National Edge AI Hub

Artificial Intelligence Theme

Data Quality and Model Quality Challenges

The vision of WS4 is to establish research directions for **developing fundamental concepts** and techniques **that can guard the data and AI algorithm learning quality against cyber-disturbances** impacting the EC architectures

Team: Newcastle, Durham, Hull, Swansea, and QUB

represented by

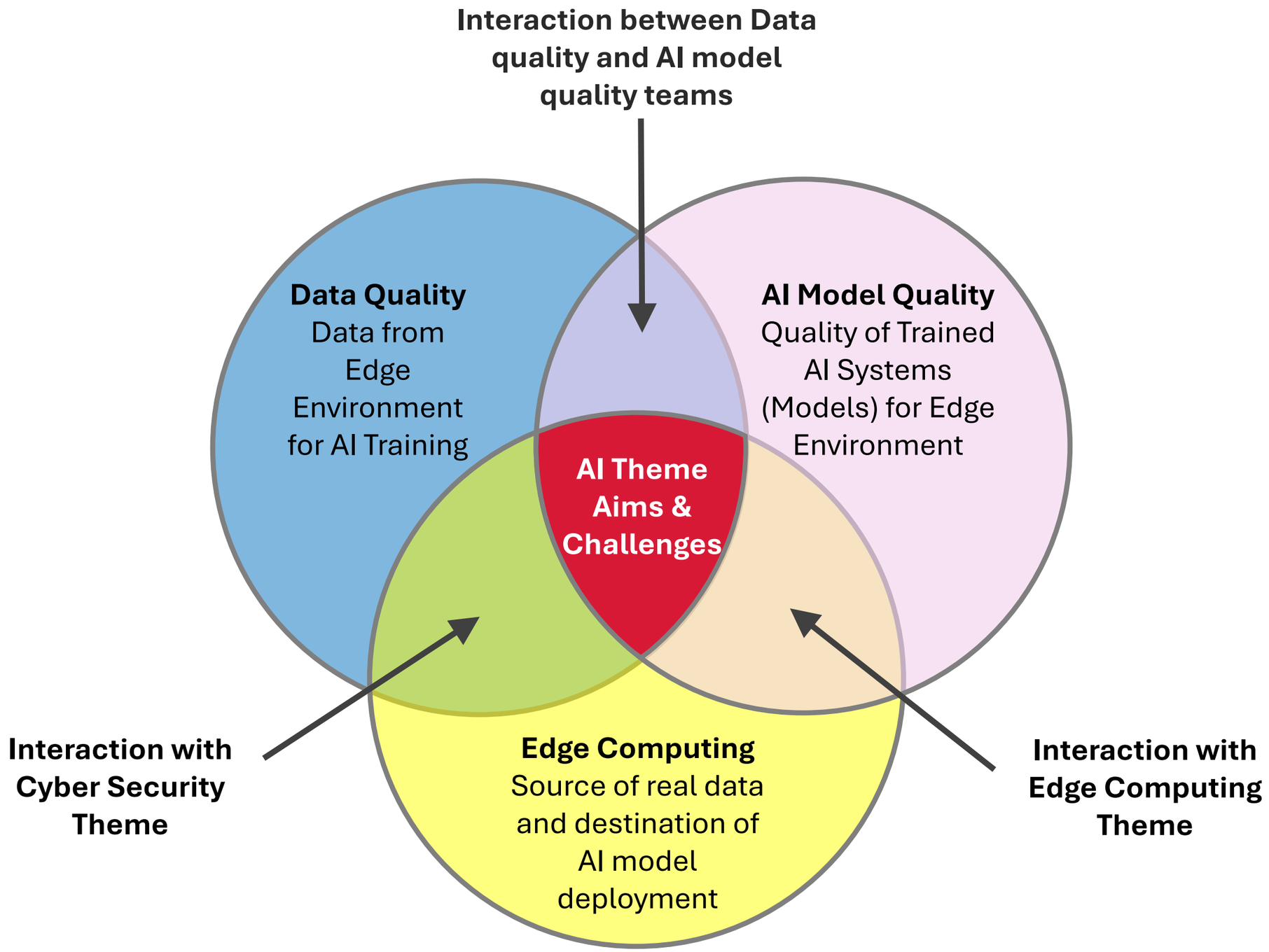
Dr Varun Ojha

@

National Edge AI Hub Lunch Day, Newcastle University, UK

3 May 2024

National Edge AI Hub



National Edge AI Hub

AI Theme Challenges / Research Aims

- **Monitoring of Data/Model Quality**

  How to monitor cyber-disturbances impact AoD, AI algorithms learning quality and the overall application resilience?

