A Service Provisioning System for Distributed Personalization with Private Data Protection

Hiroyuki KASAI

NTT DoCoMo, Inc. JAPAN Network Laboratories

28 June 2006
Service Scenario

Deliver tailored & personalized messages to users according to their private information.

On a street…
I want to send a new CD album info. to people who like pop music.

At a shopping center entrance
I want to send an event news according to customer’s profile.

Event news!
1. French restaurant is holding a spring fair at (2F-E block).
2. How about Italian Gelato on this hot day? (1F-C block)
3. Fresh Japanese noodle! (3F-A block)
Adapt **service behaviors** (select, filter, sort, etc.) according to **various data** (user’s profile/preference, location, weather, etc.).

**Service Rule**
- Specifies service behavior and necessary data, and
- Tells effectiveness caused by messages.

**Available Data**
- Favorite Cuisine
- Budget for lunch
- Gender
- Weather
- Location

**Restaurant List**

**Top Two Restaurants?**

**Service Provider**

**User**
Issue in Ubiquitous & Open World

Some data might be unobtainable.

1. **Data does not exit.**
   - A service rule might not operate properly.
   - Missing data has a different influence on the service rule.

2. **Data cannot be accessed.**
   - Privacy Problem

**Service assessment mechanism** that can judge how properly the service rule operates with missing data.

**Privacy preserving mechanism** which can provide a personalized service without revealing private data.
Privacy Preserving Service Execution Control based on Service Rule Sharing

1. Overview
2. Basic Mechanism
   - Service Rule Description based on BDN
3. Service Rule Conversion
   - Structure Conversion
   - CPT Conversion
4. Feature & Demonstration
Assumption

Check whether **user’s private data** meets a provider’s “service rule.”

### User-side

**User’s Private Data**
- Name = “Hiro”
- Age = “28”
- favorite food = “Japanese”
- favorite music = “Pop”
- cash in wallet = “$40”
- ……

### Provider-side

**Service Rule**

```plaintext
if (favorite food = "Italian" &&
cash in wallet > $20 &&
customer < 20 people &&
ingredient stock < 10kg )
  Notify message.
else
  Not notify.
```

**Private Data**
- Name = “Hiro”
- Age = “28”
- favorite food = “Japanese”
- favorite music = “Pop”
- cash in wallet = “$40”
- ……

**Matching**
Problem & Motivation

- Problems for “User side”
  - Trade-off between available services and leak of private data.
  - Big users’ burden to determine appropriate disclosure policy at each situation.

- Problem for “Service provider side”
  - Leak of service rule, that is, their know-how.

Target!

Need service executable mechanism without disclosing user’s private data and provider’s service rules.
Fundamental Policy & Proposal

- **No reveal of user’s private data:**
  - Reveal **ONLY attribute data** of user’s private data to *service providers*.
- **No reveal of an entire service rule:**
  - Reveal a **modified service rule** to *users*.

Proposal!

A service provider and a user *share* service execution procedure by exchanging a **converted (modified) service rule**.
Basic Mechanism

Service Rule description:
Bayesian decision networks (BDN) based Service Rule.

Technical Issue:
BDN-based service rule conversion.

User Side
User's Private Data
Calculation
Service Execution

Provider's Private Data
Rule Conversion
Converted Service Rule

Spring fair at 7F French Restaurant!
### BDN-based Service Rule

#### Bayesian Decision Network (BDN)

**Conditional Probability Table (CPT)**

<table>
<thead>
<tr>
<th>Humid</th>
<th>Forecast</th>
<th>Evening Weather</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Rain</td>
<td>0.9 0.1</td>
</tr>
<tr>
<td>High</td>
<td>Sun</td>
<td>0.3 0.7</td>
</tr>
<tr>
<td>Low</td>
<td>Rain</td>
<td>0.6 0.4</td>
</tr>
<tr>
<td>Low</td>
<td>Sun</td>
<td>0.1 0.3</td>
</tr>
</tbody>
</table>

