlife Conservation** Perera, Rana, Goos…

DATA OBSERVATORY

# 02 Listening to the forest

With Prof. Dulani Meedeniya's team at the University of Moratuwa

**2023** **Map the methods**
A review of forest-sound recognition at the edge

**2023** **Gather the sounds**
FSC22, a public benchmark of forest sounds

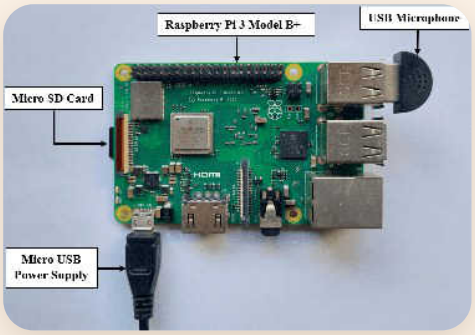
**2024** **Shrink the models**
Pruning and quantising models to fit the edge

**2024** **Design for the device**
ESC-NAS searches for models within hardware limits

**2025** **Listen for elephants**
Roars, rumbles and trumpets told apart from raw sound

## WHAT FSC22 LISTENS FOR: 27 SOUND CLASSES IN SIX FAMILIES

- **Mechanical** — axe, chainsaw, handsaw, generator
- **Forest threats** — firework, gunshot, wood chopping
- **Vehicles** — helicopter, vehicle engine
- **Human** — whistling, clapping, footsteps, speaking
- **Animals** — mammals, birds, insects, amphibians, reptiles
- **Environment** — thunderstorm, rain, wind, fire, tree falling




Test set-up: a Raspberry Pi 3 with a USB microphone.

Listening could help conservation teams recognise activity without watching every recording. With Prof. Dulani Meedeniya's team at the University of Moratuwa in Sri Lanka, the work begins with a forest-sound benchmark and a review of methods. FSC22 gathers public recordings into categories that researchers can share. The review connects sound preparation, recognition models and hardware, giving later experiments a common starting point.

The next question is how to fit recognition into small devices. The compression study reduces existing models, while ESC-NAS searches for model designs with hardware limits in mind. ElephantCallerNet then explores recognising different elephant calls directly from sound waves. Together these papers link data, methods and device constraints. Their results come from curated recordings and benchmark tests; they do not establish performance in continuous forest monitoring.

**2,025 clips**
in 27 classes in the public FSC22 benchmark. These are curated FreeSound recordings, not recordings from a single forest site.
Sensors, 2023

**89%**
accuracy distinguishing elephant roars, rumbles and trumpets from raw audio. The test set has only 27 clips from public recordings.
Sensors, 2025

**Scan for the project page**
iotgarage.net/go/forest-observatory

ALL PAPERS

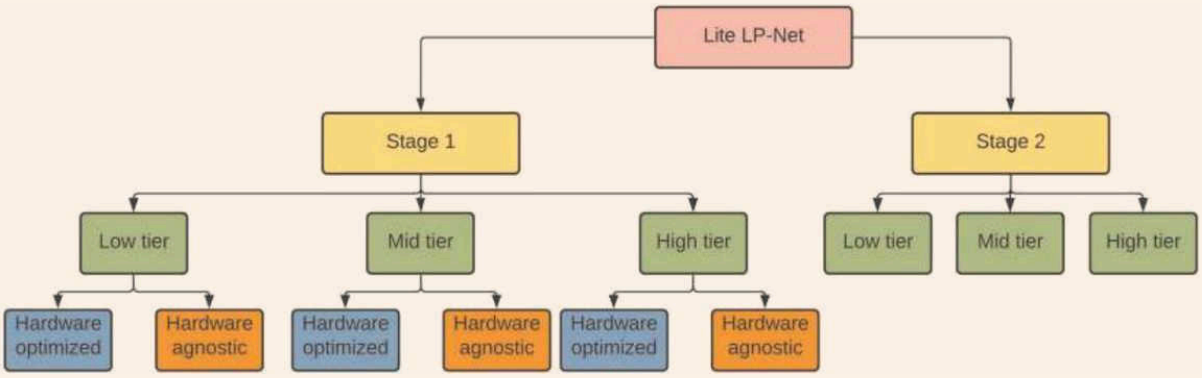
**Elephant Sound Classification Using Deep Learning Optimization** Dew…
**ESC-NAS: Environment Sound Classification Using Hardware-Aware Ne…**
**A Survey on Deep Learning-based Forest Environment Sound Classifica…**
**A Comparative Study of Preprocessing and Model Compression Techniq…**
**Forest Sound Classification Dataset: FSC22** Bandara, Jayasundara, Ariyar…

02

DATA OBSERVATORY

# Reading number plates at the edge

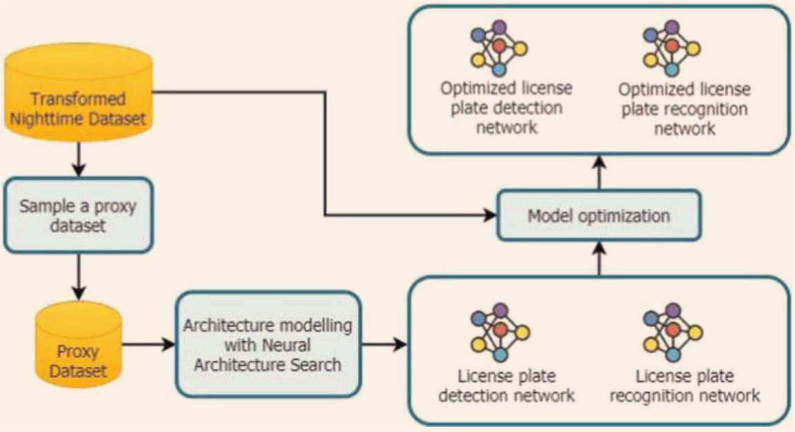
Small devices for recognising vehicles in difficult light




The Lite-LPNet family separates detection and recognition across low, mid and high hardware tiers.

Reading a vehicle's number plate becomes harder at night and away from mains power or internet access. Working with the University of Moratuwa in Sri Lanka, the survey maps existing recognition methods and their sensitivity to lighting. The model-search paper tackles that gap by designing smaller detection and reading models around the computing limits of different Raspberry Pi devices.

The companion system paper brings those models together with a camera, battery and mobile messaging. It explores a practical trade: cheaper hardware can run longer but takes more time to read a plate. The studies connect recognition methods to equipment choices rather than proving a conservation outcome. Real night-time testing is limited, so the system remains a proof of concept for difficult operating conditions.




Model search and optimisation produce separate plate-detection and plate-recognition networks.

**WHO**

Prof. Dulani Meedeniya and collaborators, University of Moratuwa, Sri Lanka

**Scan for the project page**

iotgarage.net/go/forest-observatory

## 98.73%

high-tier recognition accuracy on 100 real night-time images, compared with 98.95% for RPNet. This is recognition accuracy, not whole-system detection accuracy.

International Journal of Intelligent Systems, 2022

## about 132 hours

battery life for the cheapest build. This slower tier takes about 6 seconds per plate; the faster tiers have shorter battery life.

Sensors, 2022

- A collaboration with the University of Moratuwa, Sri Lanka.
- Models and equipment are chosen together for resource limits.

**ALL PAPERS**

**Automated License Plate Recognition for Resource-Constrained Enviro…**
**Automated License Plate Recognition** Shashirangana, Padmasiri, Meedeniy…
**License Plate Recognition using Neural Architecture Search for Edge De…**

02

DATA OBSERVATORY

# Following a poacher's vehicle through the jungle

Exploring Bluetooth checkpoints and location reports by text message

Conservation teams need to understand vehicle movements where power and connectivity are limited. These projects explore complementary approaches: record encounters with roadside Bluetooth beacons, or ask a GPS tracker to report by text message. Both focus on modest equipment and difficult connections, with careful limits on what their tests establish.



Brick model for illustration; no photograph is filed for these projects.

## Bluetooth vehicle checkpoints

**WHO** Karan Juj, Benoit Goossens, Pablo Orozco Ter Wengel, Charith Perera
**PROGRAMME** Global Opportunities Project • 2019

A concealed receiver in a vehicle can log encounters with roadside Bluetooth beacons, building a record of where it has passed. The study examines signal range, obstructions and the balance between broadcast interval and battery life. Its driving tests were carried out on a road in Watford, so they establish feasibility rather than successful tracking of poachers in jungle conditions.

**700 ms**

the slowest broadcast interval detected at 45 mph with the receiver under the bonnet. Each setting was driven only three times on a Watford road.

IEEE World Forum on Internet of Things, 2020

**Scan for the project page**
iotgarage.net/go/poacher-ble

## Location reports by text message

**WHO** Jack Burkett, Benoit Goossens, Pablo Orozco Ter Wengel, Charith Perera
**PROGRAMME** Global Opportunities Project • 2019

An inexpensive GPS locator receives a text message and replies with its position. A modem and a modified tracking platform collect the responses, while a scheduling service controls when devices are queried. The design aims to work without internet access at the tracker. Its account highlights the trade-off between frequent updates and battery life, with sensitive field details withheld.

- The locator replies through the mobile text-message network.

**Scan for the project page**
iotgarage.net/go/poacher-gps

**ALL PAPERS**

**Exploring the Suitability of BLE Beacons to Track Poacher Vehicles in Ha…**

**Low-Cost SMS Driven Location Tracking Platform Towards Anti-Poachin…**

02

DATA OBSERVATORY

# Pan-Borneo Elephants

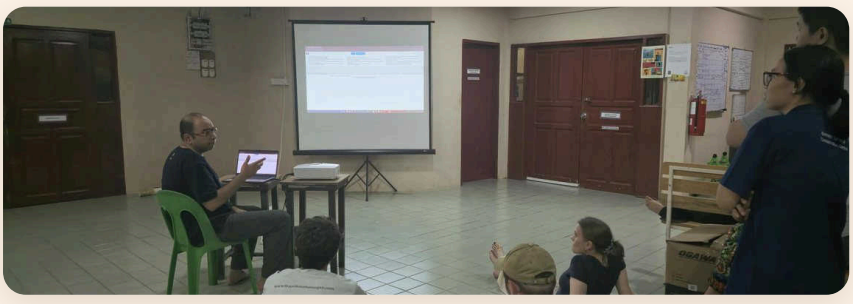
Helping elephants and a new highway share the forest in Sabah



Rainforest on the bank of a muddy river.

The Pan-Borneo Highway is Malaysia's largest infrastructure project. Several stretches in Sabah cut through forest reserves where Bornean elephants live. A road through elephant country can split herds from food and water, and it can bring more encounters between elephants and people. Planners need to know where and when the animals are most at risk before the building work reaches them.

The team plans to record how elephants use two forest reserves, using satellite images, tracking collars, camera traps and field surveys. It will then build a computer model to explore elephant movements before, during and after construction. IoT Garage contributes data pipelines, forecasting models and dashboards to support practical conservation decisions.



A talk with a projector for a small audience during the 2024 Borneo visit.

**WHO**

Benoit Goossens, Nurzhafarina Othman, Pablo Orozco-terWengel, Omer Rana, Charith Perera

**PROGRAMME**

British Council • 2026 to 2027

**Scan for the project page**

iotgarage.net/go/pan-borneo-elephants

- Led by Cardiff University and Universiti Malaysia Sabah, with the Sabah Wildlife Department and the Sabah Forestry Department.
- Focus areas are the Tawai and Kalabakan Forest Reserves.
- Planned outputs: risk areas and periods for elephant groups, elephant-safe working practices, and practical mitigation measures.

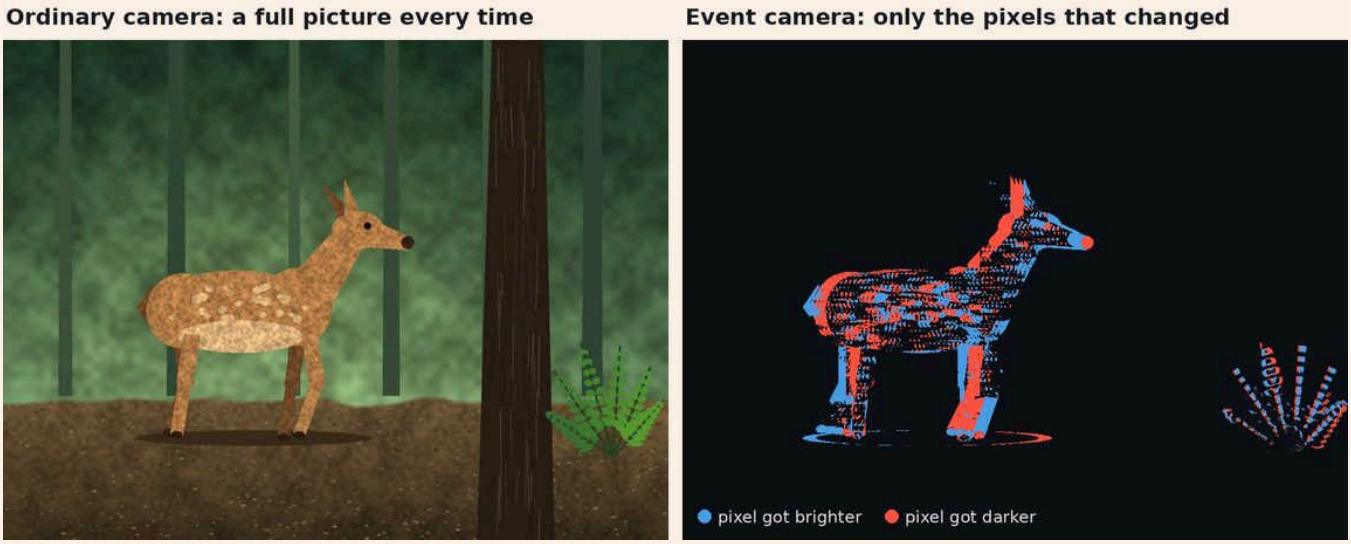


02

DATA OBSERVATORY

# EventCam.AI

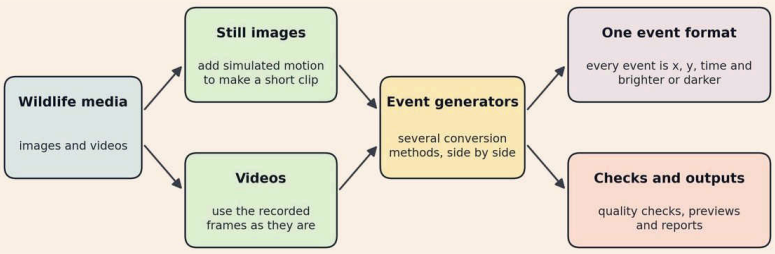
Testing low-power event cameras for wildlife monitoring




Left: one frame of a synthetic, computer-drawn forest scene with a walking animal. Right: the same moment as event data made by the project's frame-to-event converter. Only pixels that changed appear: blue where they got brighter, red where they got darker. The still trees and ground vanish.

Wildlife monitoring needs cameras that can watch quietly for long periods without exhausting power or storage. Event cameras offer a different approach: each pixel reports a change in brightness rather than repeatedly recording a complete frame. EventCam.AI explores how this sensing approach could support conservation work with the Danau Girang Field Centre in Sabah, building on earlier camera-trap research.

Wild-EV-Synth develops that vision by converting existing wildlife photographs and videos into synthetic event streams. Its software brings different conversion methods into a shared format, with previews, quality checks and records of how outputs were produced. The aim is to help researchers compare approaches before collecting field recordings. Establishing how faithfully these synthetic events represent real cameras remains a research challenge.




How the toolkit works, redrawn from the project's system overview: still images are given simulated motion, videos are used as recorded, several event generators run side by side, and the results are stored in one format with quality checks, previews and reports.


**WHO**
Charith Perera, Benoit Goossens, Hakan Kayan


**PROGRAMME**
MEDR ODA Award • 2025 to 2026

**Scan for the project page**
iotgarage.net/go/eventcam-ai

- Explores event-driven sensing for wildlife and environmental monitoring with partners in Borneo.
- Wild-EV-Synth connects source media, conversion methods and quality checks in a reproducible software pipeline.
- Synthetic event streams need comparison with real camera recordings before their value for field tasks can be established.

**ALL PAPERS**

**Wild-EV-Synth: A Reproducible Multimedia Benchmark for RGB-to-Even…**

02

DATA OBSERVATORY

# CamTrap.AI

Sorting camera-trap photos with several AI models and a human check



A camera trap in a protective metal case, strapped to a tree trunk in the forest.

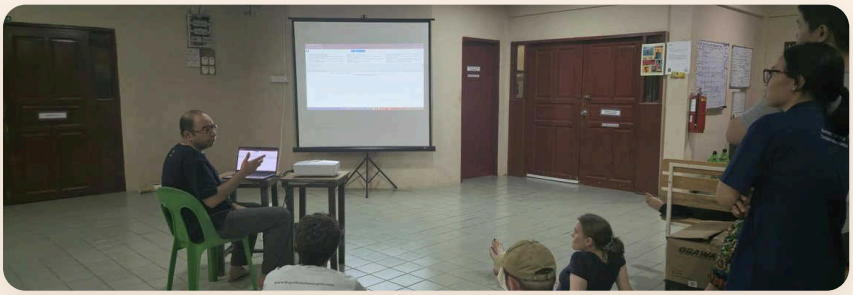
**PROGRAMME**
HEFCW ODA • 2024

**Scan for the project page**
iotgarage.net/go/camtrap-ai

- Three software tools: a classification toolkit, a benchmark suite and a bulk classifier web app (private repositories).
- Combines existing models, including MegaDetector, instead of training one new model.
- Keeps a person in the loop: the researcher can confirm or override each decision.

Camera traps are cameras left in the wild that take a picture when something moves. They let ecologists watch wildlife without disturbing it, but each deployment brings back thousands of images, and many are false triggers with no animal in them. Sorting them by hand is slow. Researchers are also wary of trusting one piece of software with images that hold valuable data.

CamTrap.AI runs several existing image classifiers on the same photo and combines their answers, an approach called an ensemble. A person can confirm or override the decision. The team built a web application with a quick check for one image and batch processing for collections, plus tools to compare models and label images in bulk.



A talk with a projector for a small audience during a 2024 Borneo visit.



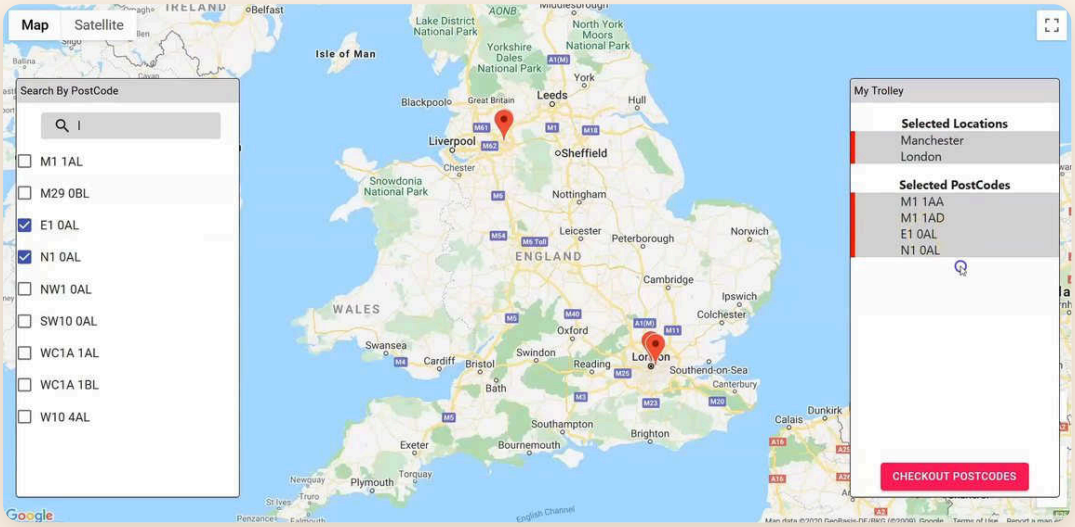
**ALL PAPERS**
**CamTrap.AI: Semi-Automatic Wildlife Image Classification Using Ensem…**

02

DATA OBSERVATORY

# Smart City Data Markets

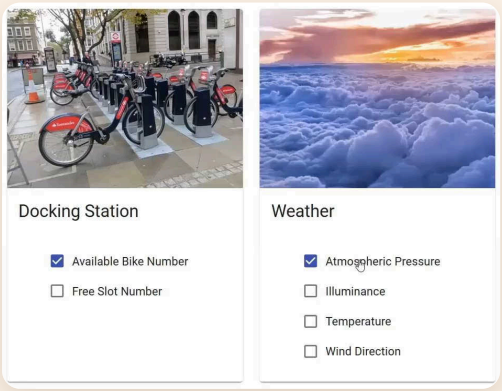
Letting buyers order only the city sensor data they need




The order form starts with place: buyers tick postcodes on a map, and their choices collect in a trolley on the right.

Cities collect sensor data on air quality, noise, parking and bike hire. Data marketplaces sell this data to companies, but usually as whole, fixed datasets. A small firm that needs a few readings from a few streets must buy and download far more than it wants. The paper names three resulting problems: pricing is difficult, network demand is higher, and buyers face information overload.

The team asked potential buyers what they needed and designed an order form built on four questions: where, what, when and how. Behind it sits an ontology, a shared vocabulary that lets software understand the data, so that a request can be turned into a database query. They tested how fast such queries ran in three ways of storing the data, as a feasibility case study using synthetic data.




Next, buyers tick only the readings they need, such as available bikes at a docking station or atmospheric pressure.