- **Recovery of Data/Model Quality**

  How to recover/ensure data and AI model quality that are impacted by cyber-disturbances and ensure suitability for AI model deployment on devices at Tiers 1, 2 of EC architectures ?

- **Assurance of Continuity of Data Quality and Model Quality**

  How to AI algorithms continually adapt to EC environments where unknown cyber-disturbances that were not presented in the original training dataset?

Potential Research Problems

National Edge AI Hub

- **Monitoring**
  - **RP1.** Investigates, characterise, and develop ontologies of data challenges and models challenges for EC environment.
  - **RP2.** Data and model quality assurance to data quality challenges, faults, missing data, hardware failure, sensor degradation; diverse data source; sensor/data heterogeneity.
- **Recovery**
  - **RP3.** Investigates and develop data and model quality certification/robustness to various challenges such as data distribution shift, impurities, adversarial attacks, hardware resources limitations, etc.
  - **RP4.** Investigates the model quality certification/robustness to cyber disturbances, cyber-attacks, on federated/distributed EC environment.
- **Assurance**
  - **RP5.** Data/Model quality verification/assurance. This will aim to identify quality issues with AI models implementation on edge and offer mitigation strategies to resolve the challenges.

Our Smart City Testbench

Newcastle University's Urban Observatory Sensors

>£8 million pounds (Capital investment)

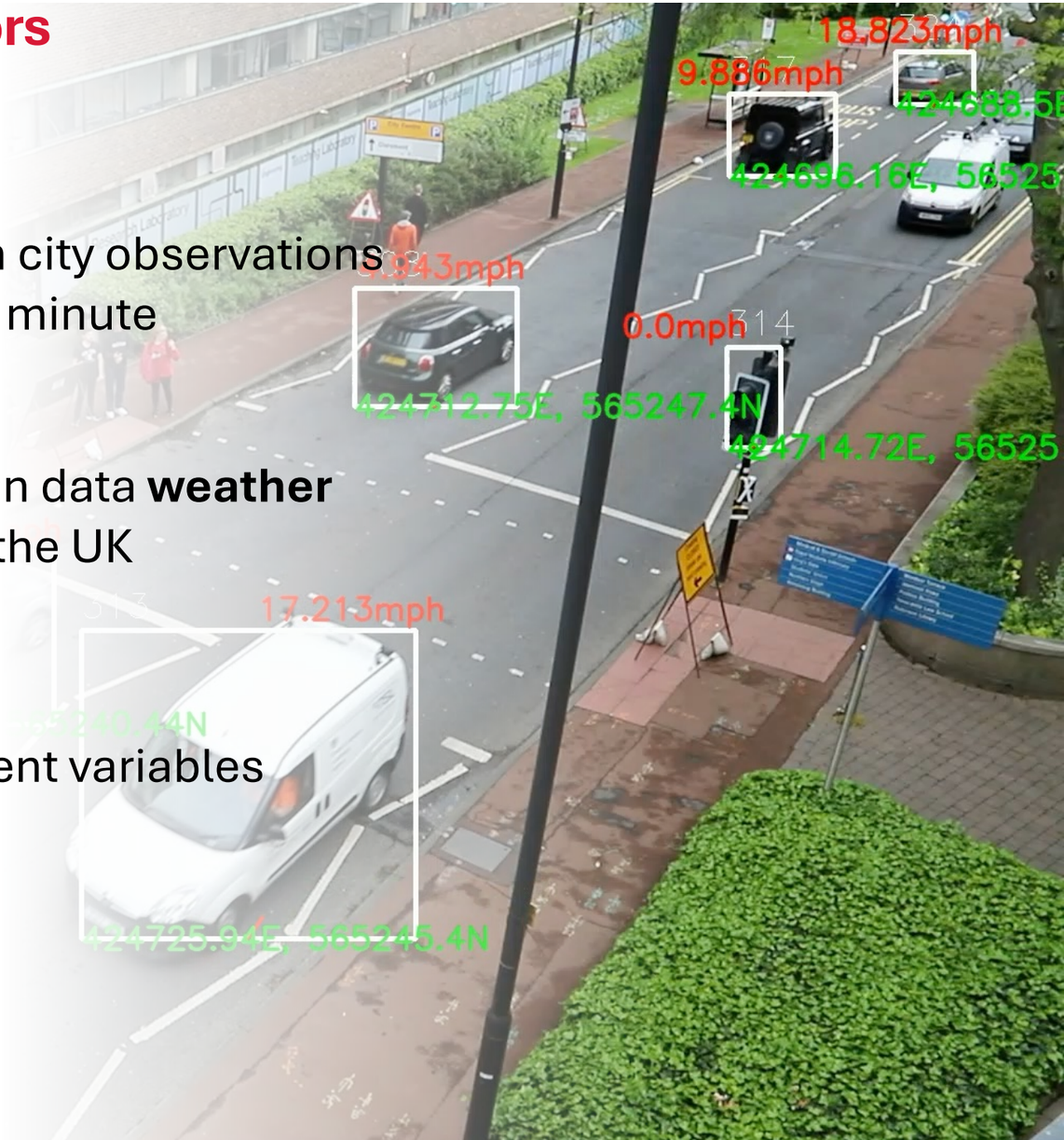
10 billion city observations 10,000 a minute

