Internet of Things Research and Teaching: Vision and Mission

Annual Report (2019)

Charith Perera (MBA, PhD)

Introducing the Internet of Things Garage

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

More formally, most of our research is ***build-driven*** and somewhat ***experimental*** and mostly applied. This means that we build things, systems, and techniques and evaluate them in real-world settings. We aim to demonstrate how they work but never focus on giving theoretical guarantees. We always like to stay closer to end-users than to the theories. In our work, the objective is to produce artefacts (software system, things) that are useful in the real world. Therefore, we felt that the name ***'IoT Garage'*** is more appropriate and describes our work well than the more traditional name ***'IoT Laboratory'***. We are not alone, see.

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

Principle Investigator: Charith Perera

Research Associates:

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

PhD Students: As of January 2020, the research group comprises of six PhD students (and two affiliated PhD students).

- **Nada Alhirabi**
  Designing Privacy by Design IoT Applications [Since OCT 2018]
- **Areej Alabbas***
  Secure Service Placement for IoT [Since JAN 2019]
- **Atheer Jeraisy**
  Reusable Privacy Components for IoT [Since APR 2018]
- **Asma Irfan** (PT)
  Influence through Data-Driven Pervasive Interactions [Since JAN 2020]
- **Lamya Alkhariji**
  Knowledge-Driven Privacy by Design for IoT [Since DEC 2018]
- **Emad Aliwa***
  In-Vehicle Edge Security [Since APR 2018]
- **Bayan Almuhander**
  Privacy-Aware Smart Home Data Management [Since OCT 2018]
- **Hakan Kayan**
  Context-Aware Security for Cyber-Physical Systems [Since JAN 2020]

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

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

Dogukan Sert
MSc (2019)
Semantic Querying for Data Science on Edge

Yasar Majib
MSc (2019)
Family Dynamics-based Security

Asma Alotaibi
MSc (2019)
Smart Home Simulation Tool

Ruslan Levond
BSc Summer (2019)
IoT Edge Analytics

Michal Malecki
BSc Summer (2019)
IoT Labs

Ahmed Hussein
BSc (2019)
Crowdsourced IoT Products Dissecting

Rhys Beckett
BSc (2019)
IoT Driven Cosplay

Karan Juj
BSc (2019)
Tracking Poachers using BLE

Luke Jones
BSc (2019)
Internet-Connected PizzaBox

Jack Burkett
BSc (2019)
Tracking Poachers using GPS/SMS

Annual Summary for 2019

- The research group is structured around five research themes related to the Internet of Things (IoT) with a significant emphasis on build-driven research method: (1) *Design-Time Privacy and Security,* (2) *Run-Time Privacy and Security,* (3) *Data Marketplaces,* (4) *Sensing Infrastructure,* (5) *Learning Technology*.
- Six PhD students have started working on these themes, including two affiliated PhD students.
- Five BSc students completed their final projects – including two publications
  - Rhys Beckett (2019) published a poster paper in Ubicomp 2019
  - Ahmed Hussein (2019) published a research paper in IEEE Internet of Things Magazine
- Three MSc students completed their dissertations.
- Developed an IoT Edge network with 100 sensor nodes with the funding received from EPSRC ECR Capital award.
  - A summer student supported by Cardiff Undergraduate Research Opportunities Programme (CUROP) received research training as part of this project.
- A postdoctoral researcher started working on a PETRAS Catalyst project (Integrity Checking at the Edge).
- Developed Internet of Things teaching materials to be delivered in 19/20 spring semester via Network Communications and Emerging Technology modules.
- Started the RCUK Catapult Researchers in Residence (RiR) project (Quarriable Smart City Data Markets) in collaboration with Digital Catapult, which will span across the next two years.
- Organised a Global Challenges Research Fund (GCRF) workshop with the help of a facilitation funding in order to develop a long-term research program in collaboration with the School of Bioscience and Danau Girang Field Centre (DGFC).

Looking forward to 2020…

Research Vision

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

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

My research group is formulated around research themes as follows:

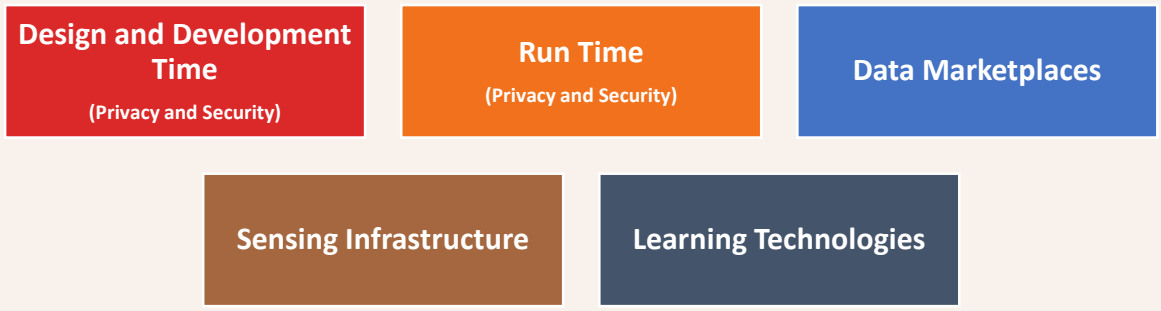


Figure 1: Primary Research Themes

Design and Development Time (Privacy and Security): In this theme, we explore how to develop efficient and effective tools to help software engineers to design privacy and security-aware application better. We also extend development time tools to support and motivate software developers too better incorporate privacy and security by design approaches.

Run Time (Privacy and Security): This theme focuses on runtime privacy and security aspects. We develop techniques to detect in-vehicle cyber attacks by examining CAN data. We also study how to optimally place and schedule of service function chaining under security constraints. We aim to understand vulnerabilities in IoT devices better when integrated into future digital ecosystems, particularly safety-critical systems.