**WHO**
Charith Perera, Hamed Hamed


**PROGRAMME**
EPSRC Researcher in Residence • 2019 to 2021

**Scan for the project page**
iotgarage.net/go/data-markets

**21**
participants with computer and data science backgrounds informed the four design principles: where, what, when, how.

ACM Transactions on Internet of Things, 2023

- A feasibility case study, not a pricing or usability trial.
- Buyers build an order from location, data type, date and time, and a service level agreement.
- Set in the SynchroniCity IoT data marketplace, with Digital Catapult.

**ALL PAPERS**

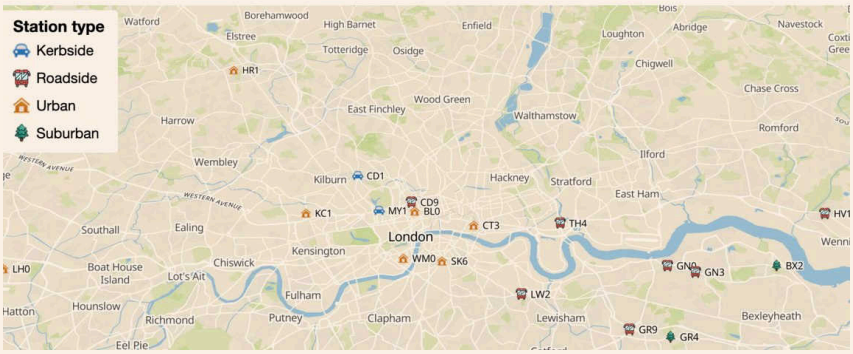
**Query Interface for Smart City Internet of Things Data Marketplaces** Ha…

02

DATA OBSERVATORY

# Reading a city's air

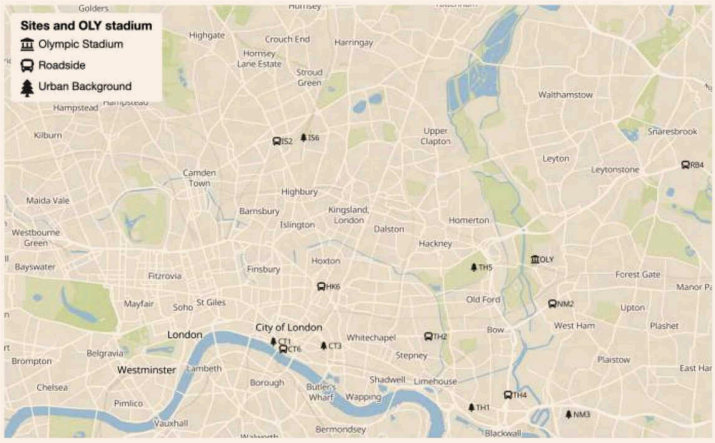
Connecting pollution measurements with the rhythms of urban life




A London map marks kerbside, roadside, urban and suburban air-quality monitoring sites.

Air pollution changes with place and time. A roadside monitor can tell a different story from a suburban one, and a major event can bring unusual patterns. This research uses London measurements to look for daily and seasonal rhythms, connect pollution changes with public events, and estimate how air quality may develop.

The studies take different routes through the data. One examines recurring pollution patterns, another combines social media posts with monitoring records around the London Olympics, and another predicts air quality using past pollution and weather. Their findings are bounded by the London datasets. Associations with commuting or events do not establish what caused a change in pollution.




A map marks pollution monitors and the Queen Elizabeth Olympic Park.

**2 daily peaks**

around 7–9 am and 5–7 pm at nearly all stations, consistent with commuter travel. The study did not test traffic or weather as causes.

IEEE Internet of Things Magazine, 2021

**0.70 / 0.51 / 0.62**

correlations between the opening-ceremony topic and nitrogen dioxide anomalies at three roadside sites. This is association during one event, not proof of cause.

Computing, 2021

**> 81%**

air-quality band prediction accuracy across the datasets for the best approach in the seven-site London case study. Linear regression was recommended where coarse particles dominated.

IEEE Access, 2018

- London monitoring sites cover contrasting urban settings.
- Event analysis joins social media and pollution records.

**ALL PAPERS**

**Inferring Latent Patterns in Air Quality from Urban Big Data** De, Jassat, …

**Data-driven Air Quality Characterisation for Urban Environments** Zhou, …

**Analysing Environmental Impact of Large-scale Events in Public Space**…

02

DATA OBSERVATORY

# Talking Aquifer

Asking questions of groundwater and climate data in plain English



Environmental monitoring instruments in white cabinets on a wooden platform, with farmland behind. Photo from the fellowship visit.

**WHO**
Charith Perera, Praveen Kumar, Daniel Hadley, Brian Pianfetti

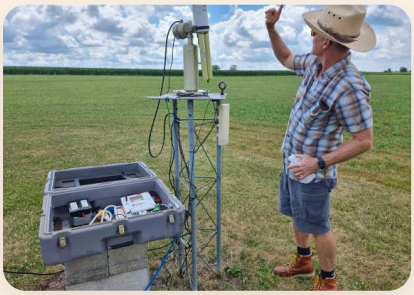
**PROGRAMME**
OECD CRP Fellowship • 2025

**Scan for the project page**
iotgarage.net/go/talking-aquifer

- A fellowship under the OECD Co-operative Research Programme: Sustainable Agriculture and Food Systems.
- Hosted by the Prairie Research Institute at the University of Illinois Urbana-Champaign.
- Designed for a wide range of users, from farmers and policy makers to research scientists and emergency managers.

Data about groundwater, weather and streams is held in separate databases and web services, each with its own format. A farmer, a policy maker and a research scientist all need answers from it, but they ask very different questions and few can write database queries. Large language models (LLMs), the technology behind AI chat assistants, could let people simply ask. Builders lack guidance on how to set them up.

Talking Aquifer is a chat-style interface where people type a question and get back text, a chart, a table or a map drawn from groundwater and climate data. The team built the same service in many different ways, from one simple AI agent to several agents working together, and compared them on questions of rising difficulty. The aim is practical design guidelines.



A man in a straw hat points to an instrument on a small mast; an open case of electronics sits beside it.



Weather and radiation sensors on a metal beam above grey equipment boxes in a field.



**ALL PAPERS**
**Talking Aquifer** 2026

PART 03

# 03



# Resilient Sensing

Systems that keep working, and stay trustworthy, when something goes wrong or someone attacks them.

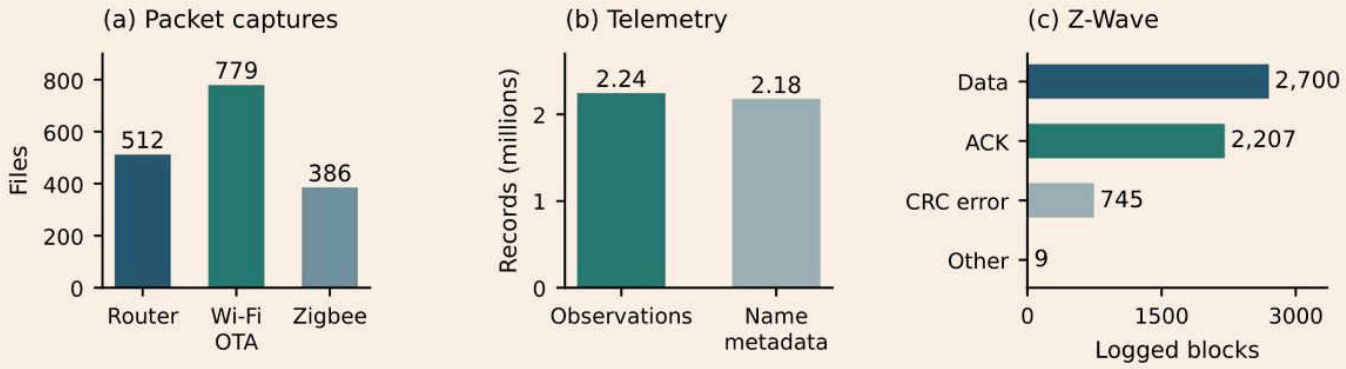

InSituHome 43
Trusting synthetic home data 44
Context Aware Security for Smart Homes 45
Industrial security foundations 46
CASPER 47
Integrity Checking at the Edge 48
Knowledge-driven Security at the Edge 49
Anomaly Detection with Tiny Cameras 50
In-Vehicle Edge Security 51
Adaptive Mobile Sensing 52
Patterns of life in buildings 53
When building context changes 54
Resilient Built Environments 55
CASPER Shield 56
Early Signs of Domestic Violence 57




RESILIENT SENSING

# 03 InSituHome

An occupied-home testbed with records of devices and attacks




Dataset composition charts for packet captures, telemetry and Z-Wave logs.

A security dataset needs more than a list of attacks. Researchers must know what was recorded, how devices behaved and whether an attempted attack achieved its intended effect. Building on a review of testbeds and evaluation methods, InSituHome documents connected devices in an occupied flat, linking ordinary household operation with a separately planned campaign of security tests.

The collection brings together router packets, over-the-air wireless observations, native device-network logs and home-automation telemetry. Each annotated test is assessed separately for its launch, visible signature, target response and objective. That distinction helps prevent a recognisable packet pattern being mistaken for demonstrated harm. The record comes from a single home and campaign, with assessments assigned by the lead author.

**WHO**
Mohammed Alosaimi, Omer Rana, Charith Perera

**WHEN**
2021–2025

**Scan for the project page**
iotgarage.net/go/anomaly-evaluation

**27 • 21 • 23**
of 36 annotated tests support a signature, target response and objective respectively. These are separate assessments from one home and campaign, assigned by the lead author.

- Collection routes retain the differences between network observations and device telemetry.
- The accompanying review provides reporting guidance rather than a ranking of detectors.

**ALL PAPERS**

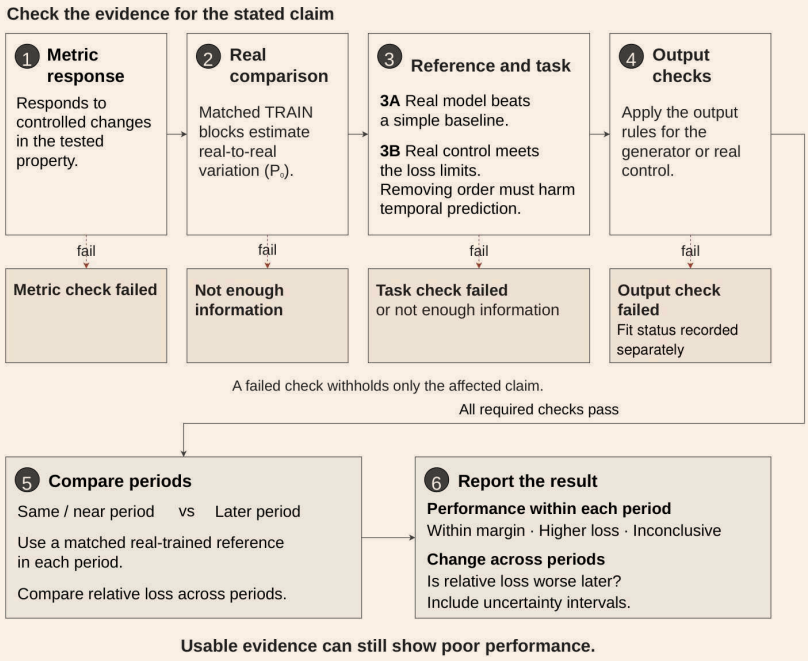
**InSituHome: A Smart Home Cybersecurity Dataset with Multiple Source…**

**Testbeds and Evaluation Frameworks for Anomaly Detection within Buil…**

RESILIENT SENSING

# 03 Trusting synthetic home data

Synthetic Fusion and Beyond the Score test what data can support

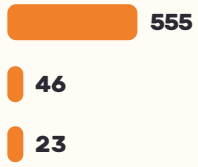



The checks an evaluation must pass before a synthetic dataset is trusted for a stated use. A failed check withholds only the claim it affects.

Artificial smart-home data could help researchers when recordings are scarce or sensitive. Yet matching a real dataset's appearance or average error does not show that the artificial version is suitable for a particular task. Synthetic Fusion asks which properties survive generation, while Beyond the Score asks whether the evaluation itself supplies enough evidence to justify the intended conclusion.

The frameworks keep failed checks visible and limit conclusions to the tasks those checks support. They examine changes over time, relationships between physical and network measurements, and comparisons with simple reference methods. A home case study and constructed examples illustrate the approach. Passing a check can still reveal weak performance, and examples used to develop the method cannot establish success on unseen cases.

**COLUMNS KEPT IN THE HOME CASE**




columns before filtering, after removing sparse drivers and after the activity-window check in the residential case. The final selection is exploratory because the test period informed its design.

**72 / 72**

constructed cases received the expected decision. These cases were used during method development, so agreement is not validation on unseen examples or proof of generator quality.

- Quality is tied to a specified use, rather than a single universal score.
- A real-data model must also be checked against a simple baseline.

**Scan for the project page**

iotgarage.net/go/anomaly-evaluation

**ALL PAPERS**

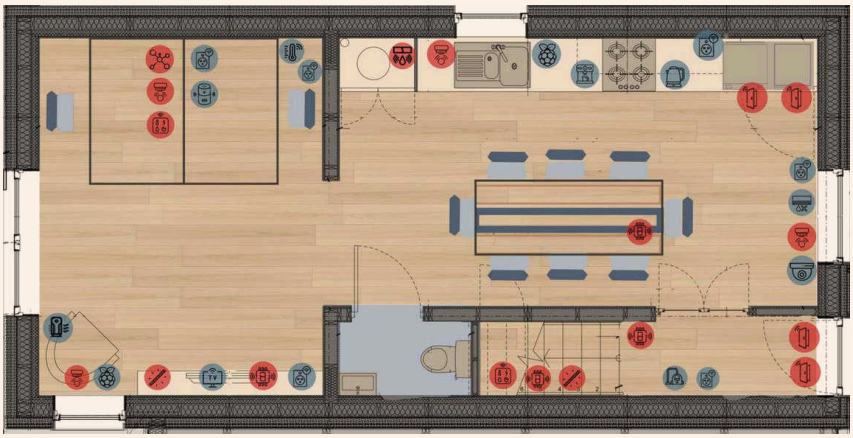
**Beyond the Score** 2026

**Synthetic Fusion** 2026

RESILIENT SENSING

# 03 Context Aware Security for Smart Homes

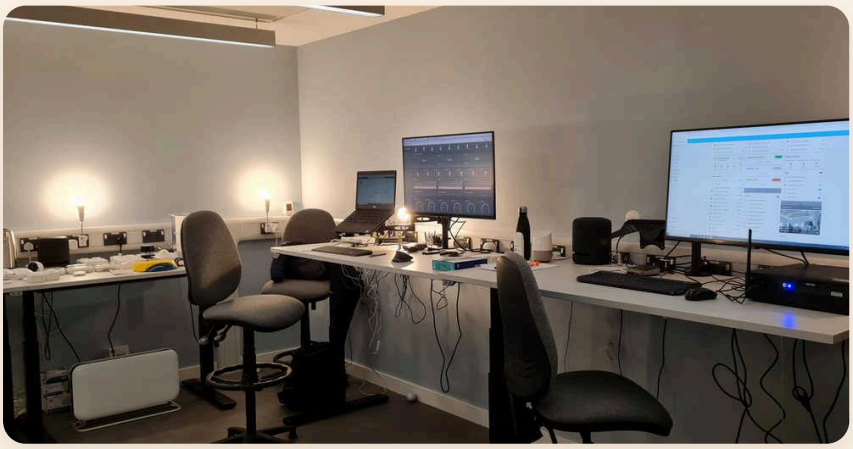
Checking network traffic against what sensors see in the home



Ground-floor plan from the CP-BASH study, with icons marking sensors and smart devices.

An attack on a smart home can show up in two places at once: in the network traffic and in the physical world, as changes in temperature, light, sound or movement. Tools that watch only the network can miss an attack that tampers with a device. This project asks whether watching both together gives a clearer picture.

The work begins with a survey of smart-home anomalies, then explores CP-BASH, which combines network and environmental readings to identify unusual behaviour. RT-SHAD extends the idea towards real-time monitoring, adaptation and human feedback. A related open dataset records normal and unusual activities alongside readings from devices, giving other researchers material to test their own methods.



Smart Home Lab benches with smart bulbs, a kettle, smart speakers, boxed sensors and monitoring screens.

**WHO**
Yasar Majib, Omer Rana, Charith Perera

**WHEN**
2020-2024

**Scan for the project page**
iotgarage.net/go/smart-home-security

**4 weeks**
of recorded data: 3.5 weeks by a main actor for normal activities and 3 days by a second actor for anomalous ones
Frontiers in the Internet of Things, 2023

- Combines two views of a home: network traffic and independent sensor readings.
- Uses low-cost, do-it-yourself sensor nodes.
- The dataset is publicly available for other researchers.



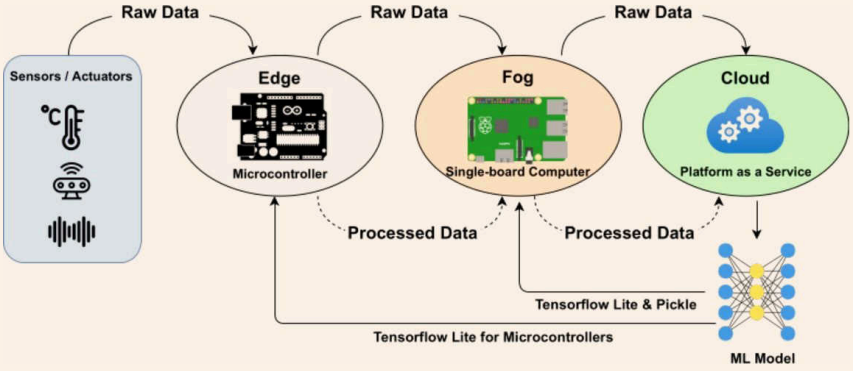
**ALL PAPERS**

**Cyber Physical Anomaly Detection for Smart Homes** 2025
**Dataset for Cyber-Physical Anomaly Detection in Smart Homes** Majib, Al...
**RT-SHAD: Real-Time Smart-Home Anomaly Detection** 2023
**CP-BASH: Cyber-Physical Behavioural Anomaly Detection for Smart Ho...**

RESILIENT SENSING

# 03 Industrial security foundations

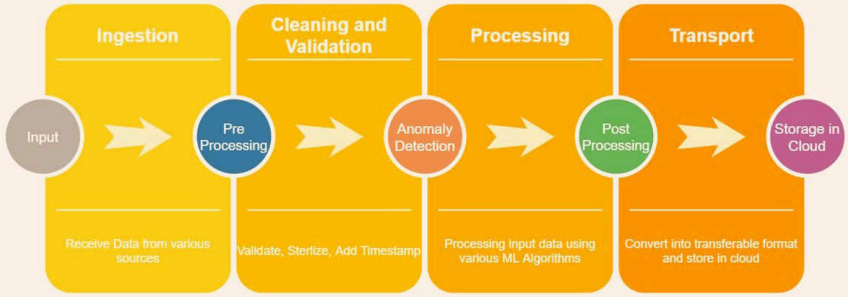
From a map of threats to a configurable sensor-analysis pipeline




Data and trained models circulate between sensors, a microcontroller, a nearby computer and cloud services.

Industrial control systems join software, networks and machines that affect the physical world. Protecting them requires understanding how attacks cross those boundaries. Hakan Kayan's review organises incidents, weaknesses and proposed defences, exposing gaps between industrial vulnerability reports and the research literature. It provides a foundation for building and evaluating security tools rather than a ready-made detector.

AnoML-IoT turns the practical challenge into a configurable pipeline. It links sensor collection, wireless communication, model training and deployment across small devices, nearby computers and cloud services. The aim is to help data scientists work with connected hardware. Its experiments test that pipeline using limited environmental readings and deliberately created anomalies, so they do not establish a generally superior attack detector.




AnoML-IoT pipeline data flow.

**WHO**
Hakan Kayan, Ryan Heartfield, Pete Burnap, Charith Perera

**WHEN**
2020-2023

**Scan for the project page**
iotgarage.net/go/casper

**15**
real industrial cyber-physical incidents examined using the review taxonomy. Incident descriptions rely largely on news and blogs; the proposed evaluation environment was not implemented.
ACM Computing Surveys, 2022

**77% / 86%**
accuracy and F1 for the baseline edge CNN. The authors' own data used temperature and humidity with hair-dryer anomalies; this evaluates a pipeline, not a better detector.
Elsevier Internet of Things, 2021

- The review maps industrial weaknesses to proposed countermeasures.
- AnoML-IoT connects data collection, learning and model deployment.

