frontiers | Frontiers in The Internet of Things

TYPE Review
PUBLISHED 09 May 2024
DOI 10.3389/friot.2024.1336564

OPEN ACCESS

EDITED BY
Oktay Cetinkaya,
University of Oxford, United Kingdom

REVIEWED BY
Ellis Solaiman,
Newcastle University, United Kingdom
Muhammad Imran Tariq,
Superior University, Pakistan

*CORRESPONDENCE
Gideon Ogunniye,
✉ g.ogunniye@ucl.ac.uk

RECEIVED 10 November 2023
ACCEPTED 15 April 2024
PUBLISHED 09 May 2024

CITATION
Ogunniye G, Hana A and Watson J (2024), PETRAS: a socio-technical framework for Internet of Things research and development. *Front. Internet. Things* 3:1336564.
doi: 10.3389/friot.2024.1336564

PETRAS: a socio-technical framework for Internet of Things research and development

Gideon Ogunniye*, Amaya Hana and Jeremy Watson

Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, United Kingdom

This paper presents a case application of a socio-technical framework for Internet of Things (IoT) research and development in the United Kingdom. Applying a socio-technical system approach to IoT, this paper seeks to provide a clear understanding of the interplay between technical and non-technical aspects of IoT research and development. It describes the socio-technical requirements for IoT design and development and provides the current snapshot of research in the United Kingdom to meet these requirements. Finally, the paper provides useful information on how to conceptualize IoT research within human-centered contexts and a useful guide for centre design and evaluation to those developing new research centres or seeking to reinvigorate existing ones.

KEYWORDS

IoT, privacy, ethics, trust, reliability, acceptability, security, socio-technical theory

1 Introduction

The Internet of Things (IoT) involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making. It envisions the ubiquitous interconnection and cooperation of smart objects over the Internet infrastructure Ziegeldorf et al. (2014). Recently, the integration of IoT-based solutions has become a global trend for governments across the world. IoT devices are widely deployed for societally vital (critical infrastructure) services, such as waste management, traffic monitoring, finance and logistics support, and air quality management Mullagh et al. (2022); Davis et al. (2014). Governments and industries around the world are investing billions of dollars to develop IoT computing Shin (2014). Examples of such projects include the Internet of Things UK programme (IoTUK); the world's leading national IoT programme, United Kingdom's Future Internet Initiatives, China's National IoT plan by the Ministry of Industry and Information Technology, IoT cybersecurity labelling programme by the US government and Europe's Internet of Things policy, among others. In all these jurisdictions, IoT is increasingly considered a highly significant strategic-level infrastructure for economic growth.

However, the scale, heterogeneity, widespreadness and dynamism of the IoT ecosystem introduce some privacy, ethics, trust, reliability, acceptability, and security issues for users and those affected by the ecosystem Kokciyan and Yolum (2020). This is because IoT systems are highly dependent on data collection and sharing, constant connectivity, and remote control ability. The importance of the IoT is largely achieved through connected data, allowing objects or things to be readable, recognisable, locatable, addressable, and/or controllable over a network. Although this presents significant opportunities, the main areas of public concern about the technology include the potential impact of information flow on user privacy Ogunniye and Kokciyan (2023a), protection of data assets and the increased capabilities of IoT devices against unauthorised access and manipulations Ghafir et al. (2018), how to minimise security and privacy risks to make the technology more acceptable, how to build public trust in the technology Mullagh et al. (2022), and ethical problems such as profitability *versus* ethics, business *versus* politics Nehme et al. (2022), among others.

As Winter (2013) points out, the discussion of the IoT so far has focused primarily on the technical aspects of design, such as connectivity, interoperability, scalability, and real-time data processing, among others. Most studies propose technical measures to mitigate digital harms, while fewer consider social prevention mechanisms Mullagh et al. (2022). With the increasing number of IoT devices being deployed across various industries and public spaces, it is crucial to understand the immense repercussions of the social dynamics and organisational, policy, management, and most importantly inherent user issues with the deployment. It is vital that an adequate governance structure and policies are designed and implemented to enhance trust, protect privacy, and user security Mullagh et al. (2022). Recently, there has been growing recognition that technical solutions alone cannot adequately address these public concerns systems Cath (2018); Nicolescu et al. (2018); Ogunniye and Kokciyan (2023a); Buil-Gil et al. (2023). The technical, social, cultural, and behavioural aspects of how we design, develop, manage, and evolve the IoT will be critical to its success Shin (2014).

In this paper, we argue that IoT is a social-technical ensemble that contains social (human-related) and technical (non-human) aspects which will interact to pursue a common goal, and therefore a socio-technical approach is crucial to uncover ongoing underlying issues with IoT and address them. To this end, we first describe the PETRAS framework for IoT research and development and case studies of its applications in real-world settings. PETRAS framework is a comprehensive framework for investigating social and technical issues related to the cybersecurity of devices, systems, and IoT networks. In each of the case studies presented, we identify the potential and importance of aligning the technical and social aspects of IoT. We use the case studies to illustrate the importance of extending socio-technical thinking to emerging technologies. We then outline socio-technical requirements for IoT design and development.

This paper attempts to identify socio-technical issues of IoT and how a socio-technical framework that finds an optimal point among appropriate technical, social and regulatory issues, industry, and user dynamics can be developed to address the issues. To this end, we consider the following research questions in this paper.

1. How can IoT research be designed as a socio-technical theory?
2. What are the socio-technical requirements for the privacy, ethics, trust, reliability, acceptability, and security of IoT?

To address these questions, this paper presents an analysis of the key socio-technical requirements, concepts and approaches, issues (social, technical, economic, and policy), best practices and tools for the deployment of IoT.

1.1 Contributions

In this paper, our contributions are as follows.

1. We describe a socio-technical framework for IoT research and we show its applicability using case studies.
2. We highlight the socio-technical requirements for IoT deployment and we present case studies on how they can be captured to guide researchers working in the area.

2 Background and literature review

2.1 The IoT ecosystem

IoT is one of the emerging topics in recent time in terms of technical, social, and financial consequences. It is an umbrella term that reflects an evolution of technology towards the proliferation of cheap “embedded systems” and “cyber-physical systems (CPS)” connected to a network. Embedded systems are information processing systems that are embedded in an encapsulating product Marwedel (2021). CPSs are spatially distributed, time sensitive, and multiscale networked embedded systems that connect the physical world to the cyber world through sensors and actuators Esterle and Grosu (2016). Nevertheless, computational systems interacting with the physical world are not new and have long been designed to interact with the real world to support humans in achieving their goals. The term IoT is used across a wide spectrum of applications, from the smallest connected sensors and ultra-low power hardware design to large-scale cloud-based solutions Ali et al. (2021). It is considered a disruptive innovation in the sense that it has the potential to fundamentally change societal and business processes within and between sectors WEF (2015).

The diversity of IoT application domains is wide: connected homes, connected public places, logistics and transportation, smart grids, smart wearables, and connected intelligent medical devices, among others. In these domains, IoT offers a new platform for services and decision-making and it has a huge impact on social interactions, business, and industrial activities. The IoT ecosystem is complex and includes developers and providers of hardware, software platform developers (e.g., data platform developers and security platform developers), system integrators, cloud service providers, big data companies and users Lee (2019). Despite its importance, there are socio-technical requirements that need to be considered to engender public trust. For example, most IoT users do not understand what kind of information is being collected about them or their environment Subahi and Theodorakopoulos (2019). Beyond disclosing and sharing private information; IoT devices can perform actions in the user’s environment that impact and potentially disturb the user while invading their privacy Ogunniye and Kokciyan (2023b); Schaub et al. (2015). For example, malicious entities can exploit the security and privacy vulnerabilities of IoT systems to gain unauthorised access to sensitive data and information about organisations, financial transactions, marketing insights, individuals, and product development.

The design of safe and secure embedded/cyber-physical systems and IoT will require interdisciplinary knowledge and skills beyond the traditional boundaries of disciplines. It is very difficult to obtain an overview of such broad knowledge due to the wide range of relevant areas. Therefore, a cross-disciplinary approach that considers the voices of all those involved in the design, development, and use of IoT technology is important Buil-Gil et al. (2023). For example, according to Weir et al. (2023), security and privacy are essential software properties and are critical in various applications. However, many cybersecurity practices may not align with modern agile development approaches and to systems involving many Internet-accessible components, such as Health Internet of Things (HIoT) systems. Additionally, the cost and lack of availability of cybersecurity professionals make it unrealistic to have dedicated cybersecurity support in small companies.

According to Tyler et al. (2018), the key considerations (technical and regulatory) for IoT systems developers are grouped into three interdependent themes: harnessing economic values, security and risk management, and adoption and implementation. These issues can be further broken down into social and technical requirements such as; what are the applications and what system architecture will they need, what communication protocols do systems need, what security is needed for the hardware and software, have issues of ethics, trust, acceptability and reliability been addressed, what are the legal requirements around data protection and security and has the impact on end-users and change management aspects been addressed, among others.