Data Marketplaces: This theme focuses on understanding future data marketplace better, from different perspectives such as data management, end-to-end infrastructure, and business model. In this work, we look at smart city data, smart home data, and personal data as well. As a consequence, we are also interested in looking at privacy challenges (ranging from privacy-preserving data trading to informed consent) around IoT data marketplaces.

Sensing Infrastructure: This theme explores how to develop and deploy IoT infrastructure to support various applications and in different domains such as agriculture, building sustainability, human behaviour, independent living, smart homes and offices occupancy patterns and usage, rural and wildlife, etc. We aim to identify different trade-offs and their applicability in different domains and finally to extract best practices.

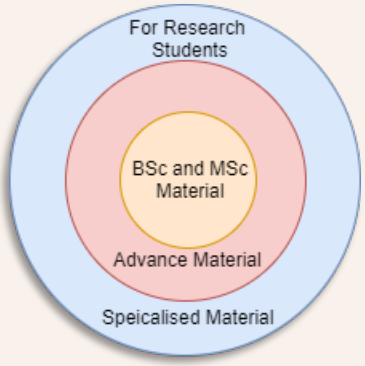
Learning Technologies: This theme aims to enhance teaching activities. We aim to understand how to teach IoT for different types of audiences (from high school to university students and beyond) with different skills levels with the help of innovative tools and techniques.

Teaching Vision

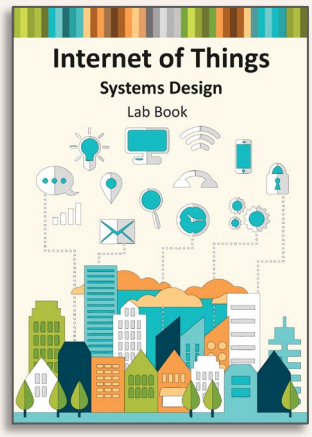
At the undergraduate level, Internet of Things related content is delivered (to second-year students) through a module titled CM2306 Communication Networks (since 19/20). At postgraduate level, IoT is delivered through a dedicated module titled Internet of Things: Systems Design (planning for 20/21). Both modules are (mostly) identical in terms of delivery and content. However, expectations (from assessment perspective) are higher at postgraduate level.

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

Modularity and Complexity: The content under each theme is developed in a modular and layered fashion based on the complexity of the content. This means that each topic has a certain amount of content that delivers the basic information to the students, which are sufficient enough to complete both undergraduate and postgraduate modules. However, if a student interested in learning more they can follow the advance material and learn by themselves. *Advanced materials* are structured and delivered in a similar fashion to the basic material (at times embedded within basic material but are clearly marked) and also provide close guidance on how to follow up and self-study the material. *Specialist materials* are less structured and less organised. they are delivered through either seminars or tutorials (pre-recorded or in-class). Advance and specialised material may help the students to complete the assignments in a much higher quality but by no means mandatory to follow. Specialised material may be useful for new research students to advance their knowledge.



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



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

Dissemination and Community Engagement

IOT Garage TV (bit.ly/2Md8vJE)

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

IOT Garage News (@IOTGarageNews)

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

IOT Garage Code (@IOTGarage)

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

Group Website (iotgarage.net)

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

Funding Support

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

(Co-Investigator)

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

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

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

(Principle-Investigator)

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

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

EPSRC Capital Award support for Early Career Researchers (Cardiff University Internal)

(Principle-Investigator)

(Internal)
36,840 GBP

This project is focused on establishing a laboratory at Cardiff University to support 'Edge Computing' research. It enables us to develop a new class of applications (and underlying computational analysis algorithms) that are 'latency-sensitive'. The laboratory will enable us to carry out internationally leading research in cybersecurity, real-time data processing and communication networks. The laboratory will be realised by a combination of Raspberry Pi and Arduino boards, that are distributed across open spaces and existing laboratories.

GCRF Facilitation Funding (Cardiff University Internal)

(Principle-Investigator)

(Internal)
10,000 GBP

Funding provided for University Research Institutes, established Networks and Centres at Cardiff University to bring together potential GCRF partners and stakeholders through the organisation of GCRF focussed workshops and networking events, in the DAC listed Least Developed and Other Low-Income Countries. We received funding to conduct two workshops in Sabah, Malaysia and Cardiff, UK in order to explore challenges faced by Sabah Wildlife.

Partners

Awen Collective

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

Airbus Group

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

Digital Catapult

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

The Things Network

The Things Network provide a set of open tools and a global, open network to build your next IoT application at low cost, featuring maximum security and ready to scale.

PETRAS National Centre for Cyber Security

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

Vortex IoT

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

iPoint

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

CloudTexo

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

Danau Gurang Field Center

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

Design & Development Time
(Privacy and Security)

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

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

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

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

The primary objective of this project is to develop an interactive design method (facilitate through a tool) that incorporate privacy-preserving techniques into the early phases of the software development lifecycle efficiently, effectively and collaboratively. We envision our tool to be collaboratively used by business analysists, requirement engineers, user experience designers, and software engineers together during the process of creating privacy by design IoT application designs. Our secondary objective is to explore whether such a tool (with minor alteration) could also be used to enhance privacy education of high school and university students. We aim to develop our prototype by extending the OWASPS's Threat Dragon Tool. This project composed of three main objectives:

- Review the existing of design notations, models, languages and tools that facilitate capturing non-functional requirements (i.e., security and privacy).
- Co-Creating visual language, notations, and set of interaction patterns toolkit for Privacy by Design Representation for the IoT.
- Evaluate the efficiency and effectiveness of PARROT (Privacy by Design for the Internet of Things) as a tool for augmenting software engineer's capabilities and enhance privacy education.