**ALL PAPERS**

**Cybersecurity of Industrial Cyber-Physical Systems** Kayan, Nunes, Ran…

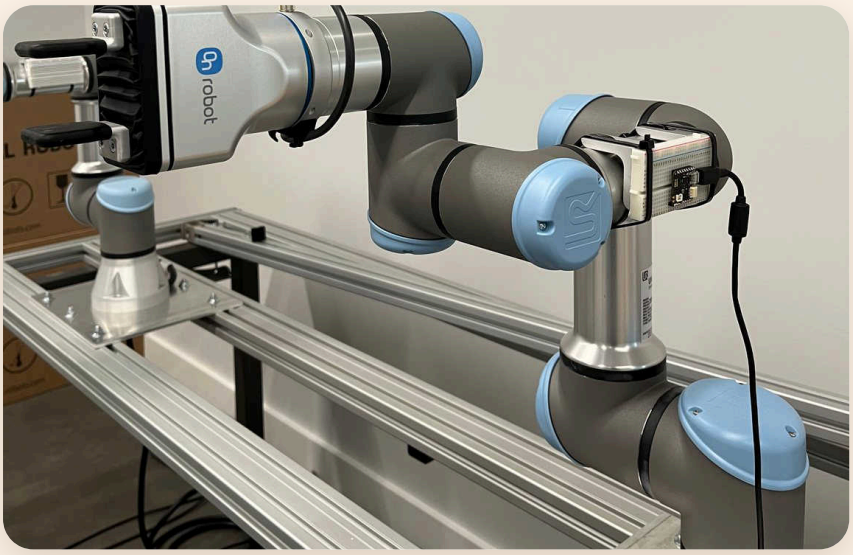
**AnoML-IoT: An End-to-End Re-configurable Multi-protocol Anomaly Det…**

03

RESILIENT SENSING

# CASPER

Independent sensing for industrial robotic-arm monitoring




A UR3e robot arm with a gripper. A small sensor board on a breadboard is strapped to one of its joints.

A robot can move wrongly even when its network traffic looks ordinary. An attacker may also falsify the readings used by existing monitors. CASPER adds an independent view of the physical machine: a small sensor board attached to the arm records its motion, allowing a separate detector to look for departures from the movements it has learned.

The CASPER paper tests this approach on a real industrial arm performing a repeating pick-and-place task. A later study moves compact neural models onto the sensor board and examines additional robotic tasks. Together they trace a path from independent sensing to local detection. The practical processing rate is lower than the headline target, and the controlled anomalies should not be mistaken for comprehensive attack coverage.



Live dashboard showing accelerometer, gyroscope and magnetometer readings from the sensor board.

**WHO**
Hakan Kayan, Ryan Heartfield, Pete Burnap, Charith Perera

**WHEN**
2020-2023

**Scan for the project page**
iotgarage.net/go/casper

**99.24%**

accuracy for the motion-based CNN on author-injected joint-velocity anomalies in one pick-and-place task. Detection ran off the sensor device.

ACM Transactions on Internet of Things, 2024

**≈ 98%**

accuracy and F1 for movement-anomaly detection on the board across the studied tasks. The evaluation finds 3 Hz practical, so operation is near real-time.

IEEE Internet of Things Journal, 2025

- A separate motion sensor supplements the robot's own network monitoring.
- The later study covers pick-and-place, painting and screwdriving.



**ALL PAPERS**

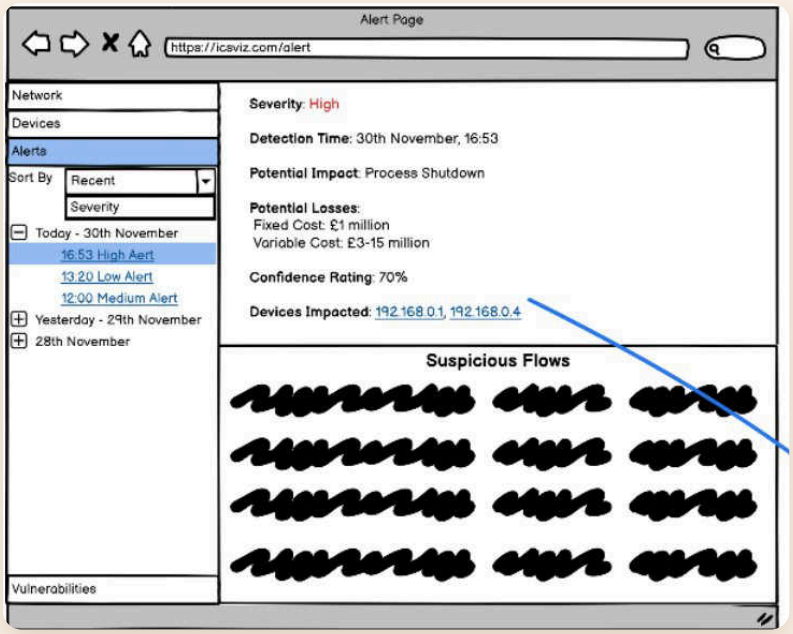
**Real-Time Anomaly Detection for Industrial Robotic Arms Using Edge Co…**

**CASPER: Context-Aware IoT Anomaly Detection System for Industrial R…**

RESILIENT SENSING

# 03 Integrity Checking at the Edge

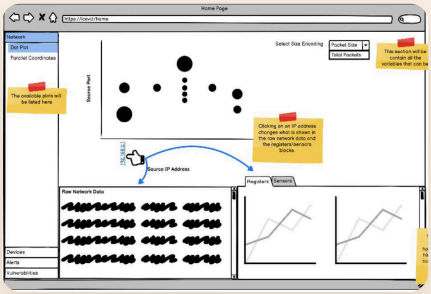
What people need to see when a factory is under cyber attack




Wireframe of the alert page, with severity, potential impact, potential losses and the devices affected (Figure 10 of the paper).

Factories and water treatment plants are run by industrial control systems. Many security tools have been proposed for them, yet few are deployed. One reason is that tools assume a single kind of user. In a plant, a network administrator, an engineer and a director each need different information when an alert appears.

The team interviewed a panel of industrial security experts, then drew up personas (short profiles of typical users) and wireframes (sketches of screens) for a monitoring tool. The sketches link suspicious network traffic to the physical process, to safety and to likely cost. The panel reviewed the designs in a second session. No working system was built or tested with plant operators.



Wireframe of the overview page, linking network traffic to register and sensor readings (Figure 8 of the paper).

**WHO**
Matthew Nunes, Pete Burnap, Charith Perera

**PROGRAMME**
EPSRC PETRAS 2 • 2019-2021

**Scan for the project page**
iotgarage.net/go/integrity-checking

**3**
industrial security experts interviewed, each from a different organisation. This is one small panel.
Frontiers in the Internet of Things, 2024

- A design study, not a new attack detector.
- Personas for the user groups in a plant: director, operation or site manager, operation controller and network administrator.
- Screen sketches show an alert with severity, potential impact and potential losses.

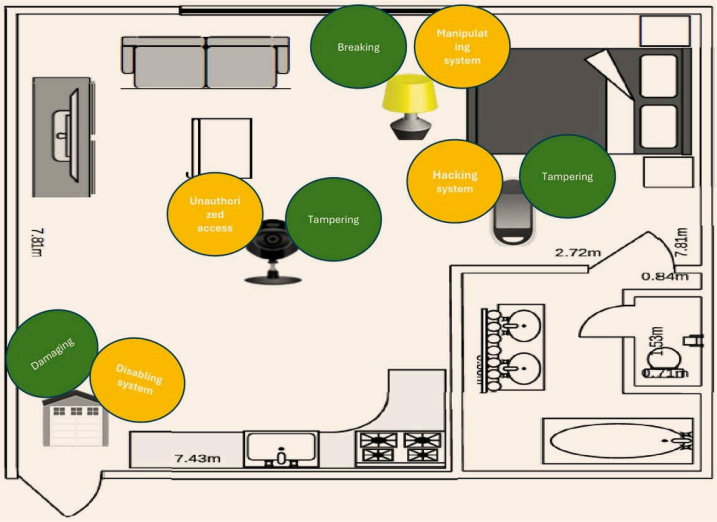


**ALL PAPERS**
**Exploiting User-Centred Design to Secure Industrial Control Systems…**

RESILIENT SENSING

# 03 Knowledge-driven Security at the Edge

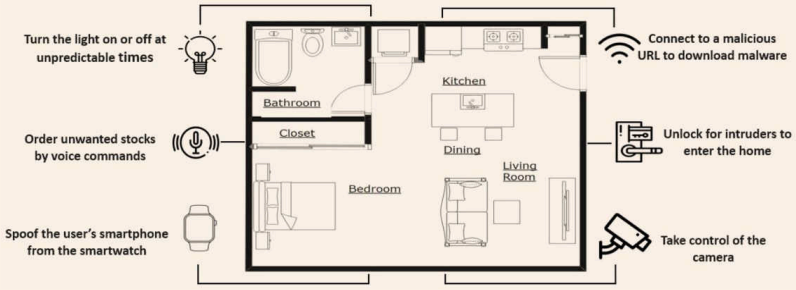
Smart homes that reason about threats and involve residents




A home layout used in the focus groups, with coloured labels marking threats such as tampering, hacking and unauthorised access.

A smart home mixes many devices, each able to sense, act and communicate in different ways. Most security research trains a model to raise an alert. An alert on its own does not say what happened, how serious it is, or what to do next. This project uses explicit knowledge about rooms, devices and routines to reason about an event inside the home.

The team reviewed knowledge-based security and asked residents about threats through questionnaires and focus groups. That work produced design criteria for people and devices investigating odd events together. A follow-on approach selects nearby devices to gather further evidence before interpreting an alert and choosing a response. It explores a strategy for investigation rather than reporting a deployed home-security product.




A home floor plan with example threats: a light switched at odd times, unwanted voice orders, a door unlocked for intruders and a camera taken over.

**WHO**
Azhar Alsufyani, Omer Rana, Charith Perera

**WHEN**
2021-2026

**Scan for the project page**
iotgarage.net/go/security-at-the-edge

**40**
people answered the questionnaire on smart-home security needs
Proceedings of the ACM on IMWUT, 2025

**4**
open challenges identified by the review of knowledge-driven smart-home security
ACM Computing Surveys, 2024

- Security decisions are based on explicit knowledge of rooms, devices and routines, and are made inside the home.
- Residents were asked what they need before any detector was built.



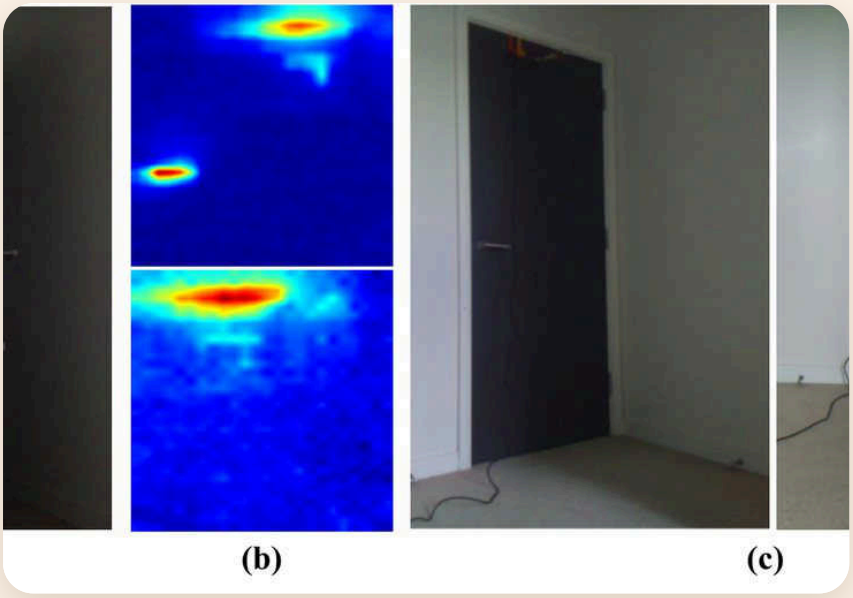
**ALL PAPERS**

**Intelligence Gathering Towards Further Exploring Cyber-Physical Ano…**
**Knowledge-based Cyber Physical Security at Smart Home** Alsufyani, Ra…
**Enabling Collaborative Anomaly Exploration in Smart Homes** Alsufyani, …

RESILIENT SENSING

# 03 Anomaly Detection with Tiny Cameras

Using a camera as little as possible to keep a smart home safe




Camera and thermal images of doors from the SenseLess paper's figure on cases where automatic labelling went wrong.

Simple sensors for temperature, humidity and motion can miss context that a camera would see, such as a door left open. Yet continuous filming raises privacy concerns. The project surveys how cameras can strengthen anomaly detection, and asks how vision and ordinary sensors can work together while limiting reliance on images in the home.

Camera as Trainer uses a camera temporarily to label sensor data before it is removed. SenseLess explores a related approach: ordinary sensors help label training images and vision is used when needed. The team tested SenseLess in a real home with a second home used for some tests. Results describe those settings, not all homes.

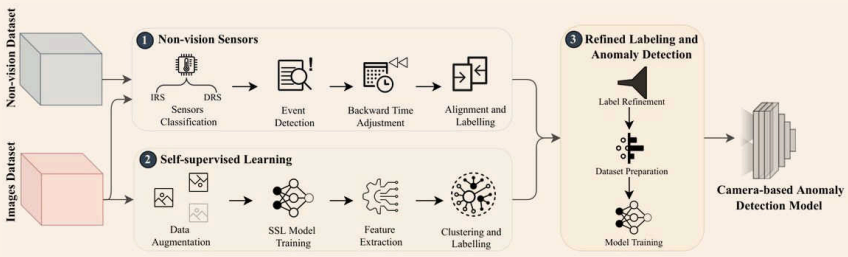
**WHO**
Norah Abdullah Albazzai, Yaser Abu Awwad, Charith Perera

**WHEN**
2021-2025

**Scan for the project page**
iotgarage.net/go/tiny-cameras

**3.42%**
of operating time used the camera in deployment. The paper measures reduced camera use, not whether residents accept it.
IEEE PerCom, 2026

- Ordinary sensors do the monitoring; the camera is a fallback.
- Training images are labelled automatically, without manual annotation.
- Reduces camera use but is not a complete privacy guarantee.




SenseLess system architecture: sensor data and images are combined to label images and train a camera-based model (Fig. 2 of the paper).



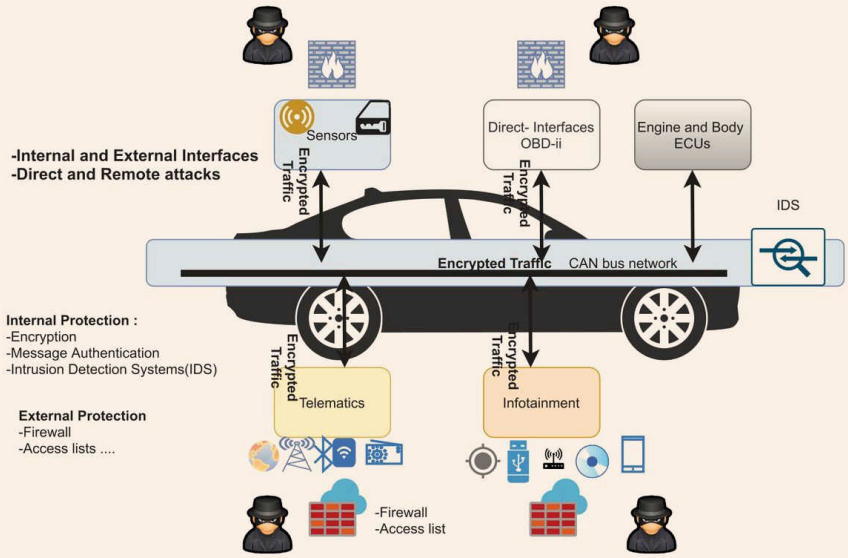
**ALL PAPERS**

**SenseLess: Minimal Vision, Maximum Insight for Smart Homes** Albazzai, ...
**Camera-Assisted Training of Non-Vision Sensors for Anomaly Detection**...
**Camera as a Trainer for Anomaly Detection** 2025
**Camera as a Sensor Towards Augmenting Anomaly Detection in the Inte**...

RESILIENT SENSING

# 03 In-Vehicle Edge Security

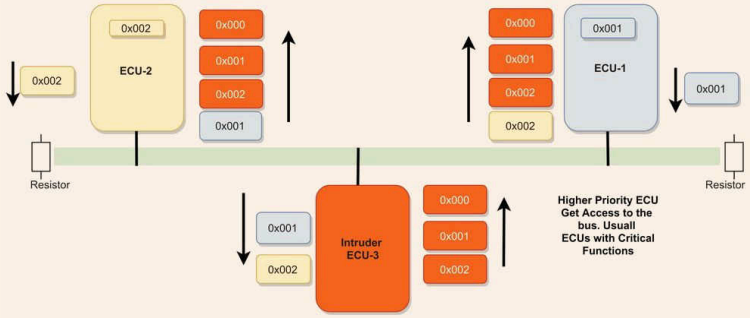
Why a car's internal network is hard to protect from attackers




A connected car and the four ways in for an attacker: sensors, direct interfaces, telematics and infotainment (Fig. 4 of the survey).

A modern car is run by many small computers called electronic control units (ECUs). They talk to each other over an internal network called the CAN bus, which was designed with no security. Connected cars add new ways in, such as telematics and infotainment systems, so the bus can now be attacked from outside the vehicle as well as inside.

The project produced a survey paper in ACM Computing Surveys. It describes in-vehicle networks, then classifies two families of defence: cryptography, and intrusion detection systems that watch the bus for odd traffic. It compares them against the limits of a car, such as tiny messages, modest computing power and strict timing. It is a review of other studies, not a new detector.




Attacks on the in-vehicle CAN bus: an intruder unit on the bus, and replay, injection, falsifying, fuzzing, sniffing and denial-of-service attacks (Fig. 5 of the survey).

**WHO**
Emad Aliwa, Omer Rana, Charith Perera

**WHEN**
2019 to 2023

**Scan for the project page**
iotgarage.net/go/vehicle-security

**≈ 70**
small computers (ECUs) in a modern car, controlling functions such as brakes, gears and engine status, as reported in the survey
ACM Computing Surveys, 2021

- A survey of cyberattacks on in-vehicle networks and the countermeasures proposed for them.
- Compares three kinds of intrusion detection: statistical, machine-learning and physical-characteristic based.
- Ends with open research challenges for both cryptography-based and detection-based defences.



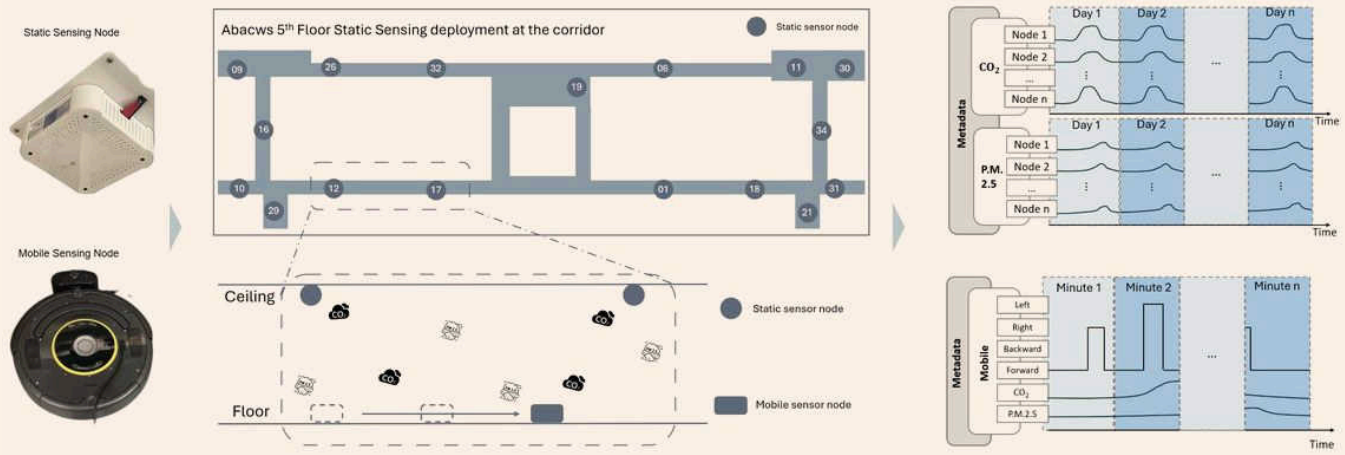
ALL PAPERS

**Cyberattacks and Countermeasures For In-Vehicle Networks** Aliwa, Ran...

RESILIENT SENSING

# 03 Adaptive Mobile Sensing

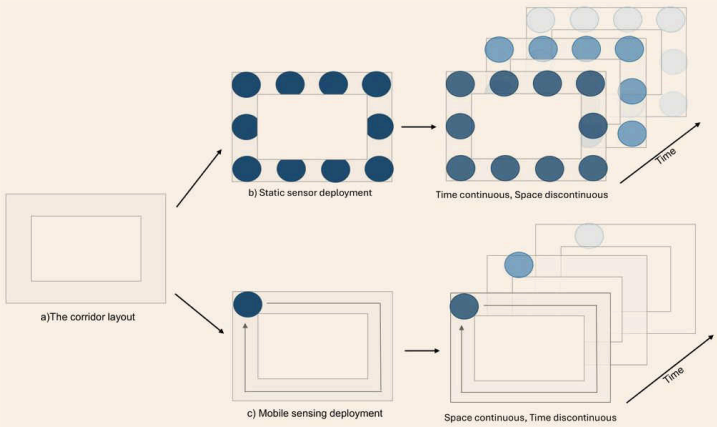
Can a few moving sensors do the job of many fixed ones in a building?




A ceiling-mounted static sensing node and a robot-vacuum mobile sensing node, the static sensor positions along the Abacws 5th floor corridor, and the kind of data each one records.

Buildings use sensors to track indoor air quality and comfort. Fixed sensors watch particular spots continuously but leave gaps between them. Sensors carried by people, robots, drones or vehicles can cover more places, although they visit each location only occasionally. The project explores how these approaches can work together to characterise indoor environments.

The team reviewed mobile sensing in buildings, comparing the different ways sensors can be carried and used. A related study uses fixed air-quality readings from Cardiff University's Abacws building to simulate measurements along a moving route. This provides a way to explore the trade-off between coverage and timing; it does not establish that moving sensors can replace fixed ones.




