Data Privacy Preservation in Telemedicine: The PAIRSE Project

Ebrahim NAGEBA, Bruno DEFUDE, Franck MORVAN, Chirine GHEDIRA and Jocelyne FAYN

INSA-Lyon, MTIC, Villeurbanne, France
INSMR, MTIC, Bron, France

MIE 2011, Oslo, Norway, 28-31 August 2011
PAIRSE Project: Preserving Privacies in P2P Environments

- **Management**
  - Funded
  - Bretagne Telecom Institute, SERES Team
  - End Time: 31 August 2012

Semsoft Company

- SWID Company of Lyon, SOC Team, Project leader
- National Institute for Applied Sciences, MTIC Team
- Paris Telecom Institute, SIMBAD Team
- Bretagne Telecom Institute, SERES Team
- Research Institute of Toulouse, IRIT, PYRAMIDE Team
- Semsoft Company
- SWID Company
Project Context, Challenges and Objectives

- **Context**
  - The medical domain requires mechanisms for enabling dynamic data sharing and exchange. But these mechanisms should take into account the security and privacy aspects.
  - Healthcare institutes need to establish policies for data access based on security and confidentiality standards, such as ISO/IEC 27002.
  - Web Services and P2P technologies are increasingly used in the field of distributed healthcare information systems.
PAIRSE Objectives

- Create and implement a services platform for medical data exchange preserving their privacy and confidentiality
- Create an approach for automatic web services composition
- Solve the problem of privacy policies conflict
- Create a trust policy to control data transfer from one peer to another, handling the questions: what?, why?, to whom?
Telemedicine Application Scenario

Data Privacy Preservation in Telemedicine: The PAIRSE Project, MIE 2011, August 28th – 31st, Oslo, Norway
Mono-Peer Query Processing

XML document encapsulating medical data and ECG signals according to the SCP-ECG ISO standard

Emergency Physician

Decision

Notification

Query « Q » Result « R »

Global confidentiality policy
Query Transformation

Web services discovery, selection, composition, and execution

EHR Portal
Integrating the future PAIRSE system

DP Web Services

Q1 = {!ssn, ?cd, ?mh, ?all, ?rf}

Q2 = {!ssn, ?ssb}

Data Privacy Preservation in Telemedicine: The PAIRSE Project, MIE 2011, August 28th – 31st, Oslo, Norway

Multi-Peer Query Processing

XML document encapsulating medical data and ECG signals according to the SCP-ECG ISO standard

Decision

Notification

Patient Transfer

Q1 = {IsSn, ?cd, ?mh, ?all, ?rf}

Q2 = {IsSn, ?ssb}

Q3 = {IsSn, ?cd}

Q4 = {IsSn, ?mh}

Q1

Q2

Q3

Q4

Legend

Q: Query
R: Result
I: Input Parameter
O: Output Parameter
WS: Web Service
IsSn: Social Security Number
?cd: Chronic Diseases
?mh: Medical History
?all: Allergies
?rf: Risk Factors
?ssb: Social Security Benefits

Data Privacy Preservation in Telemedicine: The PAIRSE Project, MIE 2011, August 28th – 31st, Oslo, Norway
PAIRSE Architecture

Multi Peer Query Processing
Query Decomposition, Peer Discovery, Query Transformation, Results aggregation

Local Peer Query Processing
- Privacy preserving RDF Query Answering
- Query Optimization

DP service and privacy policy representations
- RDF Views representations of DP services
- RDF representations of Privacy policies

SPARQL Global Query
Composition of DP services

SPARQL Local Query
Composition of DP services
A Privacy Model for Services

- For each data item manipulated by a service, we need to define:
  - In which circumstances can a data item be released
  - Applicable Privacy Operations (e.g. Anonymization, Nullification, ...)

```
<table>
<thead>
<tr>
<th>daasprivacy:Privacy Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>daasprivacy:PrivacyRule</td>
</tr>
<tr>
<td>daasprivacy:hasScope</td>
</tr>
<tr>
<td>daasprivacy:DataRight</td>
</tr>
<tr>
<td>Data Item (Datatype Property)</td>
</tr>
<tr>
<td>daasprivacy:AppliesTo</td>
</tr>
<tr>
<td>daasprivacy:hasCondition</td>
</tr>
<tr>
<td>daasprivacy:hasPurpose</td>
</tr>
<tr>
<td>daasprivacy:hasRecipient</td>
</tr>
</tbody>
</table>

- daasprivacy:Purpose
- daasprivacy:Recipient

- Physician
- Nurse

- daasprivacy:ApplicablePrivacyOp
- daasprivacy:Privacy Operation

- K-Anonymity
- Nullification

- "Yes/No"
- "SPARQL Query"
```
Automatic Web Services Composition

1. Query transformation in order to integrate the global privacy policy
2. Rewriting the transformed query in terms of web services
3. Automatic composition and web services execution
4. Results filtering according to user preferences

---

Data Privacy Preservation in Telemedicine: The PAIRSE Project, MIE 2011, August 28th – 31st, Oslo, Norway
Conclusion

The PAIRSE Project has designed a web services and P2P based architecture enabling data exchange preserving data privacy that is:

- generic and compliant with the standards and recommendations in use
- efficient for data integration via the automation of web services composition
- a valuable solution for medical data exchange between healthcare professionals