Cyber Security Risks of Adversarial AI in Mobility-as-a-Service (MaaS)

Dr. Kai Fung Chu, University of Cambridge and Cranfield University
Prof. Weisi Guo, Cranfield University and Alan Turing Institute
weisi.guo@cranfield.ac.uk

PROJECT TIMELINE

Start date: Aug 2021
End date: Feb 2024

INTRODUCTION

Mobility-as-a-Service (MaaS) integrates different transport modalities and can support personalised transport solutions. To fully achieve the potential of MaaS, a range of AI algorithms are needed to learn personal requirements and orchestrate travel arrangements.

AIM

Detecting and preventing cyber-attacks is challenging when adversarial AI can erode both privacy and performance. Our research focus on how current and emerging AI-facilitated privacy risks and adversarial AI attacks can be prevented.

WHY

To ensure a safe and trustworthy MaaS, a mature and secure software system that uses various defense mechanisms, such as input validation, outlier detection, and model watermarking, is necessary for the intelligent scheduler to connect operators and passengers, manage traffic information, and optimize passengers' journey queries and system resources, to maintain the service quality.

EXPECTED IMPACT

Given the promising benefits of MaaS, the cyber security risks should be clearly identified such that the corresponding countermeasures can be implemented in the system. We use the latest trends and technologies in the MaaS system planner, which is one of the data, algorithm, and risks hot spots, to understand the cyber security aspects of the MaaS ecosystem.

Our research in data attack vectors and defence mechanisms can help improve the security and consumer trust in the MaaS system.

We also highlight the risks in the state-of-the-art AI technologies and common practices for those AI risks. The impact of the cyber security risks and countermeasures on the MaaS business will be essential to public safety and economic efficiency. Finally, we also suggest areas for future directions in research and development, aiming to provide insights into the key issues and best practices for risks and countermeasures in MaaS.

METHODOLOGY

We expect that there are 2 key AI technologies in MaaS [1-2]:

1. **Federated learning** (a central MaaS server interfaces with local end-user clients that learn personalisation)
2. **Reinforcement learning for personalisation** (personal trust and usage is a dynamic processes with memory)

As such, our methodology focuses on 2 key areas:

I. How to preserve privacy in federated learning data exchanges [1, 3]
II. How to quantify the risks of gamification spoofing attacks that erode economic efficiency [4]

We use a range of MaaS simulations in general artificial worlds and specific city scenarios (e.g., New York) to examine the risks and prevention strategies.

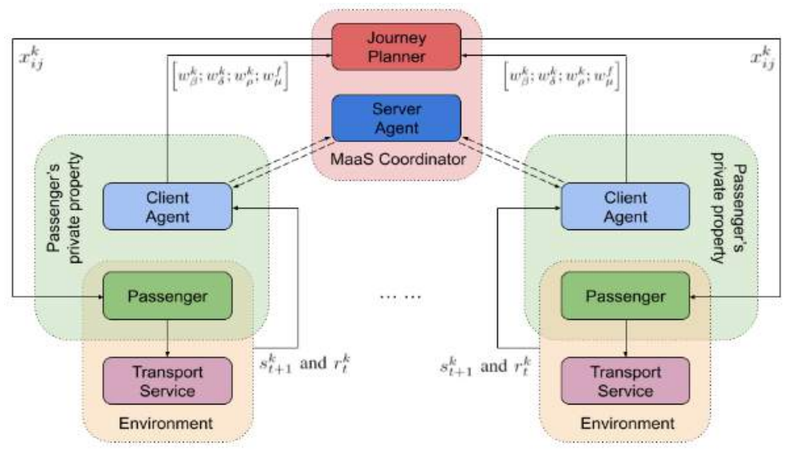


Figure 1: MaaS Controller in a federated learning structure.

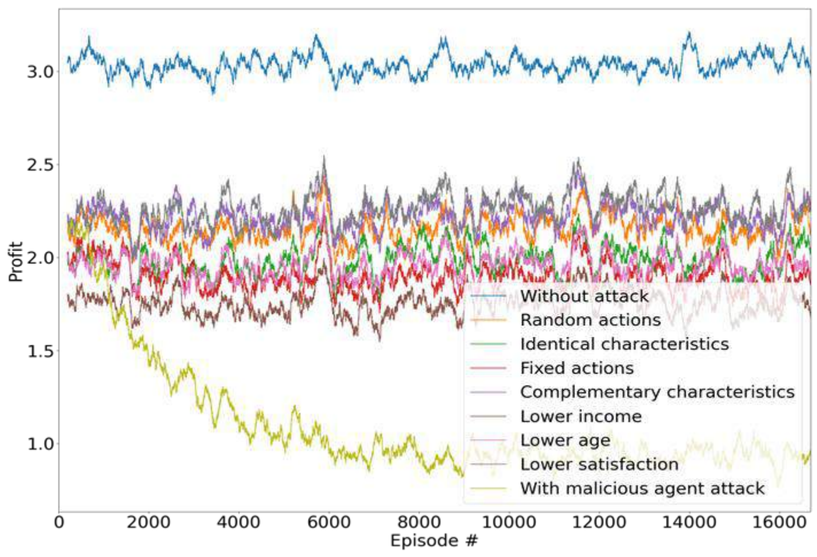


Figure 2: Gamification spoofing attack by a legitimate malicious user group can erode profits

KEY FINDINGS AND OUTCOMES

Inevitably personalised transport solutions that orchestrate across modalities and providers will use AI.

The risks to MaaS AI ecosystem comes from diverse areas, including but not limited to

- evasion attacks (evading detection of malicious behaviour),
- Eavesdropping (privacy of user personal preferences),
- Inference (model stealing), and
- spoofing (gamifying the system).

Our work believes the 2 most pertinent attacks are eavesdropping and spoofing, as they represent relatively lower level of sophistication and a higher level of adversarial impact.

Whilst the likelihood of a federated/distributed learning structure of MaaS and the reinforcement learning agent lends itself to some natural protection, the risks of compromising privacy and eroding profit/efficiency of the MaaS remains large.

PUBLICATIONS

[1] "Privacy-Preserving Federated Deep Reinforcement Learning for Mobility-as-a-Service," K. Chu, W. Guo, IEEE Transactions on Intelligent Transportation Systems, 2023

[2] "Deep Reinforcement Learning of Passenger Behavior in Multimodal Journey Planning with Proportional Fairness," K. Chu, W. Guo, Neural Computing and Applications, 2023

[3] "Federated Reinforcement Learning for Consumers Privacy Protection in Mobility-as-a-Service," KF. Chu, W. Guo, IEEE International Conference on Intelligent Transportation Systems (ITSC), 2023

[4] "Passenger Spoofing Attack for Artificial Intelligence-based Mobility-as-a-Service," KF. Chu, W. Guo, IEEE International Conference on Intelligent Transportation Systems (ITSC), 2023

USER PARTNERS

Connected Places Catapult, and Oxfordshire County Council

ACKNOWLEDGEMENTS

This work has been supported by EPSRC grant: Mobility as a service: MAnaging Cybersecurity Risks across Consumers, Organisations and Sectors (MACRO) - EP/V039164/1.

Engineering and Physical Sciences Research Council

Cranfield University

Multi-Layered Attack Detection in Home IoT Networks

Safwana Haque, *City, University of London*, Safwana.Haque@city.ac.uk
Dr Fadi El-Moussa, *BT Group PLC*, fadiali.el-moussa@bt.com
Dr Nikos Komninos, *City, University of London*, Nikos.Komninos.1@city.ac.uk
Professor Rajarajan Muttukrishnan, *City, University of London*, R.Muttukrishnan@city.ac.uk

PROJECT TIMELINE

Start date: February 2021

End date: Jan 2025

INTRODUCTION

A BT sponsored PhD in collaboration with City, University of London that explores the possibility of ***implementing*** a real-life application of ***attack detection*** mechanism on ***resource-constrained*** home hubs without overwhelming the hubs and affecting the performance of the attack detection models.

The study employs an anomaly detection unit that checks for unusual traffic behaviour that could occur because of an attack or a change in network characteristics, which the system verifies with a second step of attack detection.

This research also maps the relationship between features, attacks and layered-attacks to reduce feature set size and improve detection rates. The Edge-IIoT dataset[1] was considered in this study.

AIMS

- Identify ***features unique*** to ***attacks*** belonging to the ***same layer*** of ***architecture*** that could be used to ***distinguish*** them from ***attacks*** of ***another layer***.
- Additionally, **identify features unique** to **each attack** that could **distinguish** them from **other attacks within** the **same layer**.
- Deduce if these features are essential and could ***reduce*** the ***feature set*** size ***without reducing*** the ***efficiency*** of machine learning (ML) or deep learning (DL) models.

WHY

- Implement a ***two-tier*** intrusion detection system (***IDS***) ***unsupervised*** ML for ***anomaly*** detection and ***supervised*** ML for ***attack*** prediction with the proposed set of ***reduced*** and ***important*** features that are also ***privacy-preserving*** and do not contain any user or device-specific information.