Static sensors are continuous in time but not in space. A mobile sensor is continuous in space but not in time.

**WHO**
Siyuan Li, Hakan Kayan, Yuhua Li, Charith Perera

**WHEN**
2022 to 2026

**Scan for the project page**
iotgarage.net/go/mobile-sensing

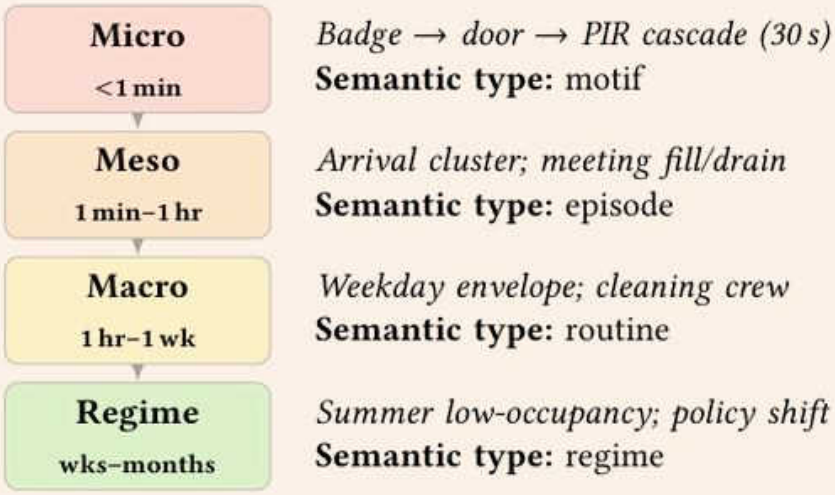
- A project on mobile sensing in smart buildings.
- The survey groups mobile sensing by carrier: people, mobile stations and robots, drones, and vehicles.
- Uses the static sensor deployment on the fifth floor of the Abacws building at Cardiff University as its testbed.


**ALL PAPERS**
**Mobile Sensing within Smart Environments** 2026
**Mobile and Static Sensor Equivalence for Characterising Environmental...**

RESILIENT SENSING

# 03 Patterns of life in buildings

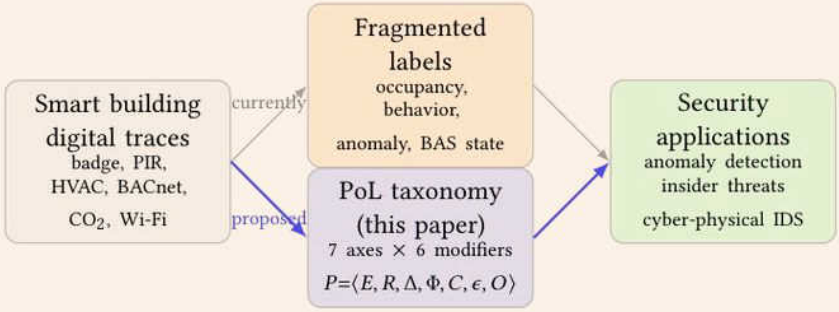
Learning how ordinary routines appear in building sensors




A ladder links motifs, episodes, routines and longer building regimes.

A building has routines: arrivals, meetings, equipment use and quiet periods. Sensors record traces of those activities, but an unusual reading is meaningful only in relation to what normally happens there. CyPhy Radar explores independent environmental sensing and a vocabulary for describing these recurring patterns, linking practical monitoring with a clearer account of what a routine actually means.

The sensing study collects physical measurements through do-it-yourself devices and compares ways to prepare and model the data. It shows why day and night should sometimes be treated differently. The companion pattern-of-life work proposes a ladder from brief observations to longer routines and changing operating conditions. That vocabulary is a conceptual framework; the deployment evidence supports only a limited account of anomaly detection.




A conceptual diagram connects building traces, pattern-of-life vocabulary and security applications.

**WHO**
Charith Perera, Yasar Majib

**PROGRAMME**
GCHQ Fellowship • 2020 to 2021

**Scan for the project page**
iotgarage.net/go/cyphy-radar

**32 • 14 • 8**
data streams, unique sensors and device sets in the building study. Only one known anomalous activity was available, so the paper cannot establish accuracy or false-positive rates.

Journal of Ambient Intelligence and Humanized Computing, 2022

- Physical measurements complement observations from the building's main systems.
- Patterns of life connect brief events, routines and longer operating conditions.




**ALL PAPERS**

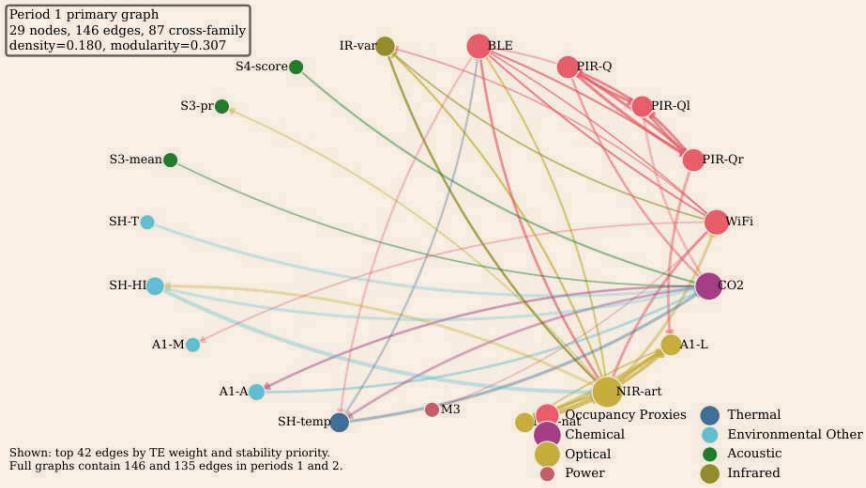
**Pattern of Life in Smart Buildings** 2026

**Detecting Anomalies within Smart Buildings using Do-It-Yourself Inter…**

RESILIENT SENSING

# 03 When building context changes

Context-aware monitoring and changing sensor relationships




Sensor features in an office building, connected by estimated directed dependencies.

### CONTEXT CAN HELP

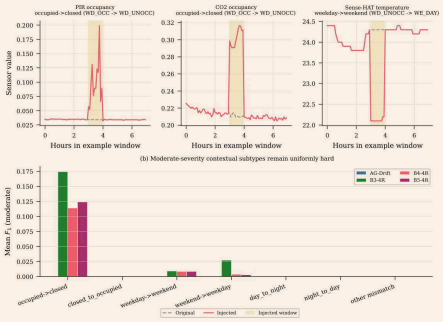
A motion reading can be normal during office hours and suspicious after the building closes.

### CONTEXT CAN HURT

The same extra information can make a detector noisier or more fragile when the room's use changes.

A motion reading can be normal during office hours and suspicious after the building closes. Adding context sounds helpful, but it can also make a detector noisier or more fragile when occupancy changes. This work asks which measurements benefit from knowing the operating conditions, and how relationships between sensors change as a building moves between those conditions.

The context study compares monitoring choices before and after a change in an office room's use. The dependency-graph study maps statistical links between sensor streams and examines how those links reconfigure with occupancy. Together they motivate selective use of context and cautious interpretation of sensor networks. A statistical link is not proof of cause, and the evidence does not establish transfer to other buildings.




Example time series with original and injected changes in context.

- Context is investigated as a selective design choice for each sensor.
- Directed graphs describe observed dependencies rather than proven physical causes.

**Scan for the project page**
iotgarage.net/go/cyphy-radar

ALL PAPERS

**Regime-Aware Directed Dependency Graphs in a Smart-Building IoT De…** **When Context Helps and Hurts** 2026

RESILIENT SENSING

# 03 Resilient Built Environments

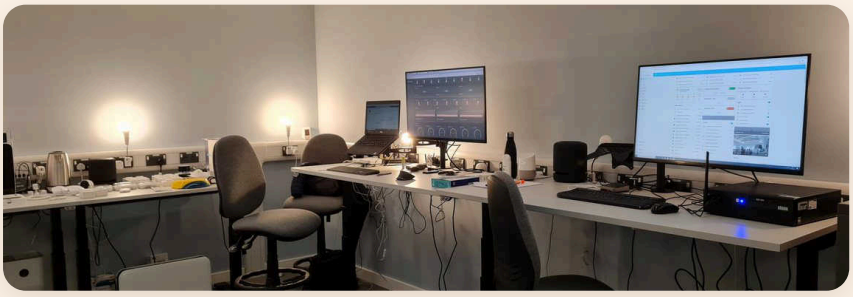
Adding extra layers of protection to smart homes and offices



A three-storey house with timber cladding, photographed at the BRE smart space workshop, October 2022.

Homes and offices now depend on connected devices for monitoring, automation and security. That makes them open to tampering that can affect the safety of the people inside. This secondment placed Charith Perera with the Building Research Establishment (BRE) to study how separate, independent layers of sensing could make smart buildings harder to compromise.

The project mapped BRE's smart homes and buildings research in a short technical report and held a smart space workshop at BRE to hear industry views. It released an open dataset on cyber-physical anomaly detection in smart homes. A linked journal review compared platforms called Personal Data Stores, which keep personal data under the control of the individual.



Smart Home Lab devices: smart bulbs, plugs, speakers and other connected devices on benches beside two monitoring screens.

**WHO**
Charith Perera

**PROGRAMME**
EPSRC PETRAS Secondment • 2021 to 2022

**Scan for the project page**
iotgarage.net/go/resilient-buildings

**11**

Personal Data Store platforms compared by capability and architecture in a literature review; no platform was built or tested

Sensors, 2023

- An EPSRC PETRAS secondment embedded within the Building Research Establishment (BRE), in partnership with GCHQ.
- Technical report: BRE Smart Homes and Buildings Research Landscape (2023), a map of BRE's projects and a workshop-derived research agenda.
- Open dataset: Cyber-Physical Anomaly Detection in Smart Homes, on IEEE DataPort (2023).



**ALL PAPERS**

**Personal Data Stores (PDS)** Fallatah, Barhamgi, Perera • Sensors, 2023

**Dataset for Cyber-Physical Anomaly Detection in Smart Homes** Majib, Al...

**BRE Smart Homes and Buildings Research Landscape** 2023

03

RESILIENT SENSING

# CASPER Shield

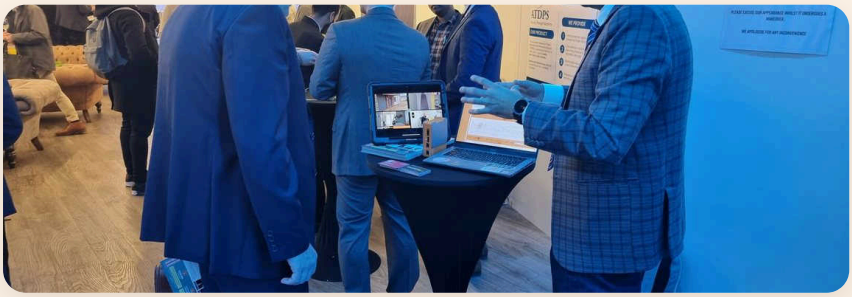
Turning smart-home attack detection research into a product idea




Four people standing in front of the CASPER Shield banner at CyberASAP Demo Day 2023.

Smart homes and smart buildings can be attacked through their networks, and an attack can also change what devices and sensors do in the physical world. Watching network traffic alone can miss this. The group's CASPER research combines network traffic with independent sensor readings and energy use, so that unusual behaviour can be spotted across both the cyber and the physical side.

Through the UK Cyber Academic Startup Accelerator Programme (CyberASAP), funded by Innovate UK, the team turned this research into a product proposition called CASPER Shield. The accelerator gave structured support for business model development, customer discovery and technology demonstration. The team showed the idea at the CyberASAP Demo Day and wrote a project report, published in 2023.



A team member explains the demonstration on two laptops to visitors at CyberASAP Demo Day 2023.

**WHO**

Charith Perera, Yasar Majib, Hakan Kayan

**PROGRAMME**

DCMS Startp Accelerator • 2022-2022

**Scan for the project page**

iotgarage.net/go/casper-shield

- CASPER Shield is a product proposition for protecting smart homes and commercial buildings.
- It combines network traffic, sensor readings and energy use to look for unusual behaviour.
- Partners named on the public page: PETRAS, GCHQ and the Building Research Establishment (BRE).

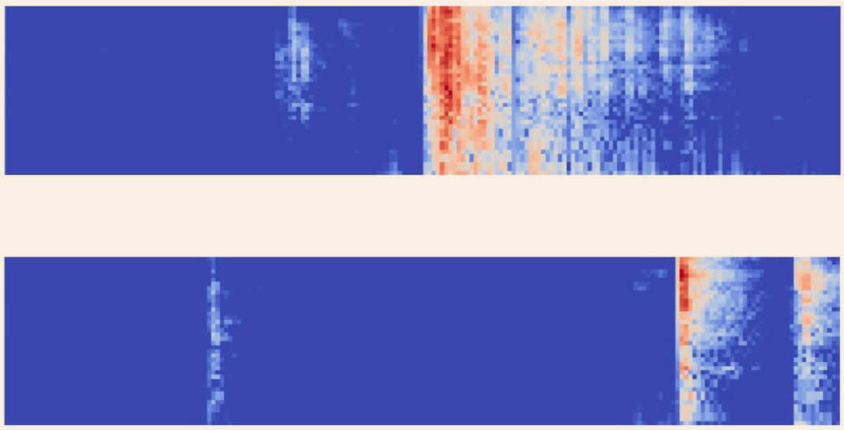


03

RESILIENT SENSING

# Early Signs of Domestic Violence

Can a tiny device on a door tell a slam from a normal close?



Spectrograms of a slam (top) and a normal close (bottom) from the same door.

Social workers and police have no cheap, low-intrusion way to notice aggressive behaviour in social housing. A microphone that is always on drains its battery and raises privacy concerns. This project asked a narrow question: can a low-cost microcontroller running TinyML, which is machine learning small enough for a tiny chip, recognise one warning sound, a slammed door?

The team fixed an Arduino Nano 33 BLE Sense board to a door. Its motion sensor notices when the door moves and only then switches the microphone on. A small neural network on the board decides whether the sound was a slam or a normal close and sends only that result over Bluetooth. It is a two-page feasibility study on one door type.


**WHO**
Osian Morgan, Hakan Kayan, Charith Perera


**WHEN**
2021

**Scan for the project page**
iotgarage.net/go/early-signs

**88.89%**

accuracy telling a slam from a normal close under test conditions with no background noise (feasibility study; no test-set size or field trial reported)

IEEE/ACM IoTDI 2022 (poster abstract)

- Runs on an Arduino Nano 33 BLE Sense using its microphone and accelerometer.
- The microphone only switches on after the door moves.
- The decision is made on the device; raw audio is not sent to external servers.



ALL PAPERS

**Feasibility on Detecting Door Slamming towards Monitoring Early Sign…**

PART 04

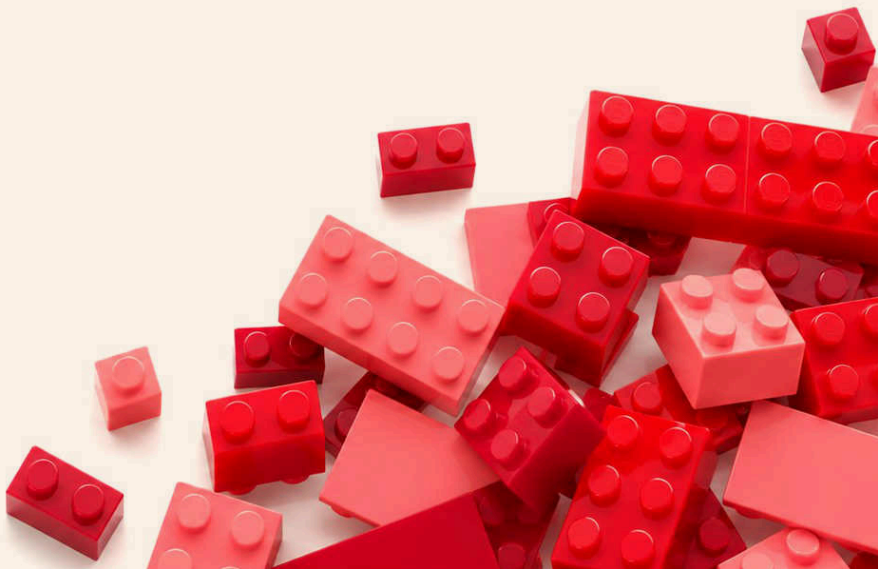
# 04

# Edge Intelligence



Small computers that think next to the sensor, and keep thinking well when conditions get rough.

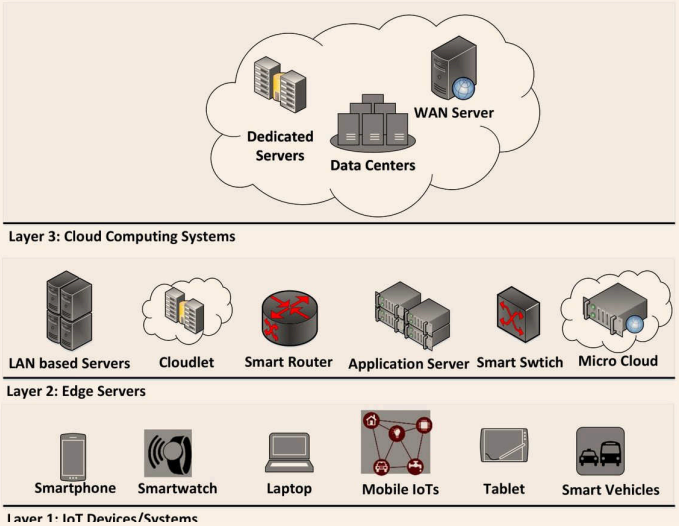

Edge-centric analytics platforms 59
Doing more with less data at the edge 60
Seeing in the dark at the edge 61
Making sensor AI explain itself 62
National Edge AI Hub 63
Edgy Organism: the data 64
Edgy Organism: the models 65
ARCADE and ScrewSet 66
FedBio-IoT 67
Secure Service Placement for IoT 68

EDGE INTELLIGENCE

# 04 Edge-centric analytics platforms

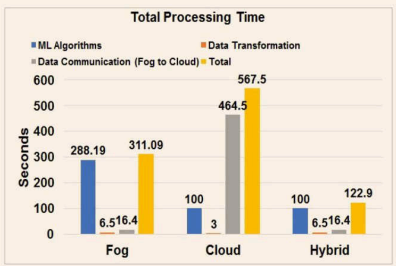
Sharing analytics between nearby devices and the cloud




Devices, nearby edge servers and cloud systems arranged as computing layers.

Sending every sensor reading to a distant server can waste bandwidth and delay decisions. Edge computing moves useful work nearer the source, while fog computing adds nearby gateways between devices and the cloud. This collection asks how those layers should cooperate, from city-wide services and industrial data pipelines to the placement of individual analytics tasks.

The platform studies split analytics into connected services and compare where those services run. Extracting useful features nearby can reduce what travels to the cloud, while larger computers still handle demanding learning tasks. The surveys explain the wider design choices. These are architecture studies and small experiments, so their benefits depend on the data, hardware and network conditions.




(d)

Processing-time comparison for fog, cloud and hybrid placements.

**WHO**

Charith Perera, Prem Jayaraman, Athanasios V. Vasilakos, Rajiv Ranjan and colleagues

**Scan for the project page**

iotgarage.net/go/edge-fog

**10–70%**

less network data after local transformation: text and numerical data respectively. Non-industrial datasets; energy was not measured.

IEEE Transactions on Sustainable Computing, 2022

**122.9 s**

total processing time for the hybrid arrangement, versus 311.09 s in fog and 567.5 s in cloud. Initial experiment on one activity dataset and one Raspberry Pi.

ACM International Conference on the Internet of Things, 2017

- Place data preparation near sensors and demanding analysis where capacity allows.
- City and industrial surveys map platform requirements rather than prove deployment performance.

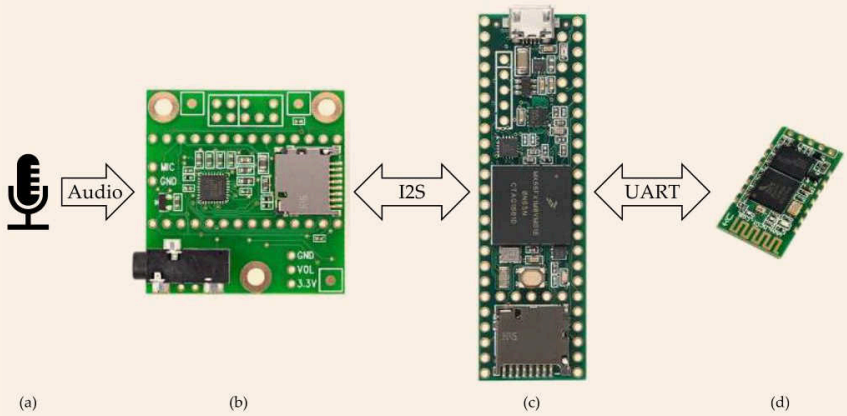
**ALL PAPERS**

**Exploring the Effectiveness of Service Decomposition in Fog Computing**…
**Fog Computing for Sustainable Smart Cities** Perera, Qin, Estrella, Reiff-Ma…
**The Emergence of Edge-Centric Distributed IoT Analytics Platforms** Re…
**The role of big data analytics in industrial Internet of Things** Rehman, …
**A Hybrid Approach for Data Analytics for Internet of Things** Alturki, Rei…

EDGE INTELLIGENCE

# 04 Doing more with less data at the edge

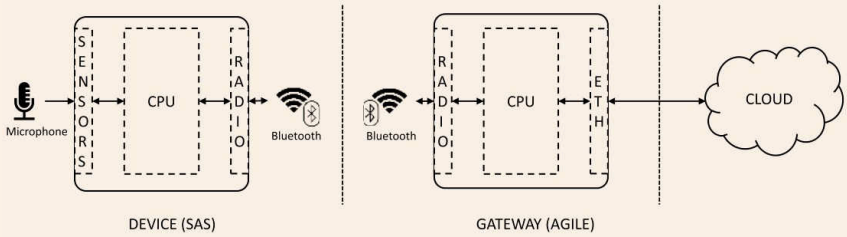
Saving communication while keeping useful sensor information




Audio hardware chain with microphone symbol, audio shield, Teensy board and Bluetooth module.