2.2 Socio-technical systems theory

Socio-technical systems are social and technical aspects involved in goal-directed behaviour Sony and Naik (2020). They consist of social subsystems (of people and society); comprising social structures, business opportunities, and legal, as well as social expectations, behaviours requirements, etc., and technical subsystems (of machines and technology); including artefacts, processes, tasks, procedures and physical environments that contribute directly or through other components to a common system goal. According to Shin and Jung (2012), the investigation of systems and applications has traditionally focused on technical aspects. This traditional approach is rather narrow and studies should highlight the interaction between technology itself, the people who use it, and the organisational and environmental context in which it is embedded Shin (2014).

Socio-technical systems (STS) theory is certain specific methods of joint optimisation to design systems that can work better with social and environmental complexity and dynamism Sony and Naik (2020). According to STS theory, although technical and social subsystems are closely interrelated, they are distinct from each other. While technical subsystems aim to achieve specified performance parameters, social subsystems consist of human beings with unpredictable behaviour Walker et al. (2008). For example, when it comes to the cybersecurity of IoT systems, studies have shown that technical solutions often fail for social and behavioural reasons Krasovec et al. (2020); Subahi and Theodorakopoulos (2019); Williams et al. (2017) Examples of this include lack of awareness, weak passwords, undeveloped cybersecurity "culture" within organisations, and splits in responsibility. By combining social and technical expertise in the co-creation of new system approaches, tools, and techniques, both social and technical hurdles are overcome simultaneously.

2.3 PETRAS National Centre of Excellence for IoT Systems Cybersecurity

A United Kingdom government Blackett Review on the "Internet of Things: Making the most of the second digital revolution" was published in 2014 Government (2014). Its recommendations identified socio-technical challenges concerning privacy, trust, security, etc. that needed to be addressed to release market opportunity for IoT and that there was a requirement for research and technology demonstration across application sectors.

2.3.1 PETRAS Hub (2016–2019)

Building on the Blackett Review and its recommendations for action, the PETRAS research hub (Hub) was established in 2016 and was jointly funded by the United Kingdom EPSRC[1] and User Partners, exploring a range of issues in the cybersecurity of IoT research domain. The Hub (as shown in Figure 1) was the predecessor of the PETRAS Centre which operated between 2016 and 2019. It was a consortium led by University College London, with Imperial College London, University of Oxford, Warwick University and Lancaster University. It brings together a large community with 12 United Kingdom academic institutions, 51 projects and 6 medium-scale demonstrators and more than 110 User Partners from various industrial sectors, government agencies and NGOs, providing a collaborative platform to conduct world-class impact research and knowledge development in the IoT security domain involving collaboration between technical and social science experts. The Hub's core programme aims to balance needs for sustained development, practical experimentation and evaluation, and disruptive research in five thematic areas (including privacy and trust, safety and security, standards, governance and policy, adoption and acceptability, and harnessing economic value), with the agility required by innovation and co-creation with users and stakeholders in a dynamically evolving environment such as the IoT.

2.3.2 PETRAS Centre (2019–2023)

In 2019, the PETRAS National Centre of IoT Systems Cybersecurity (Centre) was created and funded by the collaboration between EPSRC and Innovate United Kingdom under the Strategic Priorities Fund (SDF). The Centre is a consortium of 24 United Kingdom research institutions, over 120 User Partners, and 63 projects, and the world's largest socio-technical research centre focused on the future implementation of the IoT. As part of United Kingdom Research and Innovation (UKRI)'s Security of Digital Technologies at the Periphery

[1] Engineering and Physical Sciences Research Council.

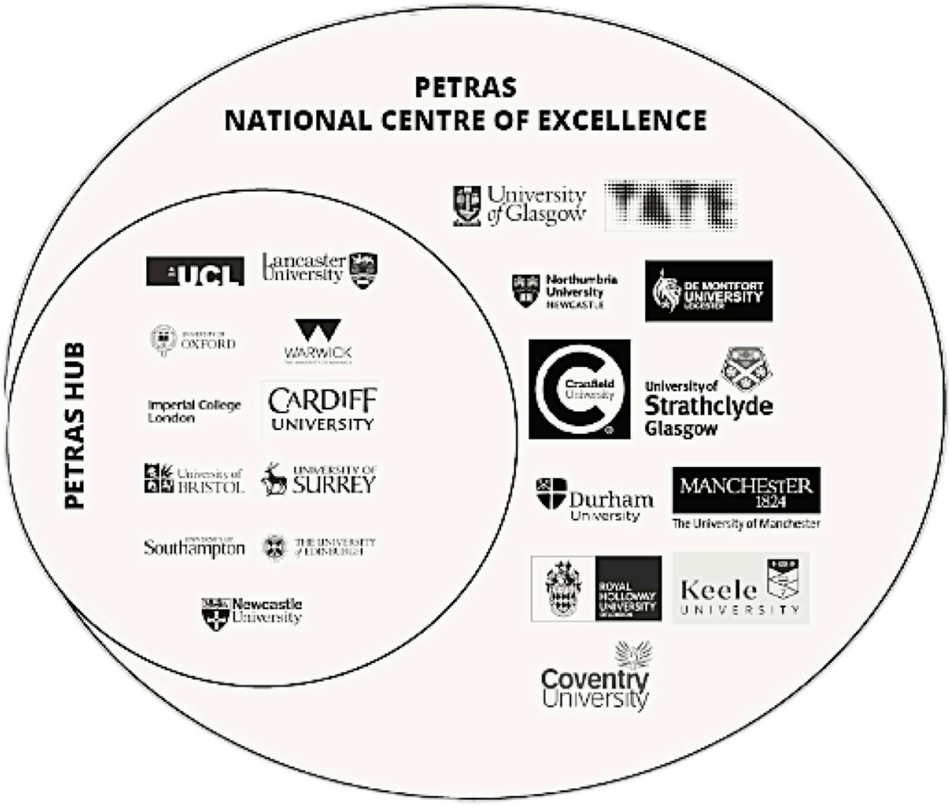

FIGURE 1
PETRAS Hub and Centre.

(SDTaP) programme, PETRAS runs open, national-level funding calls that allow it to conduct cutting-edge basic and applied research. It also supports the early adoption of new technologies through close work with other members of the Security of Digital Technologies at the Periphery (SDTaP) programme, such as Innovate United Kingdom, supporting demonstrations of new technology and commercialisation processes[2].

PETRAS's key organisation design objective is to create an inclusive research centre that can attract and closely connect experts and organisations, together forming a strategic national research capability in the cybersecurity of devices and networks at the edge of the internet. A vital element is to design in potent synergies and complementarities between collaborators as well as a scaffolding for catalysing more and communicating them going forward.

2.3.3 PETRAS framework

It is noteworthy that the transformative potential of a research centre maybe circumscribed by certain structural limitations Coen et al. (2010). Therefore, PETRAS Centre operates a framework (hereafter referred to as PETRAS framework) for collaboration between academia, industry and government to deliver research that spans the physical and behavioural sciences. The framework integrates the tangible and intangible structures that interactively underline the research centre functioning. It considers the issues of Privacy, Ethics, Trust, Reliability, Accessibility and Security as they relate to IoT devices, systems and networks. This analytical framework helps to investigate how to practically mitigate potential threats while taking advantage of the huge benefits that the application of IoT, AI and Machine Learning (ML) technologies can bring[3].