**Belief propagate**

- Humid
- Forecast
- Evening Weather

**Utility Table**

<table>
<thead>
<tr>
<th>Umbrella</th>
<th>Evening Weather</th>
<th>Utility (U(a,h))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Rain</td>
<td>9</td>
</tr>
<tr>
<td>Yes</td>
<td>Sun</td>
<td>2</td>
</tr>
<tr>
<td>No</td>
<td>Rain</td>
<td>3</td>
</tr>
<tr>
<td>No</td>
<td>Sun</td>
<td>-8</td>
</tr>
</tbody>
</table>

**Utility node**

- Select the action node with a MEU (maximum expected utility).

- **opt(A) = arg max<sub>h∈H</sub> EU(a)**

- **EU(a) = ∑<sub>h∈H</sub> U(a,h)P(h)**
Service Rule Conversion

Convert an original BDN into a new BDN with ONLY “user private data nodes” and “nodes for utility.”

Structure Conversion & CPT conversion.
Who are my parents?

Determine the nodes that have influence on user private data nodes and nodes for utility to be left.

- Which nodes can become parent nodes of the target node?
- Which nodes affect a target node as evidence nodes?
Applying “d-separation”

**d-separation**: direction-dependent separation

Point!

If two nodes are “D-separated”, they
- are conditional independent, and
- have no influence on each other.
Structure Conversion

Determine influential nodes for remaining nodes.
- List all nodes in upper stream of a remaining node.

Structure conversion has been completed!
(Parent nodes and evidence nodes have been determined!)
**CPT Conversion**

**Goal:** Calculate probabilities in all combinations of parent nodes.

<table>
<thead>
<tr>
<th>No. ((l))</th>
<th>User private data 0</th>
<th>User private data 1</th>
<th>User private data 2</th>
<th>Provider private data 0</th>
<th>Provider private data 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>0.4</td>
<td>0.6</td>
</tr>
<tr>
<td>1</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>0.6</td>
<td>0.4</td>
</tr>
<tr>
<td>2</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>3</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>7</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>0.8</td>
<td>0.2</td>
</tr>
</tbody>
</table>

**Execute Probabilistic Inference algorithm.**

**Parent nodes:**
- User private data 0 = True
- User private data 1 = False
- User private data 2 = True

**Evidence nodes:**
- Provider private data 0 = False
- Provider private data 1 = True

Directly influential node for a target node.
Features (Coverage)

- **NOT suitable for**
  - Services that handle a huge amount of information (e.g. Conventional information search application from the whole of Internet.).

- **Suitable for**
  - Service that select or sort information among a limited number of candidate information (e.g. location-aware pinpoint advertisement services, shop recommendation services).
Advantages

- **More service opportunities:**
  Users can receive and providers can give more services without disclosing their private data.

- **Mathematical Conversion:**
  Conversion can be performed based on the mathematical calculation.

- **Strong protection of an entire service rule:**
  One evidence input or one node elimination can propagate its influence on a large area inside NW.

- **Robustness for wrong user’s declaration:**
  Even if some user’s private data are missing when service execution at user-side, the converted rule can even work based on just available data.
Demonstration (1/2)

Demonstration Scenario

- A restaurant center sends select three best shops of five according to user’s private data.
- User’s private data are user’s
  - budget for lunch,
  - favorite cuisine, and
  - gender.
- Prototype system is implemented on Push-based Notification System.
Demonstration (2/2)

3G/GSM Mobile NW

Push-based Notification Server

Privacy Preserving Service Provider Server

Service Rules

Converted Service Rule

Original Service Rule

WLAN IEEE 802.11

User's Disclosure Policy

Push-based Notification Client

Push-based Notification Server

3G/GSM Mobile NW

WLAN IEEE 802.11

User's Disclosure Policy

Push-based Notification Client

Push-based Notification Server
Conclusions

- Propose a privacy preserving service provisioning mechanism by sharing service execution procedure in both user side and provider side.
- Achieve by exchanging converted service rules.
- BDN-based service rule description and service rule conversion algorithm.
Thank you for your attention!