Edge AI and Cyber-Disturbances

cerc 2024

THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Omer F. Rana
School of Computer Science & Informatics
Cardiff University, UK
ranaof@cardiff.ac.uk https://www.**linkedin.com**/in/omerrana1/

Figure from:
Manish Parashar

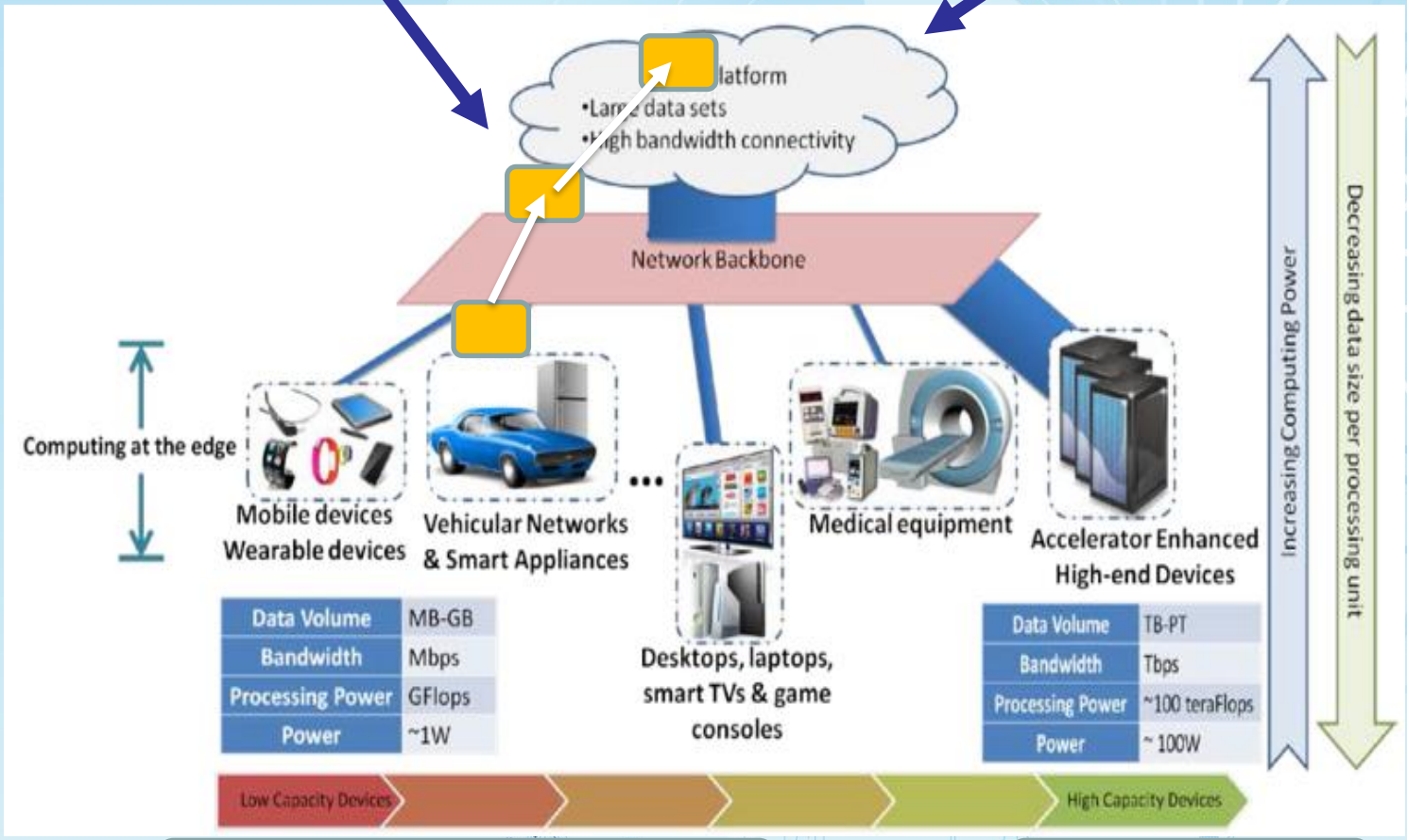
Context

User owned devices

Process automation & controllers

Software Defined Environments

Quantum Cloud Systems



Resource Capability at Network Edge

The "Mobile" Edge (5G/6G and THz)

Edge Analytics

Edge Caching & Data Storage

"Embedded" Edge Computing

Role of Aggregators and Placement

Federated Edge (Learning)

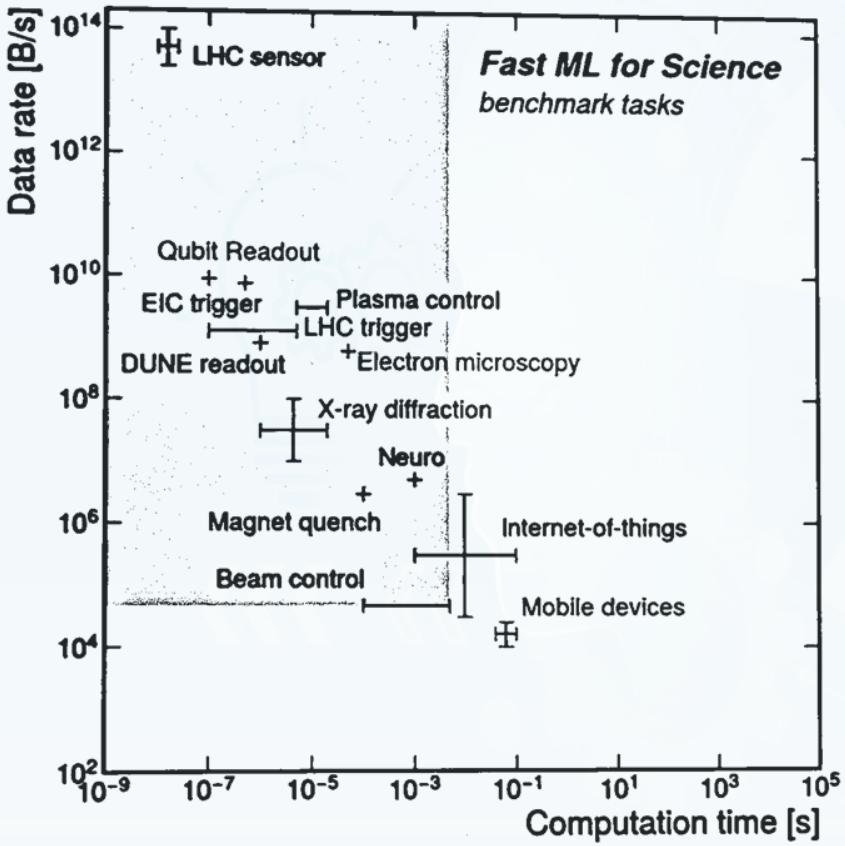
5G/6G: "Internet of Functions"

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

Custom Edge Accelerators & Views from FermiLab

Most collision "events" don't produce interesting physics
"Triggering": filter events to reduce data rates to manageable levels

"Fast" ML at the extreme edge

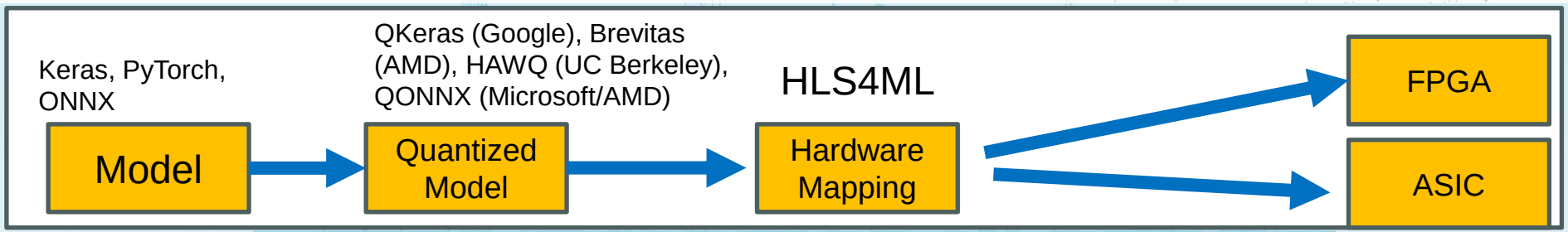


Cutting-edge scientific experiments explore nature at the **finest temporal and spatial scales**

