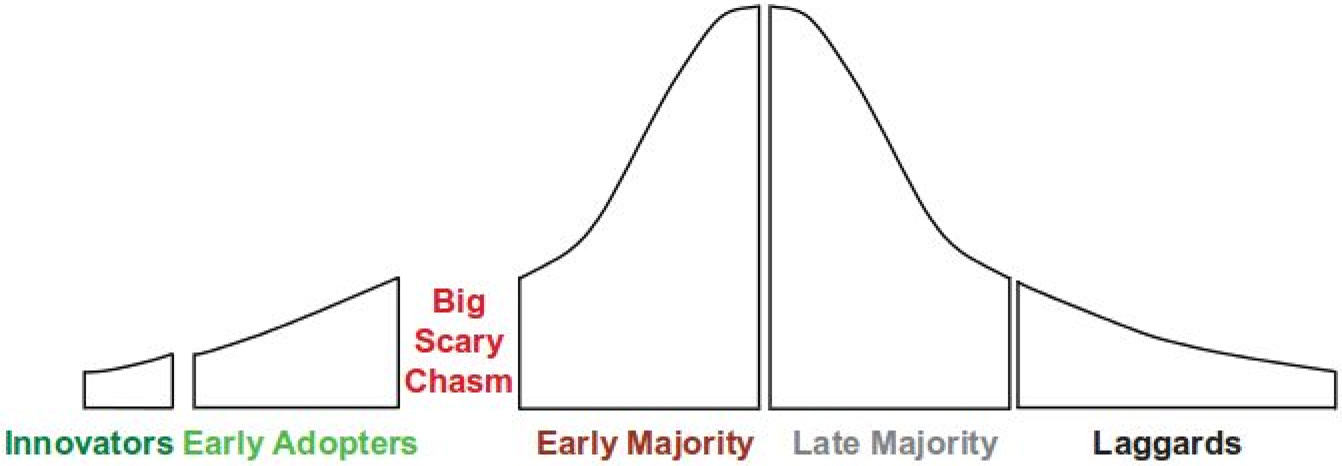
Privacy Mediators: Helping IoT Cross the Chasm

Nigel Davies[1], Nina Taft[2], Mahadev Satyanarayanan[3], Sarah Clinch[1], Brandon Amos[3]

[1]Lancaster University, [2]Google,[3]Carnegie Mellon University

The Technology Adoption Chasm



- Concern over data privacy arising from the over-centralization of IoT systems is a critical obstacle to their growth.

Evidence of Privacy Concerns

- June 2015 report on consumer perceptions of privacy in IoT(Groopman et al)
  - “Consumers are highly anxious about companies sharing their data”
  - “78% of consumers are highly concerned about companies selling their data to third parties.”
  - “While older generations show higher concerns, strong discomfort with the use and sale of connected device data is prevalent across all age groups, including young generation”.

- January 2015 report by the US federal trade commision
  - “... perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption”

Privacy Control Requirements

- While the IoT privacy landscape is complex, a simple principle can go a long way:

Users should be able to control the release of their own data.

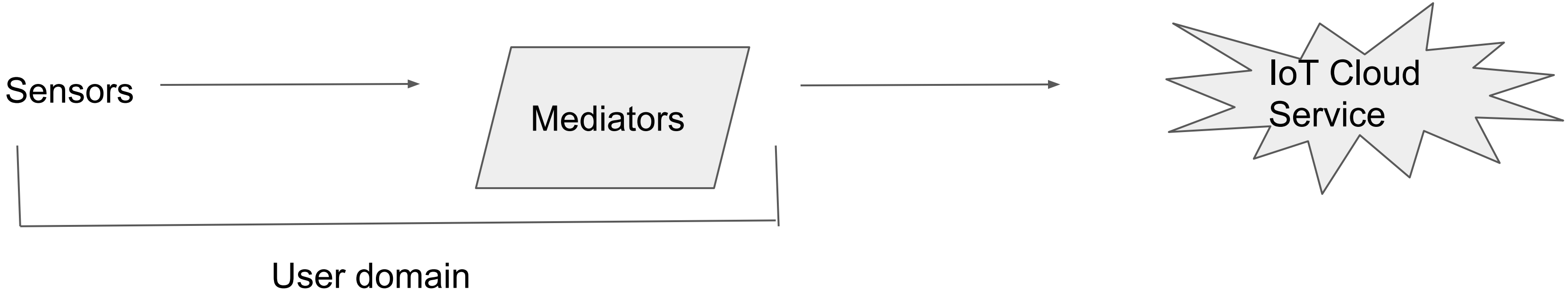
- Authors advocate the introduction of privacy mediators that enforce privacy requirements before data is released from the user’s direct control.

Sensors

IoT Cloud Service

Solution

- Plug-in architecture with trusted software modules called *privacy mediators* inserted into the data distribution pipeline.



- Privacy mediator performs data redaction and privacy policy enforcement before data is released from user’s direct control.
- It’s platform integrity is ensured by execution on a cloudlet.

