Privacy-Driven and User-Centric Resource Allocation and Offloading for Smart Homes: Simulation and Prototype Validation

Tina Rezaei, Suzan Bayhan, Andrea Continella, Roland van Rijswijk-Deij
University of Twente, The Netherlands
{t.rezaei, s.bayhan, a.continella, r.m.vanrijswijk}@utwente.nl

1. Introduction

Problem:

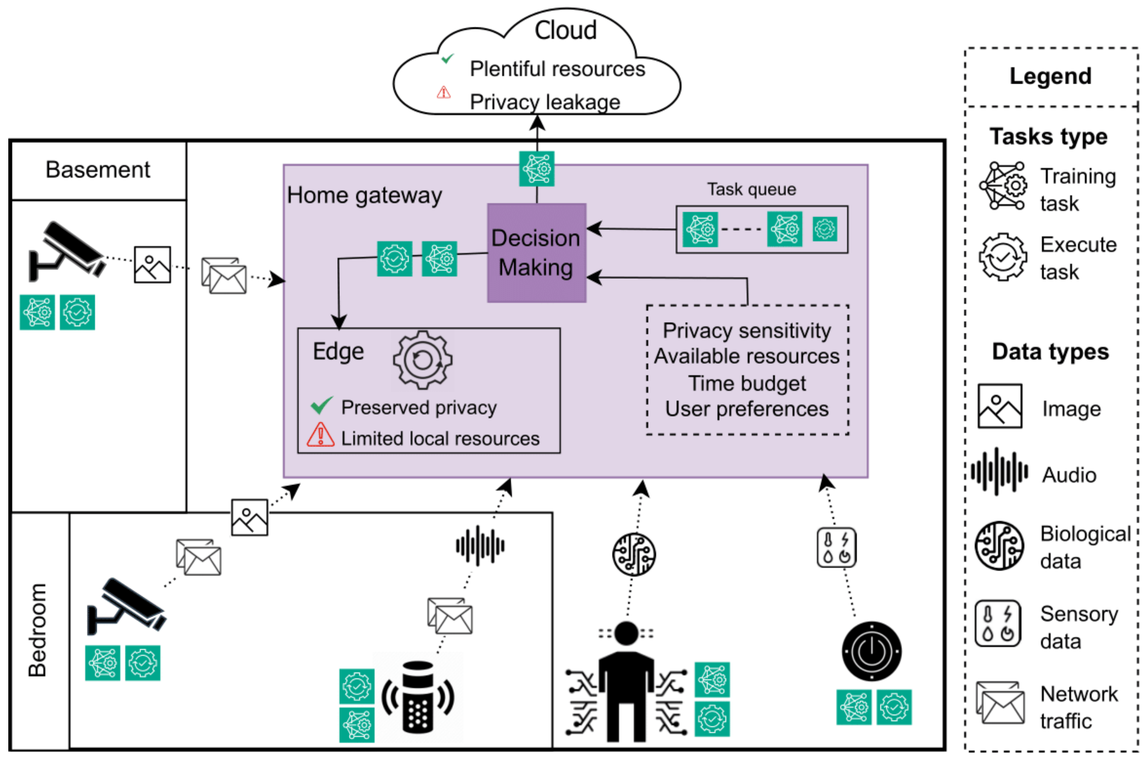
Smart home applications are growing in number and complexity.

- Edge devices risk resource overload and delay applications.
- Users want privacy, limited trust in cloud!

Solution:

A **resource allocation and offloading algorithm** that utilizes both edge and cloud resources, guided by the following design goals:

- ⚙️ Adaptive to computational load
- 🔒 Privacy-driven
- 🤦 User-centric



2. System Model

α_i: Binary decision variable (0 = local, 1 = remote)

P_i: Task privacy sensitivity, based on data type and data source location

Processing schemes:

- Local processing ($\alpha_i = 0$)
- Remote processing ($\alpha_i = 1$)

Privacy leakage model:

- $r_i = \alpha_i \, . \, p_i$

3. Problem Formulation

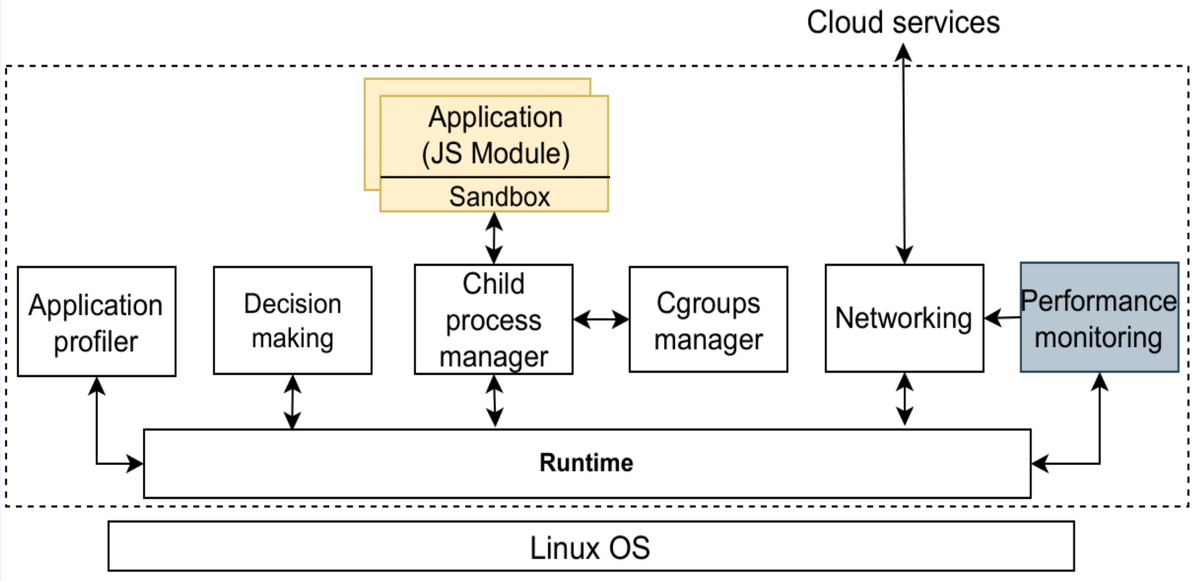
Allocate computation and bandwidth resources and decide where to execute tasks to minimize privacy leakage across all tasks.

Subject to:

- Time budget constraints
- Resource feasibility constraints

4. Simulation and Prototype Design

- Python-based Simulator: Developed using the Gurobi solver.
- Prototype Implementation: Deployed on a Raspberry Pi.



5. Results

⚙️ **Up to 3× faster application completion** compared to local-only solutions by balancing tasks between local and remote execution.

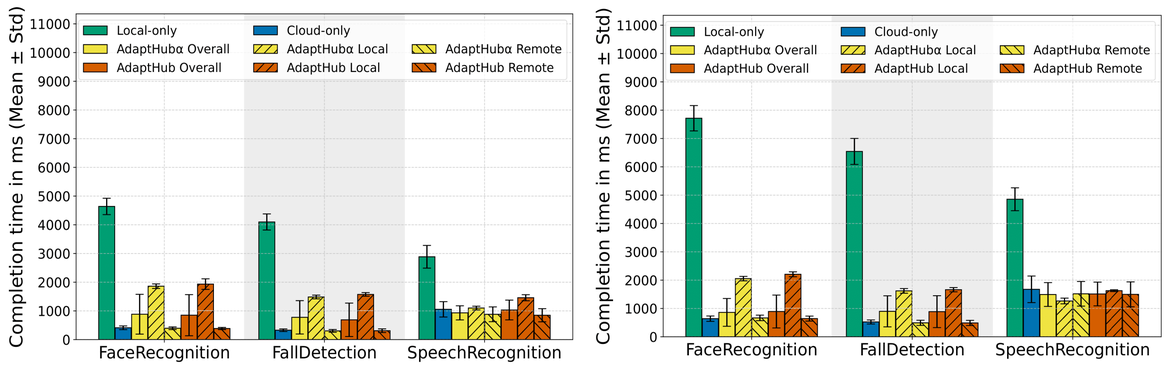


Fig 1. Distribution of completion time of applications under varying loads measured over 15 independent experiments (our approach: AdaptHub).

🔒 **65% of highly privacy-sensitive tasks executed locally**, significantly outperforming the 40% rate of privacy-oblivious baselines.

🤦 **Users enhance privacy** by relaxing completion time (e.g., doubling the time budget), enabling more sensitive tasks to be executed locally with minimal performance overhead (~300 ms).

6. Conclusion and Future Work

By selectively balancing tasks between edge and cloud, our approach not only accelerates completion times but also ensures that highly privacy-sensitive tasks are prioritized for local execution, reducing privacy exposure.

Future direction:

- Leverage trusted execution environments (TEEs) to enable secure computation in cloud.
- Apply data minimization prior to offloading.

UNIVERSITY OF TWENTE.

DACS
Design and Analysis of Communication Systems

Find the implementation here!