Making private GPS data available to policy makers

Investigating the feasibility of multi-party computation for smart mobility

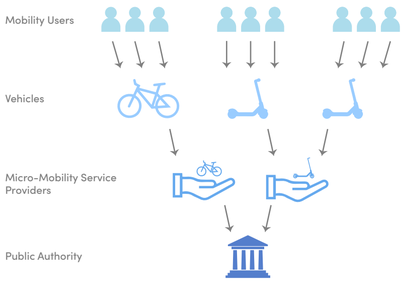
Delft University of Technology
CSE3000 Research Project

Marina Wiemers
m.c.f.wiemers@student.tudelft.nl

Supervisor: Zekeriya Erkin

1 STATUS QUO

using mobility data for infrastructure decisions



The shift in transit from using privately owned vehicles to **micro-mobility services**, such as bikes and e-scooters, has not only sparked discussions in terms of sustainability and accessibility [1] but has also introduced a surge of **personal, geolocational data** [2].

Sourcing this data from mobility providers allows public authorities to perform **quantitative analyses and validation of policies** via concrete data [3], facilitating decision-making for traffic and infrastructure management. Upon available and dependable sources, reports and strategies to optimise quality of life aspects, such as emissions, safety, sustainability, and accessability, can be made.

current barriers

Commercially Sensitive Data

Although mobility data holders can extract useful insights from aggregated data, they are still reluctant to provide their own to competitors or third parties.

Privacy and GDPR

With the introduction of the General Data Protection Regulation (GDPR), the extent of sharing identifiable data with third parties has been limited, calling for more private and secure sharing mechanisms.

2 HOW CAN MPC ENABLE A SECURE AGGREGATION OF MOBILITY DATA?

Multi-Party Computation (MPC)

MPC is a privacy enhancing technology that allows for safe and secure processing and sharing of data. Using cryptographic protocols, MPC enables computations, such as statistical aggregation or voting systems, while revealing only the output of the analysis, such that the input data remains hidden. Thus, MPC enables stakeholders and data owners to collaborate on statistics of aggregated data without needing to disclose any, commercially sensitive or personal, inputs.

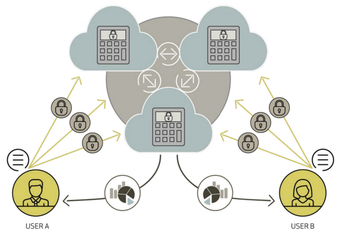


Figure 1. Multi-Party Computation: Users A and B provide data for a joint statistical analysis without revealing their inputs. [4]

3 GAINING INDUSTRY INSIGHTS

methodology

Literature Review

- Study of existing works of MPC
- Investigation of implementations and proofs of their robustness
- Exploration of real-world applications of MPC and feasibility analysis thereof

Stakeholder Interviews

- Semi-structured interviews for qualitative insights
- Establishing the status quo
- Eliciting requirements for a feasible architecture proposal

interviewees

- Ministry of Infrastructure and Water Management - *Dutch Government*
- Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk organisation Onderzoek (TNO) - *Research Organisation*
- POLIS Network - *Urban Mobility Network*
- Innopay - *Consultancy Firm*
- Argaleo - *Data-Driven Digital Twins*
- Mobidot - *Mobility ICT service provider*
- Bolt - *Micro-mobility provider*

4 A SECURE DATA-SHARING DESIGN

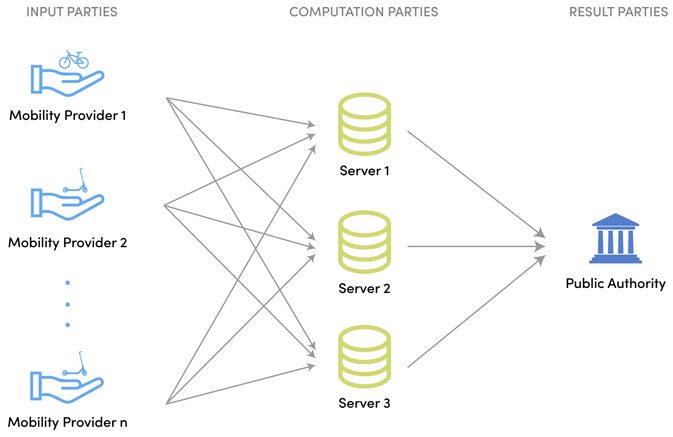


Figure 2. The input parties (mobility providers) prepare their data according to an agreed-upon database schema and share their records with the computation parties (impartial servers) via an additive secret sharing scheme. Upon receiving a query from the result party (public authority), the computation parties perform the according operation on the aggregated data and forward the result to the querier.

5 HOW FEASIBLE IS THE PROPOSED SYSTEM?

technical

Ensurable Security and Privacy

The proposed architecture follows data aggregation schemes like Sharemind [5] and uses additive secret sharing to ensure distribute private records among the computational servers. Working under the assumption of a *honest-but-curious* security model, input privacy and robustness are ensured as long as the majority of the computational servers remain uncorrupted.

Likely Scalability

Given the purely theoretical nature of this research and unavailable estimates of the size and extent of data sets to be analysed, it is difficult to draw conclusions regarden the latency. Similar implementations, however, suggest performances ranging from seconds to minutes [5], due to low communication overhead.

non-technical

Trust as a Potential Barrier

- The devised data-sharing design takes distrust among participating parties into account
- Stakeholder interviews have shown that data providers remain reluctant, sceptic and doubtful despite attempts to protect their data

Achievable GDPR Compliance

- Input privacy is ensured as third parties are oblivious to the inputs, thus personally identifiable data remains private

Need for (Data) Standards

- Mobility data standards are currently being devised and deployed
- MPC-suitable formats and regulations could be integrated in the design process

Public Acceptance: Accessibility, and Usability

- Fitting statistical models for data-driven mobility policy making are yet to be determined
- Governance, legal frameworks and subsidies pose barriers

6 REFERENCES

[1] Anna Kramers, Tina Ringenson, Liridona Sopjani, and Peter Arnfalk. AaaS and MaaS for reduced environmental and climate impact of transport. In *ICT4S*, pages 137–152, 2018.

[2] Francesco Calabrese, Mi Diao, Giusy Di Lorenzo, Joseph Ferreira Jr, and Carlo Ratti. Understanding in dividual mobility patterns from urban sensing data: A mobile phone trace example. *Transportation research part C: emerging technologies*, 26:301–313, 2013.

[3] Daniel C Esty and Reece Rushing. Governing by the numbers: The promise of data-driven policymaking in the information age. *Center for American progress*, 5:21, 2007.

[4] David W Archer, Dan Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P Smart, and Rebecca N Wright. From keys to databases—real-world applications of secure multi-party computation. *The Computer Journal*, 61(12):1749–1771, 2018.

[5] Dan Bogdanov, Sven Laur, and Jan Willemson. Share- mind: A framework for fast privacy-preserving compu- tations. In *European Symposium on Research in Computer Security*, pages 192–206. Springer, 2008.