A Policy Based Infrastructure for Social Data Access with Privacy Guarantees

Palanivel Kodeswaran* and Evelyne Viegas†

*University of Maryland, Baltimore County   †Microsoft Research

Motivation

❖ Emergence of social networks of various types where users want to share data yet retain control

❖ Large amounts of user data are held behind the vaults of large corporations due to legal requirements

❖ Researchers need access to these datasets to study user patterns and other trends

Problem Statement

Build a data sharing framework for scientific research while guaranteeing and enforcing user privacy preferences

Proposed Solution

A policy based infrastructure which

❖ Allows users to specify who can access data and its acceptable use

❖ Introduces additional access modes to control the amount of information that is released by exploiting emerging privacy preserving data analysis techniques
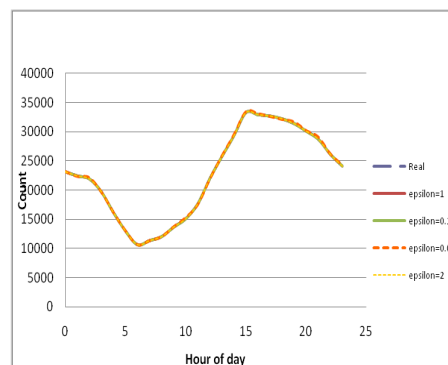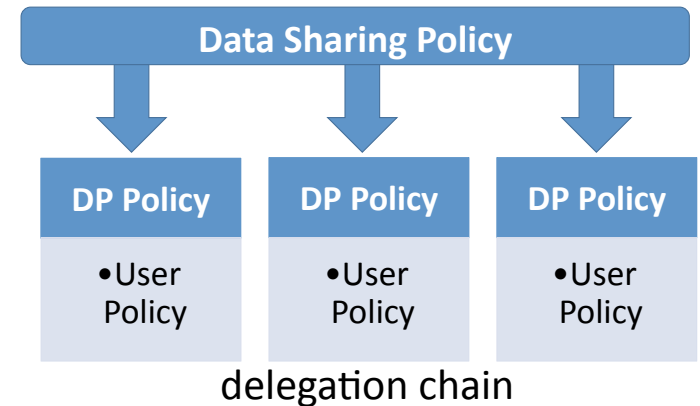
Complete Access

Abstract Access

Bonds 20% - 30%

Stocks 70% - 80%

Statistical Access

Policy Infrastructure

Data Sharing Policy

DP Policy — •User Policy

DP Policy — •User Policy

DP Policy — •User Policy

delegation chain

Implementation and Evaluation

❖ Prototype implemented using SecPAL

❖ Create new verbs from purpose and access mode

Emergency + Complete Access => EmergencyCompleteAccess

❖ Modified census dataset from UCI
  • manually generated ID and salary

❖ Abstract access on age returns age group, viz. 30-40

❖ Statistical access implemented using differential privacy