Summary of Research Activities

Cycle XXXI (31)

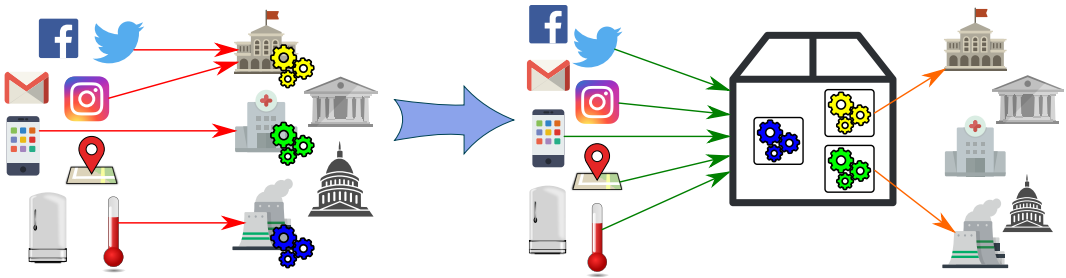
Yousef Amar
QMUL Supervisor: Hamed Haddadi
UNIGE Supervisor: Fabio Lavagetto

UNIVERSITÀ DEGLI STUDI
DI GENOVA

2017-10-12

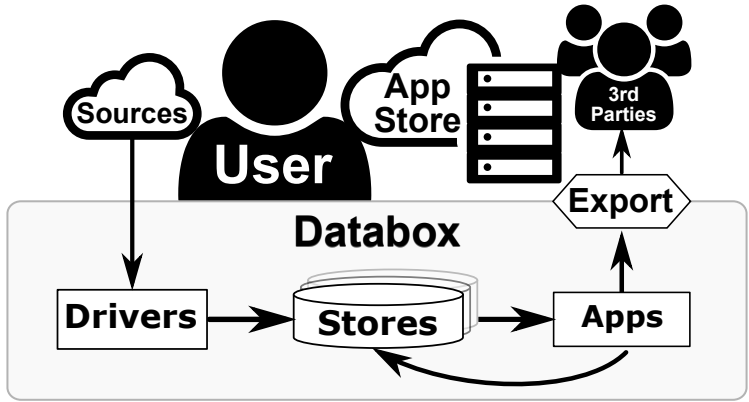
Research Context

The Databox Platform

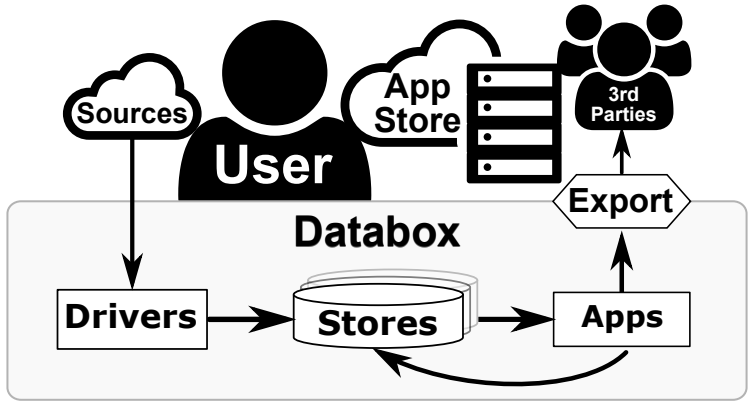


Research Context

The Databox Platform



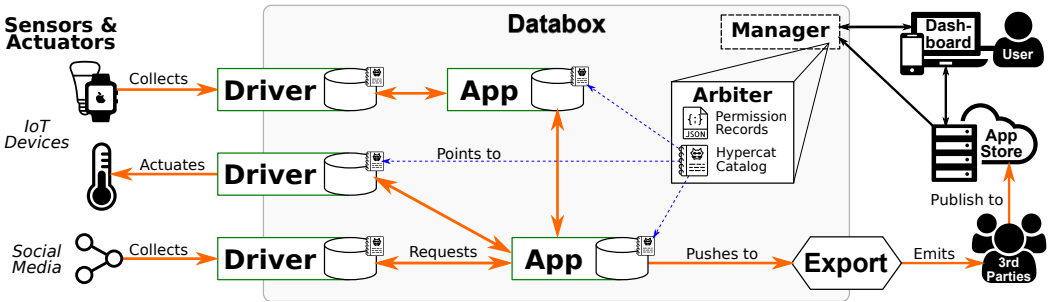
Research Context
The Databox Platform



How can we design safe, scalable access control systems with arbitrary restrictions in this context?