PRIVACY PARROT

Partners and Relevant Projects

PETRAS

OWASP Open Web Application Security Project

Outcomes

- **[Technical Report]** Nada Alhirabi, Omer Rana, Charith Perera, **Designing Security and Privacy Requirements in the Internet of Things: A Survey**, Technical Report, 2019 PDF BIB

Design & Development Time
(Privacy and Security)

Augmenting Software Design Processes using Automated Privacy-aware Internet of Things Application Design Techniques

Researcher: Lamya Alkhariji (PhD Student-2018-2022)

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

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

The primary objective of this project is to develop a method (using Knowledge-based AI) that assist software engineers by automatically incorporating Privacy by Design (PbD) techniques into a given IoT application design. We aim to develop our prototype by extending the OWASPS's Threat Dragon Tool. This project composed of three main objectives:

- Review and synthesise privacy by design knowledge through curating and systematically analysing existing privacy strategies, guidelines, principles, and patterns in the context of IoT.
- Semantically model privacy patterns and IoT systems using knowledge base AI techniques towards automated privacy pattern placement.
- Evaluate the efficiency and effectiveness of PRIVACY CAPTAIN (Context-Aware Privacy Assistant for the Internet of Things) as a tool for augmenting software engineer's capabilities and enhance privacy education. PRIVACY CAPTAIN is an AI assistant that is capable of reviewing a given IoT system design and provide advice on how optimally apply privacy patterns.

Partners and Relevant Projects

Outcomes

- **[Technical Report]** Lamya Alkhariji, Omer Rana, Charith Perera, **Synthesising Privacy by Design Knowledge: A Systematic Analysis**, Technical Report, 2020 (will be available soon) PDF BIB

Motivating Software Engineers to Develop Privacy-aware Internet of Things (IoT) Applications through Reusable Privacy Components and Gamification Techniques

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

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

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

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

Partners and Relevant Projects

PETRAS

Outcomes

- **[Technical Report]** Atheer Jeraisy, Omer Rana, Charith Perera, **A Systematic Analysis of Privacy by Design Schemes towards Complying with Privacy Laws in the Internet of Things Era**, Technical Report, 2020 (will be available soon) PDF BIB

Run Time
(Privacy and Security)

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

Researcher: Areej Alabbas (PhD Student-2019-2022)

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

Partners and Relevant Projects

PETRAS

Run Time
(Privacy and Security)

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

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

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

Partners and Relevant Projects

PETRAS

ipoint

Run Time
(Privacy and Security)

Integrity Checking at the Edge

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

ICE project will study the factories and water treatment systems of the future, undertaking composite vulnerability analysis of interactions between edge devices, cloud platforms and legacy systems. This vulnerability analysis will be complemented by the use of AI at the edge of such systems to create and improve methods to demonstrate transparent processes mapping of data flows to expected activity at the periphery of integrated systems with advanced visualisation methods, and provide security and resilience assurances for critical infrastructures of the future. Inspiration will be taken from explainable and interpretable AI, considering human-machine interaction in the context of question-asking around pathways and interactions involving data, creating links to the ICE-AI project within the usability lens. The Bristol Critical Infrastructures Testbed (which underpinned a linked PETRAS 1 demonstrator) will form a core source for the technical analysis. The project aims to understand vulnerabilities in IoT devices better when integrated into future digital ecosystems – particularly safety-critical systems. There are three main objectives to achieve this aim:

- Using AI to map actual activity to expected outcomes for data flows and behaviour in safety-critical IoT-based systems.
- To improve the visualisation of actual and expected outcomes such that anomalies and deviations in behaviour can be human-interpretable.
- To enable human-machine interaction with improved visualisations to 'dig in' to anomalous or suspicious behaviour and undertake exploratory analysis to understand malicious behaviour further.

Partners and Relevant Projects

Run Time
(Privacy and Security)

Interaction Methods for Privacy Preferences Management in Shared Spaces in Internet of Things Era

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

Smart spaces (i.e., smart homes and offices) could comprise many different IoT devices. Most of these devices comprise of different types of sensors that measure a wide range of phenomenon (e.g., temperature, presences, activities, etc.). At the moment, these devices do not have a mechanism to communicate with the user to inform them about how they manage data. Sometimes, these devices may provide very limited information about how these devices manage data during the initial configuration (setting up) process. However, no IoT product today informs the users (i.e., owner as well as other occupants who share the same space) about the data it collects and manages on an ongoing basis. In this project, we aim to develop an interaction method that allows users to manage their privacy preferences on an ongoing basis in shared spaces in Internet of Things era.

Data Marketplaces

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

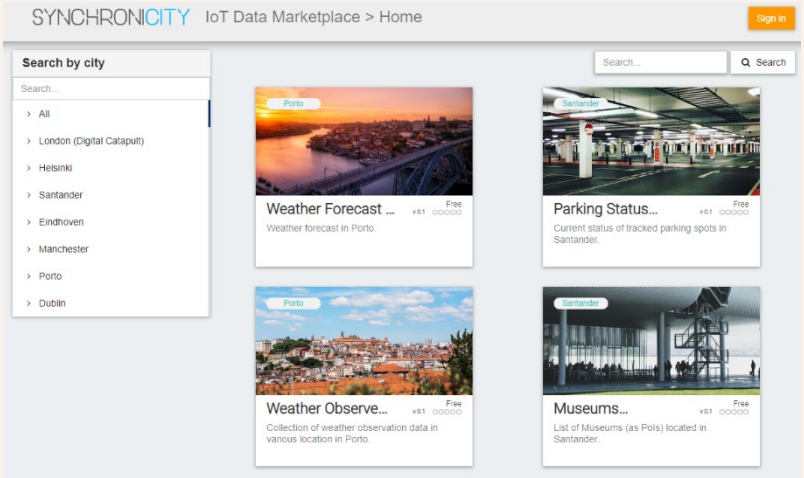
Researcher: Charith Perera (Principle Investigator-2019-2021)