Leads to data rates far surpassing industry
— requires developing **innovative techniques**

- ML in specialized embedded architectures require ***real-time*** processing to reduce and filter data
- Optimal data selection enables **more efficient operation and control, saves lost data, and accelerates time-to-discovery**

Fermilab



“Cyber-disturbances”

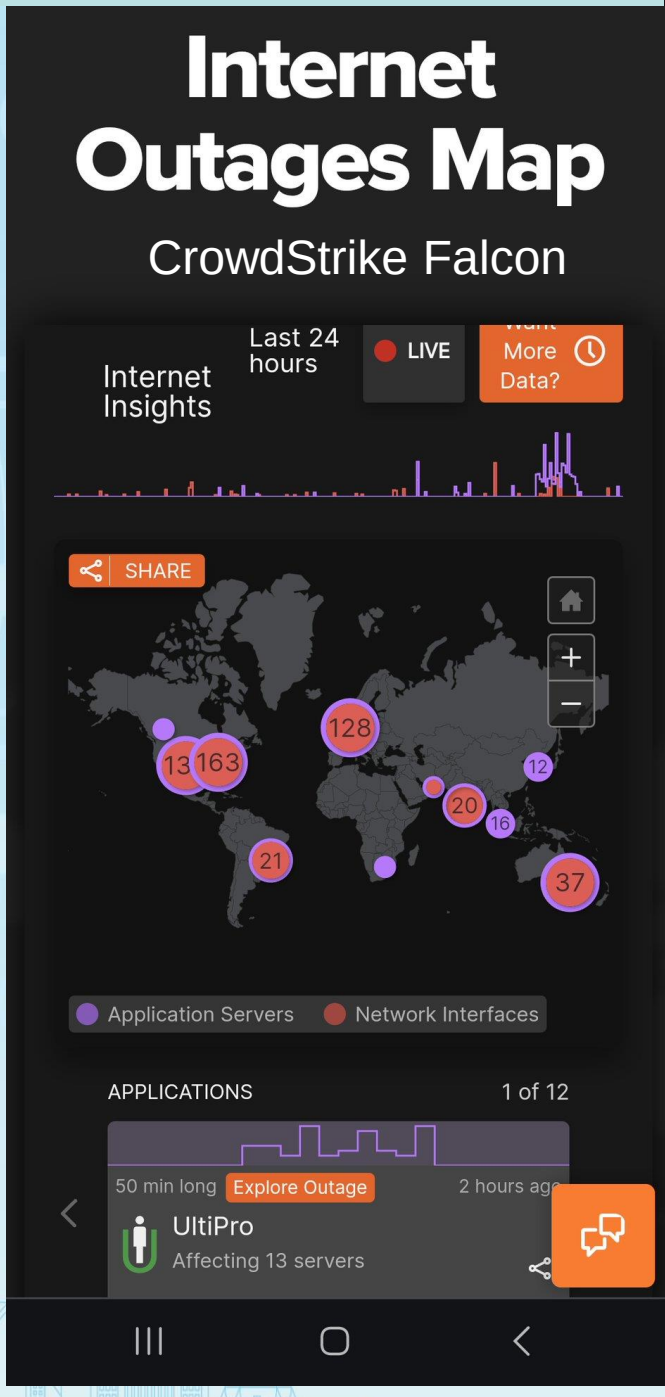
“Cyber-disturbances”: events that lead to incorrect or imprecise working of a system

How do cyber-disturbances affect the integrity and quality of the Machine Learning outcomes and data?

In a distributed system, unpredictable events are bound to happen. Many interacting components

- Hard disks can fail,
- Network can go down,
- a sudden surge in customer traffic can overload a functional component
- Software update can go wrong!

Disturbance Benchmarking & Chaos Engineering



المركز الوطني للأمن السيبراني
National Cyber Security Center

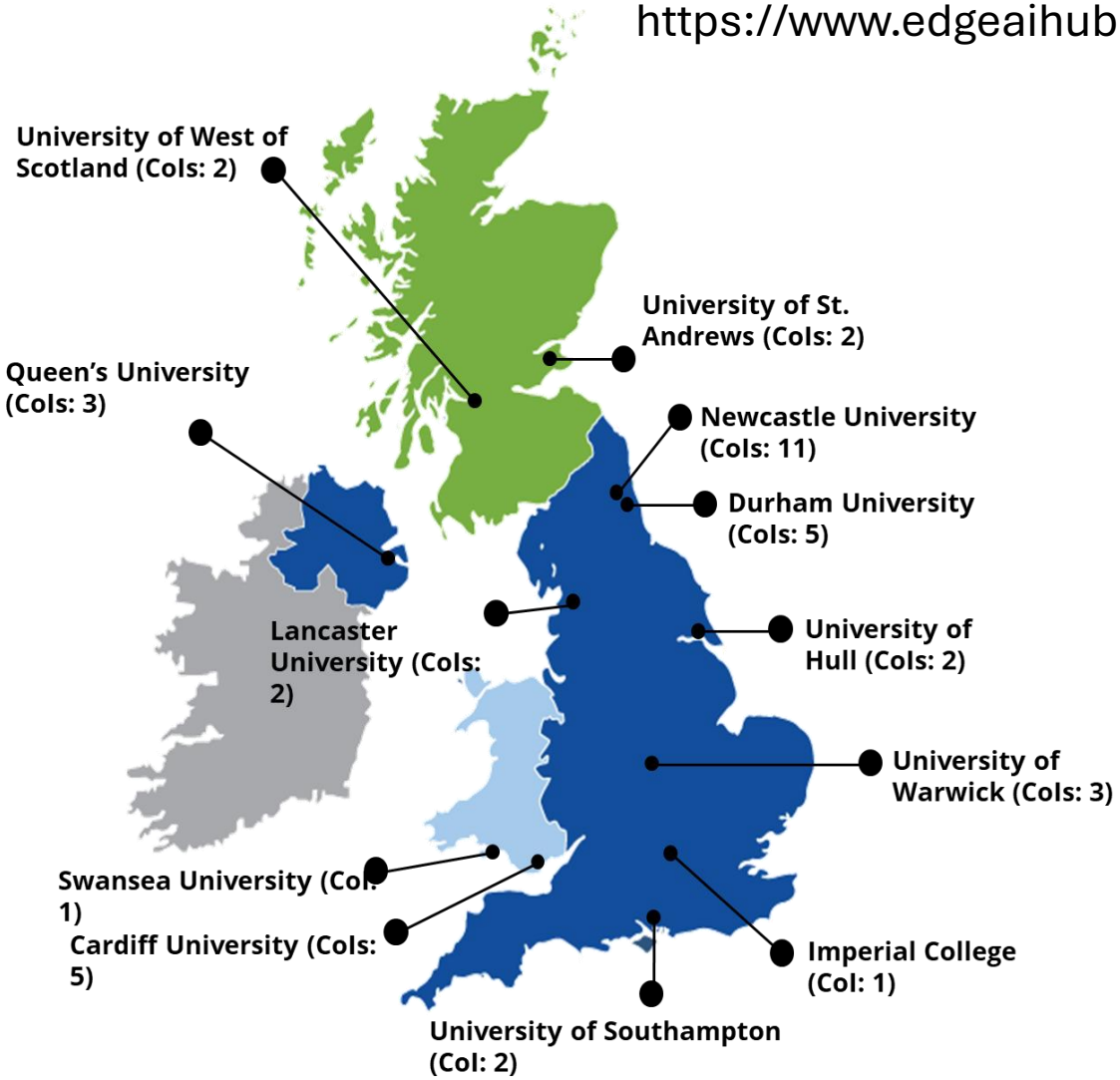
British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY

UK National Edge AI Hub for Real Data: Edge Intelligence for Cyber-disturbances and Data Quality

https://www.edgeaihub.co.uk/



- £12m 5year programme 2024 - 2029
- 12 UK Universities led by Newcastle
- 39 Co-Is, 1 PI – Prof Rajiv Ranjan – Newcastle University
- £100m UKRI Investment Programme – February '24
- 55 Industry Partners and growing

Sectors:
Healthcare
Energy Security
Autonomous Transportation

- Industry led research & Advisory Board

Specialist sectors: **Artificial Intelligence**
Edge Computing
Cyber Security

Industry Partners of Edge AI Hub

National Edge AI Hub

Hardware

DELL
NVIDIA
AMD
orange
GreenWave Technologies

Edge /IoT

life.augmented
acoem
AVSYSTEM
Vortex
Rakuten
SPARK
software AG
LUGANO
connexin
ncs

Innovation Agencies

National Innovation Centre Data
Powered by Newcastle University
CENSIS
National Innovation Centre Ageing
The home of Ageing Intelligence
Voice
CATAPULT Connected Places
THE DATA LAB value from data
Cyngor Abertawe Swansea Council
BMUCO

Healthcare

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Bae Abertawe
Swansea Bay University Health Board
TECHNOLOGY ENABLED CARE
tec CYMRU
NHS

Cyber Security

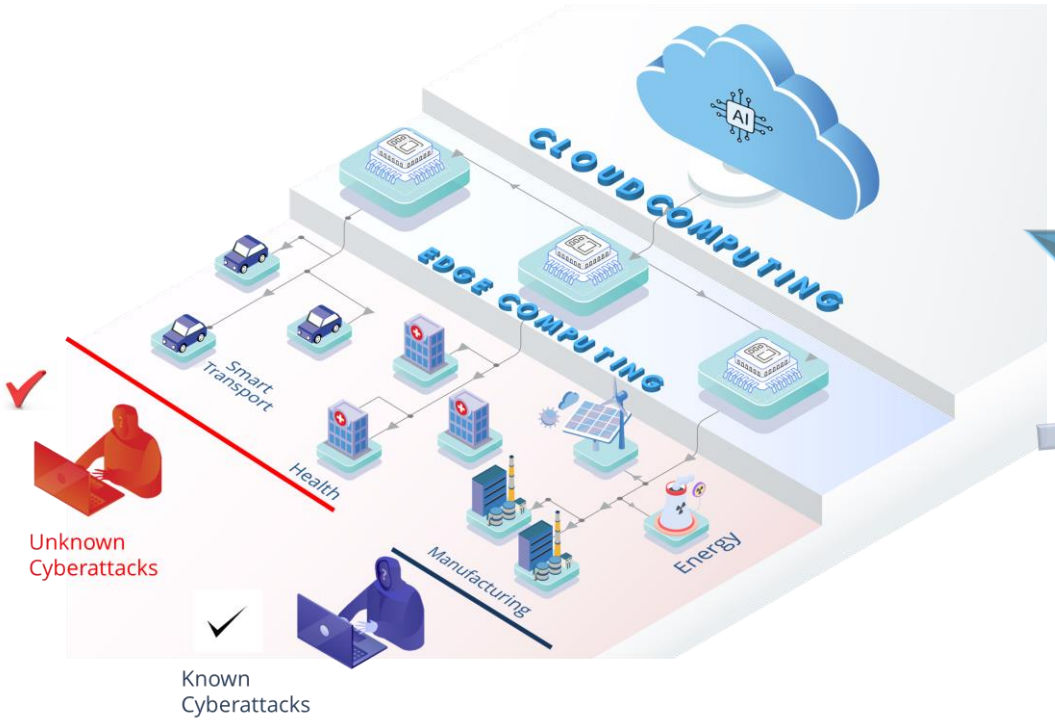
MIRA
SIS DECISIONS
Transmission Dynamics
Adobe
BOSE
intel
SENCODE CYBER SECURITY
EXALENS
DATACTICS

Applied AI

321AI
MY VOICE
nium
EQUANS
PromptxArt
Streets Systems
NWG living water

Supported by 53 organisations in 6 sectors, including 20 new partners after submission

The **Edge AI Hub** aims to deliver world class fundamental research, co-created with stakeholders from other disciplines and regions, to protect the **quality of data** and **quality of learning** associated with AI algorithms when they are subjected to **cyber-disturbances** in the Edge Computing environments.