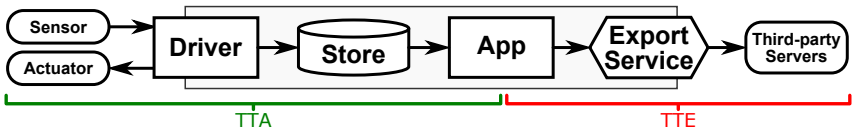
Research Context

The Databox Platform



Evaluation
Platform

- Scalability
  - Resource usage (CPU, memory, network I/O)
  - Inserts/s over stores under maximum load
  - Store launch time with and without arbiter interaction (memory bottleneck)
- Topology
  - Device → Cloud
  - Device → Cloud → Home
  - Device → Home
  - Device → Home → Cloud
- Time to Availability – High-frequency mobile sensors



The Serverless Paradigm

Background

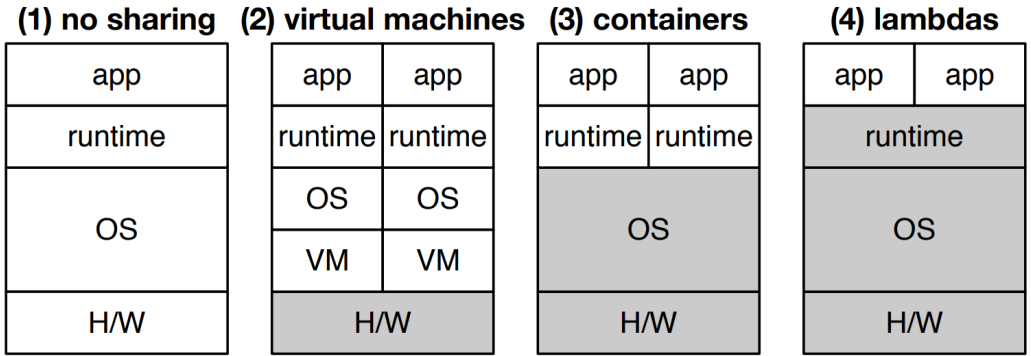


Figure 1: **Evolution of Sharing.** *Gray layers are shared.*

Figure: Hendrickson, et al. "Serverless computation with openlambda." Elastic 60 (2016): 80.