Small connected devices cannot keep sensing, storing and transmitting everything indefinitely. Some neighbouring sensors report similar changes, while raw audio can contain far more detail than a monitoring task needs. This collection explores how to send less information, share content locally and preserve enough structure for useful decisions close to where measurements are collected.

The studies take complementary routes. Sensor networks adapt sampling using relationships between readings; smart-grid records are compressed as structured arrays; and audio devices send features instead of raw sound. Another study coordinates devices that relay content to their neighbours. Each method is evaluated separately, with different data and assumptions, so the reported savings cannot be combined into a single performance claim.




Audio features move from a smart sensor through a gateway to the cloud.

**WHO**

Charith Perera, Prem Jayaraman, Athanasios V. Vasilakos, Rajiv Ranjan and colleagues

**Scan for the project page**

iotgarage.net/go/edge-fog

## 20–60%

less energy than DPCAS in simulation on one recorded sensor dataset. Savings are limited when readings are weakly related.

IEEE Access, 2019

## ≈ 90%

of original information retained when data is reduced to 5% in the recorded-trace evaluation. The real testbed trace gave weaker results.

IEEE Transactions on Knowledge and Data Engineering, 2018

## 1.7 ms

inference time for Elliptic Envelope on a Raspberry Pi gateway. One office and one sensor; F1 was only about 50–56% across the compared methods.

IEEE Access, 2018

- Correlated readings can support less frequent sensing and reconstruction.
- Local audio processing sends features in place of raw recordings.

**ALL PAPERS**

**A Spatial-Temporal Correlation Approach for Data Reduction in Cluster-…**
**Tensor-Based Big Data Management Scheme for Dimensionality Reducti…**
**Cross-Layer Optimization for Cooperative Content Distribution in Multi…**
**Smart Audio Sensors in the Internet of Things Edge for Anomaly Detect…**

04

EDGE INTELLIGENCE

# Seeing in the dark at the edge

Low-light camera analysis for connected rural communities



A parked car at night, shown without enhancement and with alternative enhancement methods.

Rural cameras may need to monitor farms, car parks or heritage sites after daylight has faded. Poor lighting makes useful objects difficult to see, while sending every frame away demands connectivity. The Connected Communities in the Rural Economy project explored connected tourism and farming services in south-east Wales, providing the wider setting for this edge-camera research.

The camera pipeline first judges which image treatment is appropriate, then enhances a dark picture before running an object detector. Nearby devices share the work. The published study compares enhancement choices on benchmark images and a smaller edge-device test. Its largest improvement comes from the server benchmark; the local test shows a much smaller overall change and weaker person detection.



(a) High light, *"Farm"* (b) Rainy weather, *"Car Parking"*

Project camera views show a farm in bright light, a car park in rain, and farm and castle scenes in low light.

**WHO**

Yaser Abu Awwad, Omer Rana, Charith Perera

**PROGRAMME**

DCMS 5G Programme CoCoRE • 2020-2021

**Scan for the project page**

iotgarage.net/go/cocore

**0.14 → 0.59**

mean average precision before enhancement and the best enhancement result on the server benchmark. In the smaller edge test, the mean moved only from 0.421 to 0.425 and person detection worsened.

MDPI Sensors, 2024

- CoCoRE connects rural innovation in Monmouthshire and Blaenau Gwent.
- The low-light study tests picture enhancement and object detection, rather than proving real-world security outcomes.

**ALL PAPERS**

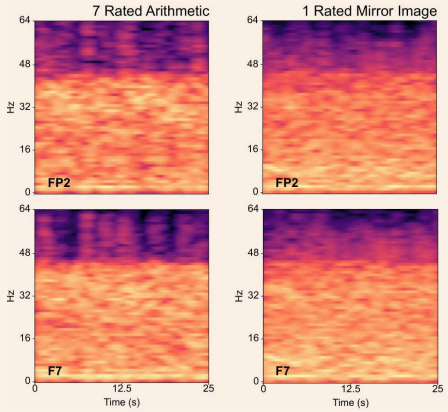
**Anomaly Detection on the Edge Using Smart Cameras under Low-Light …**

EDGE INTELLIGENCE

# 04 Making sensor AI explain itself

Understanding sensor alarms and the limits of brain-signal models

Sensor AI needs more than a prediction to earn trust. People need to understand an alarm, and researchers need to test whether a sophisticated model actually improves on simpler alternatives. These projects explore those questions through explanations for water-system sensors and a careful comparison of approaches to recognising stress from brain signals.




Brain-signal spectrograms for an arithmetic task and a mirror-image task with different reported stress ratings.

## Stress-GPT

**WHO** Catherine Lloyd, Loic Lorente Lemoine, Reiyan Al-Shaikh, Kim Tien Ly, Hakan Kayan, Charith Perera, Nhat Pham

**WHEN** 2024

Stress is personal, and the same task can feel very different to different people. Stress-GPT studies whether a model already trained on brain-signal recordings can help recognise stress from electrical activity measured at the scalp. It compares this route with conventional learning methods, using a public dataset whose stress labels come from participants themselves.

**74.4%**

average stress-classification accuracy for the encoder-only model across nine folds. Conventional methods scored 85–93% on this dataset; labels were self-reported.

ACM MobiCom, 2024

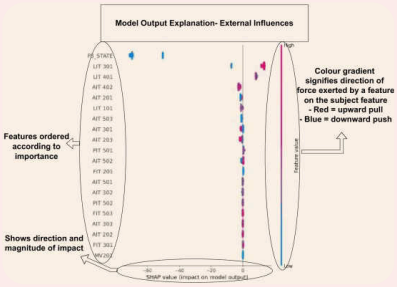
**Scan for the project page**

iotgarage.net/go/stress-gpt

## Explaining sensor alarms

**WHO** Moaz Hussain, Charith Perera

**WHEN** 2021




An explanation plot ranks sensor features and marks their upward or downward influence on the model output.

An alarm is hard to trust when it cannot explain what changed. This work studies a water-treatment sensor dataset and builds simpler stand-in models for a neural anomaly detector. Those models support explanations of a reading using its own history and other sensors. A layered dashboard is designed to offer different amounts of detail to different readers.

- Stand-in models make a complex detector easier to inspect.

**Scan for the project page**

iotgarage.net/go/explainable-anomaly

**ALL PAPERS**

**Stress-GPT: Stress detection with an EEG-based foundation model** Llo…

**Explainable Sensor Data-Driven Anomaly Detection in Internet of Thing…**

04

EDGE INTELLIGENCE

# National Edge AI Hub

Keeping AI on small devices reliable when data and networks go wrong




University logos and a map of the United Kingdom marking the Hub's university partners.

Edge AI means running artificial intelligence on small devices close to where data is produced, not in a distant data centre. In vehicles, energy networks and healthcare these devices must keep working when data is noisy, late or under attack. The Hub is a national programme that studies how to keep edge AI dependable in those conditions.

The first Hub paper recorded for the group is accepted at the IoT 2026 conference. It describes a software agent that takes a goal written in plain language, finds the FPGA boards (reprogrammable chips) that are connected, then builds, loads and measures a design on them. It was tested on two boards with one small energy-prediction workload.

**WHO**
Omer Rana, Charith Perera, Neetesh Saxena

**PROGRAMME**
EPSRC AI for Real Data • 2024-2029

**Scan for the project page**
iotgarage.net/go/national-edge-ai-hub

**3.83 M/s**

inferences per second on the ZCU104 board with the agent's own design; the hls4ml baseline gives 2.79 million (two boards, one small workload, no repeated runs)

IoT 2026 (accepted, in print)

- Three application areas: autonomous electric vehicles, energy security and remote healthcare.
- Covers the whole path from sensors, through edge devices, to the cloud.
- The Newcastle Urban Observatory is the main testbed.

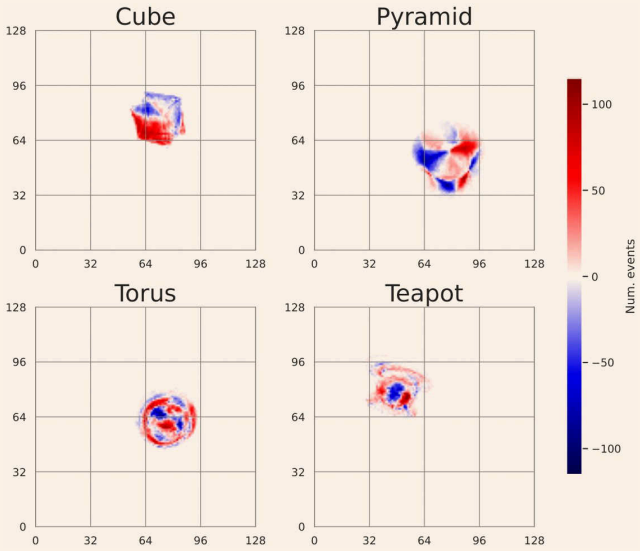
**ALL PAPERS**

**Agent-based Deployment on FPGA-based Edge Devices** Mshragi, Petri, B…

EDGE INTELLIGENCE

# 04 Edgy Organism: the data

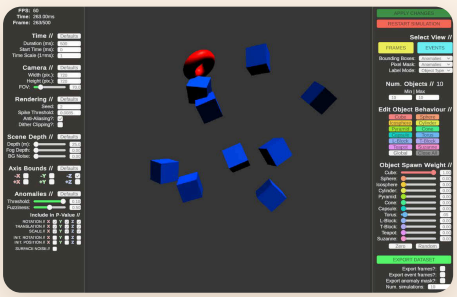
Controlled event-camera scenes for learning and testing




Four object classes from the standard ANTShapes dataset (cube, pyramid, torus, teapot), shown as accumulated events.

Event cameras record changes in brightness rather than a steady sequence of complete pictures. That can suit efficient sensing, but researchers need labelled examples to build and compare models. Edgy Organism uses controllable simulated scenes to explore this gap, allowing shapes and their behaviour to be varied while keeping a record of what the simulator considers unusual.

ANTShapes supplies the simulator, while the benchmark paper packages its output for object-classification research. The modelling paper explains how scene behaviour is generated and labelled; it is the same simulator contribution, not an additional dataset experiment. The benchmark tests a spiking neural network, a model that communicates through pulses. Its idealised object scenes do not establish performance in busy public spaces.



The ANTShapes simulator screen: a scene of moving 3D shapes (top) and the same scene as events (bottom), with the control panels at the sides.

**WHO**

Martin Trefzer, Elena Gheorghiu, Charith Perera, Oliver Rhodes, Konstantinos Gatsis

**PROGRAMME**

EPSRC UK Defence and Security • 2024-2026

**Scan for the project page**

iotgarage.net/go/edgy-organism

**92.2%**

mean classification accuracy on standard ANTShapes. One network design and idealised isolated objects without sensor noise; this is not a deployment result.

Sensors (MDPI), 2026

- Simulator behaviour and anomaly labels are deliberately simplified.
- Benchmark datasets support controlled event-based object-classification studies.
- The simulator and benchmark are separate papers; the simulator paper also covers modelling and simulation.



**ALL PAPERS**

**ANTShapes Benchmarking Datasets for Event-Based Neuromorphic Obj…**

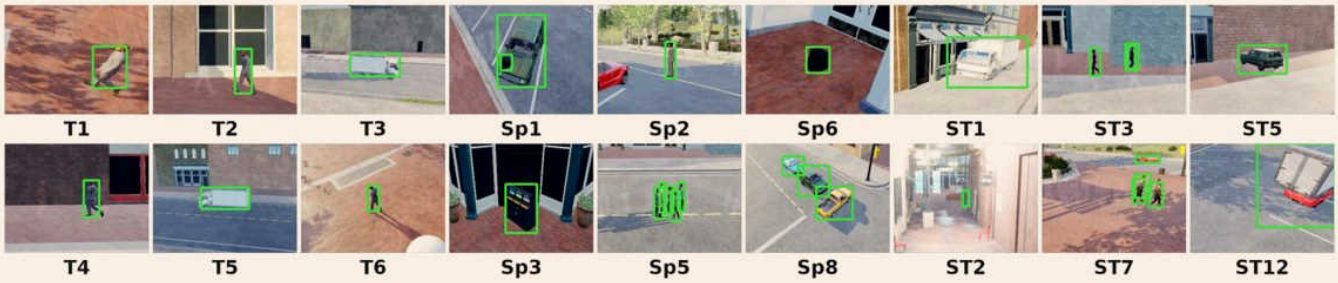
**Modelling and Simulation of Neuromorphic Datasets for Anomaly Detect…**

04

EDGE INTELLIGENCE

# Edgy Organism: the models

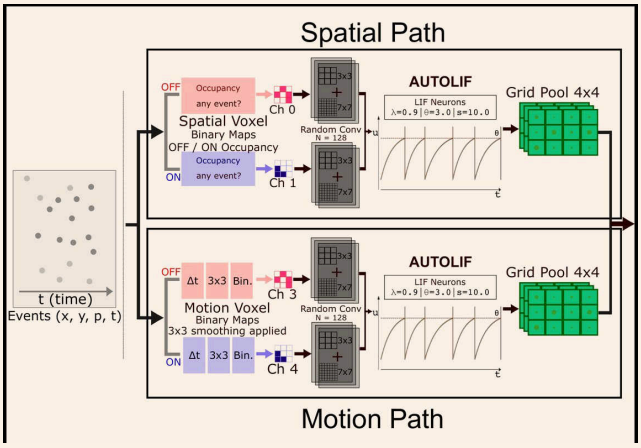
Calibrating spiking models and remembering changing routines




Simulated scenes with tracked people, vehicles and objects marked by green boxes.

A useful sensing system must learn what is ordinary without treating every new routine as a permanent threat. It also needs a practical way to configure the artificial neurons that process event-camera signals. These Edgy Organism papers address model calibration, the gradual acceptance of recurring behaviour and the importance of remembering an individual object's own past.

AutoLIF investigates setting spiking-neuron parameters from event-stream statistics. A continual-learning detector uses separate memories and a reward-guided agent to decide when recurring events should become normal. Another model retrieves the history of the same entity to judge when and where it usually appears. Their datasets and assumptions differ, and the evidence does not show a general accuracy advantage from spiking itself.




Event inputs feed spatial and motion paths with calibrated artificial neurons.

**WHO**

Martin Trefzer, Elena Gheorghiu, Charith Perera, Oliver Rhodes, Konstantinos Gatsis

**PROGRAMME**

EPSRC UK Defence and Security • 2024-2026

**Scan for the project page**

iotgarage.net/go/edgy-organism

**12–15 fps**

processing on a Xavier NX in the continual-learning study. Stable perceptual conditions are assumed and rewards depend on labelled training data.

**0.762**

macro AUROC, a measure of ranking normal and unusual events, on a synthetic benchmark. Controls without spiking cells or population coding matched it; false alarms remained above the calibration target.

- Recurring behaviour and identity-linked history are distinct model contributions.

**ALL PAPERS**

**Population-Encoded Multi-Scale Temporal Activity for Anomalous Patte…**

**AutoLIF: Closed-Form LIF Calibration for Gradient-Free Spiking Network…**

**Continual Learning of Evolving Patterns of Life for Anomaly Detection u…**

EDGE INTELLIGENCE

# 04 ARCADE and ScrewSet

Industrial vision datasets and diagnostics for smaller AI models




Clean screws on top; the same screws under physical corruptions below (sawdust, shadow, reflection, two occlusions, multiple objects).

Factory vision models must distinguish parts that look almost identical, even when dust, shadow or glare spoils the camera view. ScrewSet brings this problem into a controlled laboratory setting using photographs of screws. The dataset paper compares clean views with both software-altered images and photographs taken under deliberately created physical disturbances, making the distinction visible to researchers.

The companion paper asks whether shrinking a trained model changes its reliability. It studies FP8, a compact way of storing model numbers, and diagnostics based on how sharply the model's error changes around its settings. Together, the papers connect a practical image collection with tools for investigating robustness. Their laboratory setting leaves transfer to moving production lines and other factories unresolved.




A grid of forty labelled screw photographs, one for each screw type, on a mottled background.


**WHO**
Charith Perera, Nhat Pham, Ioan Petri, Carolina Fuentes Toro, Hakan Kayan


**PROGRAMME**
Alan Turing Institute • 2024-2025

**Scan for the project page**
iotgarage.net/go/arcade

- ScrewSet documents fine-grained screw classification and image disturbances.
- The diagnostics paper examines model compression and loss of robustness.
- Collection uses a camera on a small robot arm in a laboratory.



**ALL PAPERS**

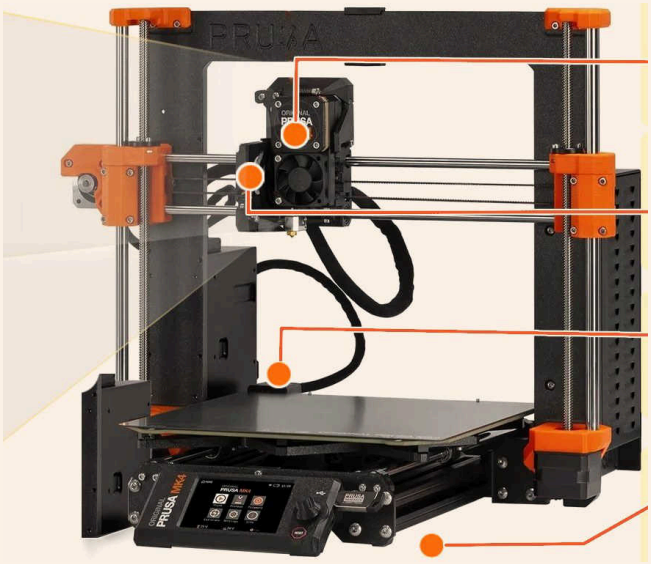
**ScrewSet: A Large-Scale Benchmark for Fine-Grained Industrial Screw …**

**ScrewSet: Hessian Diagnostics for FP8 Post-Training Quantization Rob…**

EDGE INTELLIGENCE

# 04 FedBio-IoT

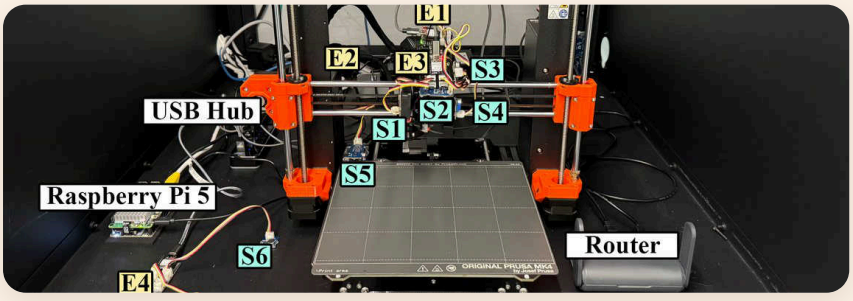
Tiny devices that keep learning together after they are deployed



Positions of the four accelerometer sensors (S1 to S4) and edge boards (E1 to E4) on the Prusa MK4 3D printer, with close-ups of the extruder head.

Federated learning lets many devices train a shared model while their raw data stays on the device. Real Internet of Things systems are unstable, though. Devices come and go, hardware differs, labelled data is scarce and attacks or firmware changes shift behaviour. The question is how such systems can adapt by themselves on very small, low-power chips.

The team reviewed the field and built TinyLearnED, using vibration sensors and small boards with a 3D printer. The boards vote on what they sense and update their model using those labels. A further approach, ReactFed, groups devices and allows reduced models to regain capacity when learning stalls. Its evaluation uses simulation rather than tiny hardware.




Photograph of the Prusa MK4 3D printer test rig with labelled sensors and edge boards, a Raspberry Pi 5, a USB hub and a router.

**WHO**
Abdulaziz Aljohani, Omer Rana, Charith Perera

**WHEN**
2021 to 2025

**Scan for the project page**
iotgarage.net/go/fedbio-iot

**0.893 → 0.924**
combined F1 score (1 is perfect) for spotting layer-thickness attacks on a 3D printer, fixed model versus the adaptive pipeline; one printer and one bolt shape, and detection collapses once two of the four boards are compromised

ACM Transactions on Internet of Things, accepted 2026

**17**
earlier studies found that combine self-adaptation with federated learning in IoT; 10 of the 17 implement adaptation with machine learning

ACM Computing Surveys, 2025

- A review and a conceptual architecture for self-adaptive federated learning in IoT, published in ACM Computing Surveys.
- TinyLearnED runs on four XIAO ESP32S3 boards attached to a Prusa MK4 3D printer, with a Raspberry Pi as the federated server.

