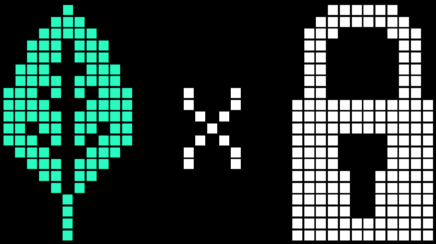
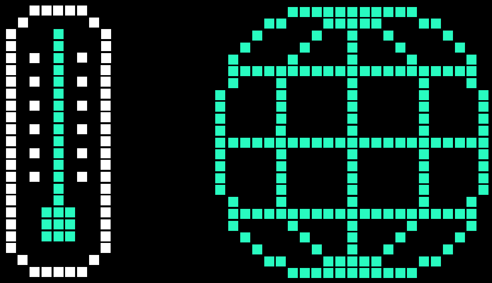
SUSTAINABLE X SECURE EDGE

DESIGN GUIDELINES FOR FUTURE DATA-DRIVEN EDGE-IoT DEVICES AND SERVICES

Michael Stead, Franziska Pilling, Adrian Gradinar and Ian Forrester



Lancaster University
imagination LANCASTER
PETRAS
BBC R&D
UKRI Engineering and Physical Sciences Research Council



CLIMATE CHANGE... WHAT'S DATA GOT TO DO WITH IT?

Alexa enquiries, Spotify listens, Netflix binges. Our everyday interactions with smart devices, digital services and the internet are generating huge amounts of data.

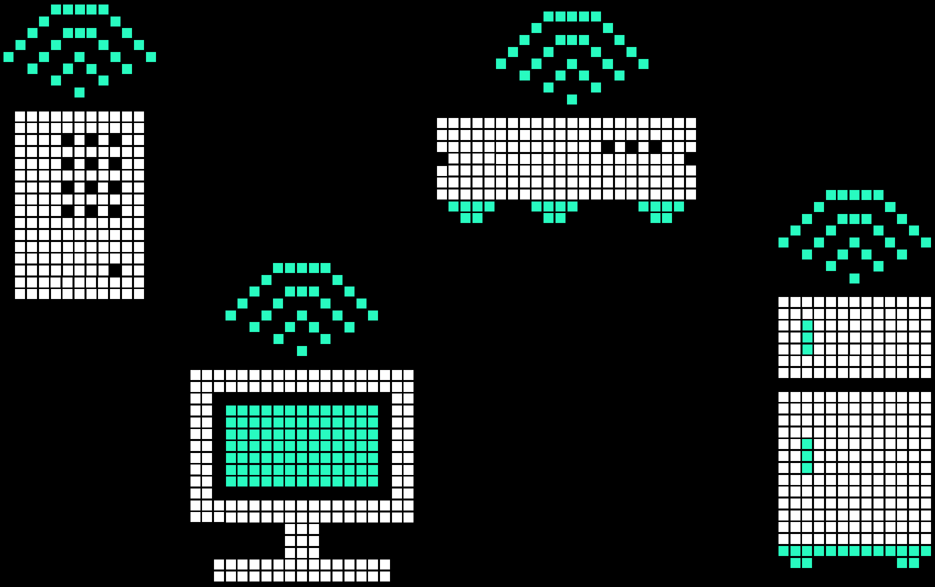
How this data is created, processed and stored is increasingly affecting the planet's natural environment as well as leading to cyber-security issues.

Generating huge amounts of data generates huge amounts of carbon emissions (CO_2). These emissions are harmful as they increase the Earth's temperature and contribute to climate change.

But we are not yet thinking about data impacts in this way.

We must therefore design and adopt new, shared visions of more sustainable and secure data-driven practices and processes.

Only then can we start to collectively work towards a sustainable and secure data-driven future.



WHY THE EDGE AND THE INTERNET OF THINGS?

Voice activated speakers and robot vacuum cleaners. More and more of our physical electronic devices are becoming connected to the internet and generating data.

It is estimated that there will be over 25 billion smart – or Internet of Things (IoT) – devices in active use by 2025.