Low-latency Serverless
Approach

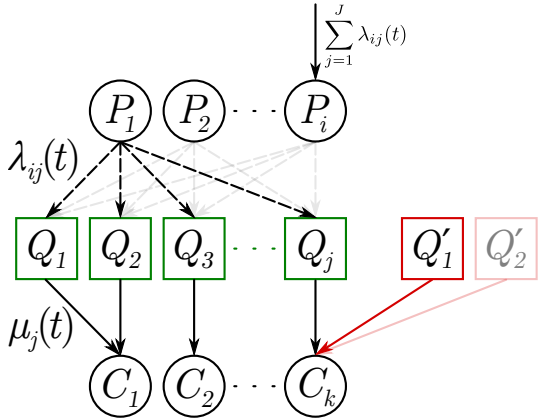


Figure: An Overview of Inter-component Relationships

Low-latency Serverless

Approach

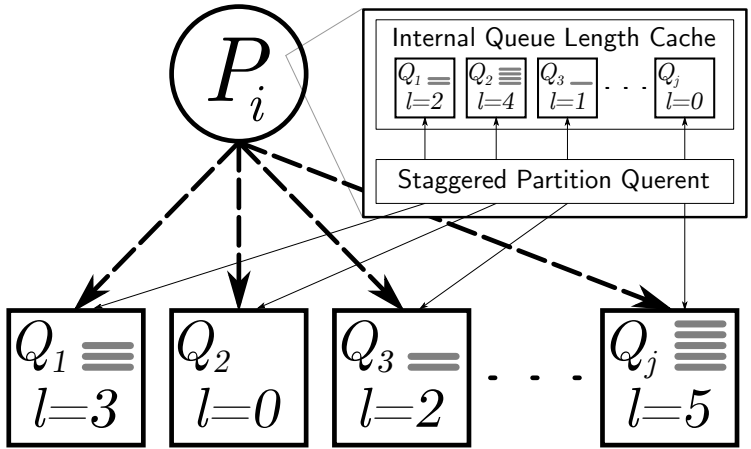


Figure: The Internal Components of a Producer

Low-latency Serverless

Approach

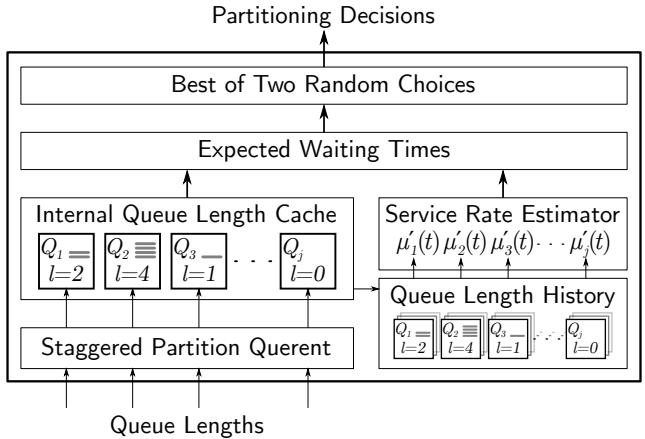


Figure: Producer-intrinsic Steps for Computing Partitioning Decisions from Stale Queue Lengths

Low-latency Serverless
Simulations

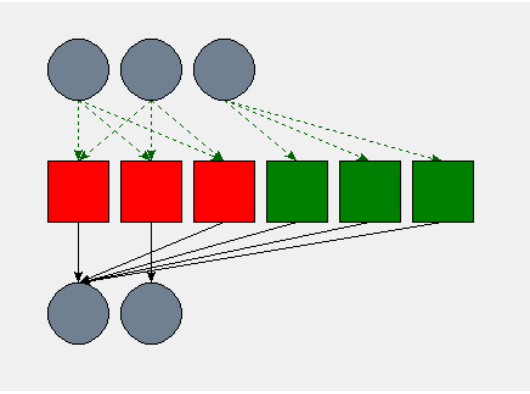


Figure: An Example of Simulation Topology

Low-latency Serverless

Simulations

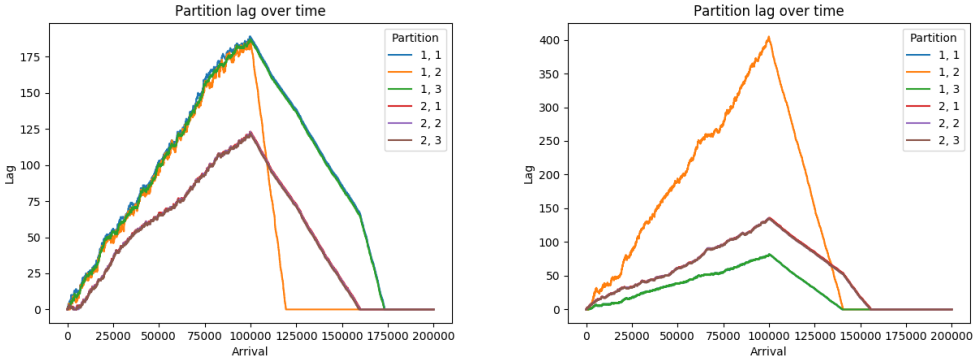


Figure: Simulation Results with Different Partitioning Algorithms

Plans
Privacy and Risk Metrics

- Measuring privacy risk is very subjective
- Information-theoretic, content-independent metrics are generalisable
- Looking just at metadata and schema of personal data, calculate objective metrics:
  - k-anonymity
  - l-diversity
  - t-closeness
- Thresholds can be embedded into tokens – privacy-aware access control for free (!)