Data Quality

Missing Data

Partially Complete Data

Duplicate Data

Poisoned Data

Spoofed Data

Noisy Data

Data Leakage

Gradient Inversion

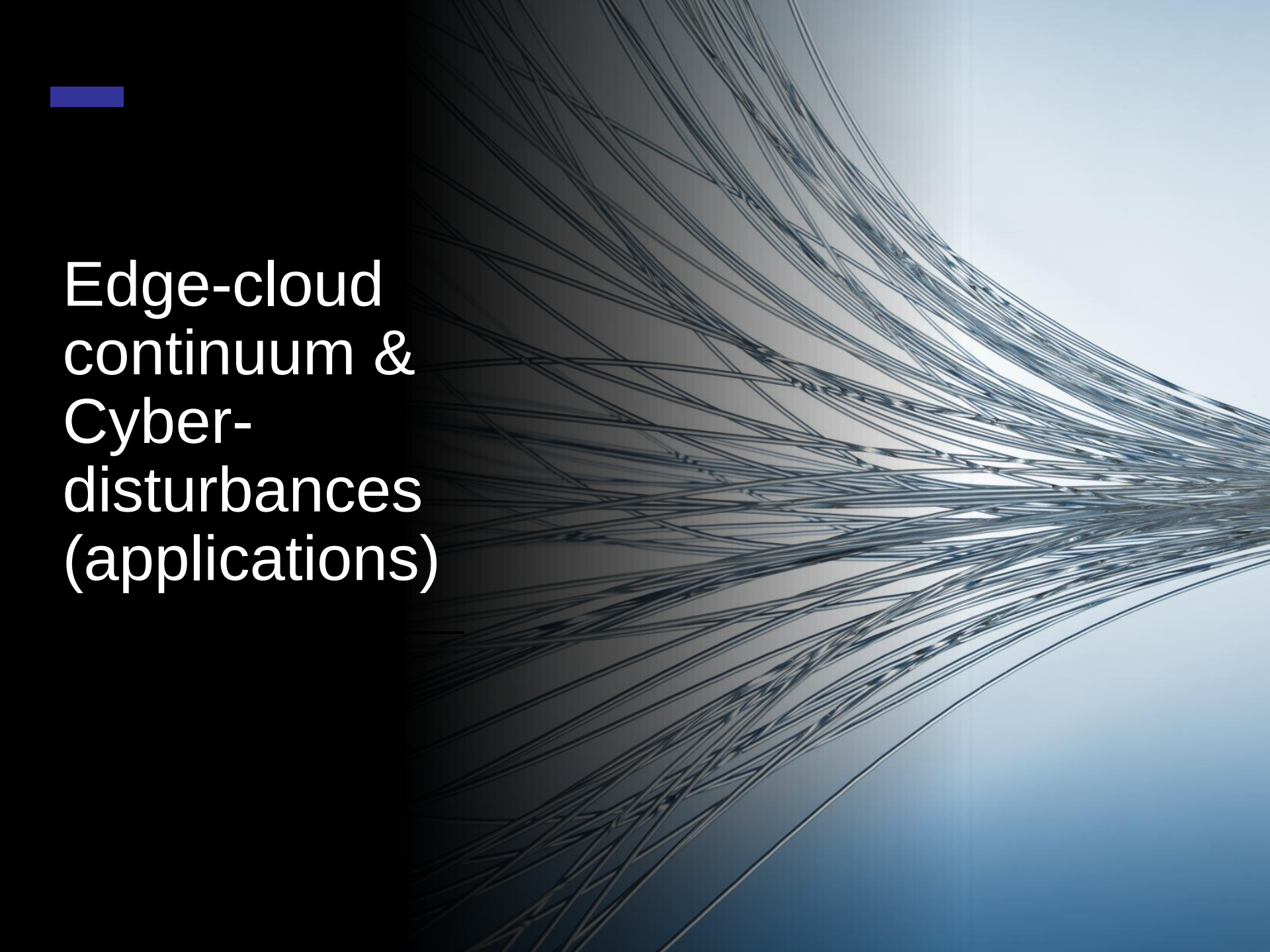
Adversarial Data Injection

Model Extraction Attack

Model Reconstruction Attack

Learning Quality

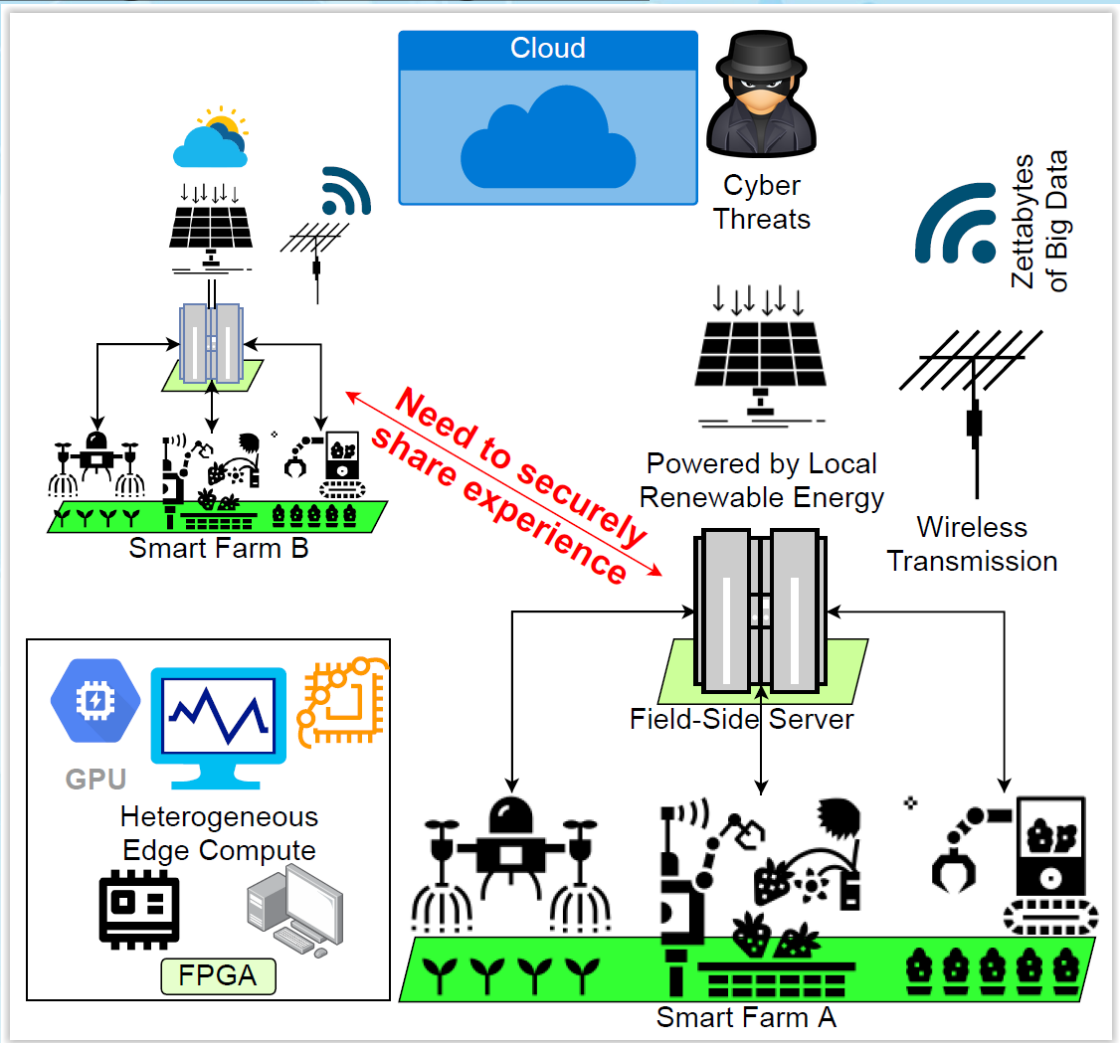
Edge-cloud continuum & Cyber-disturbances (applications)



Edge-Cloud Continuum Challenges

Prioritising the Edge …

- The “rural” challenge
  - Where does “edge” add value
  - Intermittent connectivity
- Orchestration mechanisms that **prioritise the edge**

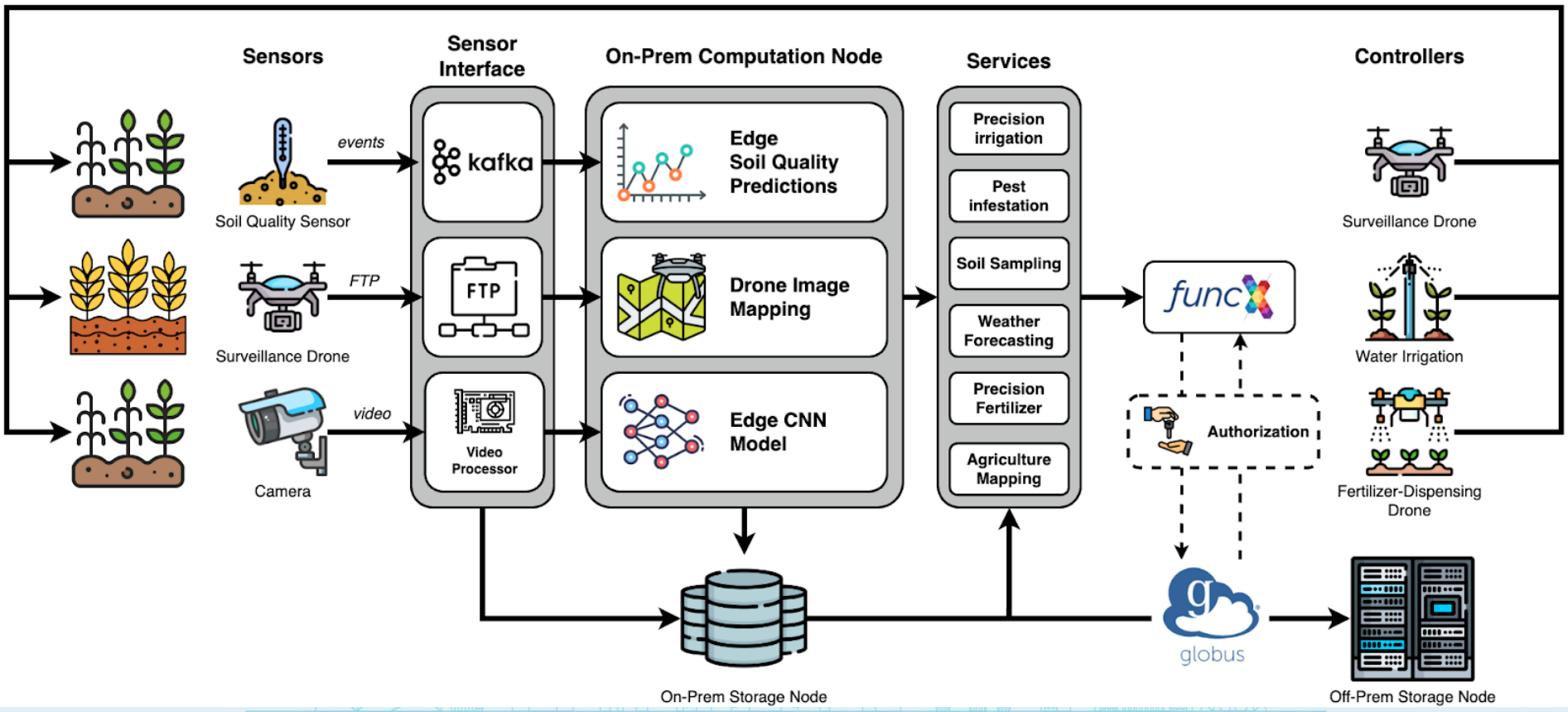


“SHIELD: A secure heuristic integrated environment for load distribution in rural-AI.” *Kaushal, Almurshed, Almoghamis, Alabbas, Auluck, Veeravalli, Rana, 2024. Future Generation Computer Systems: The International Journal of eScience 161, 2024*