2.4 An example of a socio-technical framework

We follow the socio-technical framework by Davis et al. (2014) as shown in Figure 2 to define PETRAS socio-technical framework. Davis et al. (2014) framework is based on an initial schema by Leavitt (1965). Leavitt (1965) framework was developed through his experience of undertaking organisational change and focused on the relationships between people, tasks, structures and technologies. Davis et al. (2014) extended Leavitt (1965) framework to represent

[2] https://petras-iot.org/update/petras-awards-3-6-m-to-tackle-issues-of-cybersecurity-privacy-and-trust/

[3] https://petras-iot.org/about-us/

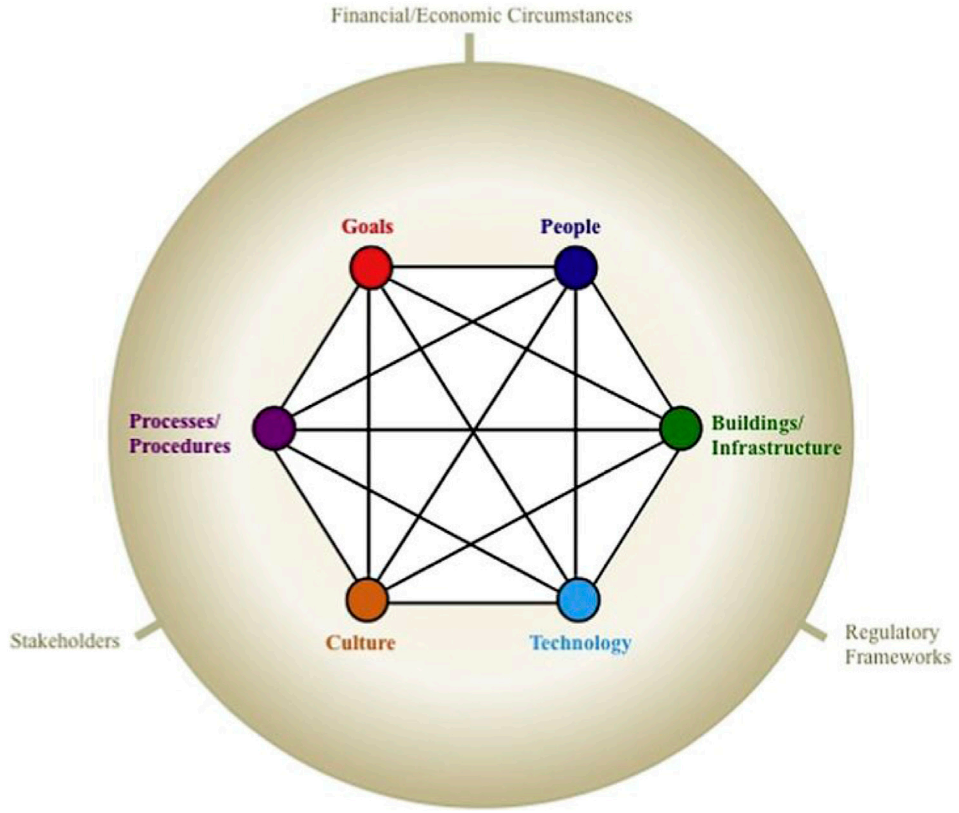

FIGURE 2
A socio-technical system adapted from Davis et al. (2014).

organisational systems using six interrelated elements, embedded within an external environment, as shown in Figure2.

Davis et al. (2014) framework defines a work system that usually has a set of *goals and metrics*, *people* (with varying attitudes and skills), using a range of *technologies and tools*, working within a physical *infrastructure*, operating with a set of *cultural assumptions* and using a set of *processes* and working practices. The system is within a wider context, incorporating a *regulatory framework*, sets of *stakeholders* (including customers), and an *economic/financial* environment. The importance of these external factors vary with each system. For example, a particular regulatory framework may well influence the goals pursued by an organisation and the metrics in use.

3 Method

The foundation of this research study is a literature review of articles from the PETRAS publication database[4] on various themes within IoT research and development and socio-technical systems. In particular, we use content analysis to explore relevant themes within the PETRAS framework. Archival materials, such as industry reports, government publications, technical reports, e-mail exchanges within PETRAS community (government officials, regulators, industry players, and researchers), project proposals, guidelines, policy briefings and any materials related to planning and development of PETRAS research, were collected and analysed. Archival materials were useful in obtaining factual data, such as the research agenda of various streams within PETRAS Centre. Such archival data complemented missing data from the peer-reviewed articles reviewed.

4 Description of PETRAS framework

In this section, we first describe the elements of the PETRAS framework and define their mapping to the elements of the Davis et al. (2014) framework. We then describe how the framework is deployed in some PETRAS projects and provide an overview of the major steps involved in designing, analysing and understanding IoT systems. We outline the elements of the PETRAS framework below and their integration with the environment existing around the framework such as stakeholders and regulatory frameworks. We note that there is no particular order to this framework.

We follow the concept of socio-technical systems Davis et al. (2014); Shin (2014); Sony and Naik (2020) to classify the PETRAS framework into three dimensions, namely, *technical subsystem*, *social subsystem* and *external environment*. The technical

[4] https://petras-iot.org/petraspublications/

subsystem focuses on the key technical challenges related to IoT and edge devices with AI and ML capabilities, such as cybersecurity challenges, including networks, and applications, that have been addressed within the PETRAS framework. It also involves the *goals* of the Centre and the processes and procedures put in place to carry them out. The social subsystem highlights the structure of the Centre (e.g., administrative and governing structures) and the Centre's collaborative approach to knowledge exchange between researchers and research project partners. The external environment highlights the Centre's crucial role in fostering public understanding, engaging with stakeholders within the IoT ecosystem and contributing to policy and regulatory frameworks.

4.1 Technical subsystem

As rapidly developing digital technologies, together with social and business trends, are providing huge opportunities for innovation in product and service markets, and also in government processes, the Centre aims to build the national capacity needed to create a comprehensive and systematic understanding of the opportunities and challenges that arise when edge computing nodes are deployed, and when AI and ML technologies are migrated to the periphery of the internet and into local IoT networks.

4.1.1 Technology

The Centre is interested in how the interactions between IoT, Artificial Intelligence (AI) and Machine Learning (ML) produced cybersecurity challenges that need to be addressed if society and the economy are to harness their full potential benefits. According to the IBM Institute for Business Value, the full potential of IoT can only be realised with the introduction of AI Tzafestas (2018). To improve the use of IoT, artificial intelligence (AI) algorithms and techniques such as machine learning, deep learning, and artificial neural networks are used to analyse and learn from the collected data to create public services and values Kankanhalli et al. (2019); Jobin et al. (2019). The convergence of AI, IoT and embedded systems as the next disruptive technology is inevitable Nehme et al. (2022). For example, the combination of AI and IoT technology into full-smart autonomous vehicles (AV) has provided several benefits in real time, such as increased safety, fuel economy, and safer regulations Baliyan et al. (2022).

In line with the fact that the convergence of IoT and AI will lead to the emergence of new economic models, several PETRAS projects have modelled the connections and interdependencies between these technologies. In this regard, these projects have focused on two dimensions.

1. AI-based anomaly detection in IoT systems. Several PETRAS projects have modelled AI-based anomaly detection models for consumer and industrial IoT. For example, *ELLIOT* project[5] developed an AI-based early anomaly detection model. This model can be applied to industrial processes to detect early signs of cyber-attacks and thereby prevent catastrophic consequences such as exploitation of security and privacy vulnerabilities in IoT systems to gain access to the sensitive data of their users and violate their privacy. The PSWaRMS project[6] developed an AI-based randomised target defence approach which could reduce the risk of severe consequences of cyber-attacks aimed at IoT assets.
2. AI-based collection and analysis of data for IoT systems. Several PETRAS project investigated how AI techniques can be used for ubiquitous data collection or tracking in IoT devices. For example, in full-smart autonomous vehicle technology, ML algorithms are used to develop behaviour patterns for driver profiles and also to provide vehicle owners with the right application for what they want in the vehicle Baliyan et al. (2022). The PubVIA project[7] investigated how data-driven innovation raises urgent and difficult challenges including cybersecurity issues, risk of digital harms, and questions of ethics, trust, and understanding. The project developed guidelines for intelligible, ethical and responsible AI and IoT. The PPIEM project[8] implemented ML techniques to evaluate the accuracy of the occupancy estimate and future CO_2 predictions in smart buildings to ensure safety, as well as to evaluate the impact of different privacy settings.

However, it must be noted that the convergence of these technologies also introduces new privacy Schaub et al. (2015), security Karale (2021), and ethical Nehme et al. (2022) issues. For example, threat actors may exploit AI to identify vulnerabilities and attack surfaces in IoT systems and exploit them. The Centre combines social and technical expertise to co-create new solutions, approaches, tools, and techniques to address both technical and social challenges with IoT simultaneously.

4.1.2 Goals

The key objectives of the Centre, guided by the PETRAS Framework are as follows:

1. Provide strategic advice and policy insight, becoming the go-to-resource on Securing Digital Technologies at the Peripheral (SDTaP) issues for the public and private sector. The SDTaP programme is a government initiative in the United Kingdom to support the development of a safe and secure IoT[9].

[5] https://petras-iot.org/project/early-anomaly-detection-for-securing-iot-in-industrial-automation-elliott/

[6] https://petras-iot.org/project/processes-for-securing-for-water-resource-management-systems-pswarms/

[7] https://petras-iot.org/project/building-public-value-via-intelligible-ai-pubvia/

[8] https://petras-iot.org/project/privacy-preserving-indoor-environment-monitoring-ppiem/

[9] https://ukri.org/what-we-do/our-main-funds-and-areas-of-support/browse-our-areas-of-investment-and-support/ensuring-the-security-of-digital-technologies-at-the-periphery-sdtap/

2. Increase the early adoption of new methods and technologies by the Centre's industry, service, and government User Partners.
3. Functionally improve the capacity of government to rise to the challenge of the "arms race" of ever more complex socio-technical systems and threats.