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

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

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

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



Current view of the Data Marketplace: iot-data-marketplace.com

Partners and Relevant Projects

SYNCHRONICITY CATAPULT Digital

Sustainable Internet of Things Infrastructure Towards Efficient Wildlife Conservation

Researchers: Charith Perera, Omer Rana, Benoît Goossens, Pablo Orozco-ter Wengel (2019)

Danau Girang Field Centre (DGFC) is located in Sabah Malaysia (marked in Figure 2). The only access to the field centre is through the river. As a result, all the research activities are conducted by going through the river. It is worth noting that Sabah Malaysia is a high humidity region where electronic components could get damaged quite quickly due to environmental factors such as moisture. Further, in jungle terrains, insects could also get attracted to copper within electronic components. We need to keep in mind this context when we are addressing the challenges. We conducted a two full-day workshop to explore and identify research challenges that could potentially be addressed using the Internet of Things (IoT) technologies. During this workshop, we identified two major areas to focus on: ***(1)*** **Sensing Infrastructure**, and ***(2)*** **Data Science**. Additionally, we also discussed **citizen engagement research,** where we could work with local schools and universities to share our technical expertise with the local community. In the long term, such activities will help local communities to develop technologies to solve their problems.

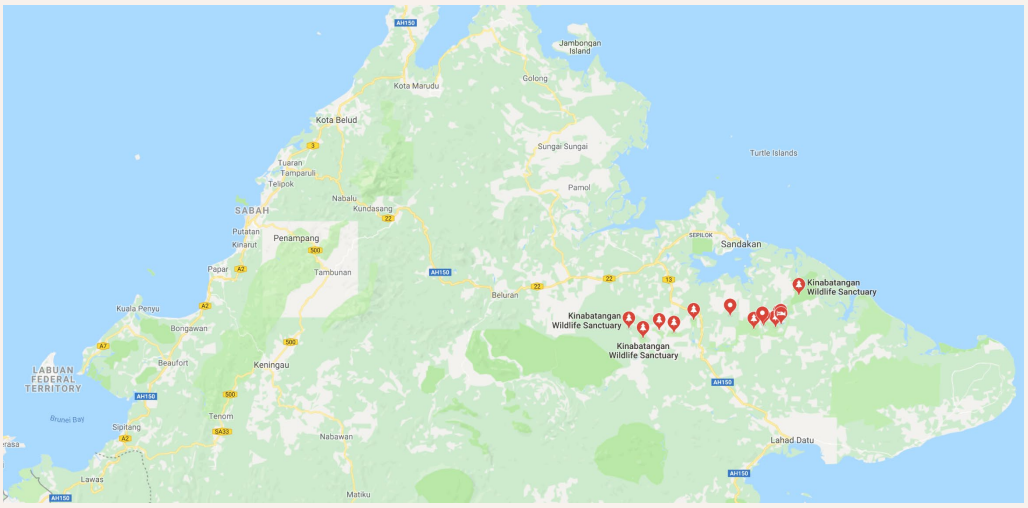


Figure 2: A map the region of the Kinabatangan Wildlife Sanctuary

Sensing Intrastructure
•Trap Activation Detection •Poacher Tracking •Poacher Detection •Data Communication in Jungle Terrains •Remote Camera Trap Battery Monitoring

Data Science
•Automated Camera Trap Image Annotation •Semantic Data Integration for Wildlife.DATA

- **[Technical Report]** Charith Perera, Omer Rana, Pablo Orozco Ter Wengel, Benoit Goossens, **Sustainable Internet of Things Infrastructure Towards Efficient Wildlife Conservation: Challenges and Research Directions,** Technical Report, 2019 PDF BIB

Incubator Projects

PizzaBox: Studying Internet Connected Physical Object Manipulation based Food Ordering

BSc

Researcher: Luke Jones (BSc Student-2019)

This project focused on designing and testing of PizzaBox, a 3D printed, interactive food ordering system that aims to differ from conventional food ordering systems and provide an entertaining and unique experience when ordering a pizza by incorporating underlying technologies that support ubiquitous computing. The PizzaBox has gone through both low and medium fidelity testing while working collaboratively with participants to co-design and refine a product that is approachable to all age groups while maintaining a simple process for ordering food from start to finish. The final evaluation was conducted at an independent pizzeria where interviews with participants lead us to develop three discussion themes: 1) end-user engagement (from entertainment to education), 2) towards connected real-time products and services, and 3) healthy eating and living.

We believe that each of the themes identified during the user study has there own merit to be investigated more in-depth independently. For example, individual IoT device base advertising is a completely new paradigm that needs to be investigated separately to examine opportunities and potential issues. Such investigation may be carried out from a different point of views such as business, psychology, and law. Other opportunities are to use PizzaBox (or similar IoT devices), as a tool for education and lifestyle changes. Such investigation may be carried out from a different point of views such as education, healthy eating, and medical (e.g., preventing risks related to allergies). PizzaBox type device could also help people who have challenges in using computational devices such as computers or mobile phones (e.g., dementia, Parkinson). Education and healthy eating would be our research focus in the future.

Participants are engaging with the prototype during the study 2 medium-fidelity tests.