This rapid expansion is creating more opportunities for external actors (human and machine) to carry out cyber-attacks upon devices and systems. In terms of sustainabilty, data generation and cyber-attacks increase both the amount of energy consumed and CO_2 emissions created by the IoT.

Today, distant, globally dispersed Cloud server farms mainly process and store our data.

The term Edge computing is used to classify a fusion of Cloud and local computing – where some data processing and storage also happens at the ‘Edge of the network’ directly on or close to the devices themselves.

Reducing our dependancy on the Cloud and developing the Edge could hold pros (and cons) for a sustainable and secure data-driven future.

THE EDGE OF TOMORROW PROJECT... WHAT DID WE DO?

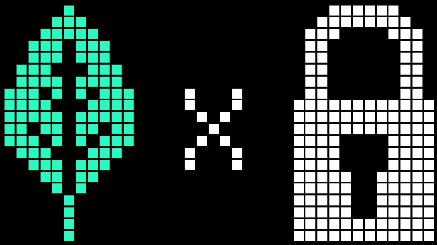
The EPSRC PETRAS funded Edge of Tomorrow research project explored the relationship between the sustainability and cyber-security of IoT data.

Lancaster design researchers collaborated with colleagues from BBC R&D to conduct workshops with sustainability and cyber-security experts, and members of the public.

Using the design methods Speculative Design and Experiential Futures, the research team embedded the workshop insights into the Prometheus Terminal – an interactive arcade style game in which participants take on the role of a hacker and must navigate the environmental effects caused by their data footprints whilst carrying out a cyber-attack on IoT devices at the Edge.

The game's main aim is to make the often illegible and intangible consequences of data choices more legible and tangible to players, specifically the extent to which our data-driven interactions with Edge-IoT devices and systems generate environmentally damaging CO_2 emissions.

Members of the public play the Prometheus Terminal interactive, arcade game at the Edge of Tomorrow event which took place at Lancaster Castle in November 2021 as part of the ESRC Festival of Social Science.



IT´S TIME TO GET SMARTER ON DATA SUSTAINABILITY & SECURITY!

Through our research, we found that the sustainability and cyber-security of Edge-IoT data are issues which are deeply intertwined.

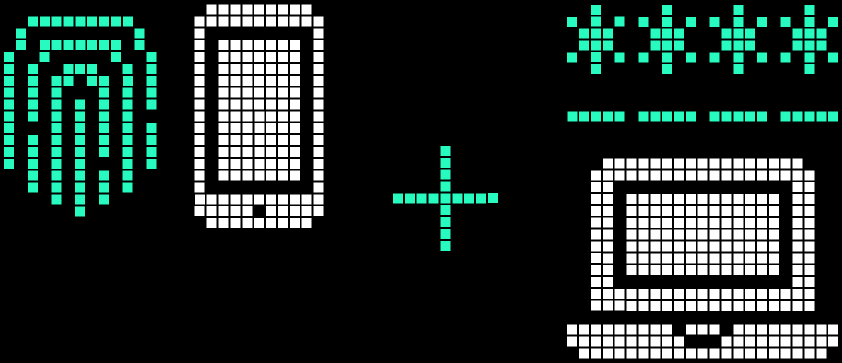
Accordingly, we have generated the following series of 8 design guidelines for improving IoT data sustainability and cyber-security at the Edge.

They were developed in collaboration with our project partners BBC R&D who are actively developing their own Edge-IoT technologies for public broadcasting.

We believe the guidelines might also offer insights for other technologists and designers who are seeking to improve Edge-IoT data sustainability and security as part of their work.

The guidelines may also be useful for wider audiences and publics as they highlight how everyday data-driven interactions with Edge-IoT systems can easily lead to unsustainable impacts and security issues.

1.



design guideline
AUTHENTICATE! AUTHENTICATE!