EXPECTED IMPACT

- ***Unique*** or ***distinguishing*** features could ***easily identify*** or ***flag*** the ***associated attack*** (for instance, are the features found in the traffic flow related to a particular type of attack such as an ICMP, UDP or TCP DoS attack?) or an ***attack class*** (e.g. are the features found in the traffic flow common to a type of layered attacks such as an application layer attack?).
- Another advantage of using ***features*** that are ***unique*** to a particular attack (or category) with ***high level*** of ***importance*** or impact is that it will allow an IDS to be ***trained*** with a ***smaller*** and ***targeted feature set***.
- A ***reduction*** of the overall ***overhead*** on the system such as processing power required, machine learning (ML) training and testing times etc.

METHODOLOGY

Home Hub Segment: concerned with attack detection and alert-generating mechanisms.

- designed on a two-tier detection scheme i.e., an anomaly detection (using a convolutional autoencoder) and an attack detection (using random forest) section as shown in **Fig. 1**.

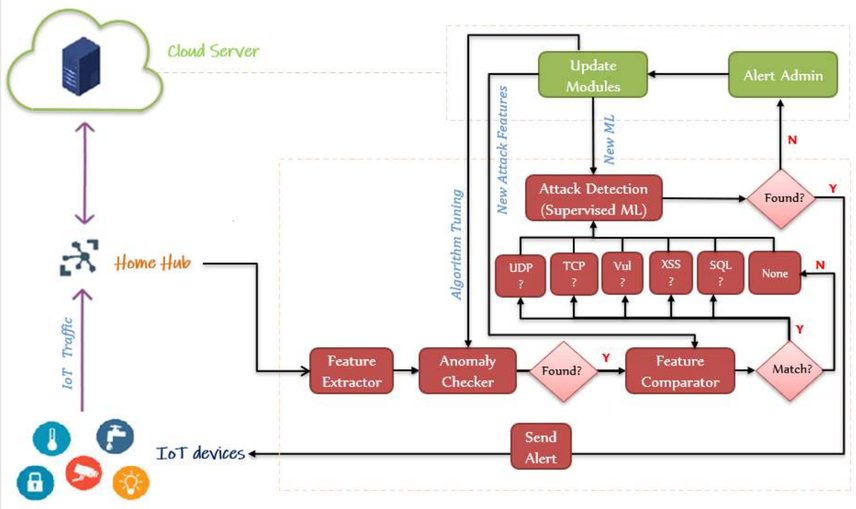


Figure 1: *Proposed Home IoT Attack Detection Architecture*

- The unique component added in this segment is the ***feature comparator***, which compares and evaluates extracted features to match the unique features for similarity or dissimilarity for each attack type .

  If a unique feature(s) such as those in **Fig. 3** is/are flagged, then the attack related to such feature(s) will be suspected to be the more likely attack underway. The collected traffic data is then passed on to the attack detector for confirmation or verification.
- The advantage of using the feature comparator is that it reduces the number of features that need to be extracted for ML analysis if unique features can be mapped to suspected attacks.

Cloud Segment: concerned with components that update, modify, and improve the existing attack detection models for further improvements. These components are implemented in the cloud to avoid exerting the home hub with training ML models that require a high amount of processing and storage power.

Others	Ours
Feature selection to select most important features to reduce overall size and improve ML performance	✓
✗	Additionally, compare the features with each attack chosen and attack class to identify unique features
Research by Ferrag et al.[1] ranked 5 important features relevant to each attack found in the dataset e.g. tcp.checksum, tcp.ack, tcp.seq etc.	Though important features, we **did not find** them to be **unique** but **common** to other **attacks**

Figure 2: *Comparison of Conventional Method vs Our Method*

[1] *M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," IEEE Access, vol. 10, 2022.*

KEY FINDINGS AND OUTCOMES

Network Layer Attacks		
ICMP DDoS	**UDP DDoS**	**TCP DDoS**
icmp.checksum icmp.resp_not_found or icmp.no_resp	udp.stream	tcp.stream

Application Layer Attacks		
Vulnerability Scan	**SQL Injection**	**XSS**
http.content_length http.referer http.request.method http.response	http.request.method	http.referer http.request.method

Figure 3: *Unique Features Mapped to Related Attacks*

Number of Features Used	NB	RF	k-NN	Performance
Initial Dataset	81	97	93	Overall Accuracy (%)
(46 features)	2.66	54.65	1534.49	Time Taken (s)
No Least Features	81	97	93	Overall Accuracy (%)
(33 features)	1.52	42.23	1255.09	Time Taken (s)
Random Forest	83.87	96.78	93	Overall Accuracy (%)
(20 features)	1.23	35.06	1222.46	Time Taken (s)

Figure 4: *ML performances with different feature set sizes*
** NB: Naïve Bayes, RF: Random Forest, k-NN: k nearest neighbour*

	precision	recall	f-score
Normal	0.99	0.90	0.94
All Attacks	0.91	0.99	0.95
accuracy			0.94

Figure 5: *Unsupervised Anomaly Detection with only 20 features*

Random Forest			
Time taken to test: 35.06s; **Overall accuracy**: 0.9678			
Class	**precision**	**recall**	**f-score**
DDoS_ICMP	1.00	1.00	1.00
DDoS_TCP	1.00	1.00	1.00
DDoS_UDP	1.00	1.00	1.00
Normal	0.94	0.96	0.95
SQL_injection	0.79	0.84	0.81
Vulnerability_scanner	0.98	0.96	0.97
XSS	0.85	0.73	0.79

Figure 6: *Supervised Attack Detection using only 20 features*

- ML-based IDS can be designed with a reduced and targeted feature set to detect specific attacks if features (as in Fig. 3) relevant to an attack are known, this reduces overhead in a resource restrained IoT environment and improves efficiency.
- Fig. 4 demonstrates that the time to run ML algorithms for attack detection can be reduced by using a smaller feature set without affecting the efficiency of the algorithms.
- Anomaly detection (Fig. 5) and attack detection (Fig. 6) rates with a reduced and targeted feature set were found to be 94% and 97%, respectively.

PUBLICATION

Haque, S., **El-Moussa**, F., **Komninos**, N. and **Muttukrishnan**, R., 2023. Identification of Important Features at Different IoT layers for Dynamic Attack Detection. In 2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS).

USER PARTNERS

British Telecommunications (BT) PLC UK

ACKNOWLEDGEMENTS

This research is funded and supported by British Telecommunications (BT) PLC UK

The Internet of Tactical Engagement (IoTE): Acceptability of Data-driven Public Communications in Smart Homes

Dr Jiahong Chen, University of Sheffield, email: jiahong.chen@sheffield.ac.uk

PROJECT TIMELINE

Start date: March 2024
End date: February 2026

INTRODUCTION

As we are moving closer towards the reality of **public authorities** and **civil society organisations** using smart technologies to communicate **public messages** to IoT users, how would new opportunities and new threats be perceived by the public? IoTE employs a **co-creation** approach to generating near-future scenarios to measure the acceptability of smartified data-driven public communications, and test the boundaries of ethical uses of these engagement strategies.

AIMS

➢ **A1:** To map data-driven smart targeting tactics in a socio-technical **taxonomic framework**

➢ **A2:** To co-create a range of **near-future scenarios** of public messaging via smart devices with a view to prompting further academic and public discussions

➢ **A3:** To capture **public perceptions** of existing and new forms of public messaging strategies expanding to the smart home

➢ **A4:** To provide important theoretical nuance to the scholarship on the **socially acceptable boundaries** of data uses in the context of domestic IoT-based public messaging

➢ **A5:** To inform **responsible smart engagement practices** by public authorities and civil society organisations, as well as policymaking on the regulation of such practices.

METHODOLOGY

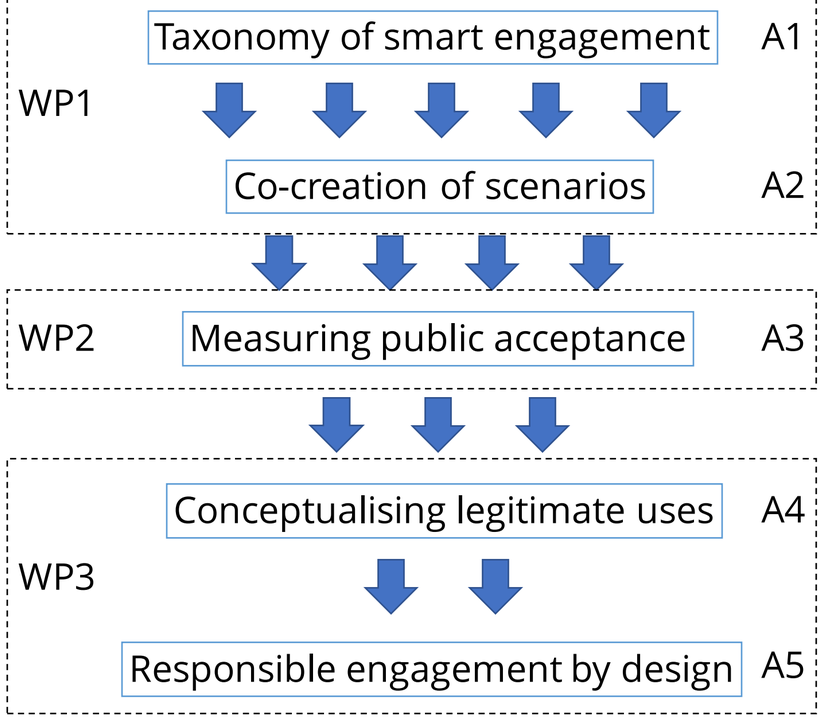


Figure 1: Workflow of project

EXPECTED IMPACT

➢ **Academic impact:**

- 'What does autonomy mean when public messages are powered by data-driven agency?' (data-driven agency theory)
- 'Do we need a new social contract to define the public/private boundaries when it comes to delivering public messages into smart homes?' (smart social contract theory)

➢ **Policy impact:**

- 'How can we ensure our regulatory framework facilitate responsible uses of IoT for public messaging while minimising risks?'