Participants engaging with the study 1 low fidelity tests[left] and final prototype used by an actual customer [right]

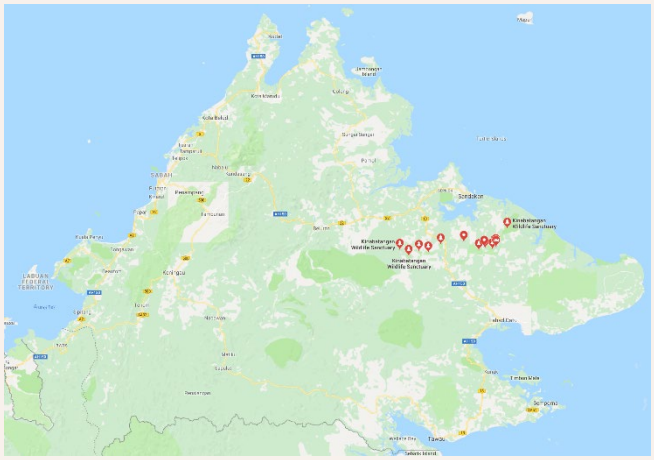
- **[Technical Report]** Luke Jones, Charith Perera, **PizzaBox: Studying Internet Connected Physical Object Manipulation based Food Ordering**, *Technical Report*, 2019
  PDF BIB CODE VIDEO VIDEO

Low-Cost SMS Driven Location Tracking System for Anti-Poaching Investigations

BSc

Researcher: Jack Burkett (BSc Student)

Throughout the world, poaching has been an ever-present threat to a vast array of species for over many decades. Traditional anti-poaching initiatives target on catching the poachers. However, the challenge is far more complicated than catching individual poachers. Poaching is an industry which needs to be fully investigated. There are many stakeholders, directly and indirectly, involved in poaching activities (e.g., some local restaurants illegally providing meat to tourists). Therefore, to stop or severely decapitate the poaching industry requires a unified understanding of all stakeholders.



A map of the Kinabatangan Wildlife Sanctuary. Sandakan is the closest major city.

The best ways to uncover these geographical and social relationships is to track the movements of poachers. However, location tracking is challenging in most of the rural areas where wildlife sanctuaries are typically located in. Internet-connected communication (e.g. 3G) technologies typically used in urban cities are not feasible in these rural areas. Therefore, we decided to develop an SMS (short message service) base low-cost tracking system (SMS-TRACCAR) to track poachers. We evaluated the proposed system in Kinabatangan Wildlife Sanctuary, Sabah, Malaysia and nearby villages and cities where poachers are typically moving around.

Our evaluations demonstrated that SMS based tracking could provide sufficient quality (granular) data (with minimum energy consumption) that enable us to monitor poacher vehicle movements within rural areas where no other modern communication technologies are feasible to use. However, it important to note that our system can be used in any domain that requires SMS based geo-location tracking. SMS-TRACCAR can be configured to track individuals as well as groups. Therefore, SMS-TRACCAR makes contributions not only to wildlife domain but in a wider context as well.

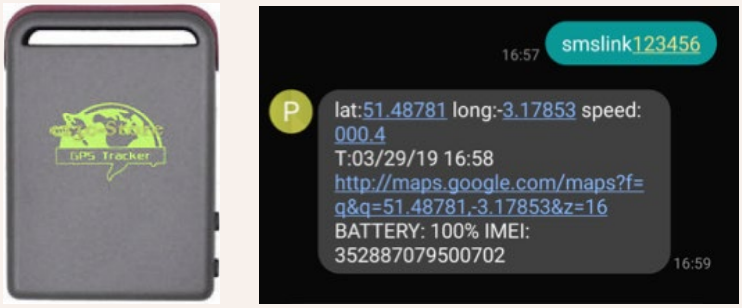


Figure 3: (a) GPS Tracker Locator Device [left] and (b) the message return if device is unable to connect to GPS [right]

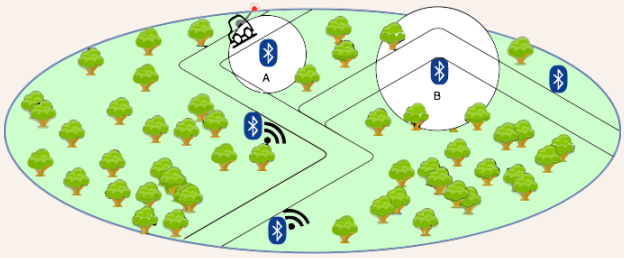
- **[Technical Report]** Jack Burkett, Tommy Rowel, Benoit Goossens, Pablo Orozco Ter Wengel, Omer Rana, Charith Perera, **Low-Cost SMS Driven Location Tracking Platform: An Anti-Poaching Case Study**, Technical Report, 2019 PDF BIB CODE VIDEO VIDEO

Exploring the Suitability of BLE Beacons to Track Poacher Vehicles in Harsh Jungle Terrains

BSc

Researcher: Karan Juj (BSc Student-2019)

Our overall aim is to explore whether we could use Bluetooth Low Energy (BLE) technology to track poacher vehicles in remote and rural areas such as Sabah, in Malaysia, especially deep inside the jungle terrain with little or no communication technologies exists. Tracking technologies are currently limited to relying on satellites or cellular towers, for environments that do not permit access to these signals, very few viable alternatives exist. This project explores the use of BLE as a method to track vehicles. It works by mounting Bluetooth beacons beside a road and placing a receiver concealed somewhere inside the vehicle. As the vehicle drives past the beacon, the receiver and beacon are momentarily in range, the receiver then stores a unique ID from the beacon, and when the vehicle is then in an area with GSM signal, an SMS is sent containing the unique IDs of the beacons that have been detected. This project is prototyped and tested in collaboration with the Danau Girang Field Centre in Sabah, Malaysia. The results offer insights for how effective BLE beacons are in a tracking situation for where the beacon and receiver are in range for a short period as well as how different obstructions will affect the range and strength of the signal. It is important to note that our objective is not to catch the poacher, instead to understand how they move around within jungle terrain, as we can use such information to develop a comprehensive plan against poaching activities. We placed the BLE beacons, as shown in the figure.



BLE Beacon Placement

During the evaluation, we tested various types of obstructions that the signal would face in deployment. As illustrated in the following Figure, we tested plastic and cardboard cases which were intended to simulate the effect that adding a case would have on the signal.