Billions of smart building observations

Only open data **weather radar** in the UK

CCTV: **500** views, **500m+** images, 24 real-time feeds

65 different variables



Source: Phil et al (Newcastle)

Our Experience with Data Quality Challenges

- **Data quality**
  - degradation of sensors over time
  - anomalous values, random spikes, or environmental issues
  - data out of range, out distribution, uncertainty
- **Data stream issues**
  - data retrieval - source API failure
  - source API failure, network failure, network overload
  - system throughput - queues building up, hardware issues
- **Cyber security**
  - adversarial attacks
  - denial of services, spoofing
- **Failure**
  - hardware failure at sensor

Source: Phil et al (Newcastle)

Data Certification (SafeML) – Example Solution

Trusted dataset for AI model training

Our Solutions:

- **D-ACE** – a framework for certifying training datasets using various characteristics
- **SafeML** – a framework for safety monitoring of ML models at run time

We will extend these to EdgeAI

- D-ACE for certifying datasets in federated Edge AI architecture
- Safety of Federated Learning algorithms in EdgeAI architecture

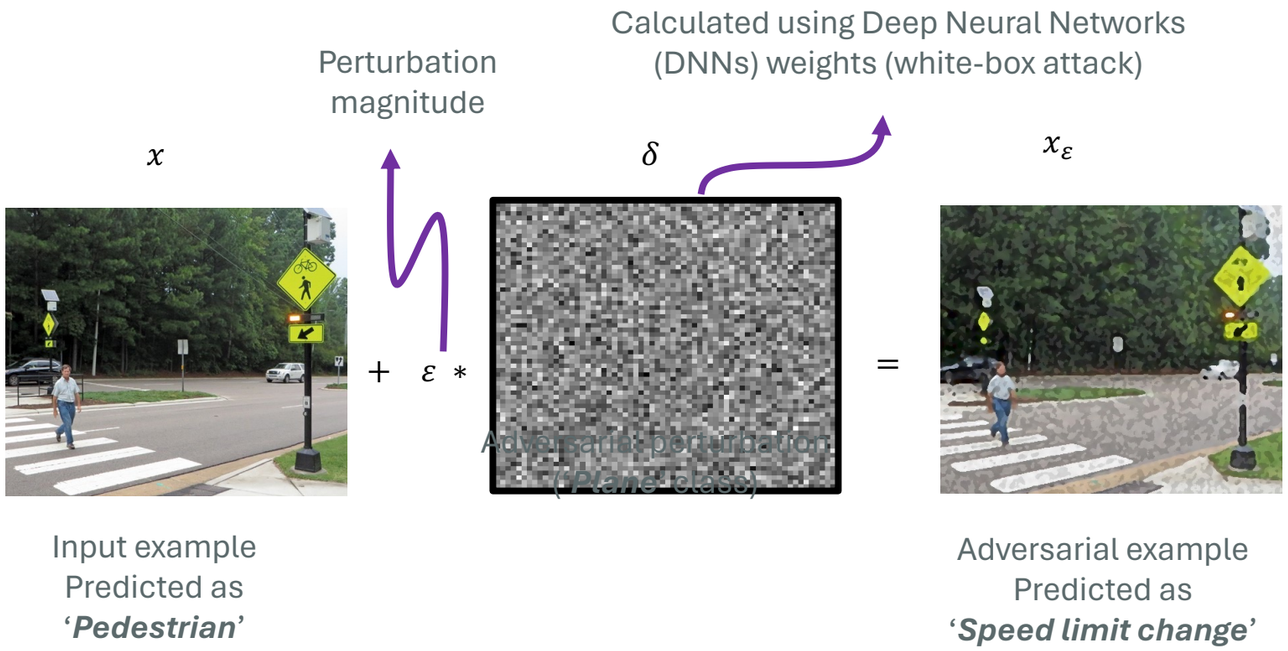
Expectation
AI model training data

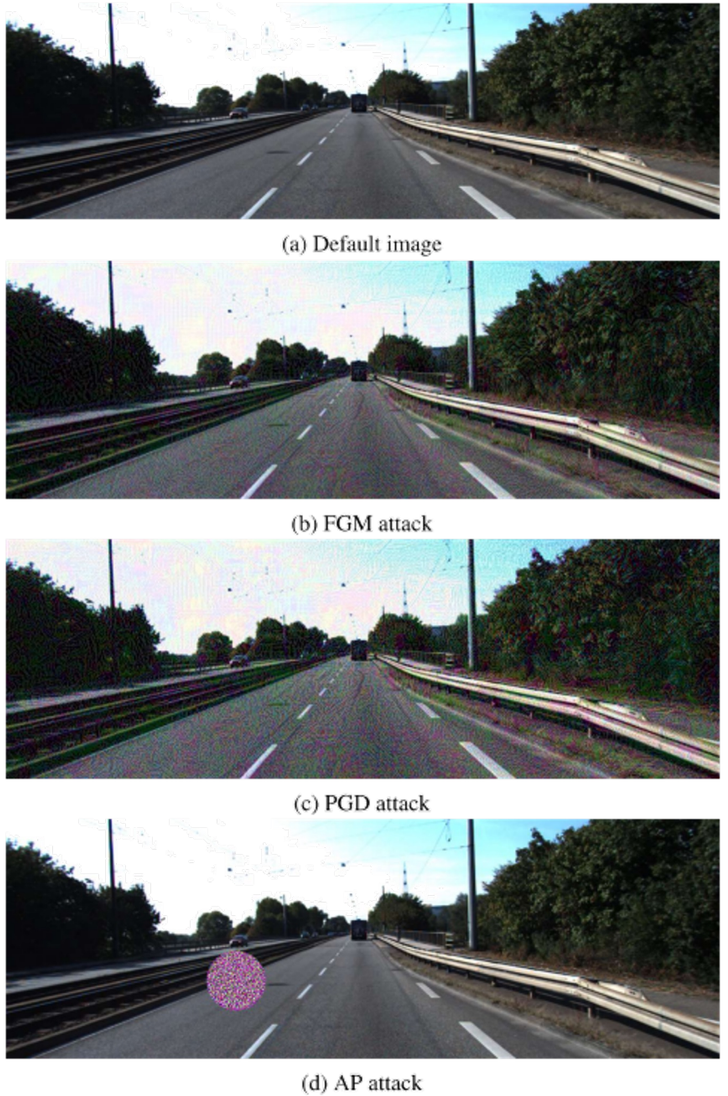
Reality
data in reality for testing AI model

Source: Thakker et al (Hull)

Model Certification – Example Solution

Models adversarial Attacks Mitigation in Autonomous Vehicle and Vehicle to Everting Transportation Communication Scenario