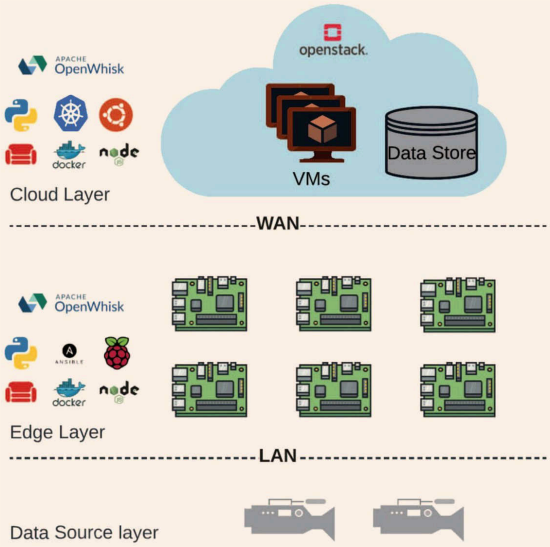
**ALL PAPERS**

**ReactFed: Cluster-Based Sparse Reactivation for Federated Learning on…**
**Self-adaptive Federated Learning in Internet of Things Systems** Aljoha…
**TinyLearnED: Adaptive On-Device Edge Learning for IoT Anomaly Detect…**

EDGE INTELLIGENCE

# 04 Secure Service Placement for IoT

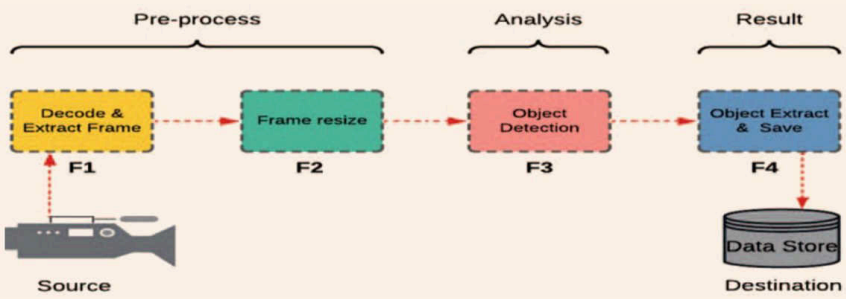
Where should small cloud functions run: nearby devices or the cloud?




The test set-up in three layers: cameras as the data source, six Raspberry Pi boards at the edge, and virtual machines with a data store in the cloud (Fig. 3 of the paper).

Serverless computing lets a developer upload small functions and leave the running of them to a platform. It suits Internet of Things applications, but a function can run on a small device near the sensor (the edge) or in a distant data centre (the cloud). The choice changes how long users wait, and most earlier studies measured cloud platforms only.

The published study deployed one open-source serverless platform, Apache OpenWhisk, on six Raspberry Pi computers and three cloud virtual machines. It ran a chain of four video-analysis functions and measured cold and warm starts, memory and input size, processor type, software package and simultaneous requests. Later work built on these measurements to propose a placement framework called EPSA.




The test application: a chain of four functions that extract video frames, resize them, detect objects and save the results (Fig. 2 of the paper).

**WHO**
Areej Alabbas, Omer Rana, Charith Perera

**WHEN**
2019 to 2022

**Scan for the project page**
iotgarage.net/go/service-placement

**118x**
lower object-detection latency on the Raspberry Pi after swapping TensorFlow for TensorFlow Lite (37x on the cloud), at the price of lower detection confidence; one testbed and one application

IEEE CLOUD, 2023

- A measurement study of Apache OpenWhisk on Raspberry Pi edge nodes and cloud virtual machines. It is not a new scheduler.
- Built a distributed Lean OpenWhisk set-up for a Raspberry Pi (ARM) cluster, with a custom Python runtime.
- Tested with a real-time video-analytics application made of four chained functions.



**ALL PAPERS**
**Performance Analysis of Apache OpenWhisk Across the Edge-Cloud Con…**

PART 05

# 05



# Sustainable Environments

Buildings that use less, and the people inside them as part of the answer.


SpaceSense & EcoCube ..... 70
D-FACT ..... 71
Knowing what a material is ..... 72
Trusting where it came from ..... 73

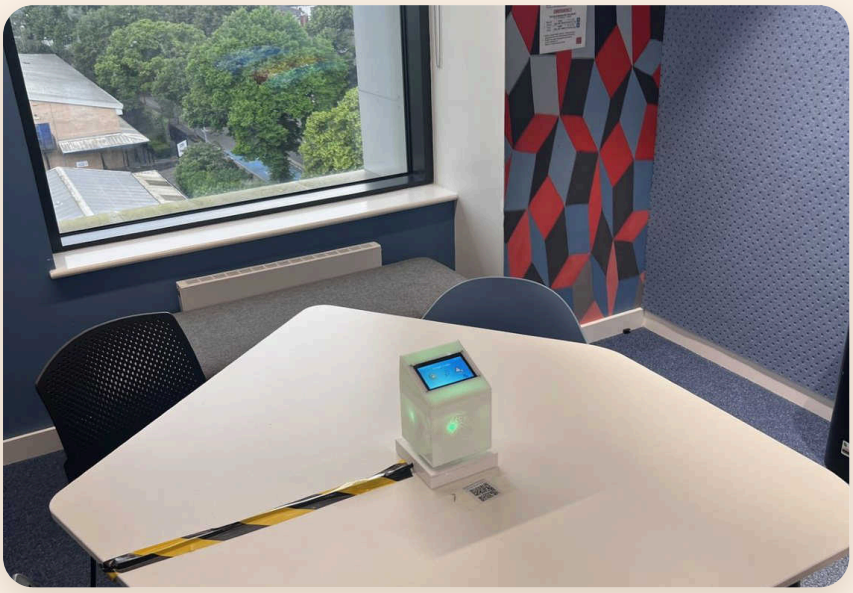



05

SUSTAINABLE ENVIRONMENTS

# SpaceSense & EcoCube

Sensing how study spaces are used, and letting students speak up



An EcoCube on a table in a study room, next to a window.

Modern university buildings offer many kinds of study space, yet how those spaces are used can be hard to understand. Occasional observation gives only snapshots, while surveys depend on replies. The project began with a review of sensing in smart buildings and explored ways to connect the people using spaces with those managing them.

SpaceSense fitted three open study spaces in Cardiff University's Abacws building with ceiling sensor nodes and desk occupancy sensors, and read the data alongside student workshops. EcoCube followed. It is a table-top cube with a small screen that lets students report issues and comfort preferences where they sit. It was co-designed with 19 students and deployed for eight weeks.



The SpaceSense toolkit: the sensor node, its ceiling placement, and the desk occupancy sensors.

**WHO**
Wael Alsafery, Omer Rana, Charith Perera

**WHEN**
2021 to 2025

**Scan for the project page**
iotgarage.net/go/spacesense-ecocube

**23.50 to 27.89**
rise in students' mean satisfaction with communicating with facility managers after using EcoCube ($N = 18$, $p < 0.05$). One building, one university.

Energy and Buildings, in press (accepted 2026)

**Nearly 10 months**
of sensor data from three open study spaces raised facility managers' awareness of space use and their confidence in decisions (both $p < 0.05$). Three facility managers, one floor of one building.

ACM Journal on Computing and Sustainable Societies, 2025

- Ran in Abacws, the home of Computer Science and Mathematics at Cardiff University.
- A reusable sensing toolkit: a ceiling sensor node plus desk occupancy sensors, feeding dashboards for facility managers.

**ALL PAPERS**

**EcoCube: An IoT-Driven Cube for Environmental Awareness and Human-... Sensing within Smart Buildings** Alsafery, Rana, Perera • ACM Computing S...

**SpaceSense: Exploring the Use of Sensors Data to Understand Occupan...**

05

SUSTAINABLE ENVIRONMENTS

# D-FACT

A card game for designing ways to stay comfortable with less energy



Two workshop participants arrange cards and sticky notes on the board.

Buildings use energy to keep people comfortable, but people also adapt locally by changing clothes or moving. This project explores how connected devices can support those everyday choices. Its D-FACT toolkit helps designers and non-designers develop ideas together, using cards and a storyboard to connect experiences of discomfort with possible actions.

The team ran collaborative workshops with the toolkit, then developed WattWise to help households see electricity use from individual appliances. Smart plugs feed a phone dashboard with alerts and activities linked to household data. A deployment in Welsh homes explored how people used the system; the longer observation involved only one household, so the findings should not be generalised.



Hands of workshop participants writing and passing cards over the board.

**WHO**
Asma Irfan, Omer Rana, Charith Perera

**WHEN**
2020 to 2025

**Scan for the project page**
iotgarage.net/go/d-fact

**40 participants**
designers and non-designers used the toolkit across four collaborative workshops
ACM COMPASS, 2025

- D-FACT supports collaborative design for thermal comfort.
- WattWise brings appliance-level electricity information to a phone.
- The D-FACT toolkit is openly available.

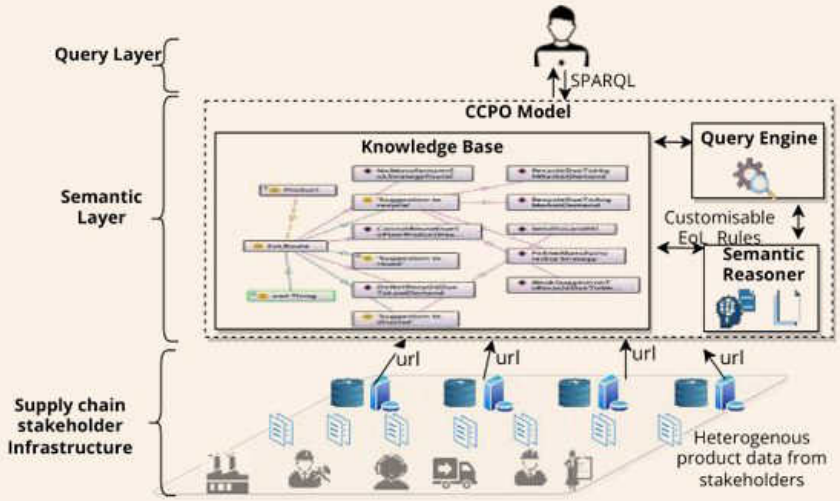


05

SUSTAINABLE ENVIRONMENTS

# Knowing what a material is

Keeping useful information with construction products




The framework connects construction-product data, a knowledge base and a query layer.

A construction product can still have value when its first building no longer needs it. Reuse depends on knowing what the product is, where it has been and whether its condition makes another use sensible. These papers explore how digital records can follow materials and support decisions about what should happen at the end of use.

The material tracking work links product passports with records of ownership across a construction supply chain. The circular construction product ontology adds a shared vocabulary and rules for reasoning about end of life. An insulated wall panel provides a worked example. The evaluation checks whether the model can answer practical questions, with broader testing still needed.

**WHO**
Charith Perera, Omer Rana

**PROGRAMME**
EPSRC Sustainable Digital Society

**Scan for the project page**
iotgarage.net/go/circular-supply-chain

## 6 questions

checked in the insulated wall-panel scenario, using database queries and reasoning rules. This is a single worked example, without a comparative performance benchmark.

ACM/SIGAPP Symposium on Applied Computing, 2025

## 4 operations

described for adding a product, changing ownership, retrieving its passport and verifying its record. The short paper does not report performance or scalability measurements.

IEEE International Conference on e-Science, 2023

- Product passports preserve information as materials change hands.
- An ontology gives software a shared vocabulary for products.

**ALL PAPERS**

**A Circular Construction Product Ontology for End-of-Life Decision-Maki…**

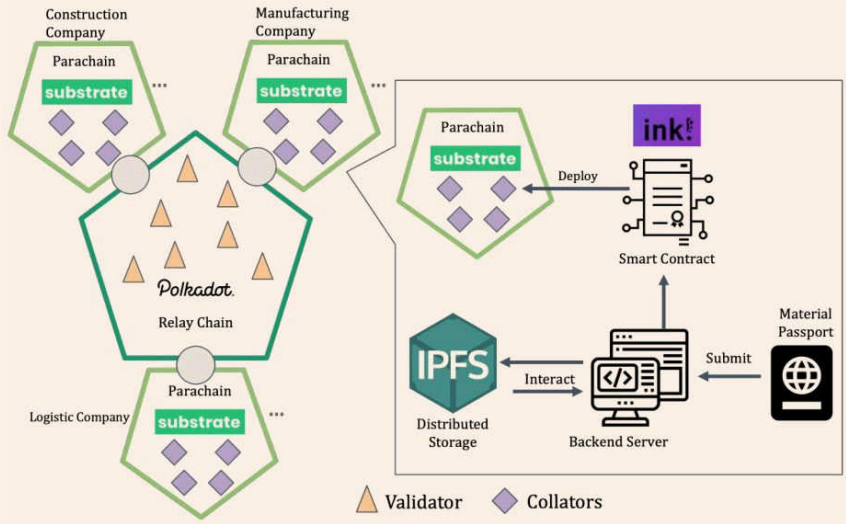
**Tracking Material Reuse Across Construction Supply Chains** Wilson, Adu…

05

SUSTAINABLE ENVIRONMENTS

# Trusting where it came from

Checking the history behind a reused construction product




The provenance architecture connects company records with a shared chain and material-passport storage.

A buyer considering a used building product needs more than an attractive listing. They need to check its history and whether its supporting record has changed. These studies explore product passports and shared records that help organisations follow ownership and make second-hand construction materials easier to assess before they are bought again.

The provenance system stores a trail of product transactions using blockchain, a shared record designed to reveal later changes. The marketplace connects this trail with product listings and checks for reuse. Prototype tests examine processing demands and attempts to alter records. Protecting a record after it is written cannot establish that its original contents were correct.

**WHO**
Charith Perera, Omer Rana

**PROGRAMME**
EPSRC Sustainable Digital Society

**Scan for the project page**
iotgarage.net/go/circular-supply-chain

## 3 scenarios

examined for a malicious seller, buyer and marketplace by comparing information with the stored record. These are controlled prototype checks.

Distributed Ledger Technologies: Research and Practice, 2026

## 168.5 ms

average time to add a product over 1 to 50 transactions on the private development chain. This laptop-based test does not establish production throughput.

Future Internet, 2024

- Digital product passports connect listings to product records.
- Verification can reveal changes made after a record was stored.

**ALL PAPERS**

**Trustworthy Second-hand Marketplace for Built Environment** Wilson, A...

**Blockchain-Enabled Provenance Tracking for Sustainable Material Reus...**

PART 06

# 06



# Labs and datasets

Where the data comes from, and the datasets we share.


Smart Home Lab ..... 75
Living Edge Laboratory ..... 76
Smart City Lego Lab ..... 77
Smart Home Anomaly Dataset ..... 78
IoT Products Dataset ..... 79

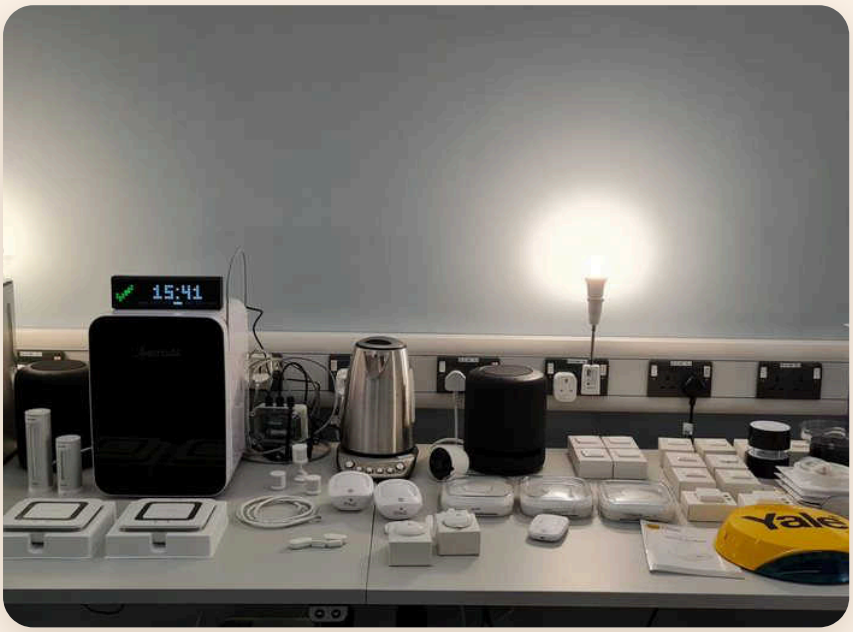



06

LABS AND DATASETS

# Smart Home Lab

A room full of smart home devices for safe experiments




A bench in the Smart Home Lab covered with smart home devices, including a coffee machine, a kettle, smart speakers, lamps, sensors and an alarm box.

Smart homes mix devices from many makers that talk in different ways. Studying how they behave, and how they could be attacked, is hard to do in a home where people live. Researchers need a place where every device can be watched, controlled and reset, and where realistic data can be recorded without risk to anyone's privacy.

The Smart Home Lab is an isolated room of smart home devices covering lighting, heating, ventilation and air conditioning, robotics, multimedia and household appliances. They are connected through openHAB, an open-source home automation platform. Researchers use it to capture datasets, try out automation rules and study security and privacy controls. Related work includes a smart-home anomaly detection dataset.



The Smart Home Lab: a desk of devices along the wall, with a heater, an air purifier and a robot vacuum on the floor.

**WHO**

Mary Zacharias, Yasar Majib, Charith Perera

**PROGRAMME**

Research Infrastructure • 2022-

**Scan for the project page**

iotgarage.net/go/smart-home-lab

- Over 170 smart home devices, according to the public page.
- Devices from multiple manufacturers and communication protocols, connected through openHAB.
- Used for dataset capture, automation prototypes, and security and privacy studies.



06

LABS AND DATASETS

# Living Edge Laboratory

A reconfigurable testbed of small computers and sensors



Brick model for illustration; no photograph is filed for this project yet.

**WHO**
Charith Perera, Ruslan Levond, Sean Savitz

**PROGRAMME**
Research Infrastructure (EPSRC) • 2019

**Scan for the project page**
iotgarage.net/go/living-edge-lab

- 100 nodes, each a Raspberry Pi 4 with Grove Pi and Arduino shields, according to the public page.
- Sensors include temperature, humidity, light, motion, loudness, air quality, dust and camera modules.
- Nodes are distributed across open campus spaces and existing laboratories.

Edge computing means processing data on small computers close to the sensors, not in a distant data centre. It suits applications that cannot wait for a slow network reply. To study it properly, researchers need many real devices in real places, with sensors and radio links that can be swapped, so that different designs can be compared fairly.

The Living Edge Laboratory at Cardiff University is that testbed. The public page describes 100 nodes, each a Raspberry Pi 4 with sensor shields and environmental sensors, plus three Nvidia Jetson Nano units. Communication shields provide Wi-Fi, Bluetooth, ZigBee and LoRa. Both what each node can do and where it sits can be changed for each experiment.

06

LABS AND DATASETS

# Smart City Lego Lab

A Lego city that shows how smart city technology works



Two people placing vehicles on the Lego smart city model.

**WHO**
Charith Perera, Hakan Kayan, Jana Jhaveri, Semih Sarisoy

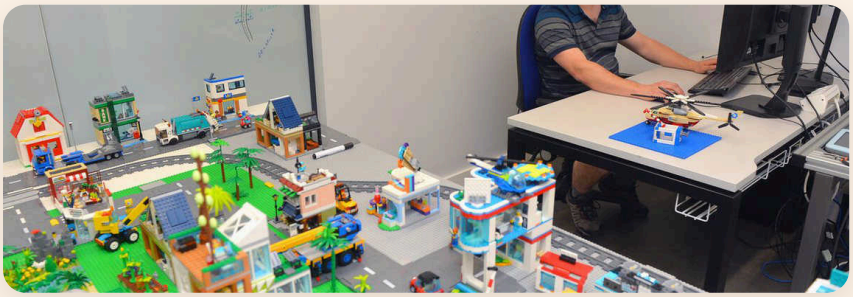
**PROGRAMME**
Research Infrastructure • 2025-

**Scan for the project page**
iotgarage.net/go/lego-lab

- A Lego model city with augmented reality layers.
- For non-specialist audiences, including schoolchildren, policymakers and the general public.
- Used for IoT education, outreach and exploring cyber-physical risks.

Smart city technology is mostly hidden. Sensors, data flows and security weaknesses sit beneath streets and inside buildings, which makes Internet of Things research hard to explain to schoolchildren, policymakers and the general public. People need something familiar they can see and touch before the ideas behind connected cities, and the risks that come with them, start to make sense.

The Smart City Lego Lab is a physical model city built from Lego, with buildings, transport networks and public spaces. Augmented reality, which places digital information over a live view of the model, shows the sensor networks, data pathways and possible security weaknesses behind each part. Researchers use it for public engagement, teaching and exploring cyber-physical risk scenarios.



The Lego city model seen from above, with a researcher working at a computer beside it.



06

LABS AND DATASETS

# Smart Home Anomaly Dataset

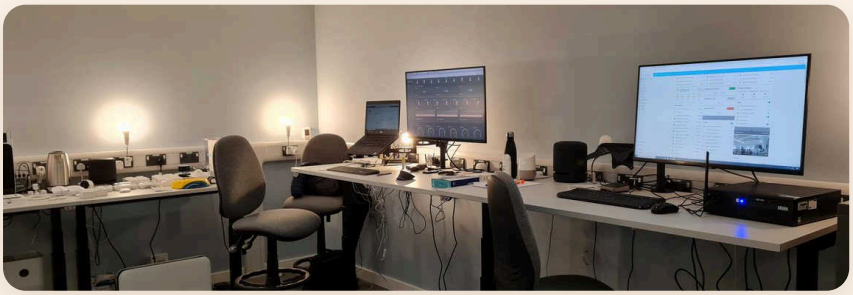
Four weeks of labelled data from a real smart home, cyber and physical



Smart-home devices laid out on a bench in the Smart Home Lab, where the dataset was recorded.