“Rural AI: Serverless-Powered Federated Learning for Remote Applications” *P. Patros, M. Ooi,V. Huang,M. Mayo,C. Anderson,S. Burroughs, M. Baughman, O. Almurshed, O. Rana, R. Chard, K. Chard, I. Foster, IEEE Internet Computing, 2022*

RuralAI (https://sites.google.com/view/rural-ai/home)

- Each robot / drone builds a local model (using locally collected data)
- Data combined with other robots or “field side units”
  - Robots and Field Side Units realised as Single Board Computers
- Intermittent connectivity between Robot & Field Side Units



Cloud/Edge-enabled Cameras – Cisco Meraki

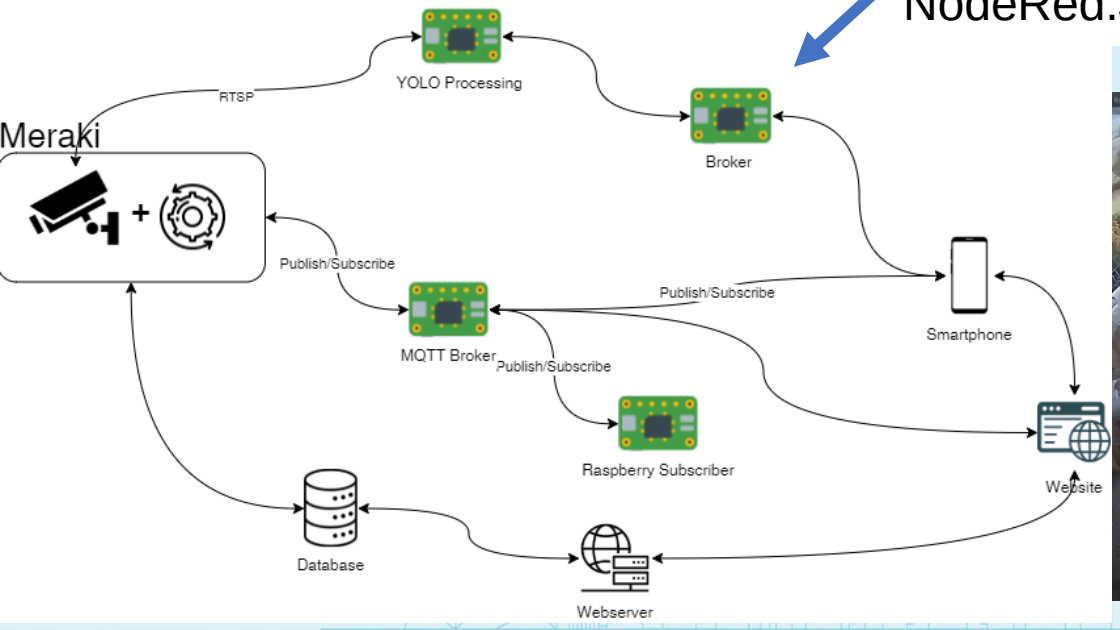
Camera pre-trained on Objects → MQTT stream

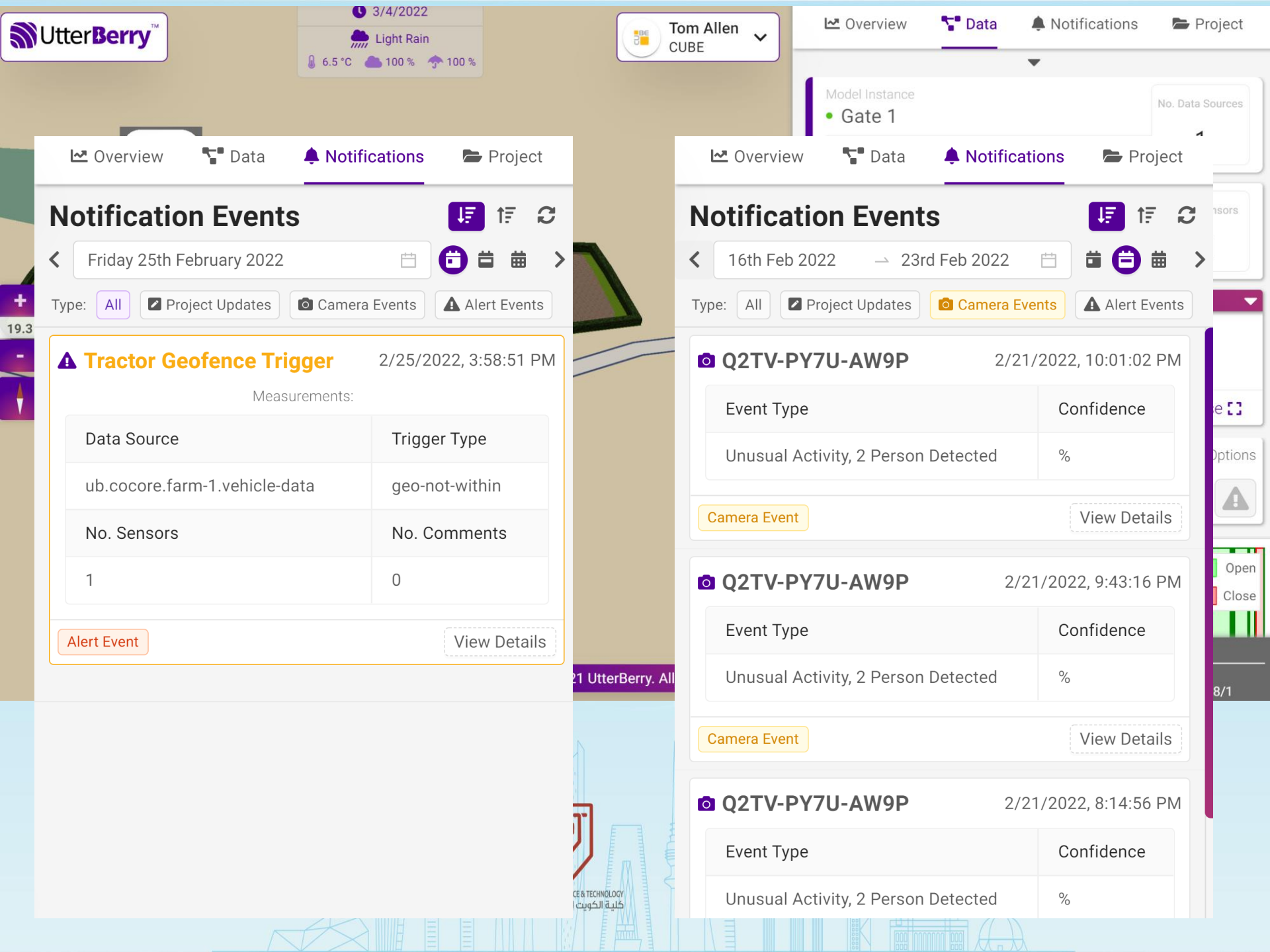
Limited access to real time RTSP stream

Remote management (farms)