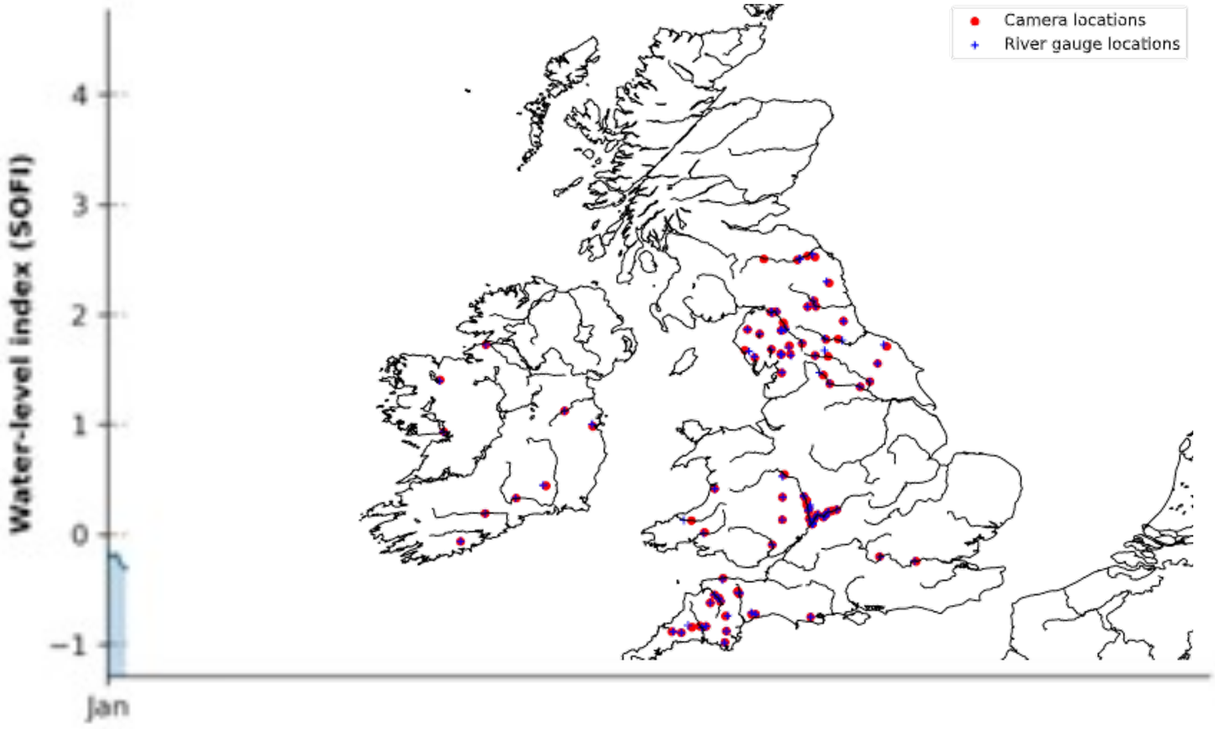
One of objectives of the AI Model Quality analysis is to subject AI model to the '**worst case conditions**' (such as adversarial cyber/attacks) and evaluate the ***ability for a model to remain invariant*** under such settings.

Source: Ojha et al (Newcastle)

