COASTmed: Software Architectures for Delivering Customizable, Policy-Based Differential Web Services

Alegria Baquero

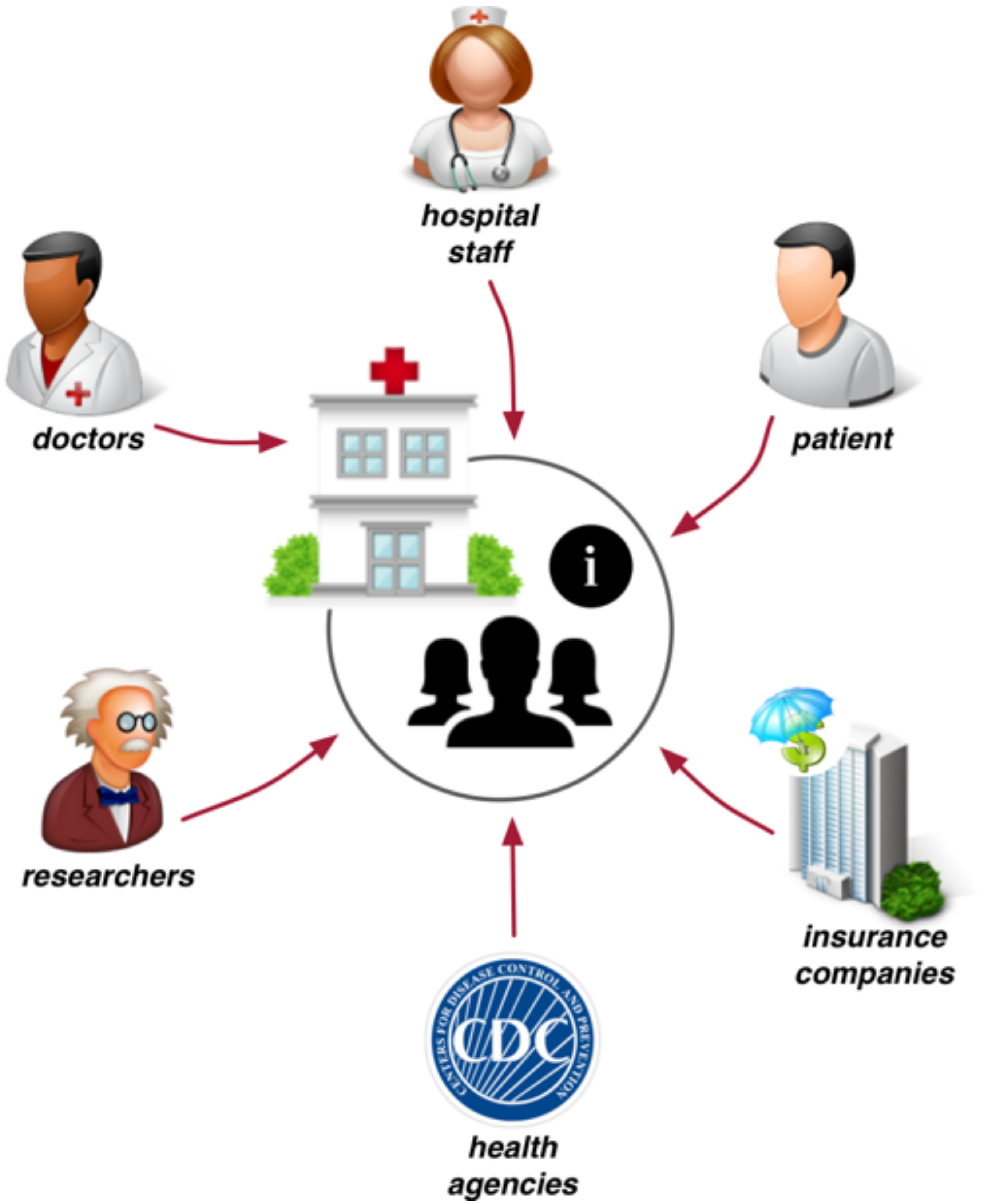
Doctoral Symposium

36th International Conference on Software Engineering

Hyderabad, India, 2014

THE PROBLEM

- Exchange of personal data raises privacy concerns.
- Trust between users and providers of personal data is not homogenous.
- Difficult to capture nuanced trust relationships in software systems.
- Complex data disclosure policies, often divorced from systems' behavior.
- Personal data is used for myriad, divergent, and unforeseen purposes.