5G CoCore Farm Architecture

Deployment of "functions" via NodeRed.JS

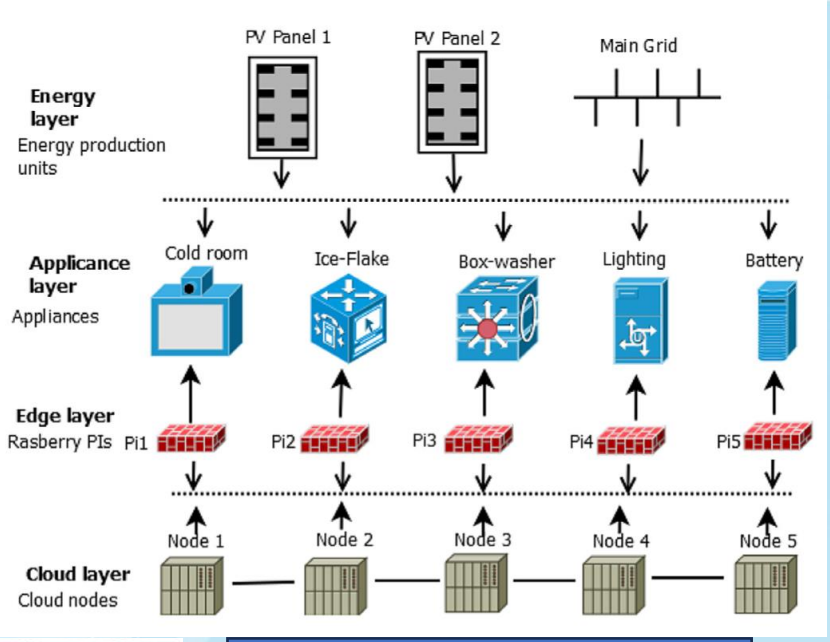


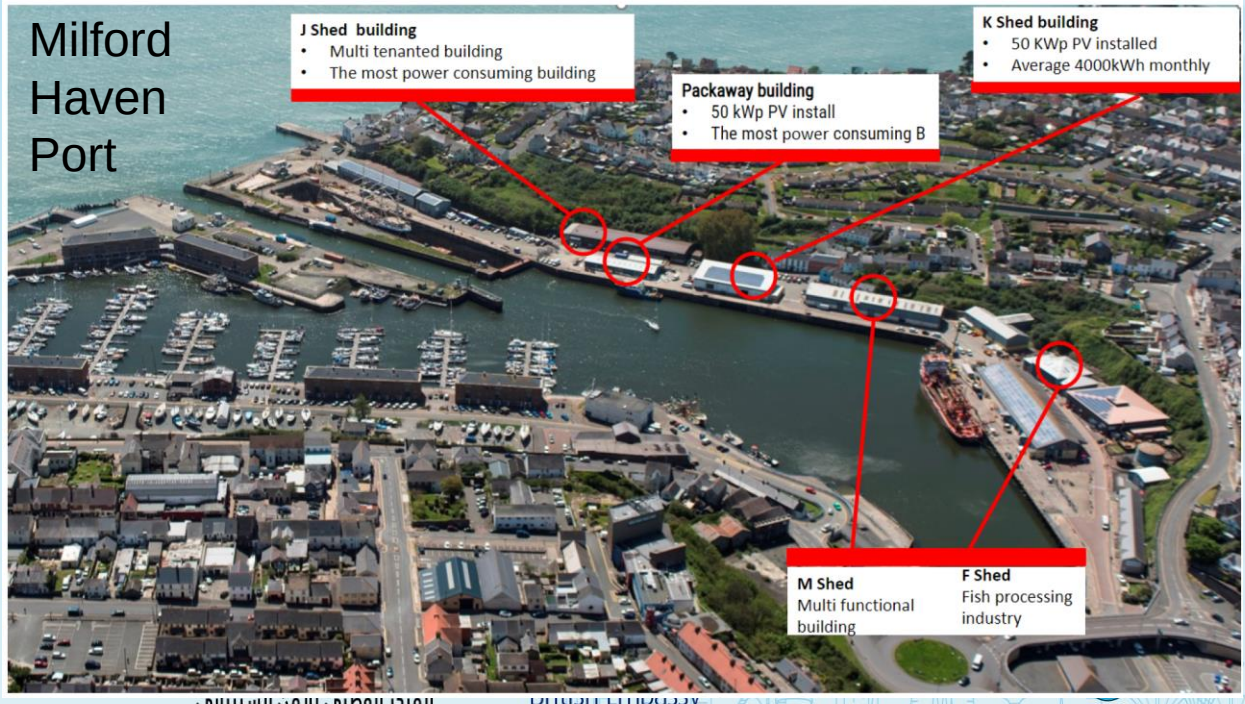

UtterBerry
3/4/2022
Light Rain
6.5 °C
100 %
100 %
Tom Allen
CUBE
Overview
Data
Notifications
Project
Model Instance
Gate 1
No. Data Sources
Overview
Data
Notifications
Project
Notification Events
Friday 25th February 2022
Type:
All
Project Updates
Camera Events
Alert Events
Tractor Geofence Trigger
2/25/2022, 3:58:51 PM
Measurements:
Data Source
Trigger Type
ub.cocore.farm-1.vehicle-data
geo-not-within
No. Sensors
No. Comments
1
0
Alert Event
View Details
Overview
Data
Notifications
Project
Notification Events
16th Feb 2022
23rd Feb 2022
Type:
All
Project Updates
Camera Events
Alert Events
Q2TV-PY7U-AW9P
2/21/2022, 10:01:02 PM
Event Type
Confidence
Unusual Activity, 2 Person Detected
%
Camera Event
View Details
Q2TV-PY7U-AW9P
2/21/2022, 9:43:16 PM
Event Type
Confidence
Unusual Activity, 2 Person Detected
%
Camera Event
View Details
Q2TV-PY7U-AW9P
2/21/2022, 8:14:56 PM
Event Type
Confidence
Unusual Activity, 2 Person Detected
%
Open
Close

Use of Cloud Security Alliance Methodology to identify resources within a federation

Effectiveness of federation manager in aggregating resources

Metrics: Capability, Competence and Decision criteria – **Cyber disturbance a key concern in this instance**





Utilise "Edge Energy" when available

Prioritise execution of tasks based on availability of edge energy generation

Ahmed, Petri, Rana, "Edge-cloud resource federation for sustainable cities". *Sustainable Cities and Society* 82, 2022

What is at the “Edge”? (Pisces Proj.)

Packaway building

Solar panel with 50 kW capacity

Appliance	How it is works
1.Box washing machine	Power capacity 50Kw. It is used to clean boxes after use for a short period
2. Lighting system	Lighting system: 17 double tubes (25 W each). Used at night for a short period
3.Flake ice	Flake ice produces small pieces of ice for use in the cold storage to preserve the fish. It consumes about 32 Kw of power.
4.Cold storage	Cold storage is under operation all the time. Considered the most power-consuming device in the building. This is because of the low temperature needed (-5 degrees).

