Privacy-Preserving Data Sharing in Cloud IoT on Solid

Fatmah Mashat and Maribel Fernández
King's College London

Solid Symposium

Motivations

- Smart home devices constantly gather sensitive personal data.
- Excessive data collection raises privacy and protection problems.
- Users struggle to properly understand and manage existing policy mechanisms.
- This motivates a user-centred architecture for controlled data sharing.

Background: Access and Data Control

- **Role-based access control (RBAC)**
  Access is based on predefined roles. This is simple to manage but less flexible in dynamic settings [10].
- **Attribute-based access control (ABAC)**
  Access is based on attributes of subjects, actions, and environment. This is expressive but can become complex [9]
- **Category-based access control (CBAC)**
  Access is expressed through categories, offering a bridge between role-based simplicity and attribute-based expressiveness[1, 3].
- **Category-based data access (CBDA)**
  Controls how IoT data is collected, transformed, stored, and shared using categories [7].

Background: Access and Data Control

CBAC in smart home [2]:

- Smart-home users include children, babysitters, visitors, and neighbours.
- Users are grouped into low, medium, and full trust categories.
- Devices are grouped into Entertainment, Cooking, Security, Cameras, etc.
- Permissions are defined over these categories.
- **Example:** children are low-trust users, so they can use lights but cannot access security devices or cameras.

Background: DataBank

- Is a four-layer privacy-preserving cloud-IoT architecture that offers mechanisms to manage data collection at the IoT-device level and data sharing at the cloud level [8].
- It separates data collection, transfer, storage, and access control.
- DataBank uses **CBDA** policies.

Background: DataBank for Smart Homes

Smart home uses **CBDASH** for data sharing

- Data categorised by sensitivity:
  - Public, Private, Secret, Top-Secret
- Services grouped by trust level:
  - Basic, Middle, Premium

Background: Solid Platform

- Is a decentralised data management framework designed to give users control over their data [5].
- Data is stored in personal online data stores called Pods.
- Solid supports access control through Web Access Control (WAC) and Access Control Policy (ACP).

Databank for Smart Homes (with CBDASH on Solid)