Figure 4: Different types of obstructions: (Left) plastic, cardboard, wood, water (right)

We found that different types of obstructions reduce the distance the BLE would penetrate. However, signals could easily research 50m under any obstructions. Usually, this distance is sufficient enough to be useful in jungle roads as the only requirement is to reach an ongoing vehicle. If obstructed by water (e.g. raining), BLE signal penetration could be reduced to 30m, which is still sufficient to be useful.

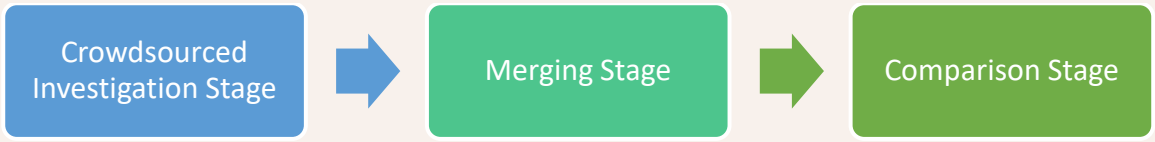
- **[Conference]** Karan Juj, Charith Perera, **Exploring the Suitability of BLE Beacons to Track Poacher Vehicles in Harsh Jungle Terrains**, IEEE 6th World Forum on Internet of Things (WF-IoT), New Oreleans, Louisiana, USA, April, 2020 PDF BIB CODE VIDEO

Crowdsourced Peer Learning Activity for Internet of Things Education: A Case Study

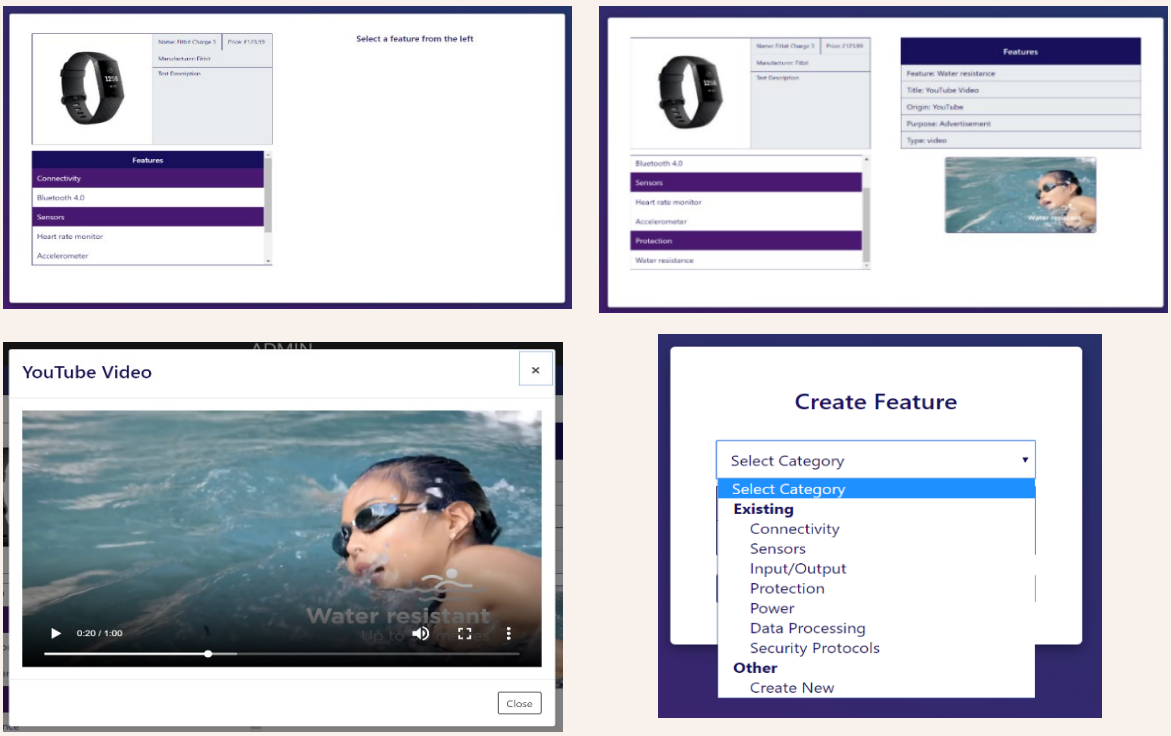
BSc

Researcher: Ahmed Hussein (BSc Student-2019)

Computing devices such as laptops, tablets and mobile phones have become part of our daily lives. End-users increasingly know more and more information about these devices. Further, more technically savvy end-users know how such devices are being built and know how to choose one over the others. However, we cannot say the same about the Internet of Things (IoT) products. Due to its infancy nature of the marketplace, end-users have a very limited idea about IoT products. To address this issue, we developed a method, a crowdsourced peer learning activity, supported by an online platform (OLYMPUS) to enable a group of learners to learn IoT products space better. We conducted two different user studies to validate that our tool enables better IoT education. We structured the learning activities into three stages, as illustrated below. Our method guide learners to think more deeply about IoT products and their design decisions. The learning platform we developed is open source and available for the community.



Stages in the proposed crowdsourced peer learning activity for IoT



These series of screens demonstrate how a to crowdsource worker add a feature of water-resistant to given IOT device and provide video-based evidence

- **[Journal]** Ahmed Hussein, Mahmoud Barhamgi, Massimo Vecchio, Charith Perera, **Crowdsourced Peer Learning Activity for Internet of Things Education: A Case Study**, *IEEE Internet of Things Magazine (IOTM)*, Volume x, Issue x, 2020, Pages xx-xx (xx)
  PDF BIB CODE VIDEO VIDEO