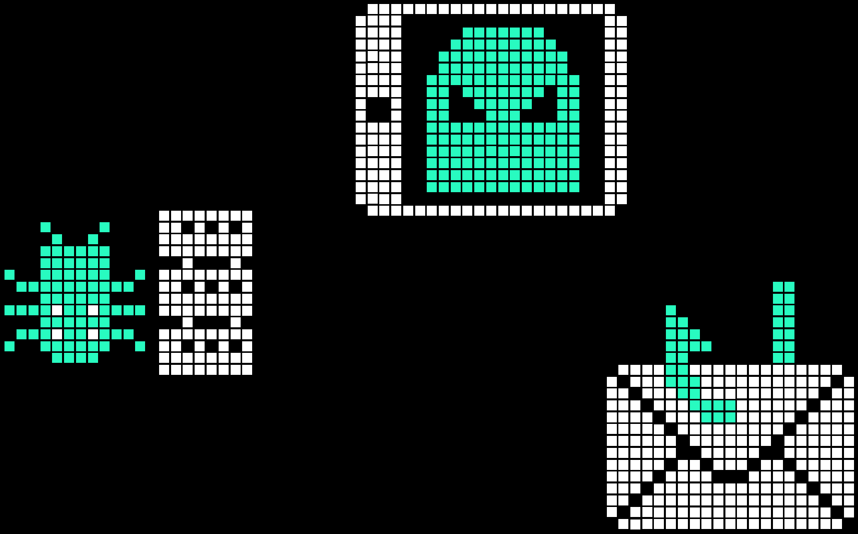
Many people regularly use weak and/or default passwords to secure their devices and networks.

They often also tolerate misconfigured access settings as well as fail to keep security software up-to-date.

This leaves their devices and networks more open and vulnerable to different forms of cyber-attack.

Designing future Edge-IoT devices to be more interoperable across different platforms and work together to provide built-in Multi-factor Authentication would better protect user's online interactions and important personal accounts like email, banking and data storage.

2.



design guideline

REDUCE ATTACK SURFACE

Billions of new IoT devices and online services are being connected at the Edge year on year.

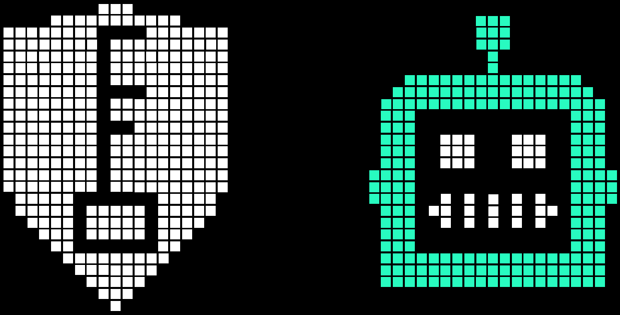
Tech manufacturers extol the supposed user benefits of rapidly adopting these new devices and services.

Internet providers are also marketing web platforms that can support ever-greater numbers of connected devices.

Yet, the greater number of smart devices that users' activate and interact with, the bigger their 'attack surface' i.e. their exposure to being the victim of a cyber-attack.

Promoting the notion of 'selective smartness' and designing and implementing fewer devices and services which possess enhanced security protocols will reduce users' attack surface.

3.



design guideline

TRUST (ALMOST) NO ONE

Devices and services should be designed to grant users the capability to implement a ‘Zero Trust Protocol’ across their personal/communal networks.

A Zero Trust Protocol can help reduce data security threats by restricting communications to only a small number of essential and/or user preferred servers and devices.

4.

design guideline

GO GLOCAL

The datafication generated through billions of everyday user interactions at the Edge is responsible for a growing CO_2 footprint.

