Quality of Context and Privacy Preservation for Context Management in the Internet of Things

Master CILS — Module IAAIO, Revision : 2443

Sophie Chabridon

Institut Mines-Télécom, Télécom SudParis
CNRS SAMOVAR UMR 5157, ACMES/MARGE

Septembre 2019
Outline

1. Requirements
2. Approach
3. QoC Management
4. Privacy Protection
5. QoC- and Privacy-aware Context Dissemination
Requirements

Context data production/consumption decoupling

- Asynchronous and anonymous communication, with time and space decoupling

Quality-of-Context-based context data distribution

- QoC requirements on the quality of the received data
- QoC guarantees on the quality of provided data

Privacy preserving context data distribution

- Privacy requirements on the provided data
- Privacy guarantees on received data
Definitions

- **Quality of Context (QoC):** Set of measurable quality criteria such as precision, error probability or freshness [Buchholz et al., 2003]. Through QoC, the worth of context data for a specific application is evaluated.

- **Privacy:** Capacity of control about what, how, when, where and with whom share to information.
Global vision
Outline

1. Requirements

2. Approach

3. QoC Management
   3.1 QoCIM: QoC Information Model
   3.2 QoCIM - UML meta-model
   3.3 QoCIM in action

4. Privacy Protection

5. QoC- and Privacy-aware Context Dissemination
## Comparison of QoC criteria

<table>
<thead>
<tr>
<th></th>
<th>Buchholz</th>
<th>Kim</th>
<th>Sheikh</th>
<th>Filho</th>
<th>Manzoor</th>
<th>Neisse</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Probability context is free of errors</td>
<td>Correctness</td>
<td>Accuracy</td>
<td>Precision</td>
<td>Accuracy</td>
<td>Accuracy</td>
</tr>
<tr>
<td>2</td>
<td>Max. distance to get context</td>
<td></td>
<td></td>
<td>Sensor range</td>
<td></td>
<td>Sensor range</td>
</tr>
<tr>
<td>3</td>
<td>Location of the real world entity</td>
<td></td>
<td></td>
<td>Entity location</td>
<td></td>
<td>Entity location</td>
</tr>
<tr>
<td>4</td>
<td>Location of the sensor</td>
<td></td>
<td></td>
<td>Sensor location</td>
<td></td>
<td>Sensor location</td>
</tr>
<tr>
<td>5</td>
<td>Time between production of contexts</td>
<td></td>
<td>Temporal resolution</td>
<td>Time period</td>
<td></td>
<td>Time period</td>
</tr>
<tr>
<td>6</td>
<td>Date of collection of context</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>Granularity of location</td>
<td></td>
<td></td>
<td>Resolution</td>
<td></td>
<td>Measurement time</td>
</tr>
<tr>
<td>8</td>
<td>Rate the confidence of the provider</td>
<td>Trust worthiness</td>
<td>Spatial resolution</td>
<td></td>
<td>Resolution</td>
<td>Timestamps</td>
</tr>
</tbody>
</table>
Meta-model to define QoC criteria which could be:

- **primitive**: a criterion not depending on any other criteria for its definition
- **composite**: a criterion built upon other criteria
- **pre-defined**: a criterion with a well defined list of possible values
QoCIM - UML meta-model

ContextInformation
- uri : EString
- value : EString
- creationDate : EDate
- unit : EString

QoCIndicator
- id : EInt

QoCCriterion
- id : EString

QoCMetricDefinition
- id : EString
- isInvariant : EBoolean
- unit : EString
- direction : Order
- minValue : EInt
- maxValue : EInt

QoCMetricValue
- id : EInt
- value : EInt
- creationDate : EDate
- modificationDate : EDate

<<enumeration>>
- Order
  - INF
  - SUP
  - UNDEF

<<primitiveDefinition>>

<<compositeDefinition>>

Description
- name : EString
- keywords : EString
- informalDefinition : EString
QoCIM

- Context information is qualified by QoC indicators: associate meta-data with one piece of context information
- A QoC criterion contains QoC metric definitions: many characterizations of a same QoC criterion may coexist within an heterogeneous system
- Defining composite QoC metric definitions: a QoC criterion can be defined from a composition of two or more primitive criteria
QoC Management

QoC in action

Distributed Context Management Service

Context acquisition

Context processing
(fusion, aggregation, summarization, inferring)

Context presentation

QoCIM framework

Context dissemination

Legend:

QoC guarantees

QoC requirements

Context and QoC data flow
Outline

1. Requirements

2. Approach

3. QoC Management

4. Privacy Protection
   4.1 European data protection rules
   4.2 Privacy Modeling
   4.3 Privacy as Confidentiality
   4.4 Privacy as Control
   4.5 Privacy as Transparency
   4.6 Privacy and context management