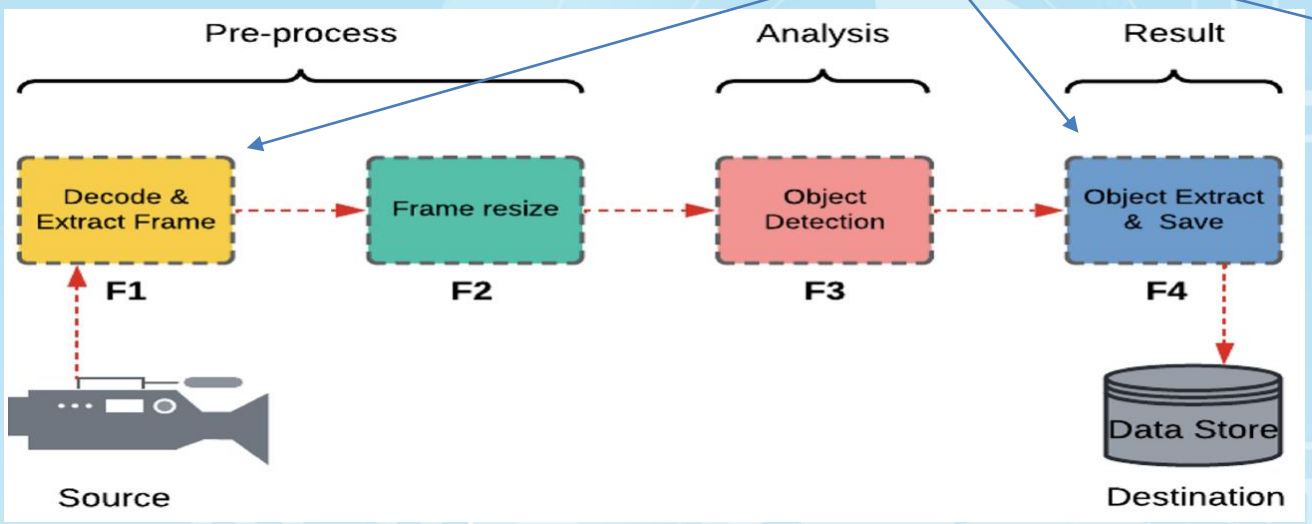
Box washing machine

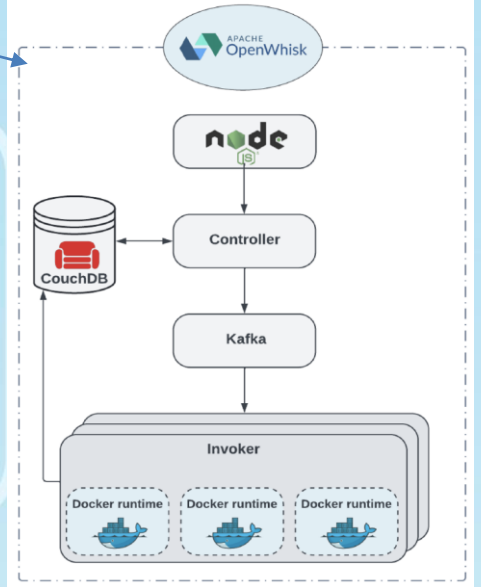
Cold room

Flake ice

Appliance	Power Rating	Minimum Run Time (mins)	Interruption	Required Usage	Required Start Time
Box washing machine	50 KWh	30	Not Possible	Once a day	Between (6:00-16:00)
Ice Flake machine	30kWh	60	Possible	Twice a day	Between (6:00-16:00)
Cold storage room	30kWh	180	Possible	Twice a day	Between (0:00-23:45)
Lighting system	25 W/per tube	60	Possible	Twice a day	Between (0:00-23:45)

Realised as “functions” Using OpenWhisk





To analyze the factors contributing to overall latency, including initialization time and execution time:

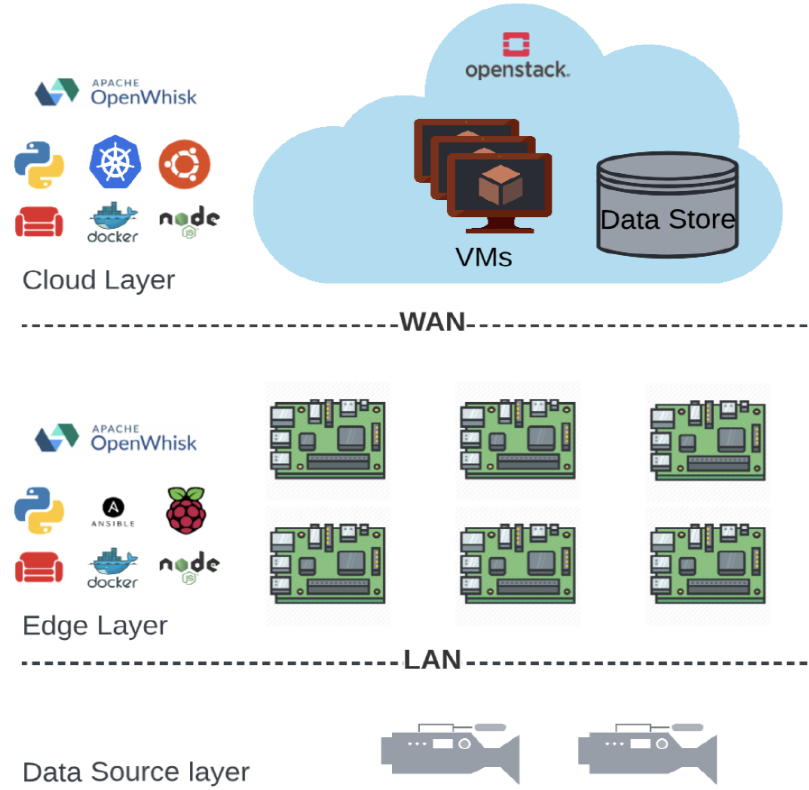
1. Cold and warm activation
2. Input size and memory setting.
3. CPU architecture.
4. Runtime packages used.
5. Rate of concurrent invocations.

- Hardware specifications:

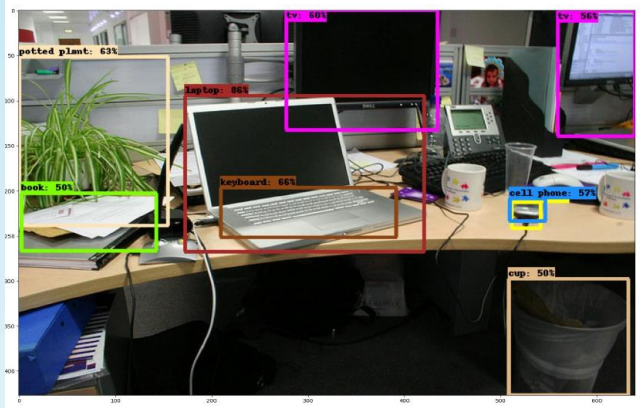
Location	No. of Nodes	Processor	Architecture	Cores	RAM
Cloud (VMs)	3	Intel Xeon	x86_64 GNU	2(vCPUs)	4GB
Edge (RPis)	6	Cortex-A72	armv7l GNU	4(vCPUs)	4GB

- Software specifications:

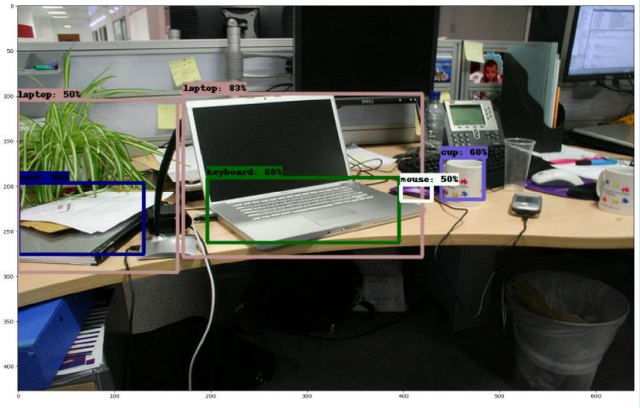
Software	Edge	Cloud
OS	Raspbian GNU/Linux 11 (bullseye)	Ubuntu 20.04.3 LTS (Focal Fossa)
OpenWhisk	incubator-openwhisk(Lean version)	1.0.0 (full version)
WSK CLI	0.10.0-incubating	v1.2.0
Ansible	2.7.9	-
Helm	-	v3.9.0
Kubernetes	-	1.20.15
Docker	20.10.16	20.10.12
Python	3.7 &3.9	3.7 &3.9
OpenCV	4.6.0-dev (Lite version)	4.6.0
TensorFlow	Lite & full(2.2.0)	Lite & full(2.9.1)



Full



Lite



Impact of Cold and Warm Activations

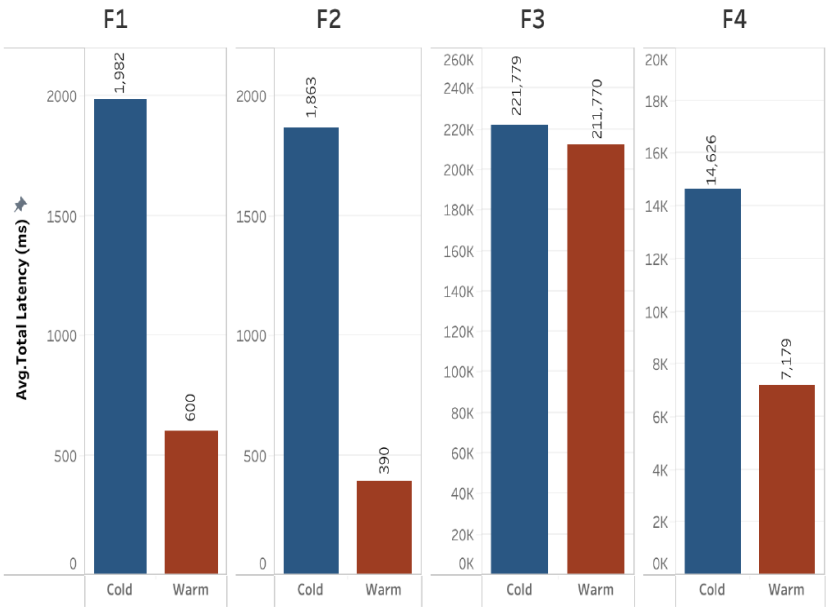


Figure: Cold and Warm activation on RPi.