To teach a computer to spot something wrong in a smart home, researchers need recordings of normal life and of unusual events, with labels saying which is which. Such data is scarce, above all data that joins the cyber side, meaning network traffic, with the physical side, meaning sensors and devices, on one timeline.

This dataset was recorded in a real smart home testbed over four weeks. A main actor carried out normal activities and a second actor carried out anomalous ones. Readings from a large number of different devices were combined into one file. It is published on IEEE DataPort and described in a 2023 article in Frontiers in the Internet of Things.



Workstations in the Smart Home Lab.

**WHO**
Yasar Majib, Mohammad Alosaimi, Andre Asaturyan, Charith Perera

**PROGRAMME**
IEEE DataPort • 2023

**Scan for the project page**
iotgarage.net/go/smart-home-dataset

**4 weeks**

of recorded smart-home data: 3.5 weeks of normal activities by a main actor and 3 days of anomalous activities by a second actor; one controlled research establishment with two actors

Frontiers in the Internet of Things, 2023

- What it contains: labelled network traffic, smart-home device and physical sensor data on one timeline.
- How it was collected: actors carried out normal and anomalous activities in a real smart home testbed.
- Where to get it: IEEE DataPort, https://dx.doi.org/10.21227/sez1-2928.



ALL PAPERS
**Dataset for Cyber-Physical Anomaly Detection in Smart Homes** Majib, Al...

06

LABS AND DATASETS

# IoT Products Dataset

A video library of Internet of Things products for teaching



Brick model for illustration; no photograph is filed for this project yet.

**WHO**
Charith Perera

**PROGRAMME**
IEEE DataPort • 2023

**Scan for the project page**
iotgarage.net/go/iot-products-dataset

- What it contains: videos of successful and unsuccessful Internet of Things products.
- Where to get it: IEEE DataPort, https://dx.doi.org/10.21227/qxbn-f510; the website also links a YouTube playlist.
- Who it is for: educators, learners, researchers, product designers and manufacturers.

People know roughly how laptops and phones are built and can choose between them. That is not yet true for Internet of Things products such as connected home gadgets and wearables. Teachers, students and product designers need real examples to compare, including products that failed, in order to understand the design choices behind them.

This dataset is a library of product videos covering successful and unsuccessful Internet of Things products. It is published on IEEE DataPort as 'Internet of Things (IoT) Products' by Charith Perera, with a matching YouTube playlist. It gives the group's product-dissection teaching, described in a 2019 IEEE Internet of Things Magazine article, a citable collection of product evidence.

ALL PAPERS
**Crowdsourced Peer Learning Activity for Internet of Things Education…**

PART 07

# 07



# Teaching and learning

Research turned into lab books, courses and free books for young readers.


IoTClass.org ..... 81
Internet of Things Education ..... 82
Looking inside the smart home ..... 83
Edge Analytics Lab Book ..... 84
Objects you play with ..... 85
IoT Kids Books ..... 86
Design Ideas for Inclusive Smart Cities ..... 87

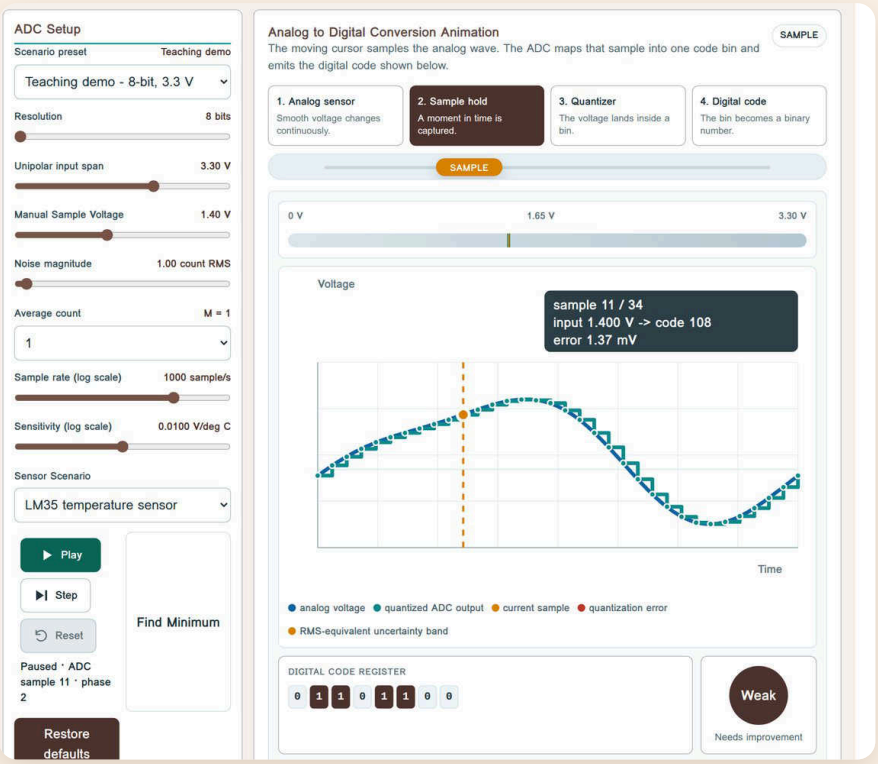



07

TEACHING AND LEARNING

# IoTClass.org

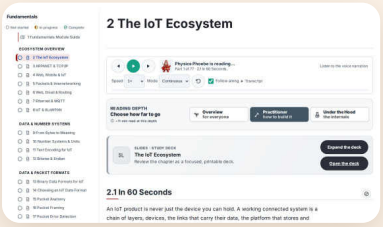
A free online classroom for learning the Internet of Things




One of the interactive tools: learners move sliders and watch a smooth sensor voltage being turned into digital codes.

People come to the Internet of Things (IoT, everyday objects that sense and share data) from very different starting points. A school pupil, a career changer and a working engineer each have different gaps and different confidence. One fixed course cannot serve them all, and missing background knowledge often stops learners before they reach the interesting parts.

IoTClass.org is an online textbook and teaching site preview built to tackle this. It covers sensors, embedded programming, networking, data analytics and application design, and explains ideas through text, quizzes, animations, games, labs and simulators. It also acts as a research testbed for adaptive teaching. Learning gains have not been measured; the site provides teaching infrastructure.




The IoT Ecosystem chapter page, with narration, reading-depth choices and a study deck.

**WHO**
Charith Perera

**PROGRAMME**
Not-for-profit learning initiative • 2026 onwards

**Scan for the project page**
iotgarage.net/go/iotclass

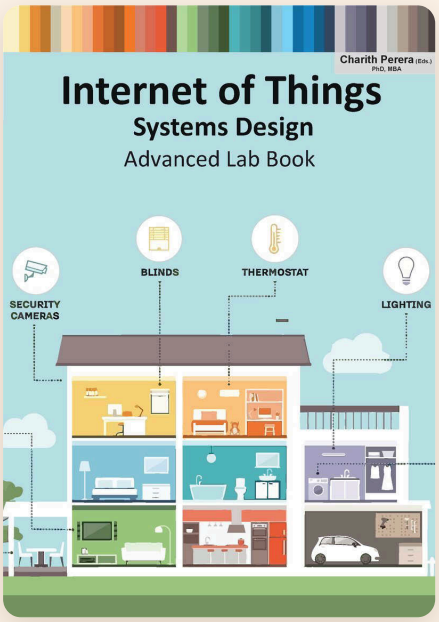
- A not-for-profit initiative for school pupils, university students, career changers, practitioners and curious self-learners.
- Guided learning journeys let people start with the basics and move to advanced topics at their own pace.
- IoT Ideator turns physical design card toolkits into a shared digital canvas for workshops.

07

TEACHING AND LEARNING

# Internet of Things Education

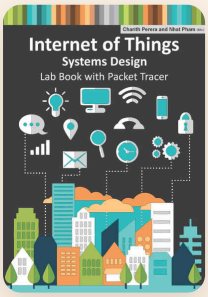
Lab books that teach students to build connected devices




Cover of the Internet of Things Systems Design Advanced Lab Book: an illustrated smart house with security cameras, blinds, thermostat and lighting.

Teaching the Internet of Things (IoT) is hard because the subject spans hardware prototyping, networking, data analytics and application design, and the tools change quickly. Students need lasting principles as well as current kit. Learners also differ widely, from children and hobbyist makers to undergraduate and postgraduate students, so one fixed set of notes does not fit everyone.

The group wrote a family of openly shared lab books and a project workbook. They guide learners step by step from sensors and microcontrollers to gateways, cloud dashboards and network analysis, with simulated labs in Cisco Packet Tracer for when hardware is scarce. A workbook then takes a learner's project from idea to privacy and operating constraints. Learning gains have not been measured.




Cover of the Internet of Things Systems Design Lab Book with Packet Tracer.

**WHO**
Charith Perera, Michal Malecki, Jamie Galvin, Hakan Kayan and colleagues

**WHEN**
2020 onwards

**Scan for the project page**
iotgarage.net/go/iot-education

- Four teaching books: the Systems Design Lab Book, the Lab Book with Packet Tracer, the Advanced Lab Book and the Project Workbook.
- The Lab Book with Packet Tracer (156 pages, January 2025) has 10 labs that link a network simulator to real hardware.
- Core topics include Arduino and Grove sensors, embedded programming, wireless protocols and cloud data pipelines.



07

TEACHING AND LEARNING

# Looking inside the smart home

Understanding connected products and the signals between them

Understanding a connected home means asking what its products do and how they interpret the space around them. These projects examine both questions: learners investigate commercial devices together, while location research studies Bluetooth signals in homes and a museum game. Both make hidden assumptions about connected technology easier to discuss.



Families use phones during the Ghost Detector museum evaluation.

## Location Aware Spaces

**WHO** Tommy Nilsson, Carl Hogsden, Charith Perera, Saeed Aghaee, Alan Blackwell, David Scruton, Andreas Lund, Robert Harle, Ramsey Faragher

**PROGRAMME** International Research Partnership

Bluetooth beacons can help an application respond to nearby places, but walls, bodies and movement complicate the signal. The home study examines this ambiguity around ordinary appliances. In the museum work, Ghost Detector makes unreliable signals part of a playful experience. Together they encourage designers to work with the limits of location sensing and the meaning of a place.

**4 homes**

in England, Australia and Sri Lanka provided the signal study settings. One researcher used one phone; the study did not evaluate the occupants or establish positioning accuracy.

IEEE Systems Journal, 2019

**Scan for the project page**

iotgarage.net/go/location-aware-spaces

## IoT Dissecting

**WHO** Ahmed Hussein, Mahmoud Barhamgi, Massimo Vecchio, Charith Perera

**PROGRAMME** Cardiff University • 2019




The learning activity moves from investigation to merging and comparison.

IoT Dissecting helps people investigate commercial connected products, bring their evidence together and compare design choices. The OLYMPUS platform supports this shared activity, including discussion of privacy and security. A related product collection preserves video material for teaching and research. Small qualitative studies explored how people engaged with the activity, without measuring a before-and-after improvement in learning.

- Learners investigate, merge evidence and compare products.

**Scan for the project page**

iotgarage.net/go/iot-dissecting

**ALL PAPERS**

**Contextual Location in the Home Using Bluetooth Beacons** Perera, Aghae…
**Internet of Things (IoT) Products** Perera • IEEE DataPort, 2023

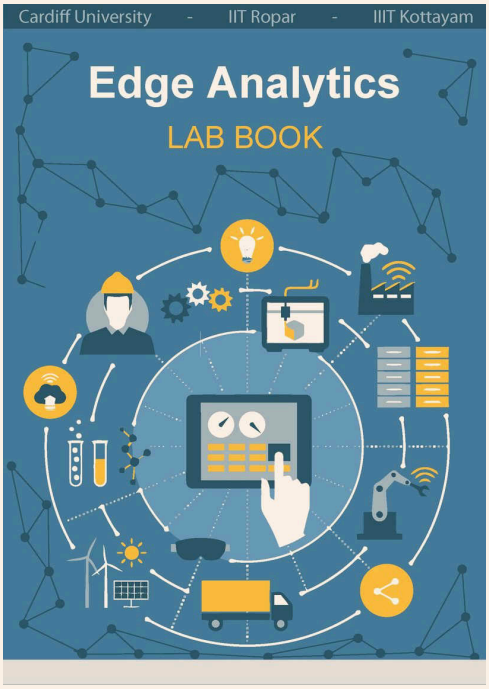
**Applying Seamful Design in Location-based Mobile Museum Applicatio…**
**Crowdsourced Peer Learning Activity for Internet of Things Education…**

07

TEACHING AND LEARNING

# Edge Analytics Lab Book

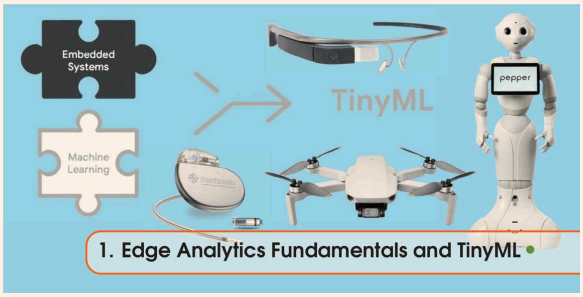
A UK and India course on running AI on tiny devices




Cover of the Edge Analytics Lab Book, naming Cardiff University, IIT Ropar and IIIT Kottayam.

Edge analytics means running machine learning on small devices close to where data is produced, instead of sending everything to distant cloud servers. It is in growing demand, yet it needs unusual skills. A model that runs happily on a laptop will not fit on a microcontroller, a tiny low-cost computer, with very limited memory.

Cardiff University, IIT Ropar and IIIT Kottayam co-created an Edge Analytics course, funded by the British Council. Its lab book teaches a repeated workflow of train, convert, quantise (shrink the numbers a model stores) and deploy. Learners work through three tiers: a notebook, then a simulator or Raspberry Pi, then a microcontroller. It is a curriculum, and student learning has not been measured.




The opening of Lab 1, Edge Analytics Fundamentals and TinyML: embedded systems and machine learning shown as two puzzle pieces that join to make TinyML.

**WHO**

Omer Rana, Charith Perera, Nitin Auluck, Shajulin Benedict, Sujata Pal

**PROGRAMME**

Going Global India • 2021 to 2022

**Scan for the project page**

iotgarage.net/go/edge-analytics

- Co-designed by faculty and students from Cardiff University, IIT Ropar and IIIT Kottayam.
- Funded by the British Council Going Global India Exploratory Grants Program.
- Topics run from TinyML basics (machine learning on very small devices) to wireless links, anomaly detection and federated learning.



07

TEACHING AND LEARNING

# Objects you play with

Connected objects turn ordering and costume-making into interaction

A connected object can make an everyday action feel playful. PizzaBox lets people handle ingredients while ordering food, and IoT Skullfort lets an audience change a costume helmet from a phone. Both prototypes explore how physical interaction changes an experience, while small qualitative studies expose opportunities and practical concerns.

## PizzaBox

**WHO** Luke Jones, Charith Perera
**PROGRAMME** Cardiff University • 2019

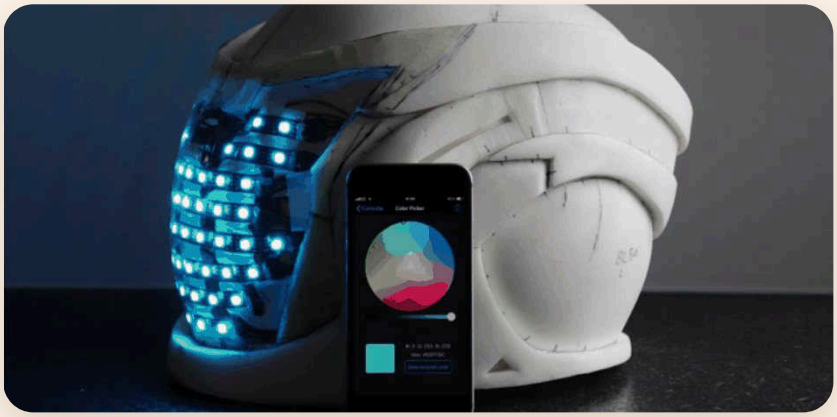


A hand places an ingredient piece on the blue PizzaBox prototype.

PizzaBox replaces a conventional ordering screen with a physical base and ingredient pieces. People place pieces to build an order and press a button to send it. The design developed through paper and modelled prototypes before a pizzeria evaluation. Participants offered ideas about play, accessibility and healthier choices, but the work did not measure changes in eating or ordering behaviour.

- Physical ingredient pieces shape the order.

**Scan for the project page**
iotgarage.net/go/pizzabox



The completed Skullfort helmet lights up beside a phone controller.

## IoT Skullfort

**WHO** Rhys Beckett, Charith Perera **PROGRAMME** Cardiff University • 2019

IoT Skullfort is a costume helmet with lights that another person can control from a phone. The prototype asks what happens when an audience gains control over part of a costume. A focus group explored possibilities for entertainment alongside crowding, safety and unwanted content. These conversations inform design choices, rather than demonstrating the experience at a public convention.

**6 experts**
joined one cosplay focus group, taking wearer and audience roles. The helmet was not evaluated with an audience at an event.
ACM UbiComp/ISWC Adjunct, 2019

**Scan for the project page**
iotgarage.net/go/iot-skullfort

ALL PAPERS

**IoT Skullfort: Exploring the Impact of Internet Connected Cosplay** Beck…

**Poster: PizzaBox: Studying Physical Object Manipulation based Fast Fo…**

07

IOTCLASS • BOOK SERIES FOR YOUNG READERS

# IoT Kids Books

Sensor Squad World: real Internet-of-Things ideas, told as stories any child can follow.




Six of the 60 books: Hello, Smart World!, The World Noticers, Message Mission, The Data Trail, The Trust Test and The Smart Home Helpers.

**60**
illustrated adventures for young readers

**60**
matching teacher guides

**11**
colourful worlds, from the first smart sticker to connected places and communities

**FREE**
All 60 student books and their teacher guides are free to read and download.




**Sammy** — the curious kid

**Gateway Gus** — the friendly gateway

**Cloud Clara** — the cloud connector

**Light Lucy** — the light sensor

**Temperature Terry** — the temperature sensor

**Motion Marley** — the motion sensor

**Moisture Maya** — the moisture sensor

## THE ELEVEN WORLDS

Foundations · Physical World · Device Foundations · Connectivity · Wireless Tech · Systems Architecture · Data and AI · Security and Trust · Human Factors · Engineering · Shared Places

## Follow Sammy and the Sensor Squad

Gateway Gus, Cloud Clara and the sensor crew discover how everyday things sense, think, talk and care. Created by Charith Perera as part of the IoTClass family. Read them at **kidsbooks.iotclass.org**.



## Design ideas for inclusive smart cities

A second free illustrated book, created with IEEE Smart Cities: 243 ideas in 14 sections that help children and communities explore how cities can be accessible, fair, safe and welcoming. Find it at **iotgarage.net**.

07

TEACHING AND LEARNING

# Design Ideas for Inclusive Smart Cities

A free picture book of ideas for cities that work for everyone



Brick model for illustration; no photograph is filed for this project yet.

Ideas about fair and inclusive cities usually live in technical standards and policy reports that children, families and community groups never read. Yet these are the people who use pavements, buses, parks and public services every day. They rarely get an inviting way to talk about how their city could work better for everyone.

This free illustrated book turns inclusive city design into short visual stories. Each idea shows a city problem, the people it affects and a possible design response, then offers Think & Talk prompts for discussion. It was created in collaboration with IEEE Smart Cities and released as a final public edition on 20 September 2026. Readership and classroom impact have not yet been verified.

**WHO**
Charith Perera

**PROGRAMME**
IEEE Smart Cities Committee • 2026

**Scan for the project page**
iotgarage.net/go/inclusive-cities-book

- Free to read and download; made for children, families, teachers, planners and community groups.
- Topics include play, safety, ageing, young people, calm and clear places, digital inclusion, homes and services, culture and belonging, and fair work.
- Created in collaboration with IEEE Smart Cities; the public page credits Charith Perera as Creative Director.

PART 08

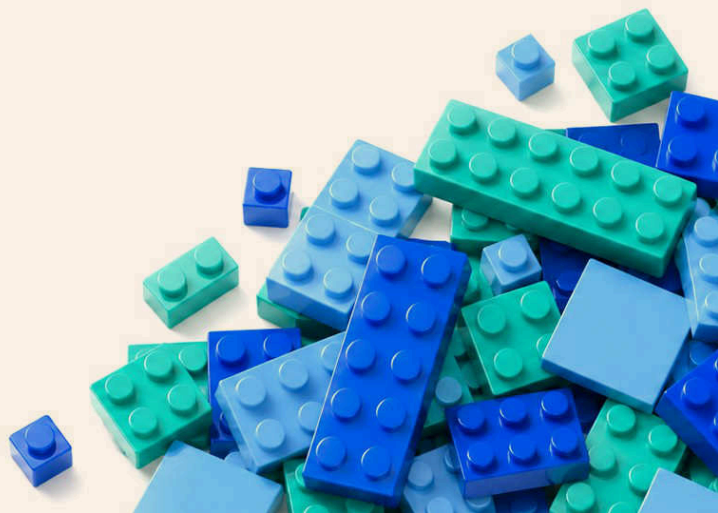
# 08



# Engagement and impact

How the research leaves the building: events, platforms and commercial routes.


