

Enhanced security guarantees for sensitive statistical studies

Baldur Kubo

Goal of UaESMC, FP7 project

To push the state of the art in the secure multiparty computation (SMC) above the threshold for applicability in many sectors of the society.

- ⊙ **How:** by identifying common problems and solving them using cryptographic, game-theoretic and engineering means.
- ⊙ **Source:** Talviste R, Laud P, 2012, Review of the state of the art in secure multiparty computation FP7 UaESMC
<http://www.usable-security.eu/files/d21.pdf>

Interesting for statisticians

Description of use cases of applying secure multiparty computations, especially:

- ⊙ **Case D4:** Statistical office collecting data with improved security,
- ⊙ **D1** researcher hosting sensitive data in a cloud,
- ⊙ **D2a:** A researcher interested in data from state databases using third-party miners and
- ⊙ **D2b:** Researcher interested in data from state databases using built-in computing possibilities of state infrastructure

Puulmann-Vengerfeld P et al., 2012, Capability Model FP7 UaESMC <http://usable-security.eu/files/D1.1.pdf.pdf>

Total list of cases discussed:

- ⊙ A: Three competitors
- ⊙ B1: Two competitors and a “neutral” computer
- ⊙ B2: energy market suppliers and customers
- ⊙ B3: Several energy market suppliers and one customer OR one supplier and several customers
- ⊙ C: An organization interested in its members’ info
- ⊙ **A researcher**
 - ⊙ D1: hosting sensitive data in a cloud
 - ⊙ D2a: interested in data from state databases using third-party miners
 - ⊙ D2b: interested in data from state databases using built-in computing possibilities of state infrastructure
- ⊙ D3: **Statistical** data collection **organizations working together** for better results
- ⊙ D4: **Statistics office** collecting data with **improved security**
- ⊙ **State database**
 - ⊙ E1: and interested non-state parties
 - ⊙ E2: and interested non-state parties (with the computation outsourced)

Current state

- ⊙ Researching the motivation and needs for enhanced security
UaESMC FP7 project <http://www.usable-security.eu/en>
- ⊙ Functionality: Privacy-preserving
 - ⊙ data acquisition (existing sources or data entry)
 - ⊙ database linking
 - ⊙ statistical analysis
 - ⊙ integration with reporting tools

Example: Income Analysis

Problem : How to analyse income over several organizations and preserve privacy of data subjects, and optimize infrastructure costs by using the cloud

Solution: Sharemind® on the public cloud:

- ⊙ Amazon EC2,
 - ⊙ Microsoft Azure and
 - ⊙ Zone Media.
- ⊙ None of the cloud service providers or customers, nor data suppliers can access data - individual incomes, or find out who they belonged to.

The screenshot shows a web browser window with the address bar containing <https://sharemind.cyber.ee/clouddemo/>. The page has a dark background with a navigation menu at the top: **INTRODUCTION** (highlighted in orange), **REPORTS**, **SOURCES**, **ABOUT SHAREMIND**, and **CONTACTS**. The main heading is **Income analysis of the Estonian public sector**, with 'Income analysis' in orange and 'of the Estonian public sector' in white. A Sharemind logo (a cloud with a circular arrow) is in the top right. Below the heading, the text reads: 'Welcome to the income analysis of the Estonian public sector! This page compiles information from several public sector institutions in Estonia **into a short analysis.** The information is collected from the ministries and municipalities of Estonia and entered into a **cloud service based on Sharemind.** Sharemind uses secret sharing to guarantee that data stays anonymous during both collection and processing. The cloud servers compute statistics without reconstructing any of the private values.' At the bottom, there is an orange button that says 'Click here to access the report'.

<https://sharemind.cyber.ee/clouddemo/>

01.21.2014

7

CYBERNETICA

Income analysis of the Estonian public sector



INTRODUCTION • **REPORTS** • SOURCES • ABOUT SHAREMIND • CONTACTS

Get report

CYBERNETICA

Hosted by Amazon EC2

Active clients: 2

- READY

CYBERNETICA

Hosted by Microsoft Azure

Active clients: 2

- READY

CYBERNETICA

Hosted by Zone Media

Active clients: 2

- READY

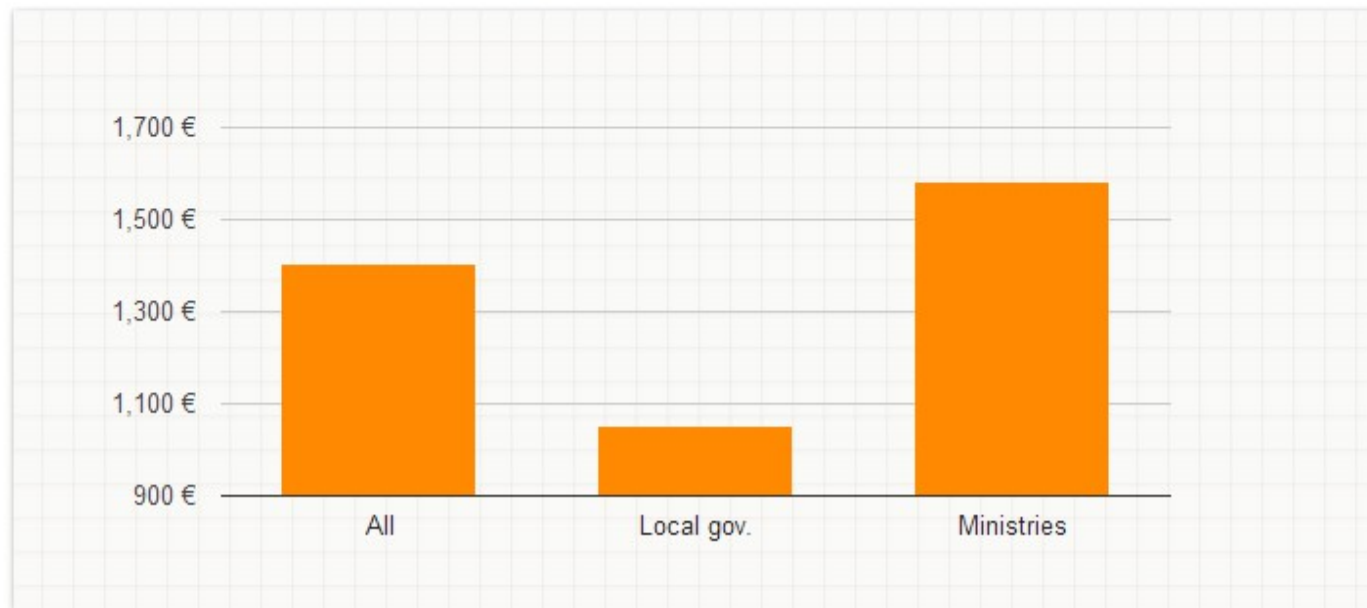
Income analysis of the Estonian public sector



INTRODUCTION • **REPORTS** • SOURCES • ABOUT SHAREMIND • CONTACTS

Please hover mouse over graphics to get additional information.

Overall average salary



CYBERNETICA

Hosted by Amazon EC2

Active clients: *disconnected*

✓ COMPUTATION FINISHED

CYBERNETICA

Hosted by Microsoft Azure

Active clients: *disconnected*

✓ COMPUTATION FINISHED

CYBERNETICA

Hosted by Zone Media

Active clients: *disconnected*

✓ COMPUTATION FINISHED

Where Next?

Future state:

- ⊙ Privacy-preserving statistical software and resulting study accuracy will be studied in 2014
- ⊙ Gathering feedback to the statistical software from researchers



CYBERNETICA