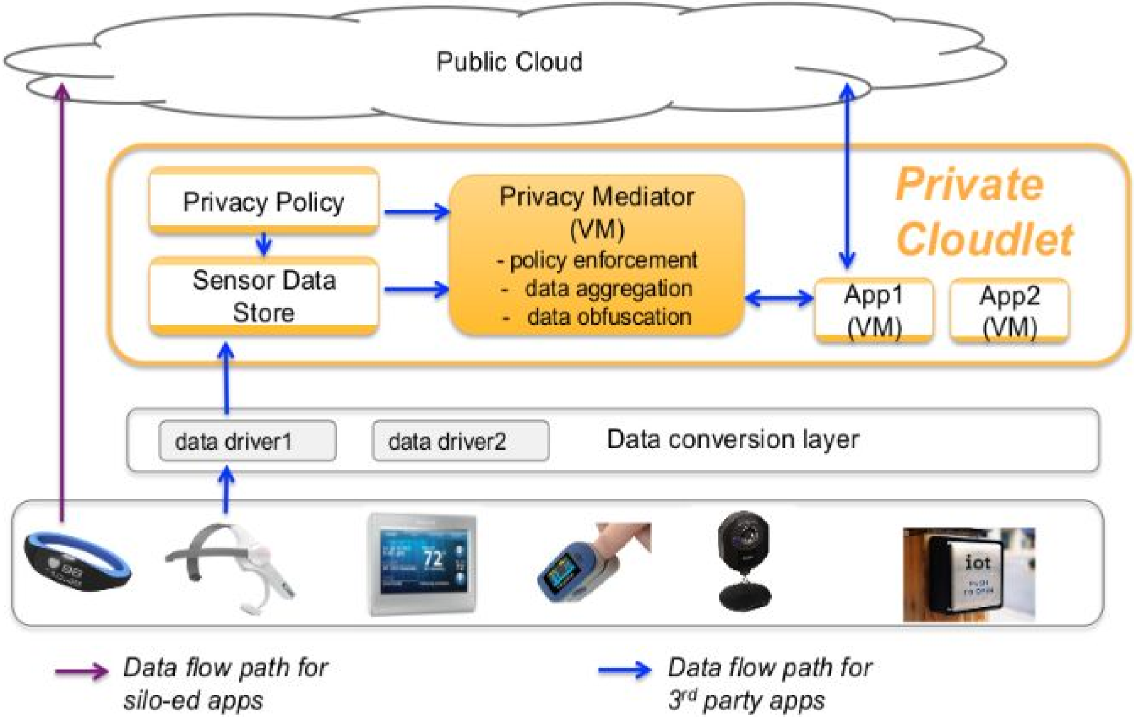
Privacy control requirements

- Deletion and denaturing.
  - Need to be able to both view data and express policies.
- Summarization.
  - Energy reporting should be different for energy provider and the government/third parties.
- Inference
  - Can the user decide what inferences can be made out of their data?
- Mobility
  - Support for privacy mediation on the move. Cloudlets to provide movement of privacy mediators.
- Ease of use
  - High level, recipient specific goals.

Key Design Principles

- Users should be able to control release of their sensor data
  - They should always have the first option to control release
  - Continuous control, not just install-time control
  - Ongoing, proactive, context-sensitive interactions to refine privacy policy during live use
- First point of infrastructure contact for sensor data should be controlled by owner of that data
- Cloudlets emerge as obvious landing zone(first infrastructure zone)
  - Small locally administered data centers at the edge of the Internet that can support code mobility.
  - Coincides with natural boundary of trust and responsibility.

Architectural Overview



Conclusions

- Privacy concerns need to be addressed for widespread adoption of IoT.
- Basic principle to follow is that users should be able to control the release of their own data.
- Architectural support for privacy control could be effectively provided using privacy mediators hosted on trusted cloudlets.
- Further work is required in a range of areas to support privacy mediation including user interfaces for expressing privacy preferences, and support for mobility.

Strengths of the Paper

- Authors have picked up the main sticking point for IoT to succeed.
- Authors have given references to other systems(ex. cloudlet) and P3P/APPEL to support their claim that implementing and deploying privacy mediators is viable.
- Authors have implemented a face recognition system OpenFace which gave good results without having to offload any video to the cloud. It can be used as a building block for IoT services running on a cloudlet.

Weaknesses of the Paper

- No detailed analysis on how a system like the one proposed will work in real world. There’s a lack of intricacies (related to the system) presented in this paper.
- Authors lack presenting how the helper systems will/should be stitched together to get the desired result.
- Authors have focused a lot on user-friendliness and at the same time they want to provide granular support of management of data. Both these can become contradicting at times.

Discussion points

- This is a position paper so no implementation. Point to discuss is, since the expectation is to have trusted cloudlets, will it limit the user’s mobility? Is there a way to overcome this situation?
- Mediators will largely be developed by independent third-parties, how to ensure that they don’t sell/use your data? Authors believe that rigorous inspection will be sufficient.
- It will interesting to have consumer-specific privacy preferences.