PETRAS Regional Networking Events ..... 89
Sustainable IoT for Wildlife ..... 90
Digital Twin Cardiovascular Care ..... 91
Smart City EDI Atlas ..... 92
SensaForge ..... 93
TraceLoom ..... 94

08

ENGAGEMENT AND IMPACT

# PETRAS Regional Networking Events

Bringing Welsh IoT researchers, industry and policymakers together



Participants in a round-table discussion at the PETRAS regional showcase.

Research on the security and privacy of connected devices only helps if it reaches the companies, councils and charities who deploy them. In any region these groups rarely sit in the same room. Without that contact, researchers cannot see where their work is needed, and local organisations do not know what expertise is available nearby.

Cardiff hosted a regional showcase as part of PETRAS, the UK National Centre of Excellence for IoT Systems Cybersecurity. Cardiff University researchers presented work on IoT security, data analytics, privacy engineering and cyber-physical systems. Participants then joined structured networking and mapping sessions. An illustrator captured the ideas as visual maps, which now help the consortium plan future partnerships.



A speaker presents to participants seated at tables during the PETRAS regional showcase.

**WHO**

Charith Perera, Theodoros Spyridopoulos, Georgios Theodorakopoulos, Omer Rana, Pete Burnap

**PROGRAMME**

EPSRC PETRAS Regional Events • 2023

**Scan for the project page**

iotgarage.net/go/petras-events

- Theme: Connected Spaces, covering privacy, trust, reliability and security in built environments, smart cities and connected infrastructure.
- Brought academic researchers together with commercial organisations, government bodies and third-sector groups across Wales and the wider UK.
- Produced visual maps of project ideas, including a digital patient record, location-based data and a digital citizen charter.



08

ENGAGEMENT AND IMPACT

# Sustainable IoT for Wildlife

A workshop with rainforest conservationists to set a research agenda



Three people handle wire cage traps at Danau Girang Field Centre during the 2019 visit (website alt text: field equipment at DGFC).

The Lower Kinabatangan Wildlife Sanctuary in Sabah, Malaysian Borneo, has little connectivity or electrical power. Danau Girang Field Centre, the research station there, is reached only by river, and humidity and insects damage electronics. Staff check animal traps daily by boat, and poaching is a significant problem. Long-range networks that work in cities fail under thick forest canopy.

In 2019 the team held one workshop over two full days with Danau Girang staff to ask what they struggle with. The resulting report lists research challenges in sensing and data science, and proposes a pilot radio network along the river bank and into the jungle. Nothing in the report was built or tested. It set the agenda for the group's later conservation projects.




Group photo at Danau Girang Field Centre; the report names, left to right, Charith Perera, Tommy Rowel, Vanpé Cécile, Grente Oksana and Elisa Panjang.

**WHO**

Charith Perera, Omer Rana, Benoit Goossens, Pablo Orozco Ter Wengel, Tanveer Ahmed

**PROGRAMME**

GCRF Facilitation Funding • 2019

**Scan for the project page**

iotgarage.net/go/iot-for-wildlife

- Partners: Danau Girang Field Centre, VortexIoT and The Things Network.
- Sensing challenges: trap activation detection, poacher tracking, poacher detection, data communication in jungle terrain, and remote camera-trap battery monitoring.
- Data science challenges: automated camera-trap image annotation and joining up different data sources.



08

ENGAGEMENT AND IMPACT

# Digital Twin Cardiovascular Care

A UK and South Korea network on wearables for heart care




Group photo of participants at the Edge-AI workshop at Cardiff University, July 2024.

**WHO**
Nhat Pham, Charith Perera

**PROGRAMME**
Academy of Medical Sciences Networking Grants • 2024 to 2025

**Scan for the project page**
iotgarage.net/go/digital-twin-care

- Overseas lead: Tae Joon Jun, Asan Medical Center. UK co-applicant: Nhat Pham, Cardiff University.
- UK collaborators: Charith Perera and Omer Rana (Cardiff University) and Niki Trigoni (University of Oxford).
- South Korea partners named in the application: Asan Medical Center, KAIST, Ulsan University of Medicine and the National Cancer Center.

People with cardiovascular (heart and blood vessel) disease are mostly monitored during hospital visits. Between visits, clinicians see little of how a patient is doing. Wearable sensors could fill that gap, but turning their signals into something a hospital can use needs clinicians, sensor engineers and data scientists working together across institutions.

The team applied to an Academy of Medical Sciences networking scheme to build a UK and South Korea network. The idea is a digital twin, a patient-specific computer model fed by wearable sensing and hospital records. The plan combined in-person events in Cardiff and South Korea with regular online meetings. Workshops were held at Cardiff University in July 2024 and at Asan Medical Center, Seoul, in April 2025.




Group photo under the '2025 Cardiff-AMC Workshop' banner at the Seoul workshop, April 2025.

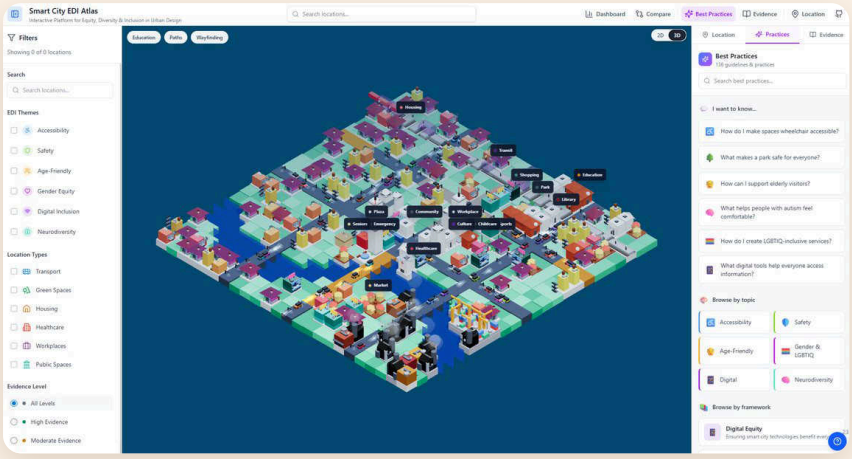


08

ENGAGEMENT AND IMPACT

# Smart City EDI Atlas

An interactive map of ideas for fairer, more inclusive cities




The Smart City EDI Atlas interface: a 3D model city with theme filters on the left and best-practice questions on the right.

**WHO**
Charith Perera

**PROGRAMME**
IEEE Smart Cities Committee • 2024 onwards

**Scan for the project page**
iotgarage.net/go/edi-atlas

- Six themes: accessibility, safety, age-friendly design, gender equity, digital inclusion and neurodiversity.
- Content draws on international frameworks, including the UN Convention on the Rights of Persons with Disabilities, WHO age-friendly city guidelines and ISO accessibility standards.
- Developed through the IEEE Smart Cities Talent, Culture, and Engagement Committee.

Cities are adopting smart technologies to improve services, yet the design of these systems often overlooks the varied needs of the people they serve. Equity, diversity and inclusion (EDI) principles exist in standards and policy documents, but they are scattered and abstract. Planners and designers find it hard to see what the principles mean for a real street or building.

The Smart City EDI Atlas makes those principles something you can explore. Users move around a 2D and 3D model city, open mapped places such as parks, transport and housing, and read design guidance and case studies for each. Every item links back to its source, with the original web address, an archived copy and a screenshot. A public preview was released in March 2026.




The atlas in 2D view, with city places grouped into districts such as Green & Recreation, Commercial, and Health & Services.

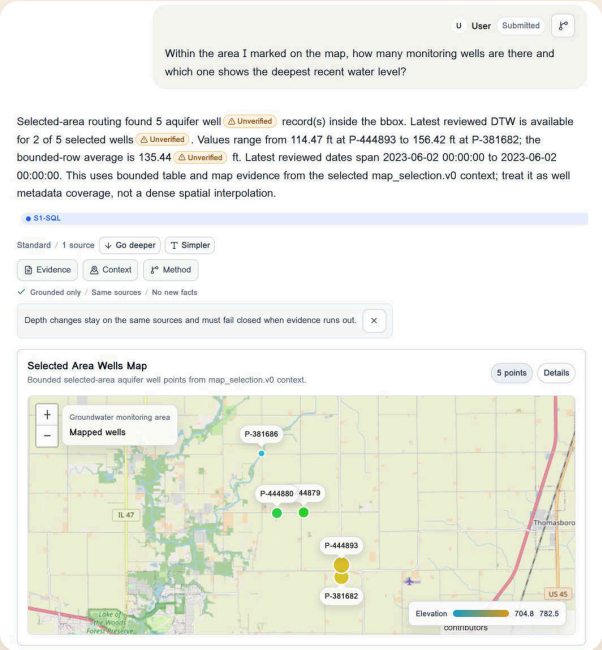


08

ENGAGEMENT AND IMPACT

# SensaForge

Plain-English questions over groundwater, climate and river data




A recorded SensaForge conversation: a question about the monitoring wells inside an area marked on the map, the written answer, and the wells plotted on a map.

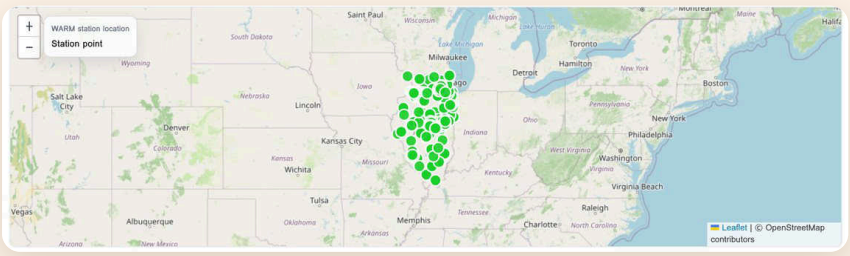
**Scan for the project page**

iotgarage.net/go/sensaforge

- What it is: a web application with sign-up, administrator approval and three user roles, plus pages that show what each data source covers.
- Who it is for: institutional users such as public agencies, researchers and water-district staff.
- Status: version 2 platform under active development with a separate product roadmap. The first Talking Aquifer release is kept as the research origin.

Groundwater, climate and river records sit in separate databases, web services, survey files and reports, and are hard for non-specialists to question. The group's Talking Aquifer project tackled this with software that lets people ask in plain English. SensaForge is the platform that has grown from it, with Talking Aquifer as its first application. Its tagline is 'Sensor-first data intelligence'.

A user types a question on the Ask chat page and gets a written answer with a table, chart or map. They can also ask about an area marked on a map. Answers draw on five registered sources: a groundwater well database, a climate station database, a live government river-gauge service, a geophysical survey and a library of reports. Each answer cites its data or says there is no evidence.



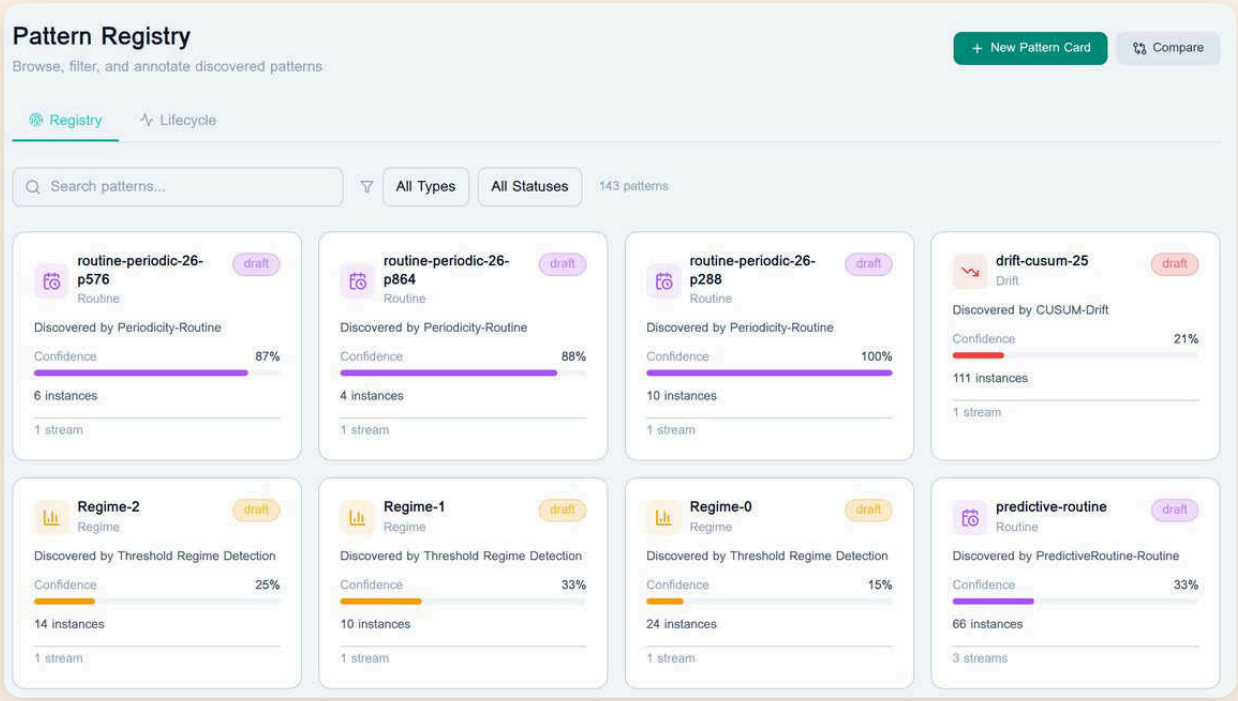

SensaForge map showing groundwater wells and climate stations in the local snapshots.



# TraceLoom

TraceLoom
PATTERN PLATFORM

Finding and explaining the patterns of daily life in sensor data



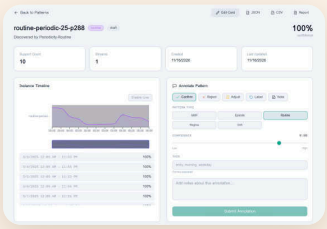

The Pattern Registry: cards for routine, drift and regime patterns, each with its discovery method, confidence and number of instances. Synthetic demo data.

Buildings, campuses and factories are full of sensors that record activity over time. Hidden in those streams are routines: what normally happens, in what order, and when things drift. This is sometimes called pattern of life. Finding such patterns, checking they are real and turning them into dependable detectors is slow specialist work today.

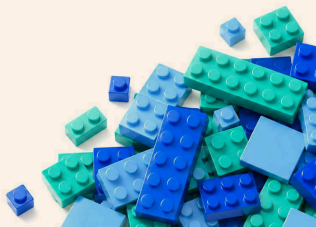
TraceLoom is a sensor-centred pattern-of-life platform, currently a developmental preview. It takes in streams of readings over time and discovers five families of pattern: motifs, episodes, routines, regimes and drift. Each pattern becomes a card that a person can inspect, confirm or reject. Chosen patterns move through a detector pipeline towards small edge devices. The first business focus recorded is smart buildings, campus facilities and IoT operations.

**Scan for the project page**
iotgarage.net/go/traceloom

- A standalone web application plus a pattern-intelligence API layer (a way for other software to use it).
- Explains its reasoning step by step, with a technical account and a plain-language account side by side.
- A detector pipeline moves a confirmed pattern through candidate, evaluating, qualified and supported stages; the demo deploys to a simulated Raspberry Pi.



One discovered routine: its instance timeline, the days on which it occurred, and the panel where a reviewer confirms, rejects or labels it. Synthetic demo data.



00

THE DECADE

# 2016 to 2026

From privacy guidance on paper to a group that builds, deploys and teaches.

**2016**

### Privacy by design for IoT

A framework for assessing IoT applications and platforms against privacy guidance.

**2017**

### Guidance people can use

The privacy guidelines cheat sheet and the Sensing as a Service roadmap.

**2018**

### Cardiff University

The Living Edge Laboratory and practical lab books for IoT teaching.

**2019**

### Into the forest

First field work with the Danau Girang Field Centre in Sabah.

**2021**

### National Resilience Fellowship

A GCHQ fellowship for resilient sensing in homes and buildings.

**2022**

### A research group

The Cardiff IoT Research Group is launched.

**2023**

### Google Research Scholar Award

And two open datasets released on IEEE DataPort.

**2024**

### Edge intelligence

The National Edge AI Hub, Edgy Organism and ARCADE begin.

**2025**

### OECD Fellowship

Talking Aquifer, and Web of Things work with W3C.

**2026**

### Learning at scale

IoTClass CIC, the IoT Kids Books and this book.



00

WHERE THE WORK HAPPENS

# Many places

Field sites, partners and co-authors behind the projects in this book.



### United Kingdom
**Cardiff University and partners**

Home of the group, its labs and most projects; secondments at BRE and Digital Catapult.

### Malaysia
**Danau Girang Field Centre, Sabah**

Forest Observatory field work, the jungle sensor network and the Pan-Borneo elephant project.

### Sri Lanka
**University of Moratuwa**

Forest and elephant sound recognition and number-plate reading on small devices.

### India
**Going Global Partnerships**

The Edge Analytics Lab Book, built with partners in India.

### Japan
**NAIST**

Event cameras for sensing smart built environments, with the UBI-Lab testbed.

### United States
**University of Illinois Urbana-Champaign**

A partner of the group; talks and visits in 2024.

### France
**Claude Bernard Lyon 1 University**

Privacy engineering: designing privacy-aware IoT applications.

### Brazil
**University of São Paulo**

Finding the right sensor: IoT resource discovery.

Co-authors on the papers in this book also work in China, Italy, Lebanon and elsewhere. Affiliations are taken from the papers.

00

TEN YEARS IN NUMBERS

# The decade, counted

Counted in November 2026 from the iotgarage.net publication list and team page.

**124**
**publications from 2016 to 2026**

**69**
**journal articles**

**37**
**conference papers**

**24**
**doctoral researchers, current and past**

**78**
**projects told in this book**

**8**
**countries in the stories on the previous page**

**170+**
**devices in the Smart Home Lab**

**2**
**open datasets on IEEE DataPort**



09

OUT THE BACK

# Tools and products

Named things that came out of the research. Each has a project page on **iotgarage.net**.

### Privacy Parrot

Interactive tools that bring privacy-preserving techniques into early IoT software design.

### Privacy Captain

A knowledge-based AI assistant that annotates IoT designs with privacy patterns.

### Canella

Reusable privacy-preserving components and gamified tooling, so applications comply with regulations by design.

### Privacy Nodes

Canella's privacy nodes for Node-RED, with real-time warnings.

### PrivacyPulz

An AI-assisted tool that helps novice software engineers learn privacy by design and legal compliance.



### PrivacyCube

A cube that shows, on its faces, what smart-home devices do with data.



### PriviFy

A tangible interface with knobs and buttons for setting IoT privacy choices.

### Forest Observatory

A linked-data observatory and analytics platform to support forest conservation.

### CamTrap.AI

A multi-model AI system that identifies and counts wildlife in camera trap images.

### CASPER

Context-aware anomaly detection that observes industrial robots with independent IoT sensors.

### CASPER Shield

The CASPER work as a product concept, taken through the CyberASAP accelerator.

### SensaForge

The platform and commercial route that grew out of Talking Aquifer.

10

OUT THE BACK

# Who backs the work

Our funders and partners, as listed on **iotgarage.net**.

**Funders**

- EPSRC
- IARU
- Microsoft Azure
- Cardiff University
- GCRF
- GCHQ
- KESS2
- DCMS 5G Programme
- British Council
- Google Research
- NVIDIA
- The Alan Turing Institute
- Academy of Medical Sciences
- OECD
- NERC
- UKCEH
- Great Britain Sasakawa Foundation
- MEDR

**Partners**

- Digital Catapult
- Danau Girang Field Centre
- DSTL
- HMGCC
- PETRAS 2
- VortexIoT
- Exalens
- Airbus Group
- Awen Collective
- Building Research Establishment
- Innovate Trust
- Digital Communities Wales
- Ofcom
- University of Illinois Urbana-Champaign
- NAIST



Visit to Sabah, Malaysian Borneo, 2024.



At the Ubiquitous Computing Systems Laboratory, NAIST, Japan, 2025.



Danau Girang Field Centre, 2019.

The work needs real places: homes, buildings, forests, aquifers, factories and classrooms, in the United Kingdom, Malaysia, Sri Lanka, India, Japan, the United States, France and Brazil. Partners make that possible.

WORK WITH US

# The door is open

1. **Visit the labs**
   See the Smart Home Lab, the Living Edge Lab and the Smart City Lego Lab at Cardiff University.
2. **Host or send a secondee**
   Our secondments with the Building Research Establishment and Digital Catapult shaped whole projects.
3. **Bring a problem for a student project**
   Undergraduate, masters and doctoral projects take on real problems from partners.
4. **Build a joint bid**
   We have worked on funded projects with partners from conservation, industry, government and the third sector.
5. **Start from what is public**
   Project pages, publications, datasets and code are linked from **iotgarage.net**.



CONTACT


## Charith Perera

Reader, School of Computer Science and Informatics, Cardiff University

Visiting Faculty, University of Illinois Urbana-Champaign


INTERNET OF THINGS GARAGE

FIND AND FOLLOW

**iotgarage.net**
The research group: projects, papers, code

**iotclass.org**
Our not-for-profit IoT learning initiative

**kidsbooks.iotclass.org**
IoT Kids Books: a free book series for children

**IoT Garage TV**
Talks and demos on YouTube

**@IOTGarageNews**
Group news on X