Expression and Deployment of Integrated Security Policies in the Context of Outsourced Data

Context and Goal

Context

- Security, privacy: major issues impacting the uptake of cloud computing, particularly in database outsourcing.
- Several mechanisms are defined in order to protect sensitive information in outsourced databases.

Goal

- According to security policies defined by database owners and the context in which these databases are outsourced, deploy the best of existing techniques allowing to efficiency enforce these security policies.

Motivating Scenario

Two entities:

- A bank.
- A credit company.

They observe different sets of attributes about the same set of individuals, e.g.:

\[ T_1 = \{ \text{SSN, Age, Address, Gender, Balance} \} \]

\[ T_2 = \{ \text{SSN, Job, ZIP, Nationality, Salary} \} \]

Each party defines a set of constraints to be satisfied

- They want to integrate their data in order to be able to make better decision making such as loan or card limit approval.

Constraints

Security constraints:

- Confidentiality constraint: A data owner may require that some information are sensitive and must be protected.
  
  Example: The values of the attribute \( a_1 \) of the table \( T_1 \) are sensitive
  
  \[ \text{Sensitive}(a_1) = \{ a_1 \} \]

- Anonymization constraint: Preventing identity disclosure by protecting personal identifiers.
  
  Example: Preventing identity disclosure in the table \( T_2 \)
  
  \[ \text{WithoutDisclosure}(t_2) \]

Utility constraints:

- A data owner may require the respect of certain particular property on his data.
  
  Example: Be able to perform aggregate operations over the attribute \( a_2 \):
  
  \[ \text{lossOfPrecision}(a_2) \]

Proposed Methodology

1. Using an Epistemic Linear Temporal Logic (Epistemic LTL), We Define an expressive language allowing to:
   - Formally express the used system.
   - Formally specify security requirements.

2. Study of the security properties of the mechanisms allowing to achieve the chosen goal

3. Express theses security properties using our language.

4. Formally identify the relevant mechanisms according to the security policy to be enforced.

Security mechanisms Properties

Goal: Data join

- Secure Join: Protect sensitive attributes using encryption
  
  Only sensitive attribute is protected, all other involved attributes are released.
  
  The join attribute will be always released.

- Anonymous Join based on local k-anonymity
  
  - Identifier attributes will not be released.
  
  - Quasi-identifier attributes values will loss precision as they will be generalized.
  
  - Ensure the k-anonymity of the join tables.

- Anonymous Join based on distributed k-anonymity
  
  - Identifier attributes will not be released.
  
  - Quasi-identifier attributes values will loss precision as they will be generalized.
  
  - Ensure the k-anonymity and the l-diversity of the join tables.

How to choose the best mechanisms?

Contact: Anis.bkakria@telecom-bretagne.eu
Website: www.telecom-bretagne.eu