PROJECT PARTNERS

Information Commissioner's Office

Ada Lovelace Institute

horizon DIGITAL ECONOMY RESEARCH

Sprite+ Security, Privacy, Identity, Trust, Engagement, NetworkPlus

REPHRAIN Protecting citizens online

ACKNOWLEDGEMENTS

This work is supported by the Economic and Social Research Council (ESRC) (ES/Y00020X/1)

UKRI Economic and Social Research Council

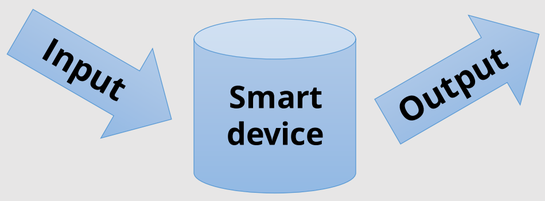
CREATE YOUR OWN SCENARIO!

Can you think of any opportunities or threats relating to the use of smart devices for public communications (i.e. by public authorities and civil society organisations)?

Use a **green** post-it note for **opportunities**

Use a **red** post-it note for **threats**

Also think about both the input (data collected from the smart home) and output (messages and interactions) aspects:



PETRAS

UKRI UK Research and Innovation

UCL

Privacy standards in IoT for independent and assisted living

Jinqian Li
UNIVERSITY OF CAMBRIDGE, UK
lijinqian1234@163.com

Dr Peter Novitzky
UNIVERSITY COLLEGE LONDON, UK
AVANS UNIVERSITY OF APPLIED SCIENCES, NL
p.novitzky@ucl.ac.uk / p.novitzky@avans.nl

PROJECT TIMELINE

Start date: March 2023
End date: September 2023

INTRODUCTION

Students from the Department of Science, Technology, Engineering, and Public Policy (STEaPP) at University College London (UCL) are examining the privacy aspects of Internet of Things (IoT) devices in living environments. The project assesses how these devices handle privacy, focusing on smart home technologies, and compares legal standards in the EU, UK, Japan, and China. The goal is to find a balance between the advantages of IoT developments and maintaining privacy.

AIM

The project aims to investigate how privacy aspects are translated into the domain of smart and assistive IoT devices that enable independent and assisted living.

The research questions are as follows:

How do developers and providers incorporate existing privacy requirements, encompassing legislation and industry standards, into their products designed for the domestic market?

To provide further clarity, we specifically explore the following sub questions:

- **Sub-question 1:** To what extent do the measures mandated by privacy regulations align with practical IoT implementations, and to what degree do they adhere to privacy-by-design principles in IoT implementations?
- **Sub question 2:** Do the regulatory and industry-specific privacy standards sufficiently address the primary privacy concerns and challenges faced by the general public? Are there different expectations of privacy in different countries?

WHY

This research explores the privacy and regulatory aspects of IoT devices in living environments, examining their privacy management and the alignment of privacy-by-design principles with regulations in smart home technologies. It aims to evaluate the current privacy standards' effectiveness in the IoT context.

EXPECTED IMPACT

This report, aims to review privacy standards in IoT devices for living environments. It provides detailed **insights on privacy practices in the IoT sector**, helping in relevant **governmental organizations** in their supervisory role. The report also likely suggests **policy and design improvements** to enhance privacy regulations and practices in the IoT industry.

METHODOLOGY

We employed both quantitative and qualitative approaches. The **quantitative** aspect included a thorough examination of 52 different IoT technologies. This involved categorizing them, analyzing their privacy policies, terms and user manuals to understand their approach to privacy.

We conducted **qualitative** research through 17 expert interviews, composed of 10 academics, 6 consultants, and 1 IoT technology provider.

Our team gathered **in-depth insights into the privacy concerns and practices in the IoT domain**, particularly in the context of independent and assisted living. All the interview data was open-coded and rigorously analyzed using various techniques, including thematic analysis, to distill patterns and themes from the conversations. The analysis highlighted counterintuitive findings, compliance with privacy requirements, and areas of consensus and disagreement among the interviewees.

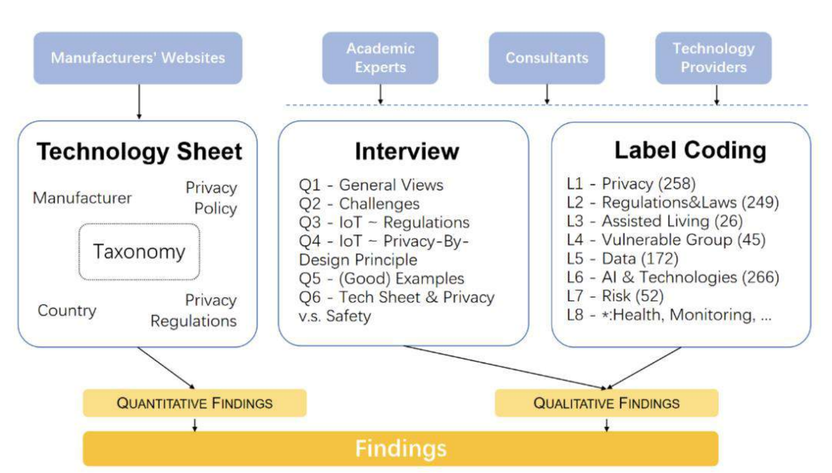


Figure 1: Mixed Methodology

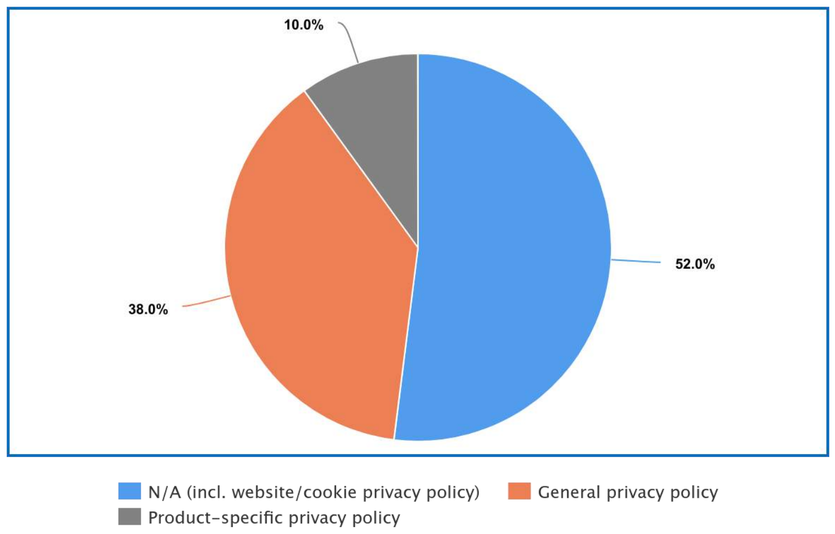


Figure 2: Proportion by privacy policy type for IoT products

KEY FINDINGS AND OUTCOMES

- **IoT Product Analysis**: Significant variation in privacy policies among 52 IoT products; less than half had product privacy policies, with 80% lacking detailed information for individual devices. Larger firms showed more privacy prioritization than smaller ones. Low public awareness of IoT privacy risks noted.
- **Expert Interviews**: Very diverse opinions on implementing privacy in IoT, with challenges in integrating privacy practices and keeping up with fast-evolving technology and regulations. Huge differences between academia and industry.
- **Impact on Vulnerable Populations**: IoT in smart homes raises privacy concerns in assisted living, potentially increasing vulnerability through data breaches.
- **Recommendations**: A combined approach of policy updates, design improvements, and research advancements needed. Emphasizes cooperation between regulators and companies to enhance IoT privacy. Stringent implementation of GDPR on IoT is needed.

PUBLICATIONS

Group members joined the ***2023 IEEE International Conference on Robotics and Automation (ICRA) competition***, focusing on vulnerable populations in IoT-enabled smart homes. Our task involved identifying and solving ethical issues in deploying a fetch robot in an elderly care setting. We analyzed ethics concerning privacy, autonomy, and fairness, and developed a design framework for the robot's engineers. Our submission included a 10-page report with models and pseudo-code, plus a video presentation of our designs. We achieved **2nd place in the competition**.