To achieve these objectives, the Centre operates in responsive ("pull") and proactive ("push") modes, recognising the value of fostering a culture of research excellence, co-creating immediately useable research with user partners while maintaining the capacity and appetite for fundamental challenges and identifying emerging issues and opportunities not yet apparent to partners.

4.1.3 Processes and procedures

The Centre runs open, Strategic Research Fund (SRF1and2) calls for research projects. The *key requirements of the funding calls* are that i) at least one (new or existing) user partner must be associated with each of the bids, prioritising connections between research projects and user partners and relevant stakeholders, and ii) each project must be associated with at least one challenge and apply its findings in at least one sector.

The Centre has built-in capacity for embedded consolidation and foresight activity in its *Synthesis Fellows* (SF) programme, to synthesise the diverse elements of the PETRAS research base to construct new understanding, ideas and insights. The aim of this synthesis activity is to increase the generability and applicability of research findings, thereby ensuring that they have relevance and impact in society and the economy–particularly, at national, regional or sectoral level.

To achieve its key objectives, the Centre operates a strategic engagement plan that focuses on placing partnerships at the centre of its research agenda, a communication plan (through its *communication team*), that focuses on supporting both the responsive and proactive mode of operation and an impact strategy (managed by its *impact leads*) that focuses on knowledge transfer between funded projects and their user partners. For example, the Centre gains insights into user needs from IUK demonstrators and commercialisation programmes, enabling it to align its themes and research agendas to user needs.

4.1.4 Infrastructure

The Centre runs governance and management models, which have demonstrated the ability to coordinate and convene collaboration across 24 universities and more than 120 industrial and government user partners, and inclusivity through open research calls for new and existing academic partners. In establishing evaluation tools, the Centre draws on ResearchFish[10] submissions at project and Centre level as a key source of evidence to evaluate the levels of activity and outcomes across projects, as well as inform future funding applications. ResearchFish is an intelligent technology to track the impact of research and evidence. In addition, the Centre runs a research knowledge base, constituting channels and conduits for knowledge transfer across United Kingdom industry sectors and government departments, enhancing knowledge diffusion, and contributing to the evolution of IoT technology. The knowledge base contains academic peer reviewed publications and grey literature for non-academic audiences, including landscape reviews, policy briefings, white papers and tools for industry and local government.

4.2 Social subsystem

The Centre considers the challenges with IoT as socio-technical. Therefore, it is designed to accommodate transdisciplinary research. This involves physical and behavioural sciences research to investigate the privacy and security risks with IoT, identify gaps in regulations, standards, and policies, and design solutions to address them. The Centre brings together experts from business schools, policy and governance programmes, and computer science to research new markets models for raw and inferenced IoT data that may be mediated through technologies [e.g., Distributed Ledger Technologies (DLTs)], standards, social incentive schemes and other mechanisms. Furthermore, the Centre puts a strong emphasis on research, development, innovation and demonstration in the wild through the use of testbeds and at-scale co-design with users. These attributes fulfil the objectives set out by the aforementioned PETRAS Framework to provide strategic advice formulated through collaboration with academia, government, user partners and industry, while encouraging the uptake of cutting edge technologies to identify and address emerging challenges.

4.2.1 People

The *people* element of the PETRAS framework is composed of the *governing* (governing board, research excellence board and user research board), and *administrative* (management team and ethics review sub-group) components, working in synergy with the operational and research (operations group) components of the Centre, as depicted in Figure 3. Note that we do not describe in detail the composition of each of the elements of the PETRAS framework, which is not our focus here. However, we provide a high-level overview of their strategic functions.

The *management team* provides links and integration between academic partners and between them and users, including government and industry. First, it provides a single point of contact in its domains of expertise and supports the communication of a coherent voice from the research base, managing the interpretation of the views to provide a coherent opinion to stakeholders. Second, it works in partnership with academic researchers within the Centre to ensure that the research outputs are synthesised and communicated in a way that is translatable to industry, government, and broader non-technical audiences. The *governing board* is composed of three major sub-groups; the *industrial advisory board*, which includes the main user partners from the private sector with significant project involvement in PETRAS, public sector (e.g., government) partners with project involvement and/or strategic interest in research outcomes and deliverables; *user research board* representing the funder (UKRI), main central funding agencies (Engineering and Physical Sciences Research Council–EPSRC,

[10] https://researchfish.com/

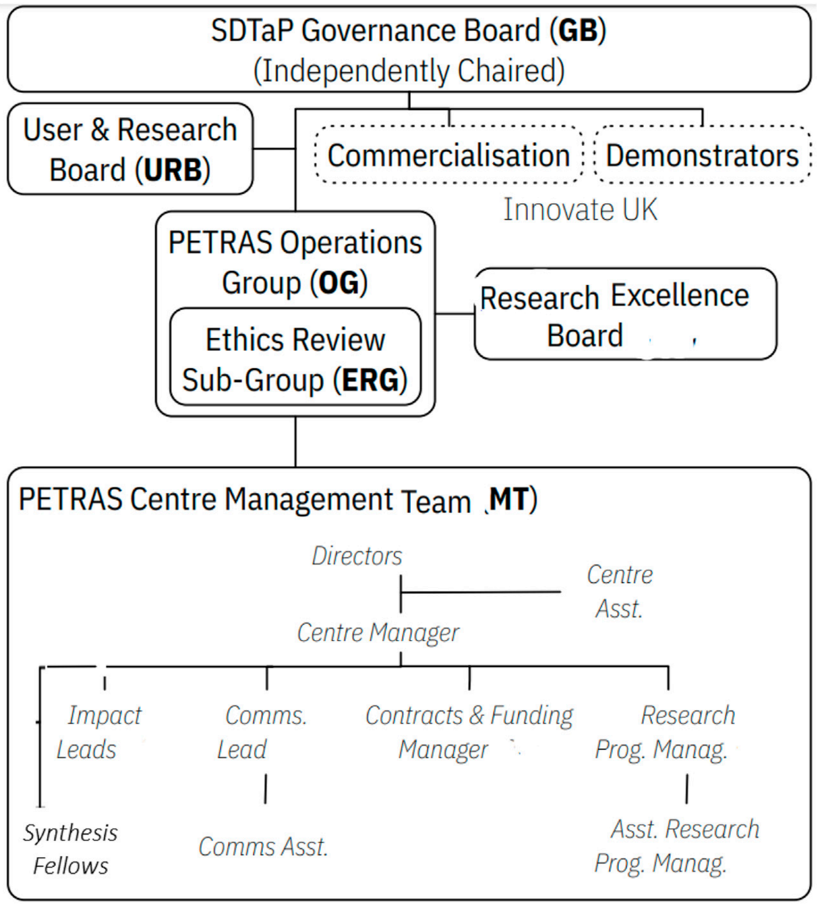
SDTaP Governance Board (GB)
(Independently Chaired)
User & Research Board (URB)
Commercialisation
Demonstrators
Innovate UK
PETRAS Operations Group (OG)
Ethics Review Sub-Group (ERG)
Research Excellence Board
PETRAS Centre Management Team MT)
Directors
Centre Asst.
Centre Manager
Impact Leads
Comms. Lead
Contracts & Funding Manager
Research Prog. Manag.
Synthesis Fellows
Comms Asst.
Asst. Research Prog. Manag.

FIGURE 3
PETRAS Centre structure.

and Innovate United Kingdom) and *research excellence board*, which includes the principal operational members of the PETRAS management team. The governing board is responsible for PETRAS, Innovate United Kingdom (IUK) Demonstrator programme and the IUK Commercialisation (start-up support) initiative. It oversees and advises on research programme portfolio content and management, ensuring the research programme activities remain aligned with the expectations of both funding bodies and end-users. It receives reports from the operations group and provides high-level steering advice to it. The *operations group* comprise the Principal Investigators (PIs), Co-Investigators (CIs) and PETRAS research partners brought in as a result of open calls. It is the team responsible for ensuring that the Centre research programmes operate as planned and are accountable to the governing board. The *ethics review subgroup*, recruited from the operations group, is responsible for maintaining a record of ethics review submissions and outcomes carried out according to the challenging issues of the host and making recommendations to the governing board.

4.2.2 Cultures

The Centre has a culture of agility and collaboration across research activities to maximise the value of responsive operation. In relation to the proactive ("push") mode, the Centre generates significant academic impact through publications in world-leading peer-reviewed journals and conferences, with over 467 peer-reviewed articles in its publication database, which is also complemented by a strategic approach to public communications.

The Centre Management also supports researchers by ensuring that the Centre is well represented externally, through the media, presentations, annual conferences, etc., and with key audiences, including governmental and regulatory bodies; research and funding councils; industry; the charitable and civil society sector; learned societies and professional bodies.