5. QoC- and Privacy-aware Context Dissemination
European data protection rules

- Reform of Directive 95/46/EC started in 2012
- Personal data must be:
  - processed lawfully, fairly and in a transparent manner in relation to the data subject;
  - collected for specified, explicit and legitimate purposes;
  - adequate, relevant, and limited to the minimum necessary in relation to the purpose;
  - accurate and kept up to date;
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
  - processed under the responsibility and liability of the controller
**Context Contract Dimensions**

- **Owner**
  - Visibility
  - Retention
  - Purpose

- **Consumer**
  - QoC

- **Producer**
  - QoC
  - Purpose
  - Retention
  - Visibility

- **End-User**
  - QoC
  - Purpose
  - Retention
  - Visibility

**Trust**
Examples of Dimensions

Trust (T)
- Very Much
- Moderately
- Slightly
- None

QoC (Q)
- SuperHigh
- High
- Medium
- Low

Visibility (V)
- Friends-of-Friends
- Third-party
- World
- Owner
- Home
- Friends
- Until an expiry condition
- Indefinitely

Retention (R)

Purpose (P)
- Owner-use
- Legal-requirement
- Vital-assistance
- Business-practices
- Any
## Privacy Concerns vs. Privacy Dimensions

Privacy concerns [Greenleaf, 2012] and associated protection dimensions

<table>
<thead>
<tr>
<th>Privacy Concern</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection: limited, lawful and by fair means; with consent or knowledge</td>
<td>QoC</td>
</tr>
<tr>
<td>Data quality: relevant, accurate, up-to-date</td>
<td>QoC</td>
</tr>
<tr>
<td>Purpose specification at time of collection</td>
<td>Purpose, Retention</td>
</tr>
<tr>
<td>Notice of purpose and rights at time of collection</td>
<td>Visibility, Purpose</td>
</tr>
<tr>
<td>Limited use (including disclosure) to specified or compatible purposes</td>
<td>Visibility, Purpose</td>
</tr>
<tr>
<td>Security through reasonable safeguards</td>
<td>Visibility, Retention</td>
</tr>
<tr>
<td>Openness of personal data practices</td>
<td>Visibility</td>
</tr>
<tr>
<td>Access: individual right of access</td>
<td>Visibility</td>
</tr>
<tr>
<td>Correction: individual right of correction</td>
<td>Visibility, QoC</td>
</tr>
<tr>
<td>Accountable: data controllers accountable for implementation</td>
<td>Visibility, Purpose, QoC, Retention</td>
</tr>
</tbody>
</table>
Outline

1. Requirements

2. Approach

3. QoC Management

4. Privacy Protection
   4.1 European data protection rules
   4.2 Privacy Modeling
   4.3 Privacy as Confidentiality
      4.3.1 Anonymity of data
      4.3.2 Anonymity in communication
      4.3.3 Data minimization
   4.4 Privacy as Control
   4.5 Privacy as Transparency
   4.6 Privacy and context management

5. QoC- and Privacy-aware Context Dissemination
Anonymity of data

- Use of cryptographic solutions to achieve properties of
  - unlinkability: two information items or two actions of the same user cannot be related
  - undetectability: an attacker cannot distinguish whether an information item exists
  - unobservability: not possible to detect whether a system is being visited by a given user
Anonymity of data

- **k-anonymity** [Sweeney, 2002]: individual cannot be identified within a set of $k$ other users

- **l-diversity** [Machanavajjhala et al., 2007]: a block of data is l-diverse if it contains at least l well-represented values for the sensitive attribute $S$

- **Differential privacy** [Dwork, 2006]: maximize the accuracy of queries from statistical databases while minimizing the chances of identifying its records
Anonymity in communication

- Who talks to whom?
- Route encrypted messages in an unpredictable path: Mix-Net [Chaum, 1981], Tor [Dingledine et al., 2004]
- Sensitive data in addition to content: locations and identities of the communicating parties, time, frequency, volume of the communication
Data minimization

- Limit the collection and processing of personal data

  - Encrypted aggregation [Canny, 2002, Mehta, 2007]

  - Perturbation: data get systematically altered using a perturbation function (e.g., adding random numbers)

  - Obfuscation: a certain percentage of data get replaced by random values (e.g., replace with the mean).
Obfuscation Strategies

- Deliberate data transformation performed for reasons of privacy preservation prior to information disclosure. [Chakraborty et al., 2012]

- **non-interactive** (database):
  - Sanitization of context data by removal of personally identifiable information (PII)
  - Operations such as generalization, suppression, permutation and perturbation.