Edge AI for Flood Tracking and Monitoring

Fusion of Environmental Agency Data Edge Data (CCTV Cameras) across UK & Ireland

Our research help automat tracking and monitoring of flood saturation

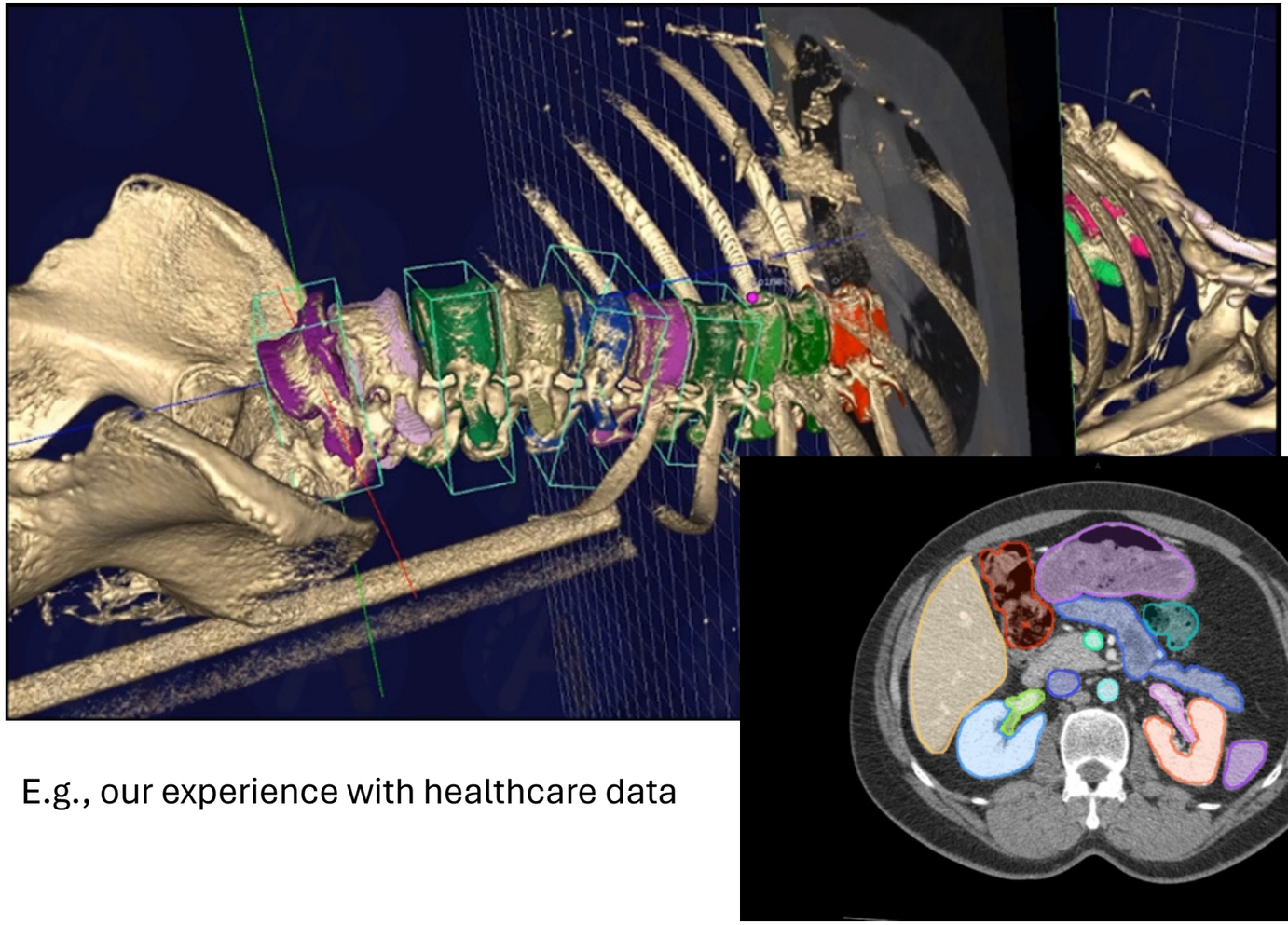


We achieve 94% accuracy in correctly predicting real flood events The River Avon and River Severn.

Source: Ojha et al (Newcastle)

Data and Model Quality Transparency

- **Privacy** Large EdgeAI Model trained by generated data to preserve user privacy and data assets.
- **Transparency** and Trustworthy EdgeAI training is achieved by language and human knowledge systems.
- **Unknown new tasks** or risks can be raised anytime in real-world applications. Our EdgeAI handle them collectively with human experts, grow and become stronger will usage.