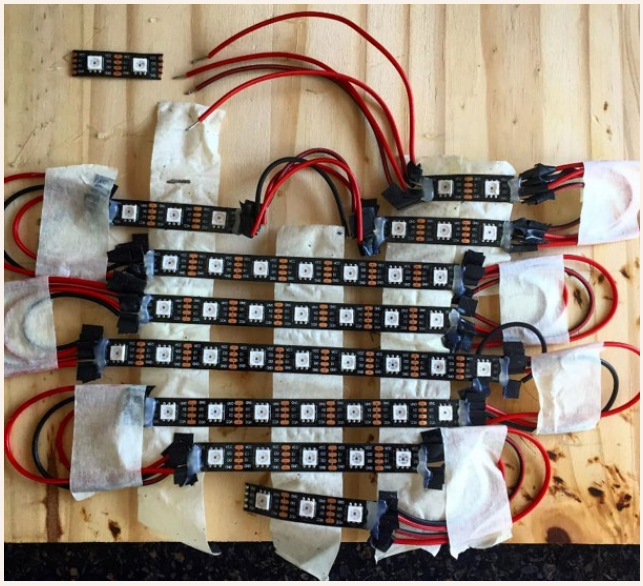
IoT Skullfort: Exploring the Impact of Internet-Connected Cosplay

BSc

Researcher: Karan Juj (BSc Student-2019)

In this project, we explored the potential impact of the Internet of Things (IoT) technology may have on the cosplay community. We developed a costume (an IoT Skullfort) and embedded IoT technology to enhance its capabilities and user interactions. Sensing technologies are widely used in many different wearable domains, including cosplay scenarios. However, in most of these scenarios, typical interaction pattern is that the costume responds to its environment or the player's behaviour (e.g., the colour of lights may get changed when the player moves hands). In contrast, our research focused on exploring scenarios where the audience (third party) get to manipulate the costume behaviour (e.g., the audience get to change the colour of the Skullfort using a mobile application). We believe such an audience influenced cosplay brings new opportunities for enhanced entertainment. However, it also creates significant challenges. By using the IoT Skullfort prototype as a concrete example, we conducted a focus group and extracted a few interesting views, including the following.

Health and Safety: It was highlighted, that if tailored, this technology could be utilised to mitigate specific disabilities. For example, an individual who has partial deafness could utilise a series of microphones scattered across a costume.
Inappropriate, abusive comments, and hate speech: If the LEDs were utilised as a matrix that allowed scrolling text, then allowing open access to the public could cause trouble. Experts agreed that the individuals wearing the device is just as liable for the content displayed, as those that wrote it. Meaning, they would be punished for any problematic content; as they facilitated the public distribution of the message.



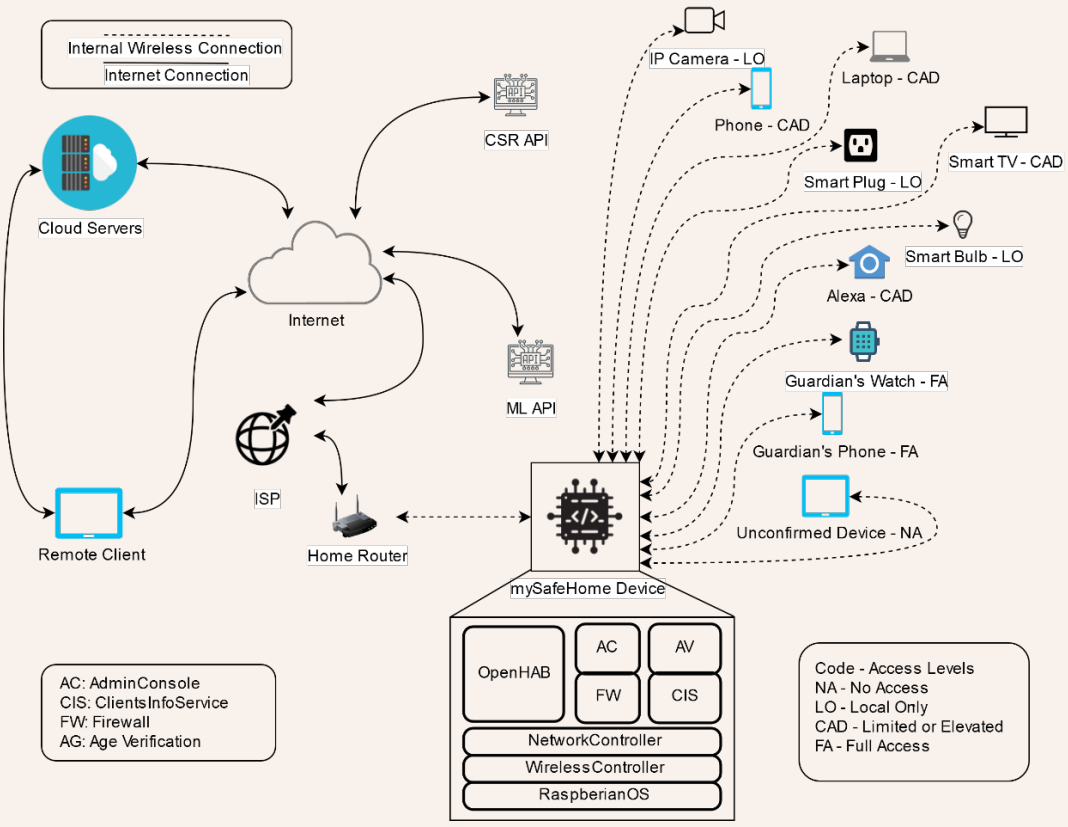
- [Poster] Rhys Beckett and Charith Perera, **IoT Skullfort: Exploring The Impact of Internet-Connected Cosplay**, *In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers (UbiComp/ISWC '19 Adjunct)*, ACM, New York, USA, 5-8.
  PDF BIB SOURCE CODE VIDEO VIDEO POSTER

Family Dynamics-based Access Control for the Internet of Things

MSc

Researcher: Yasar Majib (MSc Student-2019)