USER PARTNERS

The project was developed in partnership with ICO, but it is the independent work by the students from the STEaPP department at UCL, not the ICO's position.

ACKNOWLEDGEMENTS

This work has been supported by the project supervisors **Dr Peter Novitzky** (UCL) and **Prof Jeremy Watson** (UCL), and assisted by PhD candidate **Stefanos Evripidou** (UCL).

The original report from the STEaPP MPA course that provided the basis of this poster has been co-authored by students from the STEaPP department: **Kohei Sumida**, **Satomi Hatakeyama**, **Yuxin Xiao** and **Xueqian Ji**, who all contributed to the project results.

Security of Smart streets

Meha Shukla, University College London
Email: uctzshu@ucl.ac.uk

PROJECT TIMELINE:

Start Date: Oct 2022 , End Date: Feb 2024

Data was gathered from April 2022 to Jan 2023

RESEARCH QUESTION

"Do the security measures mitigate the cyber risks within the UK's connected place ecosystem (earlier known as smart cities) ? "

AIM

- How are cyber risks associated with the connected street ecosystem governed within Local Authorities (LAs) procurement, operations, and contract management processes for smart infrastructure services ?

- What challenges are faced by UK LAs in managing the cyber-resilience of the connected place ecosystem ?

WHY

To enable city authorities and urban planners to anticipate crime opportunities and inform the design of the smart street ecosystem to reduce risk.

IMPACT

- The recommendations for enhancement of National Cyber Security Centre (NCSC) connected place cybersecurity principles and Department of Science, Innovation and Technology (DSIT) policy were accepted.

- Findings from this research were used by UK Government to refine the scope of their Alpha Testing project to support LAs to implement Connected Place guidelines.

- Business continuity dry run included were included by an LA in the procurement contract specifications.

- Inputs on cybersecurity capability risks for the upcoming IoT-based urban street transformations were published in Horizon 2020 project (Multi-modal optimisation of Road space in Europe – MORE) report.

METHODOLOGY

Semi-structured interviews were conducted with stakeholders. the security specifications in the procurement contracts for EV charging smart services were assessed against the guidance for managing security and resilience risks specified in the connected place principles rolled out by NCSC.

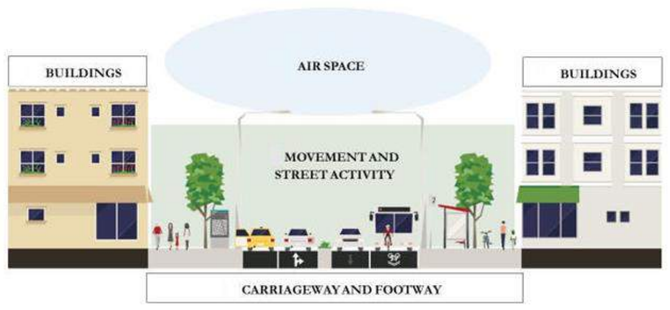


Figure 1: Urban street as an ecosystem

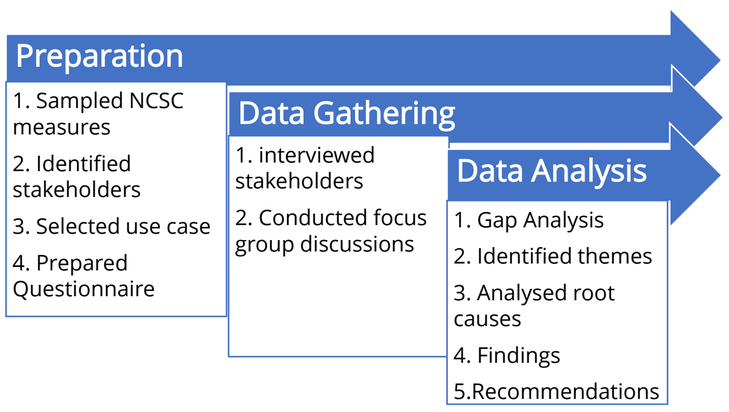


Figure 2: Stages of research

Table 1: Stakeholders

Focus Group
NCSC Connected Places Team
NCSC Energy Team
Department of Science, Innovation and Technology (DSIT)
UCL Researcher
Research Participants
Westminster local authority
Kingston and Sutton local authority
York local authority
Manchester local authority
Milton Keynes local authority
Coventry local authority
Transport for London (tfL)
EV charge point operator (Anonymous)

Table 2: Sampled NCSC security principles for connected places

NCSC cybersecurity principles for connected places (in Scope for this research)
#1 Understanding your connected place and the potential impacts
#2 Understanding the risks to your connected place
#3 Understanding cyber security governance and skills
#4 Understanding your suppliers' role within your connected place
#5 Understanding legal and regulatory requirements
#9 Designing your connected place to be resilient and scalable
#10 Designing your connected place monitoring
#12 Managing your connected place's supply chain
#13 Managing your connected place throughout its life cycle
#14 Managing incidents, planning response and recovery

FINDINGS

1. Inadequate cyber risk mitigations in the procurement process
2. Systemic risks not governed
3. Gap between national guidance and local implementation

RECOMMENDATIONS

1. Enhancements to NCSC connected place guidelines
2. Develop capabilities
3. Assess the level of accountabilities
4. Preparedness for systemic cyber events
5. Transformation of LAs' operating model

LIMITATIONS

- Small sample of stakeholders and a snapshot-in-time perspective,
- Excludes recent developments beyond the study period and,
- Findings may not be generalised

OUTCOMES

- Pioneer research on crime and place in context of connected places: Provides inputs for anticipatory policies to manage criminogenic effects of emerging disruptive technologies on connected place ecosystem
- Contributes to academic research for crime science theories specific to the smart urban ecosystem.

PUBLICATION

OSF | PhD Research - Security of Smart streets

ACKNOWLEDGEMENTS

This work is part of Meha Shukla's PhD at University College London (UCL), UK. It was supported by Prof Shane Johnson (Director, Dawes Centre for Future Crime, Department of Security and Crime Science at UCL) and Prof Peter Jones (Transport and Sustainable Development, Dept of Civil, Environ & Geomatic Eng, UCL).

PETRAS

UKRI UK Research and Innovation

UCL

Security of Smart streets

Meha Shukla, University College London
Email: uctzshu@ucl.ac.uk

Stakeholders were asked how they mitigate the risks of potential cybercrime scenarios within their procurement process to protect the connected place ecosystem using smart EV charging as a case study.

Smart EV charging – potential cybercrime scenarios
One incident at massive scale Hostile state actors could attack multiple EV chargers at the same time, turn them on and off every few seconds repeatedly or at the same time resulting in higher load on the power grid, further causing power outages/blackouts across cities [1], [2]. In July 2021, researchers had already evidenced a possibility of large-scale power fluctuations using such a method with DC fast chargers (The Byte, 2022).
Multiple incidents at massive scale A cyber-attack on the public chargers for a fleet of trucks could impact the distribution of essential food/water amenities and cause disruption across the entire supply-chain[3].
Multiple incidents at small scale simultaneously In 2022, during the Russia-Ukraine war, EV charging stations on the 450-mile highway between Moscow and St Petersburg were hacked, functions were disrupted, and the EVSEs displayed supportive messages for Ukraine [4]. Such attacks could disrupt the transport sector if most vehicles are EVs.
Multiple incidents at small scale over time Cyber thieves can steal the vehicle owner's identity, stop owners from charging vehicles, and charge their own vehicle for free. In 2021, data for more than 140,000 users of UK domestic car charging provider was stolen, potentially allowing hackers to identify their common charging locations [4].
Few incidents close to simultaneous succession Hostile state actors could attack multiple EV chargers simultaneously, turn them on and off every few seconds repeatedly or at the same time resulting in higher load on the power grid, further causing power outages/blackouts across cities [1], [2].

References:

[1] Sygensys for National Grid ESO, "Resilient Electrical Vehicle Charging: 'REV,'" Feb. 2022. Accessed: Jan. 26, 2023. [Online]. Available: https://esc-production-2021.s3.eu-west-2.amazonaws.com/2022/02/avNHxukq-Project-REV-WP1-report.pdf.

[2] The Byte, "Electric Vehicle Chargers Are Shockingly Vulnerable to Hacking," 2022. https://futurism.com/the-byte/ev-chargers-vulnerable-hacking (accessed Jan. 17, 2022).

[3] NESCOR, "Electric Sector Failure Scenarios and Impact Analyses-Version 3.0 National Electric Sector Cybersecurity Organization Resource (NESCOR)," Dec. 2015. Accessed: Jan. 27, 2023. [Online]. Available: https://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf.

[4] J. Jeffay, "Why Hackers Are Now Targeting Electric Car Charging Stations," Nocamels - Israeli Innovation News, 2022. https://nocamels.com/2022/08/why-hackers-are-now-targeting-electric-car-charging-stations/ (accessed Aug. 29, 2023).