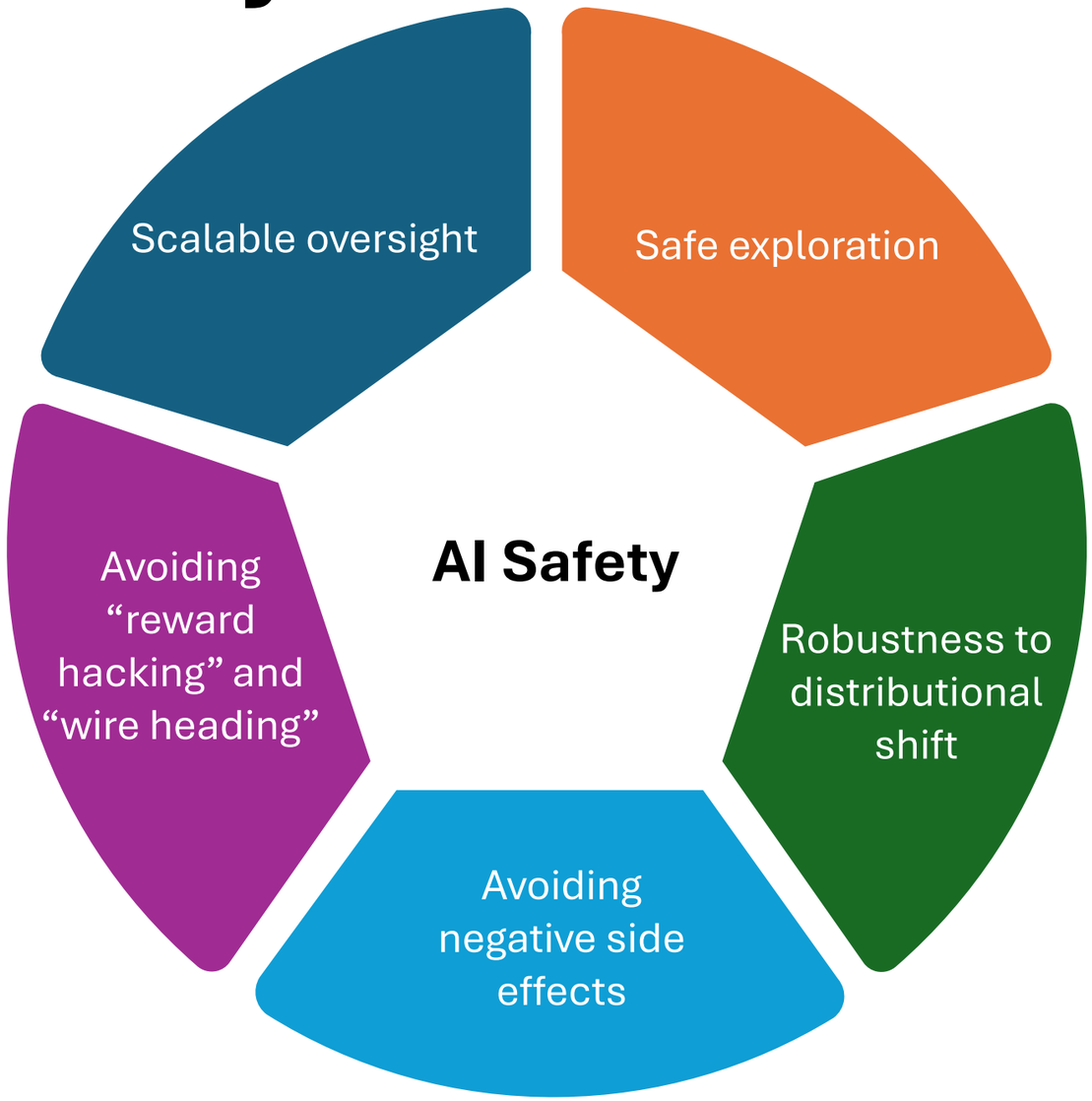


E.g., our experience with healthcare data

Source: Yang long (Durham)

Dimensions of EdgeAI Safety

Our focus has been on robustness to data distributional Shift: Issues related to changes in the AI's operational environment that differ from its training environment, which can lead to unexpected or harmful behaviour.



Source: Thakker et al (Hull)

Team AI

Rajiv Ranjan (Newcastle)
Internet of Things
raj.ranjan@newcastle.ac.uk

Phil James (Newcastle)
Urban Data
philip.james@ncl.ac.uk

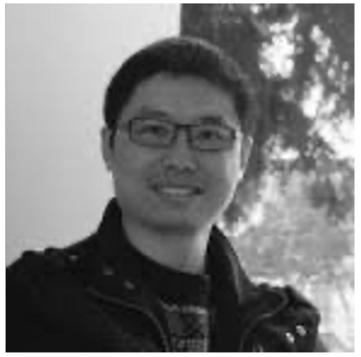
Varun Ojha (Newcastle)
Artificial Intelligence
varun.ojha@newcastle.ac.uk

Mutaz Barika (Newcastle)
Big Data
mutaz.barika@newcastle.ac.uk

Dhaval Thakker (Hull)
AI and Internet of Things
d.thakker@hull.ac.uk

Yang Long (Durham)
Computer Vision
yang.long@durham.ac.uk

Xianghua Xie (Swansea)
Machine Learning
x.xie@swansea.ac.uk



Zheng Li (Queens Belfast)
Software Engineering
zheng.li@qub.ac.uk