Today, children are increasingly connected to the Internet and consume content and services through various means. It has been a challenge for less tech-savvy parents to protect children from harmful content and services. Internet of Things (IoT) has made the situation much worse as IoT devices allow children to connect to the Internet in novel ways (e.g., connected refrigerators, TVs, and so on). In this work, we propose to utilise family dynamics to provide a more natural, and intuitive access control mechanism to protect children from harmful content and services. In our proposed approach, access control dynamically adapts based on the physical distance between family members. For example, a particular type of content can only be consumed, through TV, by children if the parents are in the same room (or hearing distance). This approach allows parents to assess a given content by themselves. This is a contrasting view to AI-based decision making where AI decide on behalf of the parents. We believe that parents are the best person to make the decision, given that they get the right opportunity. Our access control mechanism aims to guarantee that opportunity (i.e., block certain content, services, and devices when the parents are not in the vicinity). We developed a prototype using OpenHAB and several smart home devices to demonstrate the proposed approach. We also conducted a focus group to identify how family dynamics can be further used to support better security and safety for children. We believe that our approach also facilitates the creation of better relationships between family members.



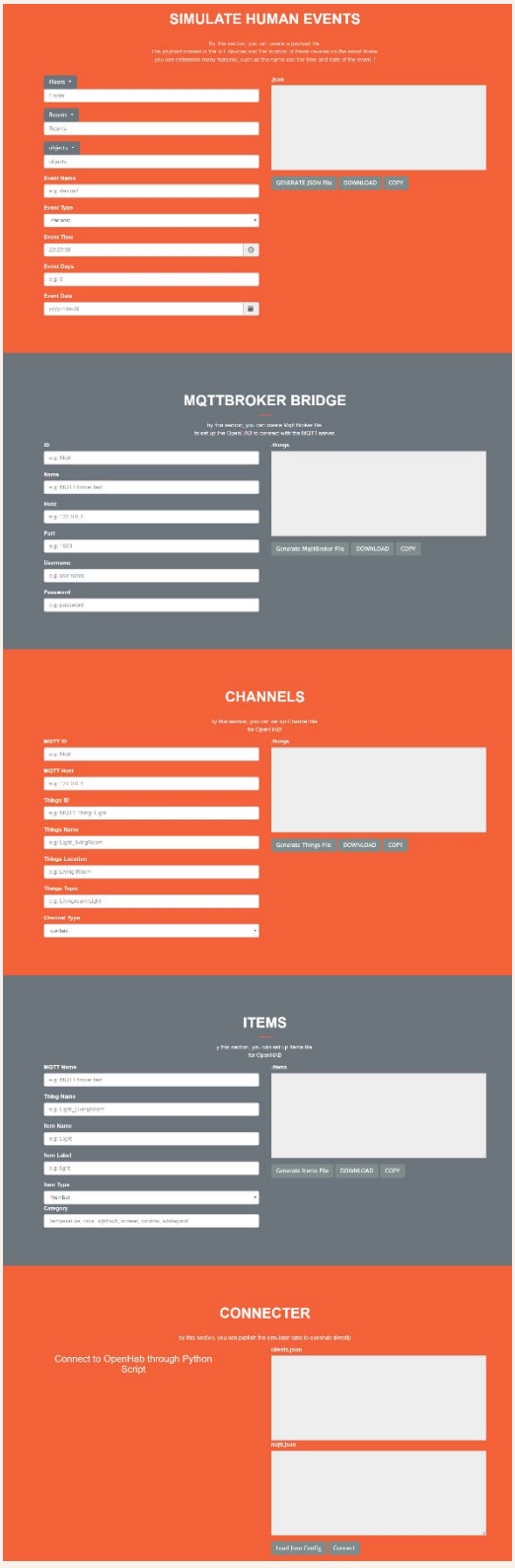
- [Conference] Yasar Majib, Charith Perera, **Context-Aware Family Dynamics based Internet of Things Access Control Towards Better Child Safety**, *IEEE 6th World Forum on Internet of Things (WF-IoT)*, New Oreleans, Louisiana, USA, April, 2020 PDF BIB CODE VIDEO

Smart Home Human Activity Simulation Tool for Research

MSc

Researcher: Asma Alotaibi (MSc Student-2019)

Over the last few years, many different Internet of Things devices has been made their way into the market. As a result, many smart home solutions have been introduced by different companies. However, at this point, most of the smart home solutions are engineering products built with limited attention to the end-user need. Many researchers are working towards developing more meaningful smart home solutions and looking at the problem from different perspectives such as human-computer interactions, edge computing, psychology. Another aspect is to explore how these smart home solutions could be useful for independent living, disable and vulnerable people. Further, these smart homes systems need to be privacy-aware and secure. These research activities, at some point, need some kind of human activity simulation tool.



Recognising this problem, this project developed a tool capable of simulating human activities in a smart home. A set of pre-created scenarios can be made through the simulator tool interface, which will then be published into OpenHAB interface. The OpenHAB platform is used to enable the researcher to display IoT devices of the smart home in its user interface and at the end, obtaining a synthetic dataset ready to research. This was done by setting up the tool with the GUI interface and writing python code to publish the data using the MQTT protocol.

A tool interface has been designed to help simulate various human events, enabling the creation of data to be played out so that research can be conducted. Furthermore, it is allowing the creation of multiple files. This will help to set-up devices on OpenHAB the same as with real devices. The goal is to create a simulation tool that allows researchers to create realistic synthetic smart home data sequences. Such data sequences could be used for research and evaluation purposes. Furthermore, it offers a list of smart sensors and devices that can be expanded to include future emerging technologies.

- **[Technical Report]** Asma Alotaibi, Charith Perera, **Smart Home Human Activity Simulation Tool for OpenHAB-based Research**, *Technical Report*, 2019 PDF BIB CODE VIDEO

gitlab.com/IOTGarage

bit.ly/2JMoSd

@IOTGarageNews

INTERNET OF THINGS
GARAGE
iotgarage.net