Example quotes from stakeholders

a) "*The cyber risks are not thought through in the context of these scenarios that you have described. Utter ignorance on the subject is phenomenal*"

b) "*City authorities do not analyse the ecosystem. Private operators run the connected place. Not everyone carries out due diligence and projects are not actioned with confidence. The big picture is lost as contract compliance is what remains.*"

c) "*The consequence of the local authorities not being fully liable for cyber security of services is that the impact to end users is not thought through by everyone.*"

d) "*It is a good challenge as to whether the cyber security and resilience requirements in the procurement frameworks and bid pack are sufficient.*"

e) "*There is less awareness about the connected places ecosystem. Focus is on individual rollouts such as Go Ultra-low city scheme for lamp posts, car sharing (as well as mobility solutions) and EV transition.*"

f) "*Resilience tests should happen within the local authorities across London through coordination in future.*"

g) "*Analysing the outward dependencies and risks is not prescribed within the procurement frameworks used for EV charging contracts.*"

h) "As a security intervention, police have provided the specifications for the Modern slavery policy to be placed in all public sector contracts as a requirement. Something similar should be provided to local authorities for smart service procurement contracts."

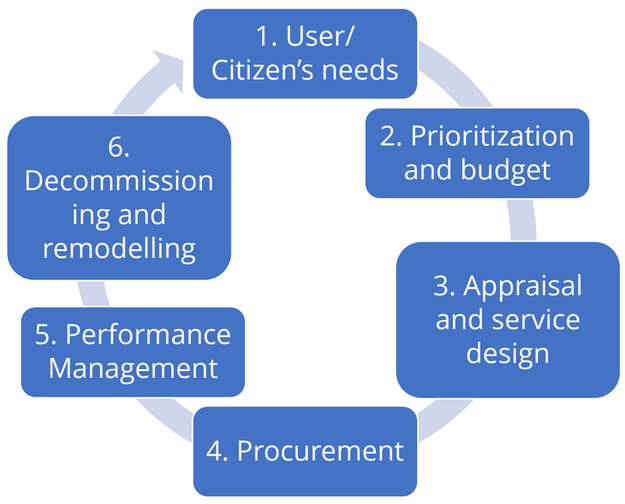
i) "*There is no guidance available for managing cyber resilience of the connected place ecosystem in the procurement process. Operational risks are managed by the private operator. The local authorities don't share risks with the private operators as they do not have skills or resources to get involved*. Hence the private operators lead on the smart service operations, putting them in position of power.

PETRAS
UK Research and Innovation
UCL

Security of Smart streets

Meha Shukla, University College London
Email: uctzshu@ucl.ac.uk

A questionnaire was created using the NCSC cybersecurity principles for connected places. The gaps in the local authorities' procurement processes from were analysed against the detailed guidance within the NCSC cyber security principles for connected places. The results from this analysis found enhancement opportunities for NCSC cybersecurity principles for connected places.



Analysis of cybersecurity principles within Local authority commissioning process for Smart services

Theme 1: Lack of accountability for cyber risk management for the connected ecosystem

Theme 2: Insufficient and inconsistent cyber resilience specifications in the CPO contracts

Theme 3: Lack of Operational Governance by the LAs for cyber risks across smart services

Theme 4: Lack of Assurance by the LAs for cyber risks for smart services, as well as the ecosystem

Theme 5: Inadequate skilled resources and capabilities in the LAs

NCSC principles for cybersecurity of connected places	Recommendations for enhancements
#1 Understanding your connected place and the potential impacts	Assessment of external dependency risks on the connected place ecosystem
#2 Understanding the risks to your connected place	Analyse how common cyber threats and vulnerabilities could develop into a systemic event within a connected place ecosystem
#3 Understanding cyber security governance and skills	• Cyber risk governance • Skills and capabilities
#4 Understanding your suppliers' role within your connected place	a) Assess maturity level of the security operations, b) Assess threats from hostile countries.
#5 Understanding legal and regulatory requirements	No gaps observed
#9 Design your connected place to be resilient and scalable	Cyber risk indicators
#10 Designing your connected place monitoring	How relevant security events from the logs across the interconnected systems within the networks owned by various organizations can be joined up to interpret a threat?
#12 Managing your connected place's supply chain	• Audit process • Assurance framework for the connected place ecosystem. • Selecting appropriate and proportionate measures
#13 Managing your connected place throughout its life cycle	Same as above
#14 Managing incidents and planning your response and recovery	• Requirements in the procurement process to test the response plans and, • Dry runs to manage recovery of the services in the event of systemic event

PETRAS
UK Research and Innovation
UCL

Cyber Security for Robotics with Dynamic Processes

Motivated by the increasing attack surface, this work focuses on data security aspects of robotics in manufacturing. The AMRC has created a simulation based monitoring system that is capable of detecting anomalies in a dynamic assembly process.

Aim

- Apply intrusion detection on systems where baselining is not feasible.
- Demonstrate the automated anomaly detection through simulated attacks.
- Built a demonstrator to increase cyber awareness by visualising anomaly detection.

Why

- Robot path is unknown dynamic processes, how can intrusions be detected?
- What can be done to increase cyber awareness in manufacturing and demonstrate the impacts of an attack?
- What are the impacts of subtle changes in parameters by attackers?

Methodology

- Malicious actor aiming alter assembly process so that parts were assembled incorrectly. Multiple products and could be affected before quality inspection would detect the changes.
- Simulated attacks on MQTT and ROS node were implemented respectively to apply minor changes to parameters.
- In each cycle, the box and tray are randomly placed to simulate a dynamic environment.

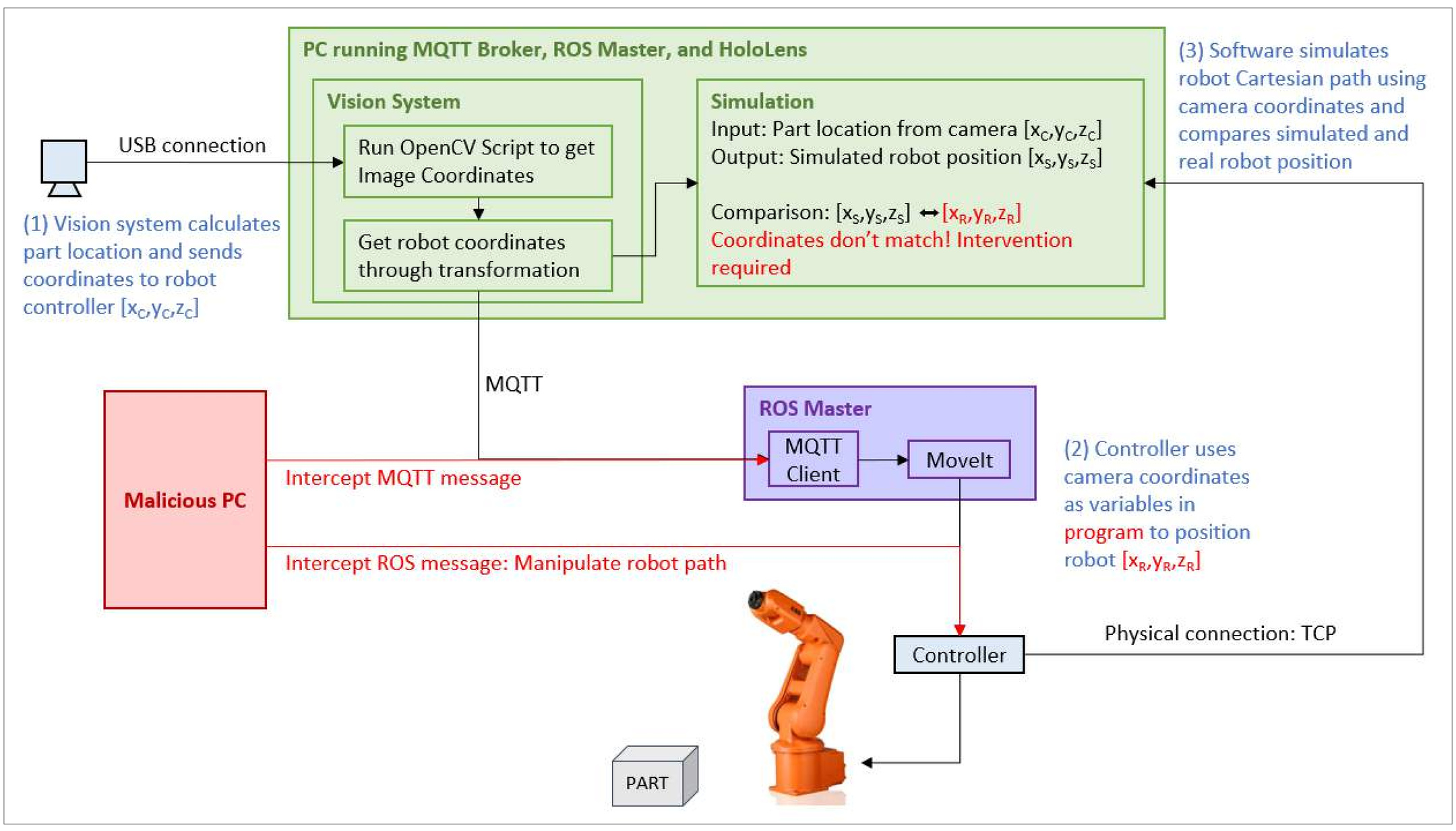
- Vision system generates an assembly path for the robot based on component locations.
- Monitoring system simulates robot path based on vision system data and compares with actual robot path to detect deviations.
- Anomaly detection visualised by changing the colour of the robot in augmented reality.