4.3 External environment

The Centre, through its Framework, mobilised cross-disciplinary expertise in IoT and edge technologies to contribute to public understanding of the emerging challenges and solutions and how a large multi-university team can work effectively together, and with user partners from public and private sectors. The Centre's research outputs feed into its internal research knowledge base, which could be drawn upon, for example, in developing policy-relevant evidence. PETRAS framework provides the structure to articulate these outputs and make them applicable to the external environment.

4.3.1 Stakeholders engagement

In addition to the participation of the PETRAS Centre frequently in conferences and workshops to widely disseminate its research, and raise the profile of the Centre itself and its outputs, the Centre also engages with key research user partners (industry and public sector) to advance particular research areas.

PETRAS Centre projects and engagements span six industry sectors including; ambient environments (25%), supply chains and control systems (19%), agritech (3%), health and wellbeing (13%), infrastructure (29%) and transport and mobility (11%) and lenses including; law and economics at the edge (33%), building public value at the edge (15%), securing the edge (30%) and useful and useable decentralisation (22%). Sectors and lenses help to define research challenges in a real-world context. Lenses are research challenge domains. Sectors have specific application-focused contexts in terms of technology, regulation, economics, interventions, and innovation. Lenses and sectors are points of contact for accessing the Centre's programmes and expertise, as well as special interest groups. The projects' investigators and post-doctoral research associates (PDRAs) resource provides instances linking the four challenge-based lenses to the six application-focused sectors.

The Centre hosts a series of industry-specific workshops covering seven industry sectors in the United Kingdom, involving academia, industry, and government partners to investigate the challenges associated with the implementation and adoption of IoT technology. This workshop series aims to identify emerging cybersecurity challenges of IoT, explore future research priorities, and provide strategic advice and policy insights for the public and private sectors to address the potential implications and challenges for the adoption and use of IoT. For example, the PETRAS synthesis report on the future challenges of IoT cybersecurity in the United Kingdom industry sectors brings together inputs from academics, industry representatives, and representatives of public bodies on two themes: (i) the challenges to the integration of IoT-based solutions in the United Kingdom industry sectors and (ii) how academic-industrial research collaboration can help in addressing the challenges Ogunniye (2023).

The Centre also organises PETRAS Community Development events to provide opportunities for the wider PETRAS community to network and discover new research areas. These Community Development sessions are monthly events in which the wider PETRAS community can present their work, discuss topics of interest, and join in discussion with both the PETRAS and non-PETRAS network. The topics of discussion focus on particular themes, topics or industries stemming from PETRAS' lenses and sectors.

4.3.2 Influencing regulatory frameworks

The Centre works closely with multiple policy communities, including government policymakers (national and local), innovators, industry, academia, and the public, to address key policy issues related to cybersecurity of the Internet of Things. For example, the *PETRAS United Kingdom Code of Practice for Consumer IoT Security: where we are and what next* Burton et al. (2021) was highlighted in a parliamentary debate on an amendment to strengthen cybersecurity in children's products in the Product Security and Telecommunications Infrastructure Bill[11].

4.4 Case studies: examples of using participatory methods to engage with a variety of stakeholders in IoT research

In this section, we describe a PETRAS project to illustrate the technical and social subsystems and the external environment of PETRAS framework.

4.4.1 PETRAS project: Participatory policies for IoT (at the edge) ethics (P-PITEE)

When IoT sensors are deployed in public spaces, the technology might not be visible at first sight to the local residents and community groups. Therefore, local governments must account for their practical, technical, and ethical implications. In this regard, the P-PITEE project[12] used design methods to develop new policies for transparent and ethical deployment of secure IoT sensors in public spaces. Through a partnership with a local council, the project developed policy and guidance tools relating to the use of secure IoT sensors in public spaces. The policy and guidance tools cover the collection, use and sharing of data, considerations of data transfer *versus* edge processing, cybersecurity questions related to data storage and sharing, and how all these concerns can impact privacy.

4.4.2 Technical subsystem

4.4.2.1 Technology

The project is interested in how to design and develop a new, robust policy for ethical use of IoT data in United Kingdom cities, and the ethical management and cybersecurity implications of public space IoT and associated data, and a fully implemented IoT Transparency Guidelines tool which can be used by organisations who are considering IoT deployments and wish to consider the transparency aspects and ethical data use.

4.4.2.2 Goals

The project has three key objectives.

- Understanding the ethical and cybersecurity implications of public space IoT (and edge technology) deployments.
- Using design methods to develop effective local policies for the governance of city-based IoT deployments and the resulting data.
- Developing the existing transparency prototype into a fully developed tool which will support organisations in their assessment of system cybersecurity, transparency, and ethical practices.

[11] https://bills.parliament.uk/bills/3069

[12] https://petras-iot.org/project/participatory-policies-for-iot-at-the-edge-ethics-p-pitee/

4.4.2.3 Processes and procedures

In addition to user studies and a series of virtual and face-to-face workshops conducted, the project developed a novel walking workshop approach "Taking IoT for a walk" to explore and interact with a range of speculative and real IoT and edge computing deployments. The first walk was conducted in Lancaster, United Kingdom as part of the United Kingdom Economic and Social Research Council (ESRC)'s Festival of Social Sciences. Members of the public were guided on a *walkshop* around Lancaster, where they encountered real and fictional instances of IoT deployment, discussing the benefits, risks, and language. The aim of the walking workshop was to gather understandings of how experts perceive IoT and Edge deployments in public spaces, which will help to inform the policies to be developed in collaboration with the district council. This *walkshop* method received EPSRC Telling Tales of Engagement funding to deliver similar events in several United Kingdom cities including Leeds, East Riding, Dorset and the London Borough of Hounslow. The different levels of technical maturity and live projects within these local authorities further informed the consultation tool developed and the design of the method.

4.4.2.4 Infrastructure

The project launched a new interactive tool called *TrustLens* aiming to help organisations use technology in public spaces. The tool is interactive and can be used in a variety of formats, the primary being a downloadable MS Powerpoint Presentation. A facilitator can download the workshop materials from the project website, which guides them through the process of using the tool Mullagh et al. (2022).

4.4.3 Social subsystem

4.4.3.1 People

The *people* component involves project members of Lancaster University and the University of Aberdeen and Lancaster City Council as user partner. This component also includes workshop participants from the United Kingdom Department of Digital, Culture, Media and Sport (DCMS) Connected Places team, and members of TrustLens project.

4.4.4 External environment

This project demonstrated how different stakeholders are engaged in the investigation of ethical and cybersecurity implications of public space IoT and the co-creation of policy guidelines and tools to address them. Importantly, the project considered IoT as a social-technical ensemble involving social (human-related) and technical (non-human) aspects, interacting towards a common goal. It is important to note that in addition to modelling technical requirements for the privacy and cybersecurity of public space IoT, the project models different social requirements such as user contexts, perspectives, preferences and expectations which are crucial requrements for the deployment of public space IoT. This involves modelling of communication between different stakeholders to resolve conflict of opinion and elicit requirements for policy guidelines and tools.

5 Socio-technical requirements for IoT

In this section, we present research streams that addresses the key areas of research for PETRAS as a whole, showing the interplay between technology and social structures, industry and policy with respect to some of the socio-technical requirements for IoT. Note that the research streams and projects we have opted to include in this section encapsulate the core themes that were prevalent throughout PETRAS Hub and Centre phases. The overarching themes, also the PETRAS acronym, are Privacy, Ethics, Trust, Reliability, Acceptability and Security.

5.1 Adoption and acceptability

The key objective of PETRAS research stream on adoption and acceptability of IoT systems is to contextualise the factors that shape the adoption and acceptability of IoT now and in the foreseeable future. According to Baig et al. (2019), many factors affect the level of acceptance or adoption of IoT systems including technology awareness, user attitude, privacy concerns, lifestyle and hardware compatibility. In their work, they emphasise user feedback as one of the essential components for developing an acceptable system. Falcone and Sapienza (2018) argued that a good way to address adoption and acceptability issues is through the concept of trust. The key point is, in fact, that users do not trust these systems; they do not understand their internal working process or what they can do. In this regard, a PETRAS research Cannizzaro et al. (2020) carried out a nationally representative survey of United Kingdom smart home consumers to measure adoption and acceptability, focusing on awareness, ownership, experience, trust, satisfaction, and intention to use. Their study revealed that trust is fundamental to consumer technology in which transmission of personal and sensitive information is involved.

Following STS theory, this research stream investigates how user experience and perceptions (people) of IoT (technology) interact with adoption patterns (culture), with the aim of providing an accessible means for IoT product and service providers to take advantage of the benefits of the IoT for their customers while balancing risks (goal). The stream investigates ways to communicate and encourage the responsible development of IoT technologies (regulatory frameworks), which is an integral part of the overall aim of the Centre to position the United Kingdom as a global leader in the design, manufacture and deployment of IoT products and services Lindley et al. (2019). This is in line with the UKRI AREA framework for responsible research and innovation Zhao et al. (2023).