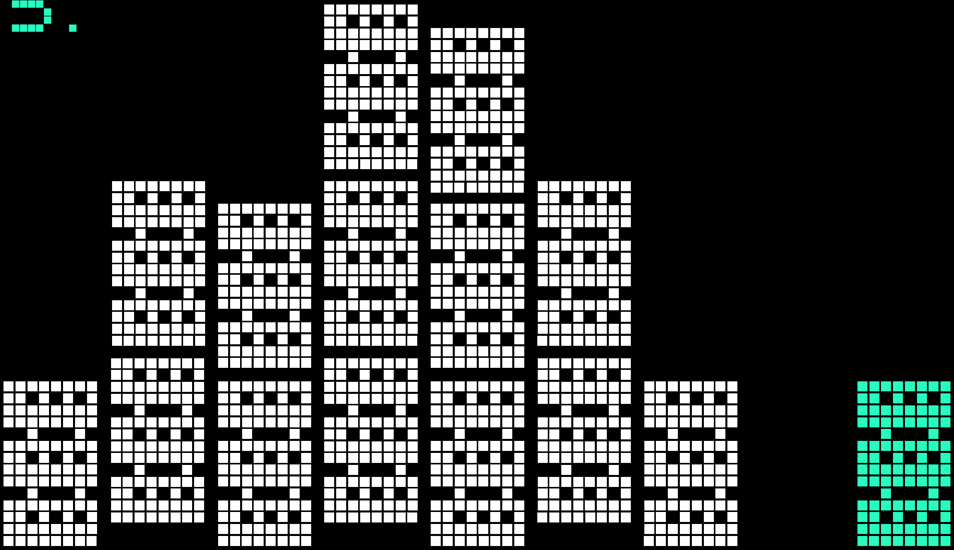
The transmission of such data between the Edge to Cloud can increase environmental impacts and security risks.

While some essential processing tasks must be carried out in the Cloud, many others could be completed at the Edge.

There are growing abilities for regulated and responsible forms of Artificial Intelligence (AI) and Machine Learning (ML) to recognise specific computing facilities i.e. to enable processing via local Edge servers rather than transmitting data across the planet to Cloud farms and back to our devices again.

New devices and services should be designed to offer users the choice to actively choose how their data is handled.

5.



design guideline

STREAMLINE STORAGE

There is no need to send all data to the cloud and store it as not all data is useful.

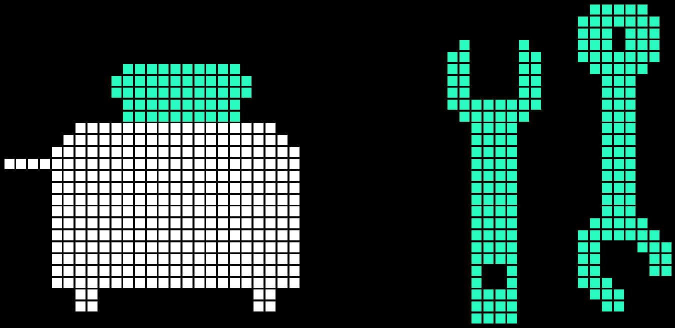
Future devices and systems should therefore also be designed to allow users to decide what types of data is ultimately stored – both in the short and long-term.

Streamlining data storage would avoid the build up of so-called ‘data swamps’ and limit opportunities for clandestine data mining and surveillence by platforms and providers as well as reduce bait for hackers.

Baking in such features during the design stages would improve security and reduce resource redundancy across networks.

Again, regulated and responsible forms of AI and ML could also be employed in such decision-making.

6.



design guideline

HARD-WEARING HARDWARE

Edge-IoT data-driven footprints can also be reduced by slowing the release and adoption of new smart gadgets and gizmos.

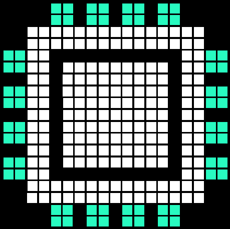
Their manufacture, materials mining and global distribution consume huge amounts of energy and generate huge numbers of CO_2 emissions.

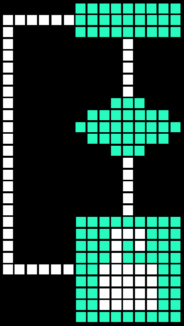
Their processors, memory and day-to-day runtime also increase the impacts.

To extend device lifecycles and avoid unnecessary obsolescence, we must begin to design future Edge-IoT hardware – and their accompanying software – to allow for better repair, servicing and reuse.

This will minimise future electronic waste – which is also environmentally and socially hazardous.

7.





design guideline
PREVENT THE PARADOX

When it comes to the use of resources and lifecycle emissions, future Edge-IoT hardware should strive for better hardware/software performance and efficiency.