University of Sheffield /AMRC Advanced Manufacturing Research Centre

TOMORROW. DONE BETTER.

Key Findings and Outcomes

- The simulated attacks was successfully disguised as one-off system failures to the unknowing eye.
- The monitoring system successfully detected and flagged the attacks.
- The advantage and restriction of the proposed solution is that the approach is restricted by the tolerance of each robot. Attacks within tolerance are deemed to not be a successful attack and will not be flagged.



Expected Impact

This work has demonstrated the proof-of-concept for an intrusion detection system based on a live simulation of a dynamic robotic system.

This system has demonstrated the capability to detect deviations in the movement of a robot that could be caused my multiple different attack vectors.

Such a system could prove useful for detecting day zero attacks, but this system could also detect degenerative changes in the robot's movement.

Further development using machine learning techniques to recognise the potential cause of the robot deviations would be needed to industrialise this system.

Future Development

Data analysis can be used to predict a dynamic tolerance through forming a baseline with building management system (BMS) data, and by attaching sensors to the robot joints to attain robot temperature data, vibration data, etc.

The current approach has effectively identified when malicious activities have succeeded.

Acknowledgement and User Partners

This work was conducted on behalf of Airbus and other AMRC Partners. The authors would like to express their gratitude towards Airbus for the opportunity to explore this area of overlap in interest.

Jon Hall (j.hall@amrc.co.uk)

Grace Lim (j.lim@amrc.co.uk)

The Implementation and Integration of Technology Hardware in Place

PhD Researcher: Rebecca Hartley
Supervisors: Professor Lizzie Coles-Kemp and Dr Andrew Dwyer
Contact: Rebecca.Hartley.2021@live.rhul.ac.uk

Introduction

Using a sociotechnical approach, the research investigates security in the context of technology hardware in public places. It considers material factors and discourses. As a *form* of discourse, narrative is a key focus because it can tell us about the context from which it arises[1,p.340], such as assumptions and influences.

Aim

The research aims to understand the factors shaping digital security during the process of implementing and integrating technology hardware into public places. The research questions are:

- What factors shape digital security in the implementation and integration of technology hardware in place?
- What role do narratives play in this context?
- How can digital security be improved in this context?

Why

- The term “hardware” is used to emphasise the current research focus on technologies which are physically integrated into public places, e.g. a sensor on a streetlight.
- There is little sociotechnical research focusing on digital security in this area.
- Narrative is a focus to explore the communication of key ideas. Research has shown the lack of conceptual clarity of “smart cities” [2,3,4,5,6], an idea central to the introduction of technology in place.

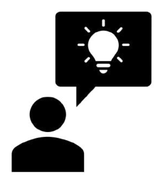
Project Timeline

2021-2025

Methods

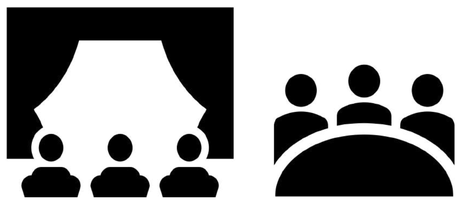
The first stage of this research looked at place-based technology projects, which are projects which seek to integrate digital technologies in particular locations, often led by a local authority. It included two forms of data collection which were analysed using thematic analysis.

Interviews



6 conversations with actors in the UK in the private and public sectors.

Event observation



Based on methods established to explore technology in military and commercial spaces [7,8,9]. Attendance at 4 events in the UK included observation of content and atmosphere. Events attended linked to the research focus.

References

[1] R.R. Warhol. 1999. Guilty Cravings: What Feminist Narratology Can Do for Cultural Studies. In *Narratologies: New Perspectives on Narrative Analysis*, David Herman (Ed.). Ohio State U.P, Columbus, 340-355.
[2] R.G. Hollands. 2008. Will the real smart city please stand up? *City* 12, 3 (Dec. 2008), 303–320. DOI:10.1080/13604810802479126.
[3] S. Joss, F. Sengers, D. Schraven, F. Caprotti, & Y. Dayot. 2019. The Smart City as Global Discourse: Storylines and Critical Junctures across 27 Cities. *Journal of Urban Technology* 26, 1 (2019), 3–34. DOI:10.1080/10630732.2018.1558387.
[4] R. Kitchin. 2022. Conceptualising smart cities. *Urban Research & Practice*. 15, 1 (2022), 155–159. DOI:10.1080/17535069.2022.2031143.
[5] T. Shelton, M. Zook & A. Wiig. 2015. The ‘actually existing smart city’. *Cambridge Journal of Regions, Economy and Society*. 8, 1 (2015), 13–25. https://doi.org/10.1093/cjres/rsu026.
[6] R-M. Soe, L. Schuch de Azambuja, K. Toiskallio, M. Nieminen, & M. Batty. 2022. Institutionalising smart city research and innovation: from fuzzy definitions to real-life experiments. *Urban Research & Practice*. 15, 1 (2022), 112–154. DOI:10.1080/17535069.2021.1998592.
[7] M.F. Rech. 2015. A critical geopolitics of observant practice at British military airshows. *Transactions of the Institute of British Geographers*. 40, 4 (2015), 536–548. DOI:10.1111/tran.12093.
[8] A.H. Jackman. 2016. Rhetorics of possibility and inevitability in commercial drone tradescapes. *Geographica Helvetica*. 71, 1 (2016), 1–6. DOI:10.5194/gh-71-1-2016.
[9] A. Ertan. 2022. *Exploring the Security Implications of Artificial Intelligence in Military Contexts*. Ph.D Thesis. Royal Holloway, University of London. Retrieved 26 July 2023 from https://pure.royalholloway.ac.uk/ws/portalfiles/portal/46513266/2022ErtanAPhD.pdf.

Findings

Highlights of the preliminary findings from the first stage of the research are:

Interviews showed that both discourses and material factors challenge digital security in this context.

- Technology projects have a difficult business case and tend to be short-term.
- Silos are a significant challenge within and between organisations.
- Unclear conceptualisations of projects make it difficult to identify impacts.

Event observation illustrated the different actors and dominant narratives in discourses. The findings show that security is a concern but is challenged by other priorities.

- Digital security perceptions vary depending on the context of discourse.
- Governance is pitted against innovation and portrayed as a major challenge.
- Technology is the subject of narratives which emphasise its power.
- Competition between places at different scales is present.

Next stage

22 international interviews and additional event observation have been completed. This data will be analysed to investigate the international aspect of implementing technology hardware in place.

Acknowledgements

This research is funded by the EPSRC as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London.

xAuth: Using Inertial Sensors in Authentication

Jack Sturgess, Sebastian Köhler, Simon Birnbach, and Ivan Martinovic
Department of Computer Science, University of Oxford; {firstname.lastname}@cs.ox.ac.uk

Motivation

Passwords are still the primary mechanism by which users authenticate themselves to digital services. Passwords must be long and random to resist guessing attacks and they must be often changed and not reused to resist dictionary attacks, all of which makes them burdensome to use effectively at scale.

Biometrics, such as fingerprints or face geometry, provide a promising alternative. The initial barriers to adoption that biometric systems faced, such as high error rates and deployment costs, have evaporated in recent years as smartphone-based sensors have become readily available. But there are risks in using biometric authentication, as these characteristics can be captured by an attacker and used in impersonation—and, unlike passwords, they cannot be revoked or changed once compromised.

To address this, behavioural biometrics have started to attract interest. Instead of measuring a physical characteristic, behavioural biometrics measure patterns of movement over time, such as gait or typing dynamics, and therefore can be collected unobtrusively without any effort on the part of the user and are more difficult to capture and impersonate. These systems were regarded as impractical due to the need for continuous measurement, but the widespread use of wearable devices (and therefore continuously worn sensors) has opened up new opportunities for implementation.