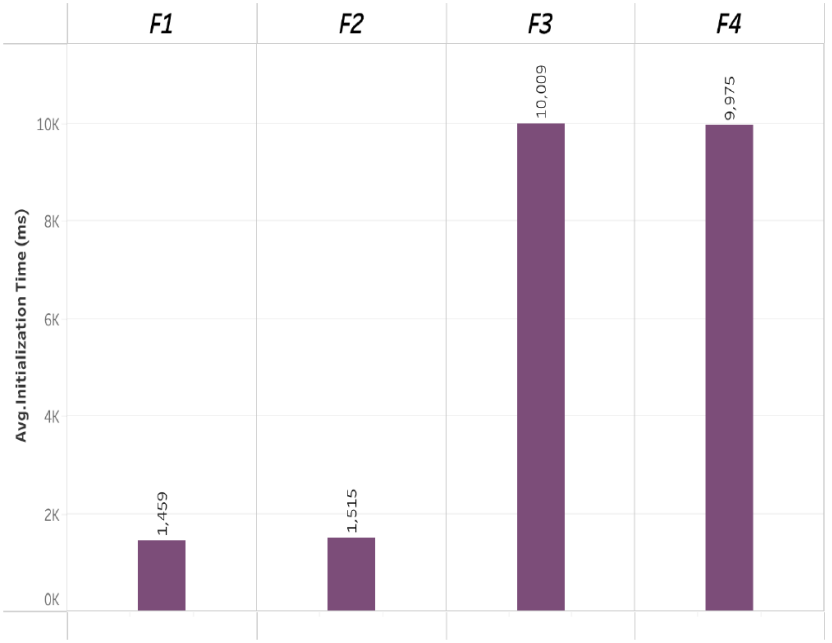


Figure: Initialization time on RPi

Alabbas, Areej, Kaushal, Ashish, Almurshed, Osama, Rana, Omer , Auluck, Nitin and Perera, Charith. ***Performance analysis of Apache openwhisk across the edge-cloud continuum****. 16th International Conference on Cloud Computing (CLOUD), July 2023, Chicago, USA*

Impact of Input Size and Memory Setting

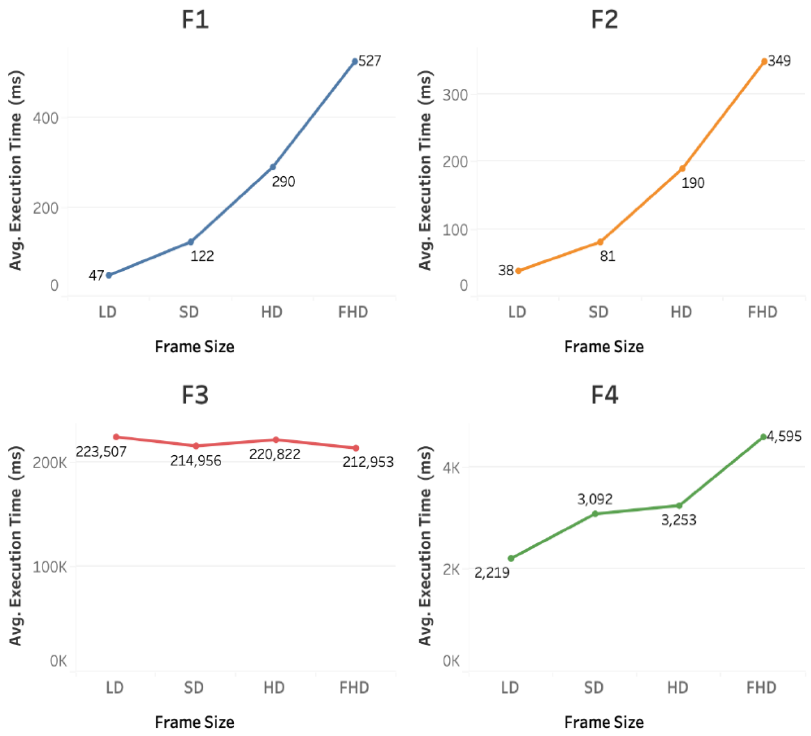


Figure: Execution Time for the different frame sizes on RPi.

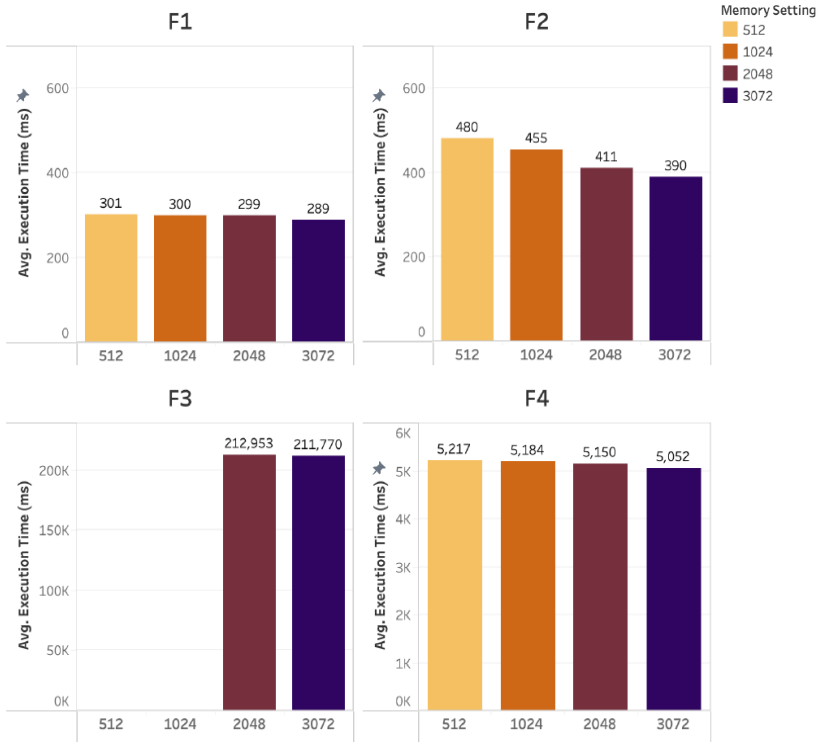


Figure: Execution Time for different memory settings on RPi

Cybersecurity → Cyber-disturbances

- **Cyber-disturbance modelling, detection and mitigation mechanisms**
  - Application and context dependent
  - Reliance on electrification in vehicles → traffic jams when electricity grid fails

- **Predicting cyber-disturbance and proactive handling**
  - Likelihood of occurrence: based on performance degradation, function launch variability
  - Intermittent & variable speed connectivity

Concluding Comments

- Cloud-Edge continuum – a key deployment mechanism for many (future) applications
- Cyber-disturbances and resilience a key requirement
  - The cause of the disturbance can be many, the outcome on the system is important
- Both modelling and deployment mechanisms are important
- Cyber-disturbance benchmarking
  - Align with work in Chaos Engineering