- **interactive** (discloses information as responses to user queries):
  - Providing control over disclosed context data.
  - Addition of calibrated noise (i.e., using an application-specific noise models). [Fung et al., 2010, Dwork et al., 2006]
Outline

1. Requirements

2. Approach

3. QoC Management

4. Privacy Protection
   4.1 European data protection rules
   4.2 Privacy Modeling
   4.3 Privacy as Confidentiality
   4.4 Privacy as Control
      4.4.1 From static to contextual access control policy models
      4.4.2 Usage control policies
      4.4.3 Identity Management
   4.5 Privacy as Transparency
   4.6 Privacy and context management

5. QoC- and Privacy-aware Context Dissemination
Privacy as Control

- Control what happens with personal data
- Prevent abuses
- Rely on access control (define access authorization rules) and usage control policies
From static to contextual access control policy models

- Access control policies rely on
  - Subjects: users (or applications) who can perform actions
  - Objects: resources or services that subjects want to control access to
  - Permissions: determine how subjects can access resources

- In traditional models (such as Identity-based Access Control models, Mandatory Access Control models or Role Based Access control): no notion of context

- Attribute Based Access Control (ABAC): based on any attribute of the subject, resource, action or the environment
Usage control policies

- Obligation policies allow to control the usage of context information

- Actions required to be performed by a consumer before, during or after the usage of the context information

- Examples: UCON [Lazouski et al., 2010], XACML [OASIS, 2012], Ponder2 [Twidle et al., 2009] or OSL-based framework of [?]

- Sticky policy: Obligations are kept travelling with data along the context processing chain [Pearson et al., 2011, di Vimercati et al., 2011]
Identity Management

- Separate Service Provider (SP) from Identity Provider (IdP)
- SP: provides a personalized service to users by using information of users
- IdP: authenticates users and stores data about users
- Ex: Shibboleth [Shibboleth, 2013] allows IdP administrators to define whose attributes are sent to specific SPs
Outline

1. Requirements

2. Approach

3. QoC Management

4. Privacy Protection
   4.1 European data protection rules
   4.2 Privacy Modeling
   4.3 Privacy as Confidentiality
   4.4 Privacy as Control
   4.5 Privacy as Transparency
   4.6 Privacy and context management

5. QoC- and Privacy-aware Context Dissemination
Help users keep control of their data

- Provide information about the intended collection, storage and/or data processing
- Provide an overview of what personal data have been disclosed to what data controller under which policies
- Provide online access to the personal data and how they have been processed.
- Provide counter profiling capabilities helping the user to guess how the data match relevant group profiles, which may affect future opportunities or risks
Privacy and context management

- Study on 50 research projects on context-aware computing [Perera et al., 2013]
- Only 11 projects over 50 (about 20%) provide some security and privacy solutions
Privacy Protection

Privacy and context management

- At collection time
  - Use anonymization techniques to protect data from being linked to the user
  - Not sufficient as de-anonymization becomes easy under an open world assumption
  - Differential privacy: use perturbation techniques to make data sets indistinguishable [Dwork, 2006]

- At processing time
  - Use anonymization with identity management techniques to control data disclosure
  - Use data minimization techniques like perturbation and obfuscation

- At presentation time
  - Combine confidentiality techniques, identity management, and access and usage control policies
Outline

1. Requirements
2. Approach
3. QoC Management
4. Privacy Protection

5. QoC- and Privacy-aware Context Dissemination
   5.1 Overlay Architecture
   5.2 Context information dissemination
   5.3 Context contracts translation into routing filters
Overlay Architecture

QoC- and Privacy-aware Context Dissemination

Sophie Chabridon

Quality of Context and Privacy Preservation for Context Management
Context information dissemination

Legend:
- Subscription routing filter
- Advertisement routing filter
- Context data flow with meta-data
Producer contract

- Advertisement filter with QoC guarantee + Privacy requirements
- Privacy requirements = XACML policy
Consumer contract

Subscription filter with QoC requirements + privacy guarantees

Privacy guarantees = ABAC information
Quality of Context Information: What it is and why we Need it.
In 10th Int. Workshop HPOVUA, Geneva.

Canny, J. (2002).
Collaborative Filtering with Privacy via Factor Analysis.
In 25th ACM SIGIR.

Balancing Behavioral Privacy and Information Utility in Sensory Data Flows.
Pervasive and Mobile Computing, 8(3):331–345.

Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.
Comm. ACM, 24(2).


Tor: The Second-Generation Onion Router.
In 13th USENIX Security Symp., San Diego, CA, USA.
Differential Privacy.
In *ICALP*. Springer.

Calibrating noise to sensitivity in private data analysis.

Privacy-preserving data publishing: A survey of recent developments.

The influence of european data privacy standards outside europe: Implications for globalisation of convention 108.


L-diversity: Privacy beyond k-anonymity.
Learning from What Others Know: Privacy Preserving Cross System Personalization.
In 11th Conf. on User Modeling.

OASIS (2012).
Extensible Access Control Markup Language (XACML).

Sticky Policies: An Approach for Managing Privacy across Multiple Parties.
IEEE Computer, 44(9):60–68.

Context Aware Computing for The Internet of Things: A Survey.
ArXiv e-prints, Submitted to IEEE Communications Surveys & Tutorials.

Shibboleth (2013).

k-anonymity: a model for protecting privacy.

Ponder2: A Policy System for Autonomous Pervasive Environments.
In ICAS.