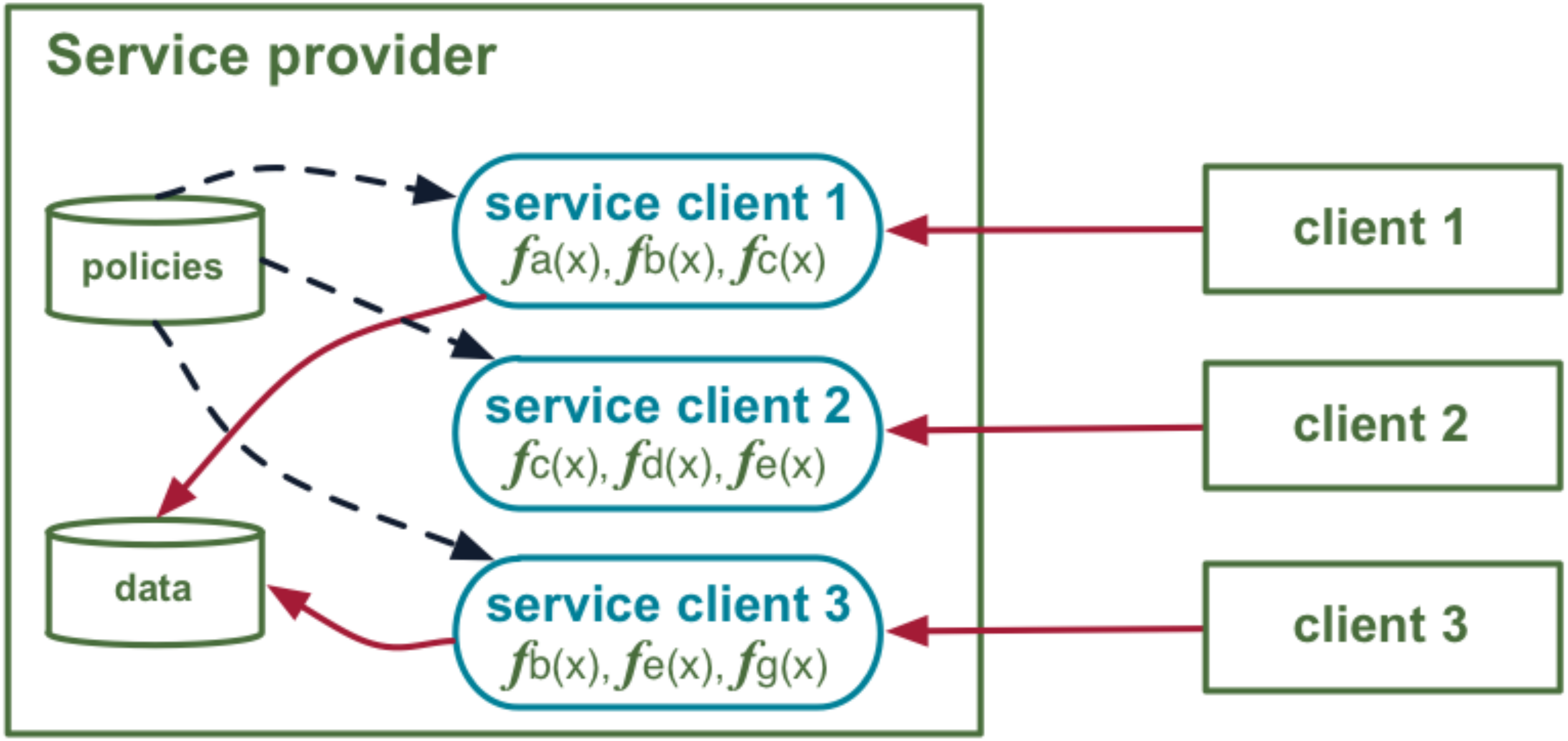
RESEARCH GOALS

- Enable **providers** to create privacy-aware services that conform to formally defined privacy policies.
- Enable **users** to customize services, allowing the fulfillment of specific data needs within the authority granted by providers.