Plans
Privacy and Risk Metrics

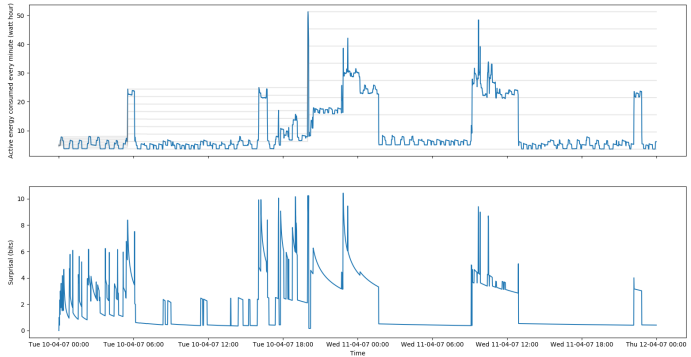
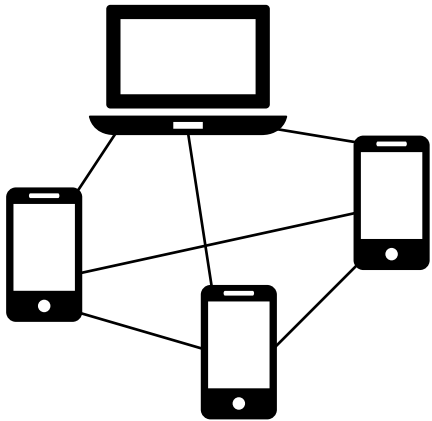


Figure: One Proof of Concept Experiment – Surprisal over Real Smart Meter Data

Plans

Serverless over Transient Clouds

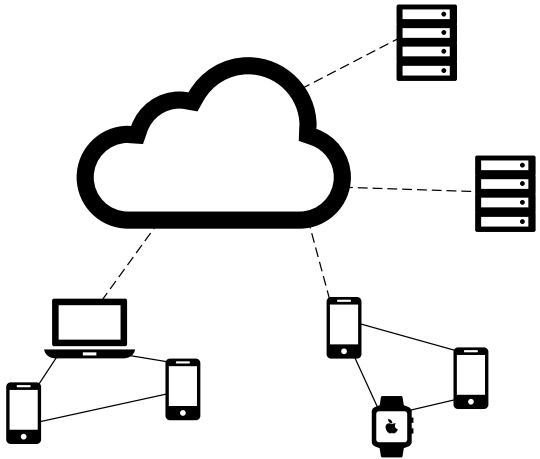
- Serverless on the edge
- Optimising for context through latency
- Processor selection based on arbitrary metrics, e.g. surprisal



Plans

Transient Privacy-Aware Clouds

- Encoding user-defined thresholds into bearer tokens
- Joint context at hierarchical levels
- TCACs $\rightarrow$ TPACs?



The Big Picture

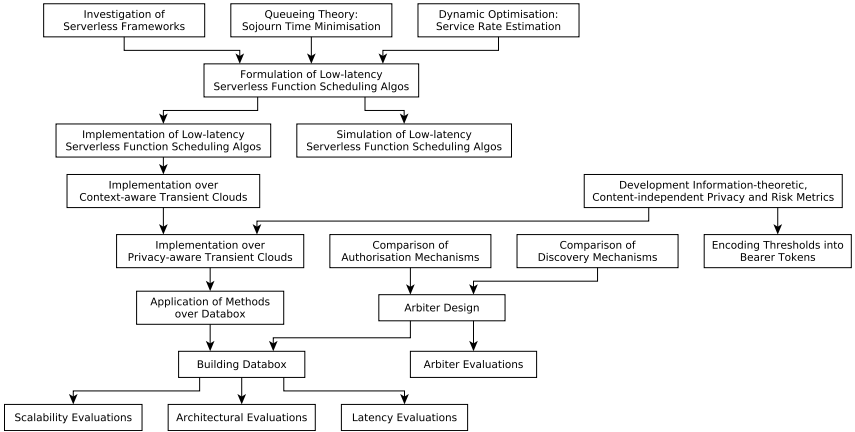


Figure: A High-level Dependency Graph of Research Activities

Thank you for your attention!

Questions?

More info: `http://yousefamar.com/`
Slides at: `https://github.com/yousefamar/unige-presentation-year2`