5.1.1 Unpacking adoption and acceptability

Adoption and acceptability pertain to two perspectives associated with the spread and uptake of technology within society Lindley et al. (2019). At its core, acceptability is defined as the time it takes for a technology to bring its user benefits. However, acceptability can also be prescriptive in nature as it also determines factors that make a technology desirable, thus requiring moral judgement Van De Poel (2016). Hence, acceptability provides a normative notion of what is good and ethically acceptable with respect to a technology. Adoption, however, is regarded as more of a process than a qualitative judgement. This aforementioned process commences from the instance a user becomes aware of the technology, and concludes when the user embraces and makes full use of a technology Renaud and van Biljon (2008).

In partnerships with a range of the Centre's partners (stakeholders), the stream used a variety of research approaches to investigate how to address the complexity of IoT adoption including i) clarification and development of adoption, acceptability and acceptance theories and checking how these notions overlap and diverge in the scientific literature, and ii) design and analysis of a nationally representative consumer attitudes survey to investigate whether user opinions correlate with acceptance models, among others Lindley et al. (2019).

5.1.2 Understanding attitudes

Due to the lack of focus on user perspectives, the stream carried out a survey to investigate consumer attitudes towards IoT Lindley et al. (2019). An initial systematic review conducted to frame the survey design revealed a regional bias where most empirical studies on adoption, acceptability and acceptance of IoT systems were carried out in East Asian regions, suggesting that entities in these regions may be in a better competitive position to use IoT for economic and public good than Europe Hsu and Yeh (2017); Hsu and Lin (2018).

The systematic review revealed that most of the studies conducted on IoT adoption and acceptability have not used a nationally representative sample, as the largest study consisted of 426 respondents Karahoca et al. (2018). To fill these gaps, the survey carried out was based on a nationally representative sample of over 2,000+ respondents in the United Kingdom. This survey addressed the theoretical-methodological gap in IoT research using a more recent and comprehensive model, such as the Unified Theory of Acceptance and Use of Technology 2 (UTAUT 2) Venkatesh et al. (2012) unlike the modified versions of popular technology acceptance models used in previous studies.

Preliminary findings of this research stream suggested that adoption is a broad issue, and the most significant way to make IoT more acceptable is by reducing the anxieties stemming from user concerns about privacy, trust, and security. In addition, it is crucial to consider the broader implications of the adoption of IoT in advance Lindley et al. (2019).

5.2 Safety and security

The PETRAS Safety and Security Stream investigated the current and emerging safety and security challenges with IoT systems in different application domains including the critical national infrastructure such as transport and mobility, healthcare, and finance, among others. To develop efficient IoT systems that are capable of scaling and supporting a variety of end-to-end network and services, the stream investigated how to understand and manage complex systems, and also the changing nature of safety and security Nicolescu et al. (2018).

Findings from the stream research reveal:

- The need to evolve towards *Security Ergonomics by Design* in cyber-physical systems such as IoT Craggs and Rashid (2017). This involves the implementation of safety and security requirements from the design phase and throughout the lifetime of a device and possible varying contexts of use.
- The need for a dynamic assessment of safety and security requirements. The need to implement a dynamic risk assessment to understand and cope with the dynamic nature of IoT.
- The need to maintain a security and safety culture that is constantly evolving with improved skills.
- The need to study emerging security and trust economics. For example, understanding the beneficiaries of attacks and monetising the compromise of new systems can be explored to prevent counter-attack crime.

5.2.1 Training and skills

The stream researched the cybersecurity training and skills initiatives in the United Kingdom to analyse the extent to which the international community currently cooperates on global cybersecurity policy for the IoT. The research stream identified a lack of focus on IoT-specific educational initiatives, which will fast become a pervasive issue as IoT systems become more widespread.

This lack of awareness of the dynamics and potentials of IoT could be exploited by malicious entities, especially against vulnerable groups, specifically children and victims of domestic abuse. This suggests the need for adequate investigation into this niche area of emerging technologies. The stream suggests the need to prepare support services to be resilient to these ubiquitous technologies that can cause harm to vulnerable communities. The stream resonates strongly with the notion of preparing society for this evolving ecosystem, working closely with the United Kingdom National Cyber Security Centre (NCSC) and some other related United Kingdom Government departments. To foster trust, users must understand the level of functionality of these systems.

5.2.2 Global governance of IoT security

The stream was involved in a variety of engagements at the international level and has monitored the developments of international organisations and representative stakeholders, including the World Economic Forum (WEF), the European Union Agency for Network and Information Security (ENISA) and the United Kingdom Department of Culture, Media and Sport (DCMS) Nicolescu et al. (2019).

Furthermore, in collaboration with the United Kingdom National and International Policy for Critical Infrastructure (NIPC), the stream developed a research repository for interested parties who wish to inform themselves on IoT governance issues. This will help in mapping on-going initiatives in this domain, as well as rival interests and tensions for politics and standards in IoT governance. In line with this international outlook, the technical and operational communities, in particular, Computer Security Incident Response Teams (CSIRTs), and their growing role in IoT security and internet infrastructure were studied. The findings, presented and discussed at the United Nations Internet Governance Forum in 2017, highlighted how IoT's security issues were diffusing into the work of these stakeholders Nicolescu et al. (2019).

5.3 Privacy and trust

Privacy requirements specify the capabilities and functions that must be embedded in a system to protect the personal data of end users and to empower them with control of their data Ogunniye and Kokciyan (2023a). These requirements are generally based on fundamental privacy objectives specified in the relevant privacy regulatory policy or guidance, such as GDPR Voigt and Von Dem Bussche (2017). Importantly, privacy requirements are fundamental requirements at the start of any IoT service-design process Perera et al. (2016) and they involve some other sub-requirements such as trust requirements. Trust is an important factor that affects how people make privacy decisions Ogunniye and Kokciyan (2023b) and impacts the levels of user adoption and acceptability. For example, people are more likely to interact with devices that they trust. Without trust, there will be limited acceptance of IoT by government, industry, and citizens. Research within the Centre's Privacy and Trust Stream has focused on the gaps in the current research literature on privacy and trust in IoT, from a socio-technical perspective Maple et al. (2019). The stream carried out a meta-analysis of social science and humanities research on privacy and trust in IoT and identified wide-ranging primary ethical issues such as: control and oversight of data flows; the balance between authentication and privacy; criteria to foster users' trust in IoT; trade-offs between identification and privacy; the limits of the GDPR; transparency and auditing of autonomous and machine learning algorithms; responsible innovation; and consent mechanisms Maple et al. (2019). The stream identified some high-priority areas and recommendations for different actors in the IoT ecosystem Maple et al. (2019).

- Privacy assurance approaches; control of data and the corresponding data flows were identified as one of the key issues initially identified for privacy and trust research. Various privacy assurance approaches were suggested including technical features and privacy policies to protect user privacy, industry self-regulation, and government regulation to enhance user perceived control of their data in the provision of their IoT services.
- Information transparency was suggested as an essential element to enhance users' perception of control and privacy protection.
- Trustworthiness requirements; from a technical point of view, this involves trust negotiation (the exchange of credentials that allows a consumer and a service party to complete a service or resource transaction) is key to the development of a trustworthy system Maple et al. (2019). Such a negotiation requires additional requirements, such as identity management and access control. Any trust negotiation mechanisms developed in the IoT must have appropriate access control and ensure that the mechanism is fine-grained but not burdensome, and must incorporate effective identity management systems, to record the identity of objects and their authentication, authorisation, roles and privileges. Technically, trustworthiness is contextual: it needs to be addressed in a context and should be goal-oriented. Different variables need to be considered for different contexts Maple et al. (2019).

5.4 Standards, governance and policy

Given the complexity of the IoT ecosystem and its associated challenges, governance principles and practices must be developed to effectively address the emerging threats to the ecosystem, particularly the "culture of security" around emerging digital technologies. In addition, skills development and training are crucial. In line with these requirements, the Centre's Standards, Governance and Policy Stream investigated whether the current governance approaches are adequate to promote the benefits that the IoT promises, while mitigating the complex and interdependent challenges that it raises Brass et al. (2019).

5.4.1 A fragmented and complex standards landscape

The stream, in collaboration with BSI and DCMS carried out review which identified three main trends in the current standards landscape for IoT security Brass et al. (2018).

1. There is a fragmented and complex regulatory landscape as the development of IoT security standards and guidelines have been developed by industry consortia and associations such as GSMA and IoT Security Foundation with varying and possibly conflicting motivations.
2. There is difficulty in monitoring the adoption, implementation, and effectiveness of IoT security standards and best practices for both the public and private sectors.
3. There is difficulty in establishing a baseline for IoT security across all application domains and sectors of IoT deployment. IoT is an emerging technology, thus obscuring the boundaries between established standards and regulatory regimes for physical and cybersecurity, safety, liability for defective products, data protection and trust.