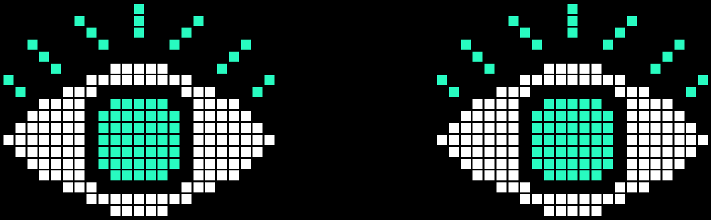
But we must also be aware of unintended consequences of improving effciency through technological means alone – specifically the notion of ‘Jevon’s Paradox’.

The paradox is where resource efficiency is increased through technological improvements which in turn results in a rebound effect that ultimately leads to more resources being consumed due to increasing demand.

Previous examples of the paradox include the sharp increases in coal-use as new technologies were adopted during the Industrial Revolution.

This will likely become a key challenge for design in relation to enabling sustainable and secure data-driven futures.

8.



design guideline

LEVELLING UP LEGIBILITY

To ensure a sustainable and secure data-driven future, it is essential we improve the legibility of growing data-driven device and system impacts.

While recent years have seen increasing emphasis placed on data security, the important environmental implications of Edge-IoT data has received significantly less attention.

BBC R&D's own 'Carbon Calculator' (2021) and the Shift Project's 'Carbonanalyser' (2019) begin to demonstrate the potential for empowering audiences and wider users with greater 'sustainable legibility' regards their data usage and impacts.

Applications and interactions like the above should be actively incorporated into future smart device and service design – particularly those operating at the very Edge of IoT networks.

SUSTAINABLE x SECURE EDGE

design guideline summary

1. **AUTHENTICATE! AUTHENTICATE!**
Enable Multifactor Authentication across Edge-IoT networks

2. **REDUCE ATTACK SURFACE**
Less devices can mean more security

3. **TRUST (ALMOST) NO ONE**
Implement Zero Trust Protocols

4. **GO GLOCAL**
Process data in the Cloud AND at the Edge

5. **STREAMLINE STORAGE**
Not all data is useful – store less

6. **HARD-WEARING HARDWARE**
Improve the ability to repair and reuse existing devices

7. **PREVENT THE PARADOX**
Be resource efficient but wary of using more resources because of it

8. **LEVELLING UP LEGIBILITY**
Make illegible data impacts legible and easy for all to see

MEET THE RESEARCH TEAM

Dr Adrian Gradinar

Adrian is Lecturer in Smart Home Futures at ImaginationLancaster, Lancaster University's School of Design. He designs and builds Experiential Futures as a means to explore key, interdisciplinary socio-technical challenges such as the adoption of immersive physical/digital objects and spaces. His work has been exhibited internationally including the EPSRC Living Room of the Future at the Tate Modern, V&A London and FACT Liverpool.

Dr Michael Stead

Michael is Lecturer in Sustainable Design Futures at ImaginationLancaster. His research applies approaches including Research through Design and Speculative Design to prototype radical new visions for low carbon futures. His work critically and creatively interrogates the evolving relationship between emerging data-driven technologies like the Internet of Things, Edge Computing and Artificial Intelligence and key sustainability challenges Net Zero 2050 and the Circular Economy.

Franziska Pilling

Franziska is a Design PhD candidate at ImaginationLancaster and funded through PETRAS NCE. Embedding philosophical thinking into Speculative Design practices, Franziska is developing More-Than-Human design methods for making AI systems and processes more legible to users and designers. Franziska advocates AI as a material for design and was previously a researcher on the EPSRC PETRAS Uncanny AI project.

Ian Forrester

Ian is Senior Firestarter Producer at BBC Research & Development. His research focuses on forging disruptive opportunities for innovation via open engagement with startups, early adopters and hackers. From rethinking narrative and storytelling via Perceptive Media to a designing a decentralised Public Service Internet, Ian combines novel approaches with creative collaboration to explore the future of data-driven interactive broadcasting.

EDGE OF TOMORROW

Lancaster University imagination LANCASTER PETRAS BBC R&D UKRI Engineering and Physical Sciences Research Council

This work was conducted as part of the Edge of Tomorrow research project.

The project 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.