BENEFITS

Secure access and customized use of dispersed personal data according to desired trust relationships between parties.

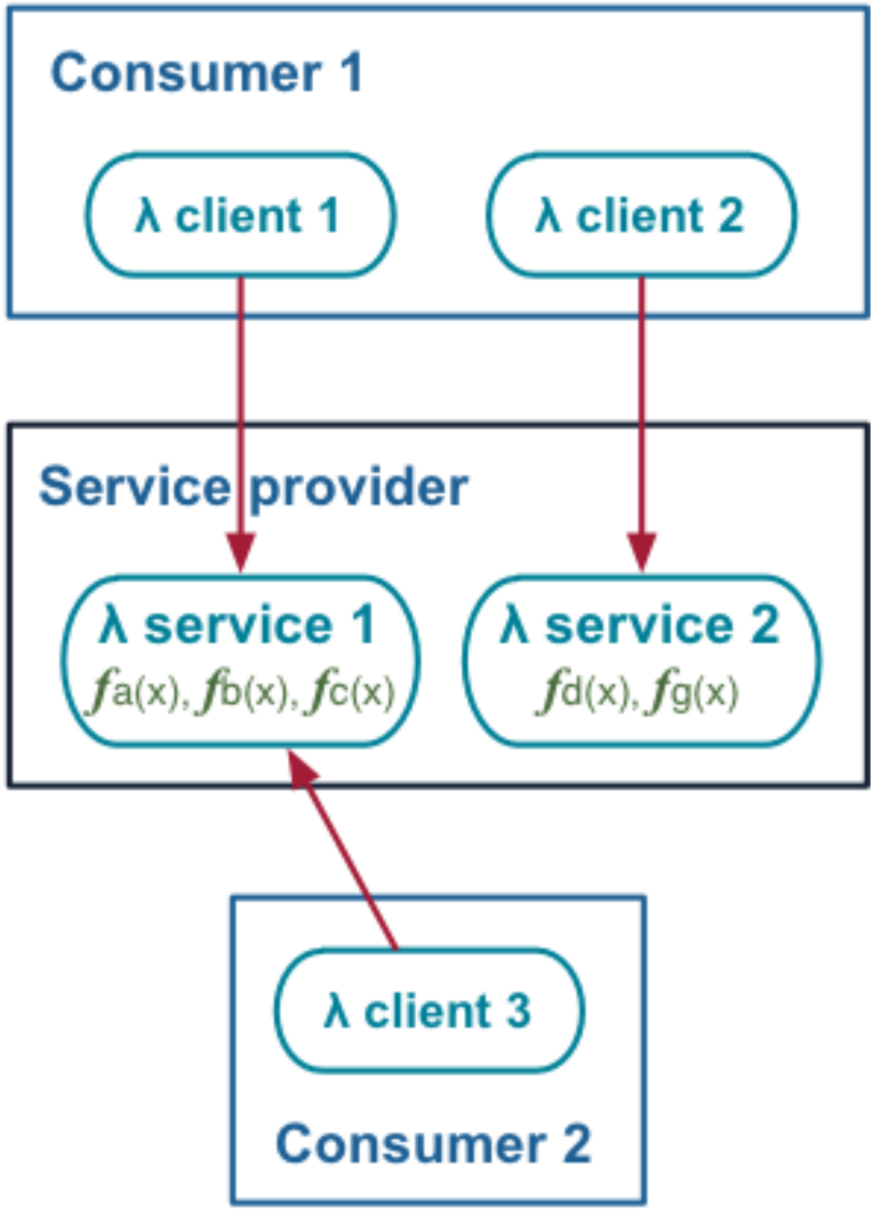
THE MAIN IDEA



BACKGROUND

The COAST architectural style (Gorlick et al., 2012)

- All services are computations which communicate through asynchronous messages.
- A computation is the execution of a closure c by execution engine E within the lexical context of binding environment B (execution site <E, B>).
- Computations are named by capability URLs (CURLs), unforgeable, cryptographic structures conveying authority to communicate.