5.4.2 The development and adoption of IoT standards

A PETRAS project, the IoT Multidisciplinary Standards Platform (IoT-MSP)[13] investigated the barriers to the engagement of cybersecurity standards for IoT, as well as the potential development of a crowd-source database and online portal designed to peer review and evaluate the appropriateness, effectiveness and ease of implementation of relevant standards for IoT. This project collaborated with the BSI, the Institution of Engineering and Technology (IET), the Digital Catapult and United Kingdom Government Communications Headquarters (GCHQ) to conduct a survey to identify the main barriers to navigate, adopt and implement relevant IoT standards. The results informed the SGP IoT Security Standards Landscape Review and further investigation was carried out on the basis of these findings, by BSI and PETRAS, into the key challenges that Small and Medium-Sized Enterprises (SMEs) face in the development and design of secure IoT products and services.

[13] https://petras-iot.org/project/iot-multi-disciplinary-standards-platform-iotmsp/

5.5 Harnessing economic values

The Centre pursued two main objectives. Firstly, it aimed to identify the economic value of present day IoT technology and services that typically reside with the owner of data sources, to investigate new opportunities to create economic and social value, and to identify areas where new sectors can emerge. This involved a better understanding of complex market design, taking into consideration platforms and ecosystems, institutional constraints (e.g., regulation, IP), data provenance and licensing, competition, incentives and ethics, and acceptability of data and meta-data sharing.

The second objective was to identify how to gain optimisation in complex IoT-systems, taking into account conflicting interests. This requires insight into how IoT systems and humans interact with each other and how design principles can influence such behaviour. These two objects are interrelated, as the data in IoT systems are not under sole ownership and require effective market mechanisms to ensure effectiveness and optimisation of IoT systems.

6 Discussion

The proliferation of the IoT will lead to several exciting opportunities and transformations in human society, and drastic changes in all aspects of human society including regulation and policy Brass et al. (2019), ethics, and operations, among others. From a socio-technical perspective, a legitimate question will be how to design the IoT to provide solutions in real-world scenarios, produce efficient enhancements, welfares, and assist human works, boost existing information and communication technologies and improve business models without violating the social and legal rights of the users. Generally, human society is based on social contracts for which individuals and organisations consent to submit some of their freedoms to defend their remaining rights Parise et al. (2018). Therefore, the innovative impacts of IoT within human society must be advanced with adequate consideration of the rights of its users.

Although the development of IoT is very actively carried out in the United Kingdom, there are significant obstacles to be addressed before it is fully accepted by individuals and organisations looking to maximise its potential and progress. Such issues involve who is responsible for the privacy and security of IoT deployment, and how? How do we effectively bring together stakeholders in industry, academia, civil society bodies, and the public, as well as regulators to identify issues such as regulatory gaps and co-create solutions to address them? How do we develop IoT cybersecurity policies and regulations for United Kingdom industry sectors? How do we make business case for IoT projects, among other competing demands for a limited budget, among others?

IoT research and development is a cutting-edge activity that will require substantive design, development, deployment, and evolution. At its core, there is a challenge of bringing together diverse, disparate components, cultures, services and technologies and people (including individuals and organisations) to develop IoT-based solutions. Moreover, these pieces are owned, operated and supported by users and vendors across multiple groups. Therefore, the operation and management of large-scale IoT research and development will require highly coordinated activities. This is a socio-technical design challenge. This paper describes a socio-technical framework for research into these questions.

We note that there are several socio-technical frameworks for emerging technologies research in the United Kingdom. An example of these frameworks is *The Research Institute for Sociotechnical Cyber Security (RISCS)* framework, funded by the United Kingdom National Cyber Security Centre (NCSC) and hosted at the University of Bristol[14]. It is the United Kingdom's first academic research framework, focusing on understanding the overall security of organisations including their constituent technology, people, and processes. It takes an evidence-based and interdisciplinary approach to addressing these sociotechnical cyber security challenges. It provides a platform for the exchange of ideas, problems, and research solutions between academia, industry, and the policy community, and promotes and supports world-leading, multidisciplinary, and scientifically robust research into sociotechnical approaches to cyber security. Although related, the RISCS framework differs from the PETRAS framework presented in this paper in several ways. First, it does not capture the *Synthesis Fellows* programme (c.f., Section 4.1.3). The programme has been proven to be pivotal in the dissemination of findings throughout the PETRAS research base to the public. Second, unlike the PETRAS framework, bidding for projects does not require an associated user partner. Third, the PETRAS framework considers sectors and lenses that help define research challenges in a real-world context and are points of contact for accessing the Centre's programmes and expertise, as well as special interest groups.

7 Conclusion

In this work, we have outlined case studies and a methodology of how large-scale IoT research and design can integrate technical and non-technical elements. Using an exemplary socio-technical framework where a research centre and its public and private user partners work together, we have shared some best practices and tools that can be used to engage critical stakeholders in IoT research and development.

The strategy of co-designing an IoT research project with critical stakeholders is a balanced approach. This can help set more realistic expectations for all stakeholders. The approach outlined here have significant implications for eliciting socio-technical requirements for IoT and for addressing public concerns about its acceptability and adoption, safety and security, privacy and trust, standards, governance, and policy, and harnessing the economic benefits of IoT.

Author contributions

GO: Conceptualization, Investigation, Methodology, Software, Supervision, Writing–original draft, Writing–review

[14] https://riscs.org.uk/

and editing. AH: Conceptualization, Investigation, Methodology, Software, Writing–original draft, Writing–review and editing. JW: Conceptualization, Funding acquisition, Project administration, Resources, Supervision, Writing–review and editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity which has been funded by the UK EPSRC under grant number EP/S035362/1.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Ali, O., Ishak, M. K., and Bhatti, M. K. L. (2021). Emerging IoT domains, current standings and open research challenges: a review. *PeerJ Comput. Sci.* 7, e659. doi:10.7717/peerj-cs.659

Baig, M., Hosseini, H., Afifi, S., and Mirza, F. (2019). Current challenges and barriers to the wider adoption of wearable sensor applications and internet-of-things in health and well-being. CONF-IRM 2019 Proceedings.

Baliyan, A., Dhatterwal, J. S., Kaswan, K. S., and Jain, V. (2022). “Role of AI and IoT techniques in autonomous transport vehicles,” in *AI enabled IoT for Electrification and connected transportation* (Springer), 1–23.

Brass, I., Kruakae, P., Tanczer, L. M., and Carr, M. (2019). Standards, governance and policy. *Cybersecurity Internet Things (IoT) PETRAS Stream Rep.* doi:10.13140/RG.2.2.15925.42729

Brass, I., Tanczer, L., Carr, M., Elsden, M., and Blackstock, J. (2018). *Standardising a moving target: the development and evolution of IoT security standards.*

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., et al. (2023). The digital harms of smart home devices: a systematic literature review. *Comput. Hum. Behav.* 145, 107770. doi:10.1016/j.chb.2023.107770

Burton, D. S., Tanczer, L. M., Vasudevan, S., Hailes, S., and Carr, M. (2021). The UK code of practice for consumer IoT cybersecurity: where we are and what next. *Tech. Rep.* University College London. doi:10.14324/000.rp.10117734

Cannizzaro, S., Procter, R., Ma, S., and Maple, C. (2020). Trust in the smart home: findings from a nationally representative survey in the UK. *PLOS ONE* 15, e0231615. doi:10.1371/journal.pone.0231615

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Trans. R. Soc. A Math. Phys. Eng. Sci.* 376, 20180080. doi:10.1098/rsta.2018.0080

Coen, S. E., Bottorff, J. L., Johnson, J. L., and Ratner, P. A. (2010). A relational conceptual framework for multidisciplinary health research centre infrastructure. *Health Res. Policy Syst.* 8, 29–10. doi:10.1186/1478-4505-8-29

Craggs, B., and Rashid, A. (2017). “Smart cyber-physical systems: beyond usable security to security Ergonomics by design,” in 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS) (Buenos Aires, Argentina: IEEE), Buenos Aires, Argentina, 21-21 May 2017, 22–25.

Davis, M. C., Challenger, R., Jayewardene, D. N., and Clegg, C. W. (2014). Advancing socio-technical systems thinking: a call for bravery. *Appl. Ergon.* 45, 171–180. doi:10.1016/j.apergo.2013.02.009

Esterle, L., and Grosu, R. (2016). Cyber-physical systems: challenge of the 21st century. *e i Elektrotechnik und Inf.* 133, 299–303. doi:10.1007/s00502-016-0426-6

Falcone, R., and Sapienza, A. (2018). On the users' acceptance of IoT systems: a theoretical approach. *Information* 9, 53. doi:10.3390/info9030053

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., et al. (2018). Security threats to critical infrastructure: the human factor. *J. Supercomput.* 74, 4986–5002. doi:10.1007/s11227-018-2337-2

Government (2014). *The internet of things (Blackett review): making the most of the second digital revolution*. London: Government Office for Science: Tech. rep.