CableAuth [3]

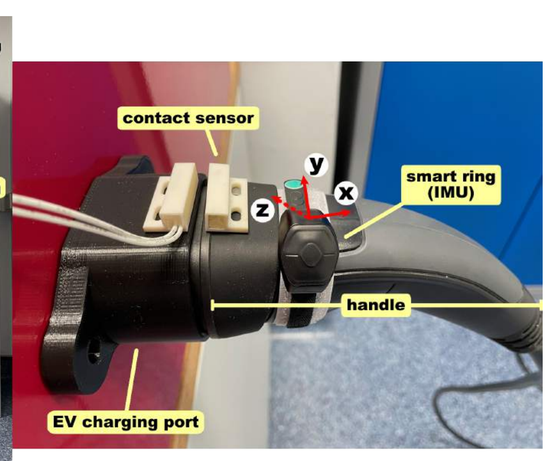
Electric vehicles (EV) are becoming more common. To recharge its battery, the user must park the vehicle next to a charging station, connect a charging cable, and make a payment to initiate the charging process. EV batteries charge more slowly and must be recharged more often than the refuelling of vehicles with a combustion engine, so user-friendliness and convenience in the charging process are important. As such, zero-interaction payment schemes, such as AutoCharge and Plug & Charge, are most desirable.

These systems work by sending information from the vehicle to the charging station via the charging cable once it is connected; this information is linked to a payment instruction, typically administered by an application on a paired smartphone, to facilitate automatic billing. These schemes treat the vehicle as a token and authenticate the vehicle rather than the user. This could allow a thief to charge a stolen vehicle at the owner's expense or an attacker to capture information from a victim's vehicle and to inject it into the communication channel to charge a different vehicle at the victim's expense. To address this, the system requires some form of user authentication that does not inconvenience the user.

- User study (n=20)
- Replicated a charging station and a Volkswagen ID.3 in our lab
- Attached inertial sensors to the charging cable handle
- Collected 30 charging sessions from each user

- Affixed contact sensors to the cable enclosures to timestamp the unhook and plug-in events
- Segmented gestures around each timestamp, to collect **unhook** and **plug-in gestures** and to disregard variable travel time in between

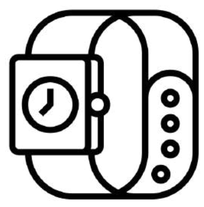
- Tuning model for security, added a layer of protection that rejected 82% of attacks without any user effort
- Tuning model for usability, reduced the number of unnecessary authentication requests made by 41% at no cost to security



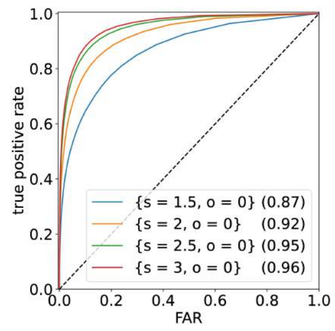
WatchAuth [1]

In a mobile payment context, we showed that smartwatch-users can be authenticated to the system using only the inertial sensors in the smartwatch. The movements of the arm and wrist that are performed by the user when making a payment, which are collectively called a **tap gesture**, are sufficiently unique to each user.

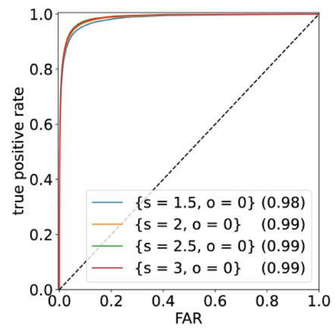
- User study (n=31)
- Replicated a payment environment in our lab
- Collected 210 gestures from each user
- Users attempted to impersonate recordings of each other
- De-noised data in each gesture, extracted 220 features, and trained random forest classifiers
- Used sliding windows to find optimum gesture parameters, effective with as little as 0.5s of data
- EERs of 0.07, AUROC 0.95 for user authentication

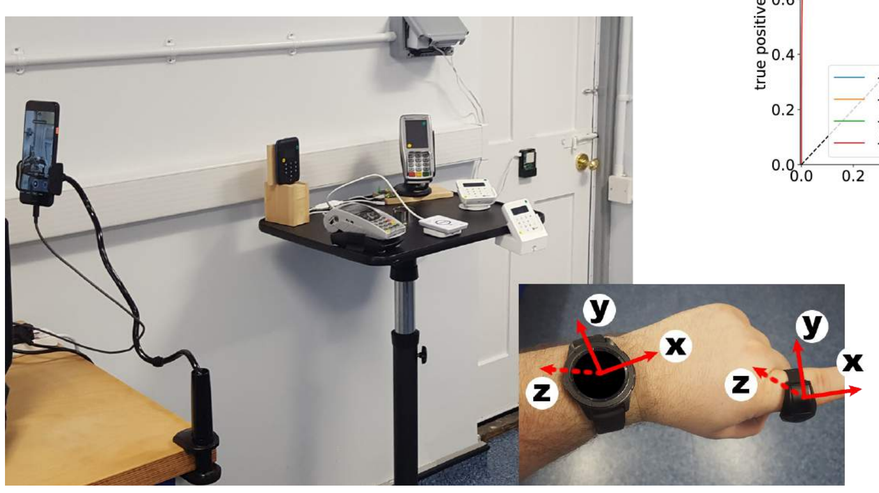


- Subset of users (n=6) returned after 18 months
- EERs worsened by only 3 percentage points when tested on new samples, showing stability over time



- Subset of users (n=9) collected 17 hours of non-tap gestures from daily activities
- Intent-to-pay inferred from gesture recognition
- Used as a defence against skimming attacks
- EERs of 0.03, AUROC 0.99 for intent recognition





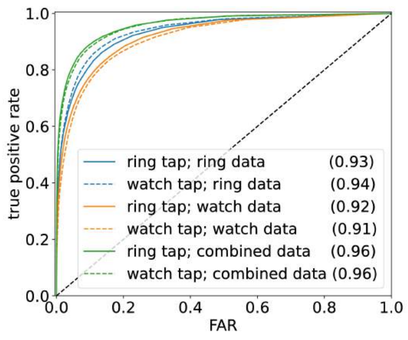
RingAuth [2]

As smart ring technology evolves and ring-based services start to require greater confidence in the identity of the user, they will require authentication capabilities. The tiny form factor of a smart ring restricts its input capabilities, which would make password- or PIN-based authentication user-unfriendly. To address this, we investigated the use of inertial sensors for ring-based systems.

- User study (n=21)
- Smart ring and smartwatch worn on the same arm
- Collected 510 gestures from each user

- Payment context: users made **tap gestures** with each device
- Inertial sensor data from each device treated separately
- Same approach as WatchAuth for each
- EERs of 0.06, AUROC 0.96 for user authentication

- Access control context: users made **knock gestures** against a door while wearing the devices
- Knocking in sets of three, sets of five, and in a 'secret knock' pattern of the user's choosing
- EERs of 0.02, AUROC 0.98 for user authentication



- Inertial sensors on the 'smart door'
- Very little data, surprisingly promising results
- EERs of 0.17, AUROC 0.82 for user authentication

- Inertial sensor data from either device can be used to authenticate gestures made with either device
- Each can be used as a second (or primary) factor for the other

References

[1] J. Sturgess, S. Eberz, I. Sluganovic, and I. Martinovic. “WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch”, IEEE European Symposium on Security and Privacy (EuroS&P), 2022.
[2] J. Sturgess, S. Birnbach, S. Eberz, and I. Martinovic. “RingAuth: Wearable Authentication using a Smart Ring”, arXiv preprint arXiv:2301.03594, 2022.
[3] J. Sturgess, S. Köhler, S. Birnbach, and I. Martinovic. “CableAuth: A Biometric Second Factor Authentication Scheme for Electric Vehicle Charging”, Symposium on Vehicle Security and Privacy (VehicleSec), 2023.

PETRAS
UKRI
SSL Systems Security Lab
UNIVERSITY OF OXFORD

Own Your Vehicle Data

Tooska Dargahi, Manchester Metropolitan University,
T.dargahi@mmu.ac.uk
Meisam Babaie, University of Leeds,
M.babaie@leeds.ac.uk

INTRODUCTION

- by 2035, there will be over 850 million connected vehicles in the world [Statista]
- Each vehicle generates over one terabyte of data per hour
- The dataset comprises a wide range of data, including geolocation and driving patterns
- Global revenue from data monetisation could reach $750 billion by 2030 [McKinsey]
- This data can be monetised by selling to stakeholders, such as insurers and fleet management companies
- Individual data owners often gain minimally in this ecosystem, with many unaware of how their valuable data is being monetised by various stakeholders

WHY - RELATED WORK

Some projects and research studies in the literature have proposed architectures for data sharing and/or trading in the IoT domain, including connected vehicles.

Problem:

- Main existing architectures are centralised: posing several challenges, including a single point of attack and failure.
- Scalability and performance challenge: a central trusted authority exists to perform the user registration and authorisation, or they use symmetric key encryption, which requires secure key management.
- In limited previous studies, the data owners can exert control over their data. However, the data owners can "deny" critical consumers' access to data, which is unreasonable in real-world scenarios.
- Certain entities, such as manufacturers and authorities, require access to specific types of data for legitimate purposes, including safety applications and accident analysis.

AIM

Two main research questions are considered in this research:

1. How can we provide transparency and give ownership to users, enabling them to have full control over their data and the ability to monetise their data?
2. Considering that some organisations need to have access to this data for functionality and safety purposes, how can this be facilitated without the data owners' ability to intervene?