BACKGROUND

The Rei policy language *(Kagal et al., 2003)*

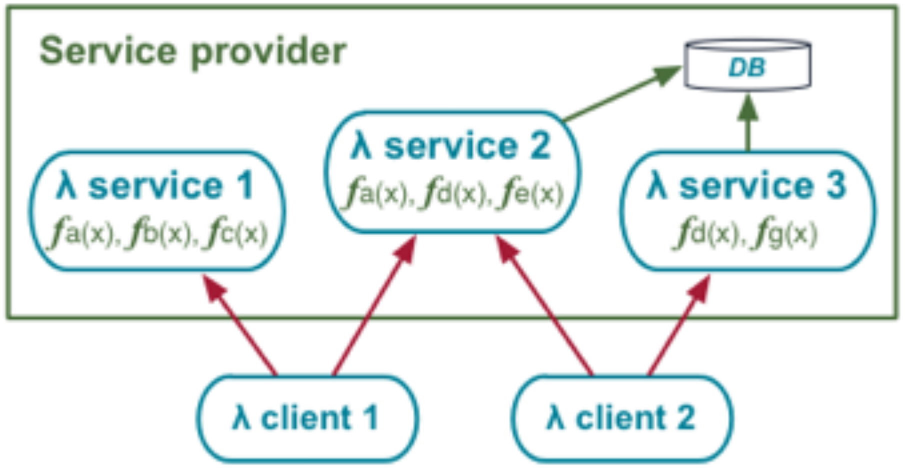
- A logic-based language.
- Policies are expressed in terms of rights, prohibitions, obligations, and dispensations.
- Policies are formally represented as `has(`**`Subject`**`, PolicyObject)`. Example:

  has(Person, right (printAction, (employee (Person)))).

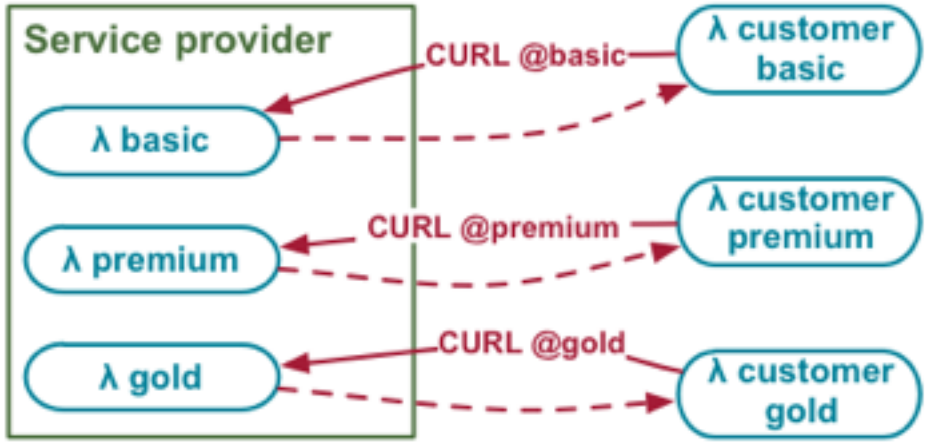
- Actions can be more detailed: **`action`**`(ActionName, `**`TargetObjects`**`, Pre-Conditions, Effects)`.
- Order and cardinality: `seq(A,B)` (A then B), `nond(A,B)` (A or B), `repetition(A)`, and `once(A)`.
- Complex conditions using the logical conjunctions `and` and `or`, and the negation `not`.

