Hippocratic PostgreSQL
Jalaja Padma1, Yasin N. Silva1, Muhammad U. Arshad2, Walid G. Aref1
Department of Computer Science, Department of Electrical and Computer Engineering
Purdue University, West Lafayette, Indiana

Motivation

• Privacy preservation:
  - An important component of information systems that deal with personal data
  - Laws recognize the right of data owners to control
  - Personal data is handled in compliance with its associated privacy definition
  - Hippocratic database system (HDB):
    • Has privacy as a core principle
    • Allows automated, fine-grained data disclosure at the database level
  - HDBs are an answer to data owners' privacy requirements
    • With whom their data is shared with
    • Purposes for which data can be shared

• Previous work has discussed the main guidelines and proposed an initial architecture
  - We implement HDB components as an integral part of an open-source DBMS
  - The requirements of privacy are addressed at the database level
    ➤ Developers can build more easily information systems that protect the privacy and ownership of data

Main Components

• Open-source privacy-aware DBMS
• Framework to test-and-integrate new privacy related components
• The project includes the implementation of components to support:
  • Limited Disclosure
  • Retention Time
  • Management of Multiple Policies and Policy Versions
  • Support for K-anonymity and Generalization Hierarchies

Architecture of Hippocratic PostgreSQL

Limited Disclosure and Retention Time

• Hippocratic PostgreSQL’s "Privacy-Aware Query Processor"
• Privacy Policy Metadata tables and the data owner preferences

Translation Process

Privacy Policy Translation

• Policy Translator
The Hippocratic PostgreSQL command to perform the translation:

```
TRANSLATE POLICY <policy-path> [FROM <language>]
[POLICY_ID <policy-id> POLICY_VERSION <policy-version>]
```

• Translation Process
• Privacy Policy Translation Catalog
• Privacy Policy Metadata