Hsu, C.-L., and Lin, J. C.-C. (2018). Exploring factors affecting the adoption of internet of things services. *J. Comput. Inf. Syst.* 58, 49–57. doi:10.1080/08874417.2016.1186524

Hsu, C.-W., and Yeh, C.-C. (2017). Understanding the factors affecting the adoption of the Internet of Things. *Technol. Analysis Strategic Manag.* 29, 1089–1102. doi:10.1080/09537325.2016.1269160

Jobin, A., Ienca, M., and Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nat. Mach. Intell.* 1, 389–399. doi:10.1038/s42256-019-0088-2

Kankanhalli, A., Charalabidis, Y., and Mellouli, S. (2019). IoT and AI for smart government: a research agenda. *Gov. Inf. Q.* 36, 304–309. doi:10.1016/j.giq.2019.02.003

Karahoca, A., Karahoca, D., and Akso¨z, M. (2018). Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes* 47, 742–770. doi:10.1108/K-02-2017-0045

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet Things* 15, 100420. Publisher: Elsevier. doi:10.1016/j.iot.2021.100420

Kokciyan, N., and Yolum, P. (2020). TURP: managing trust for regulating privacy in internet of things. *IEEE Internet Comput.* 24, 9–16. doi:10.1109/mic.2020.3020006

Krasovec, A., Pellarini, D., Geneiatakis, D., Baldini, G., and Pejovic´, V. (2020). enNot quite yourself today: behaviour-based continuous authentication in IoT environments. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 1–29. doi:10.1145/3432206

Leavitt, H. J. (1965). “eng*Applying organizational change in industry: structural, technological and humanistic approaches*,” in *Handbook of organizations*. Editor J. G. March (Chicago, IL, USA: Rand McNally OCLC).851695803

Lee, I. (2019). The Internet of Things for enterprises: an ecosystem, architecture, and IoT service business model. *Internet Things* 7, 100078. doi:10.1016/j.iot.2019.100078

Lindley, J., Cannizzaro, S., Procter, R., and Coulton, P. (2019). “Adoption and acceptability,” in *Cybersecurity of the internet of things (IoT): PETRAS stream report* (Tech. rep., PETRAS IoT Research Hub).

Maple, C., Wakenshaw, S., and Taddeo, M. (2019). *Privacy and trust”, cybersecurity of the internet of things (IoT): PETRAS stream report*. London: Tech. rep., PETRAS IoT Research Hub.

Marwedel, P. (2021). *engEmbedded system design: embedded systems foundations of cyber-physical systems, and the Internet of Things. Embedded systems*. Cham: Springer. fourth edition, corrected publication edn.

Mullagh, L., Jacobs, N., Kwon, N., Markovic, M., and Wainwright, B. (2022). *Participatory IoT policies: a case study of designing governance at a local level.*

Nehme, E., El Sibai, R., Bou Abdo, J., Taylor, A. R., and Demerjian, J. (2022). *Converged AI, IoT, and blockchain technologies: a conceptual ethics framework*. AI and Ethics *2*. Publisher: Springer, 129–143.

Nicolescu, R., Craggs, B., Lupu, E., and Rashid, A. (2019). “Safety and security,” in *Cybersecurity of the internet of things: PETRAS stream report. Tech. Rep.* (London: PETRAS IoT Research Hub).

Nicolescu, R., Huth, M., Radanliev, P., and De Roure, D. (2018). Mapping the values of IoT. *J. Inf. Technol.* 33, 345–360. doi:10.1057/s41265-018-0054-1

Ogunniye, G. (2023). A synthesis report on PETRAS industry-specific workshops on future challenges of IoT cybersecurity in UK industry sectors. *Tech. Rep.* PETRAS National Centre of Excellence for IoT Systems Cybersecurity. doi:10.13140/RG.2.2.25308.77446

Ogunniye, G., and Kokciyan, N. (2023a). A survey on understanding and representing privacy requirements in the internet-of-things. *J. Artif. Intell. Res.* 76, 163–192. doi:10.1613/jair.1.14000

Ogunniye, G., and Kokciyan, N. (2023b). Contextual integrity for argumentation-based privacy reasoning. *Proc. 2023 Int. Conf. Aut. Agents Multiagent Syst.* 23, 2253–2261. (Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems), AAMAS. doi:10.5555/3545946.3598903

Parise, G., Parise, L., and Parise, M. (2018). “Evolution of human society and of things assisted by IoT,” in 2018 IEEE International Symposium on Technology and Society (ISTAS) (Washington, DC, USA: IEEE).

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., and Nuseibeh, B. (2016). “Privacy-by-Design framework for assessing internet of things applications and platforms,” in Proceedingsof the 6th International Conference on the Internet of Things (Stuttgart Germany: ACM), 83–92.

Renaud, K., and van Biljon, J. (2008). “Predicting technology acceptance and adoption by the elderly: a qualitative study,” in Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology, New York, NY, USA: Association for Computing Machinery, 210–219. SAICSIT 08.

Schaub, F., Ko¨nings, B., and Weber, M. (2015). Context-adaptive privacy: leveraging context awareness to support privacy decision making. *IEEE Pervasive Comput.* 14, 34–43. Publisher: IEEE. doi:10.1109/mprv.2015.5

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: a human-centered design for the Internet of Things. *Telematics Inf.* 31, 519–531. doi:10.1016/j.tele.2014.02.003

Shin, D.-H., and Jung, J. (2012). Socio-technical analysis of Korea’s broadband convergence network: big plans, big projects, big prospects? *Telecommun. Policy* 36, 579–593. doi:10.1016/j.telpol.2012.03.003

Sony, M., and Naik, S. (2020). Industry 4.0 integration with socio-technical systems theory: a systematic review and proposed theoretical model. *Technol. Soc.* 61, 101248. doi:10.1016/j.techsoc.2020.101248

Subahi, A., and Theodorakopoulos, G. (2019). Detecting IoT user behavior and sensitive information in encrypted IoT-app traffic. *Sensors* 19, 4777. doi:10.3390/s19214777

Tyler, P., Allpress, S., Carr, M., Lupo, E., Norton, J., Smith, L., et al. (2018). *Internet of Things: realising the potential of a trusted smart world Publisher*. Royal Academy of Engineering.

Tzafestas, S. (2018). Synergy of IoT and AI in modern society: the robotics and automation case. *Robotics Automation Eng. J.* 3. doi:10.19080/RAEJ.2018.03.555621

Van De Poel, I. (2016). A coherentist view on the relation between social acceptance and moral acceptability of technology. *Philosophy Technol. after Empir. Turn* 23, 177–193. doi:10.1007/978-3-319-33717-3_11

Venkatesh, V., Thong, J. Y. L., and Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Q.* 36, 157–178. doi:10.2307/41410412

Voigt, P., and Von Dem Bussche, A. (2017). *en*The EU general data protection regulation (GDPR). Cham: Springer International Publishing. doi:10.1007/978-3-319-57959-7

Walker, G. H., Stanton, N. A., Salmon, P. M., and Jenkins, D. P. (2008). A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theor. Issues Ergonomics Sci.* 9, 479–499. doi:10.1080/14639220701635470

WEF (2015). *Industrial internet of things: unleashing the potential of connected products and services*. White Paper, in Collaboration with Accenture.

Weir, C., Dyson, A., and Prince, D. (2023). Do you speak cyber? Talking security with developers of health systems and devices. *IEEE Secur. Priv.* 21, 27–36. doi:10.1109/MSEC.2022.3221616

Williams, M., Nurse, J. R. C., and Creese, S. (2017). “Privacy is the boring bit: user perceptions and behaviour in the internet-of-things,” in 2017 15th Annual Conference on Privacy, Security and Trust (PST) (Calgary, AB: IEEE), Calgary, AB, Canada, 28-30 August 2017, 181–18109.

Winter, J. (2013). “The Internet of Things: scenarios for a human-centered design and policy process,” in The world futures studies federation 40th anniversary conference *(bucharest, Romania)*.

Zhao, J., Patel, M., Inglesant, P., Portillo, V., Webb, H., Dowthwaite, L., et al. (2023). Navigating the labyrinth of RI through a practical application — a case study in a cross-disciplinary research project. *J. Responsible Technol.* 15, 100064. doi:10.1016/j.jrt.2023.100064

Ziegeldorf, J. H., Morchon, O. G., and Wehrle, K. (2014). Privacy in the internet of things: threats and challenges. *Secur. Commun. Netw.* 7, 2728–2742. Publisher: Wiley Online Library. doi:10.1002/sec.795