We designed a novel privacy-preserving owner-centered data trading model:

- Categorise the data consumers into 'primary' and 'secondary' consumers
- Classify the data types based on the requirements of the critical applications
- Establish smart contracts between the data owners and consumers
- Use cryptographic algorithms to enforce fine-grained access control, ensuring the minimum access requirements of critical applications
- Attribute-Based Encryption (ABE) mechanism is used for the primary consumers
- Identity-Based Encryption (IBE) is used for the secondary consumers

EXPECTED IMPACT

While there is a growing financial interest in vehicle data through the concept of "data monetisation", the data producers are often neglected. On the other hand, granting full control to the data producers presents a challenge for certain organisations, such as legal authorities, in accessing critical data.
The expected output of this project is:

- a decentralised vehicle data marketplace with suitable privacy safeguards, tailored to the unique data collection and processing requirements within this industry.

METHODOLOGY

Our proposed model consists of four different groups of entities, which we refer to these groups as layers:

- (1) Data Production Layer,
- (2) Data Storage Layer,
- (3) Smart Contract Layer,
- (4) Data Consumption Layer.

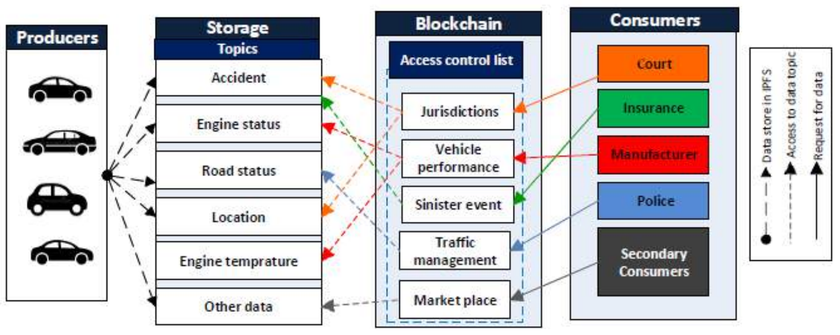


Figure 1: A schematic example of the components in each layer, and the interaction between them.

Data Production Layer
Connected vehicles reside in this layer, and it is assumed that these vehicles generate various types of data.

Data Storage Layer
We consider the InterPlanetary File System (IPFS) protocol for storing vehicle data and logs.
IPFS is a peer-to-peer network that enables vehicles to store their data on the nearest node, thus fulfilling the aforementioned conditions more effectively compared to the cloud or other external servers.
We assume that the data is encrypted and labelled before transmission to IPFS.

Data Consumption Layer

(1) Primary consumers: requiring access to the data for critical purposes such as vehicle functioning, safety, and legal requirements.
(2) Secondary consumers: potential data consumers willing to pay for access to the data. This group includes researchers, advertising companies, other vehicles, and any other organisation or individual in need of vehicle-generated data.

Smart Contract Layer

- Functions for registering the vehicle ownership contract, controlling data access, managing payments, and facilitating communication between the owner and the consumer.
- Higher security and integrity, as well as the establishment of trust in a trustless environment.
- This layer has three primary smart contracts:
  (1) certificate SC,
  (2) permission SC,

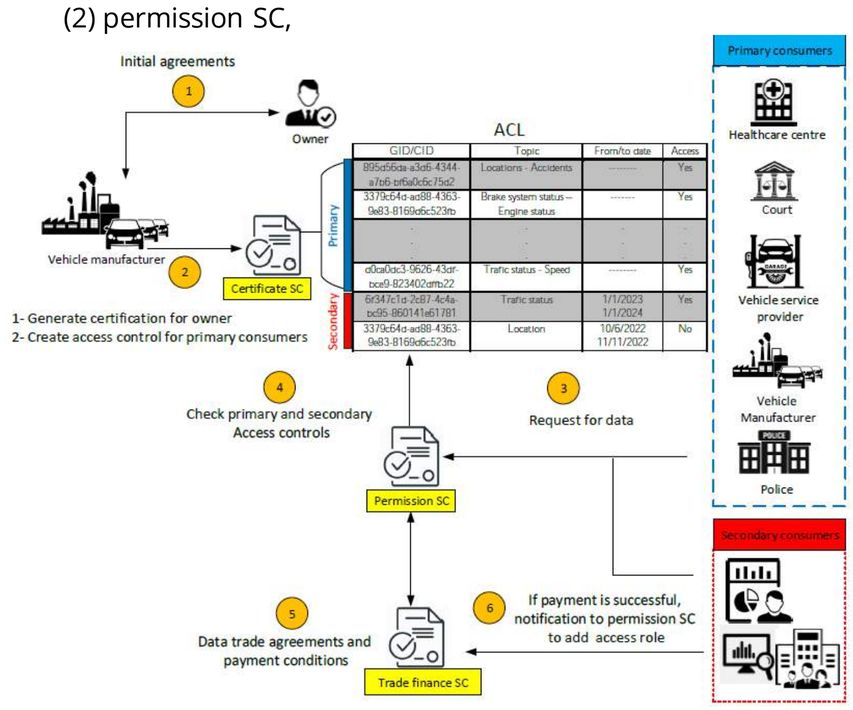


Figure 2: An exemplary scenario to demonstrate the function of

KEY FINDINGS

Figure 3 compares the time consumption of different cryptographic operations and required time for data storage in the system.

- In Case 1, primary customers use their attributes-based keys to access their required data items and decrypt them.
- In Case 2, vehicles encrypt requested data items with the identity of the secondary customers; they will in turn use their

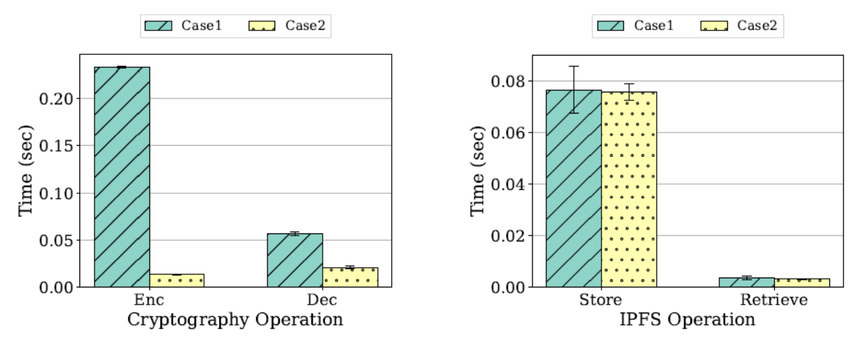


Figure 3: Required time for cryptographic operations (i.e., encryption and decryption) and data storage (i.e., IPFS)

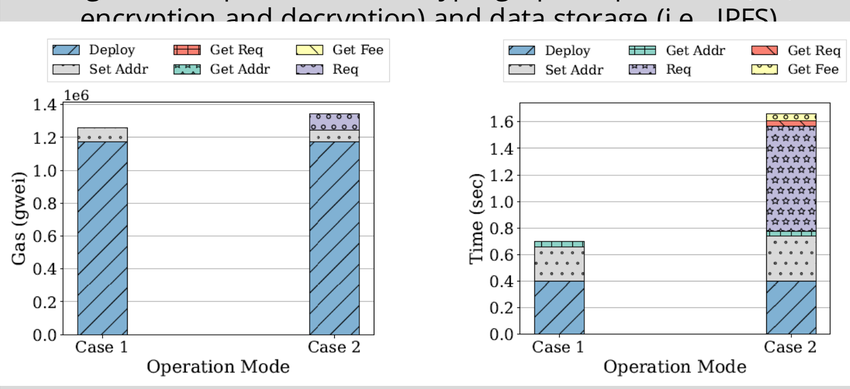


Figure 4: The gas consumption and required time of contract operations in Cases 1 and 2.

Figure 4 shows that setting an address consumes between 0.07 × 10^6 to 0.09 × 10^6 units of gas, submission of a request consumes 0.1×10^6 units, and deployment of the contract 1.1×10^6 units.
We also can see that basic operations (i.e., deployment, setting an address, and getting an address) are similar in both cases. The operations, respectively, consume 0.4, 0.26-0.34, and 0.34-0.39 seconds.

CONCLUSIONS

In this study, we addressed the issue of connected vehicle data monetisation and data privacy.

- RQ1 (regarding transparency and users' data ownership): we propose a scalable and fault-resilient blockchain based solution.
- We implemented a decentralised architecture for storing and exchanging data, as well as handling payments.
- RQ2 (concerning granting critical access to relevant organisations): we propose the usage of a set of smart contracts.
- These contracts enable vehicle owners to maintain full control over their data in a fine-grained and privacy-preserving manner, while also providing transparent access to legal and governmental entities.

- Our proposed model has low overhead in terms of run-time, cryptographic operations and blockchain-related computations.
- Our proposed model achieves a 23 times speed-up in encryption time and a 3 times speed-up in decryption time through consumer differentiation and the adoption of the IBE method.

Future research direction:

- Exploring the utilisation of private blockchain and sharding

PETRAS
UK Research and Innovation
UCL