APPROACH

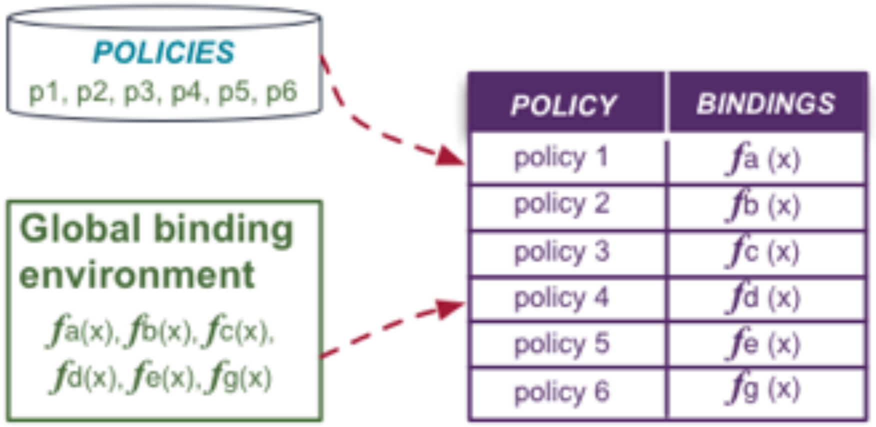
1 Exploit COAST's binding environment sculpting to ***expose functional capabilities as services***.



2 Leverage COAST's capability-based security to ***differentiate among service users***.

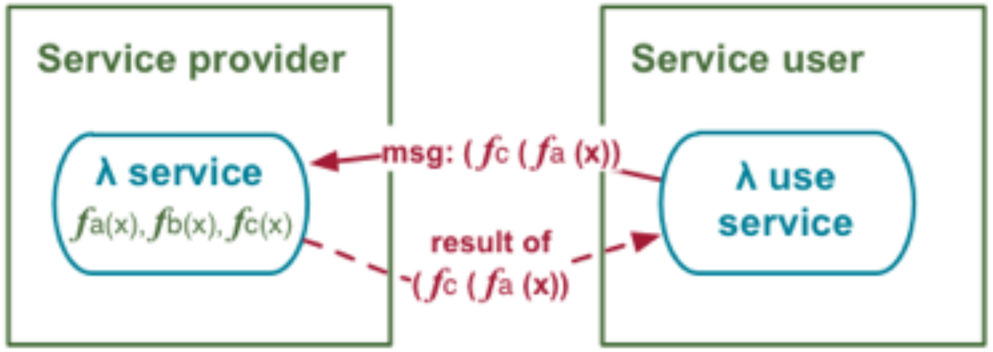


3 ***Associate*** a system's functional ***capabilities with*** a set of provider-defined privacy ***policies***.



POLICY	BINDINGS
policy 1	fa (x)
policy 2	fb (x)
policy 3	fc (x)
policy 4	fd (x)
policy 5	fe (x)
policy 6	fg (x)

4 Exploit computation composition and mobility to ***allow users to create custom services***.



WHAT'S NEW?

- Simultaneously enabling, through capability-based security and code mobility:

  (a) differential access to services and

  (b) user-controlled customization

- Dynamically creating personalized and customizable services through policies and system capabilities associations.

EVALUATION

- Qualitative comparative analyses with systems approaching similar challenges.

  (a) expressively capture policies;

  (b) offer policy compliant services;

  (c) provide user-specific services, and;

  (d) allow service customization.

- Technical feasibility assessment through prototyping -> the COASTmed decentralized EHR system offers services to diverse users.

- Scenario-based evaluations -> a set of simulations involving complex inter-agency processes of patient data exchange.

PROGRESS TO DATE

- Evaluation of candidate policy languages.
- Early prototype of COASTmed and implementation of exploratory a set of data access scenarios involving customization and differential access.
- Specification and evaluation of simple policies.
- Association of policies with system capabilities.
- Automated generation of user-specific service CURLs -> simulation of incoming service requests.
- Automated creation of user specific service at incoming requests.

CONTRIBUTIONS

- Enable the secure, privacy aware, customizable use and sharing of personal data through computational exchange.
- Enable simultaneous provider-controlled policy-based differential access to services and user-driven customization.
- Provide novel techniques for binding policies to personal data services.
- Provide design guidance for using the developed technique through COASTmed.

APPLICABILITY

Decentralized domains where trust among parties is heterogeneous, and so is the authority to access information services.

THANK YOU.