Sensors and Devices Layer

- IoT devices generate raw data streams

Hub and Data Pocket Layer

- Collects and filters data
- Categorises and stores data temporarily

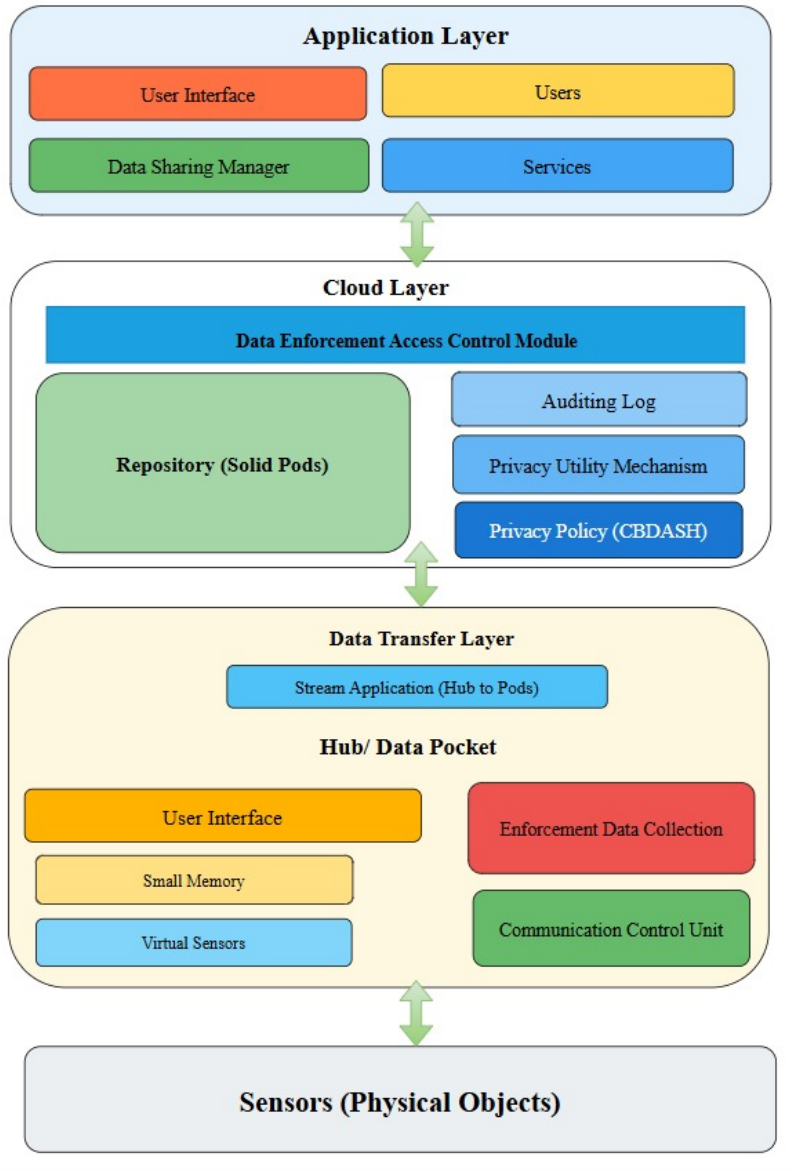
Cloud Layer

- Provides data storage
- Enforces access control policies

Application Layer

- Users and services interact with the system
- Access authorised data based on policies

Architecture Overview



Why local filtering matters

- Data is filtered and categorised locally at the hub before cloud transfer.
- Only approved categories are sent onwards to Solid pods for longer-term storage.
- Local filtering also reduces the volume of data transferred to the cloud.

How data is stored in Solid

Data organisation in Solid

- **Public Pod**
  Stores Accessible data
- **Encrypted Private Pod**
  Stores sensitive data with restricted access
- **Anonymised Pod**
  Stores partially de-identified data for trusted use

Additional structure:
Data can be organised into service-specific folders when needed.

Where access control is enforced

There are two ways to implement Databank on Solid, depending on where access control is enforced.

Model 1: Solid-mediated enforcement

- Applications access the Solid pods directly.
- Each pod enforces local access control using a predefined Solid access control policy.

→ **This approach requires awareness of the components.**

Model 2: Databank-mediated enforcement

- Applications access data **through the Databank**
- Solid Pods are **not directly exposed**
- The Databank acts as the **single enforcement point**

Solid-mediated vs Databank-mediated

Aspect	**Model 1: Solid-mediated**	**Model 2: Databank-mediated**
Access path	Direct access to Solid pods	Access via the Databank
Enforcement point	Local enforcement at each pod	Single enforcement point (Databank)
Pod visibility	Pods exposed to applications	Pods hidden from applications
Policy style	predefined policies	External category-based rules

Future work

Next steps:

- Automate the generation of Solid access control policies
- Explore richer policy primitives for direct pod-level enforcement
- Combining data management with access control [4].

References I

S Barker.

The next 700 access control models or a unifying meta-model?
SACMAT '09, pages 187–196. ACM, 2009.

C Bertolissi, M Fernandez, and B Thuraisingham.

An Axiomatic Category-Based Access Control Model for Smart Homes.
Lecture Notes in Computer Science. Springer, September 2024.

Clara Bertolissi and Maribel Fernández.

A metamodel of access control for distributed environments: Applications and properties.
Inf. Comput., 238:187–207, 2014.

Clara Bertolissi, Maribel Fernández, Jenjira Jaimunk, Fatmah Mashat, and Bhavani Thuraisingham.

Access control and data sharing in cloud-iot architectures: A category-based approach.
In *Proceedings of the ACM Workshop on (SaT-CPS)*, 2026.

Sarven Capadisli, Tim Berners-Lee, and Kjetil Kjernsmo.

Solid protocol, 2024.

Chatchawan Chaichana, Maribel Fernández, Jenjira Jaimunk, Sarit Theppitak, and Kan Tippayamontri.

A smart home databank:.
In Mahdi H. Miraz, Garfield Southall, Maaruf Ali, and Andrew Ware, editors, *Emerging Technologies in Computing*, pages 226–238, Cham, 2026. Springer Nature Switzerland.

M Fernández, Alex F Tapia, J Jaimunk, Manuel M Chamorro, and B Thuraisingham.

A data access model for privacy-preserving cloud-iot architectures.
In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, SACMAT '20.

Maribel Fernández, Jenjira Jaimunk, and Bhavani Thuraisingham.

A privacy-preserving architecture and data-sharing model for cloud-iot applications.
IEEE Transactions on Dependable and Secure Computing, 20(4):3495–3507, 2023.

References II

Vincent C Hu, D Ferraiolo, R Kuhn, A Schnitzer, K Sandlin, R Miller, K Scarfone, et al.

Guide to attribute based access control (abac) definition and considerations.
NIST special publication, 800(162):1–54, 2014.

R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman.

Role-based access control models.
Computer, 29(2):38–47, 1996.