

Privacy-Preserving Production Process Parameter Exchange

Jan Pennekamp, Erik Buchholz, Yannik Lockner, Markus Dahlmanns, Tiandong Xi, Marcel Fey, Christian Brecher, Christian Hopmann, and Klaus Wehrle

github.com/COMSYS/parameter-exchange

INTERNET OF PRODUCTION | RWTH AACHEN UNIVERSITY

https://comsys.rwth-aachen.de/

Austin / ACSAC 2020, 10th December 2020

Vision of an Internet of Production (IoP)

- **Federal-funded research cluster in Aachen, Germany**
  - Over 35 institutes in Aachen, ~ 50 Mio € in funding

INTERNET OF PRODUCTION | RWTH AACHEN UNIVERSITY

- **Goal is to create a "World Wide Lab"**
  - To *utilize data* from production, development and usage
  - In real time (adaptively) with an adequate level of granularity
  - Even in *cross-domain collaboration*

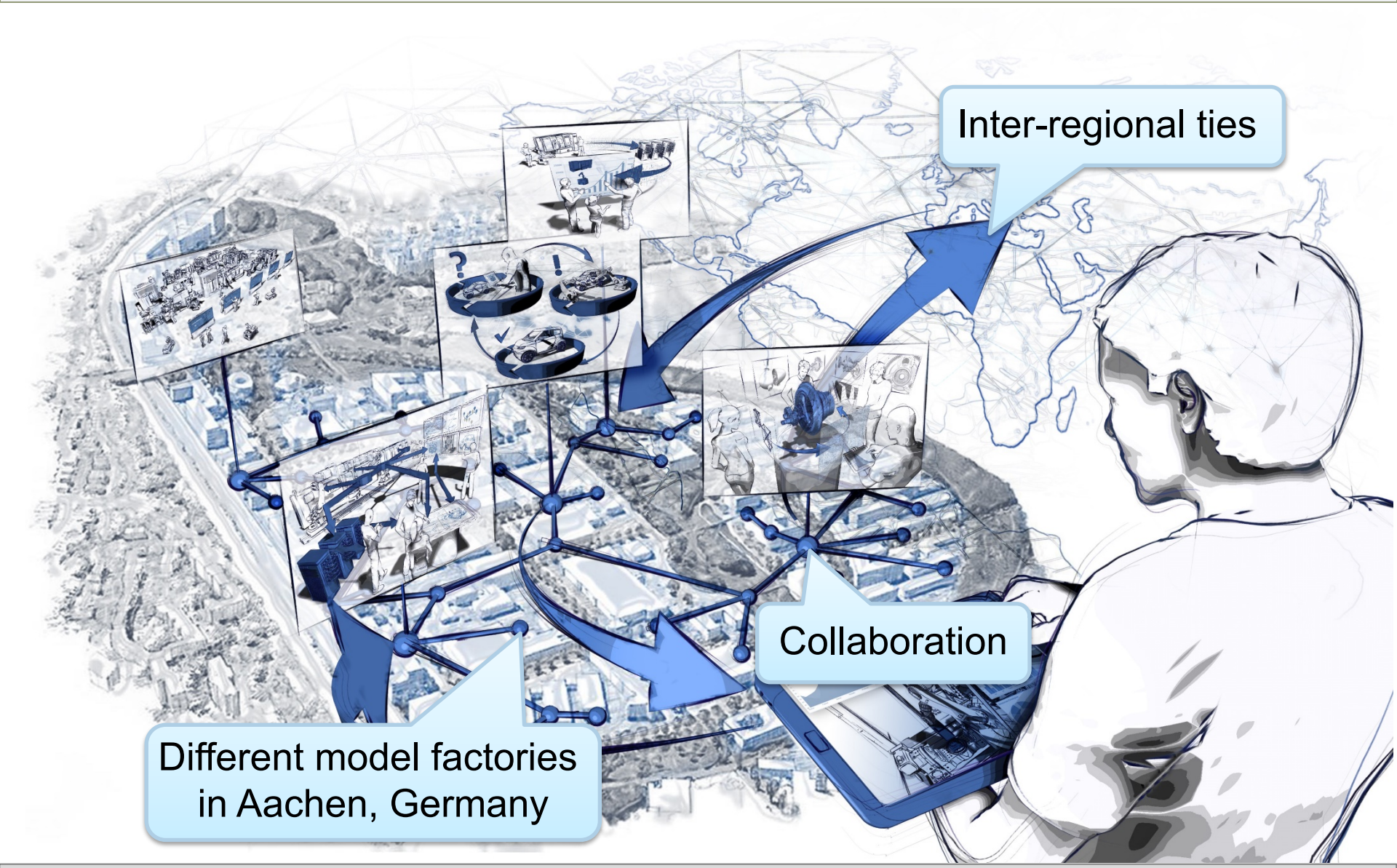
- **Establishing a Google-like engine for production queries**
  - Merging models and massive data to optimize processes



Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany 's Excellence Strategy – EXC-2023 Internet of Production – 390621612

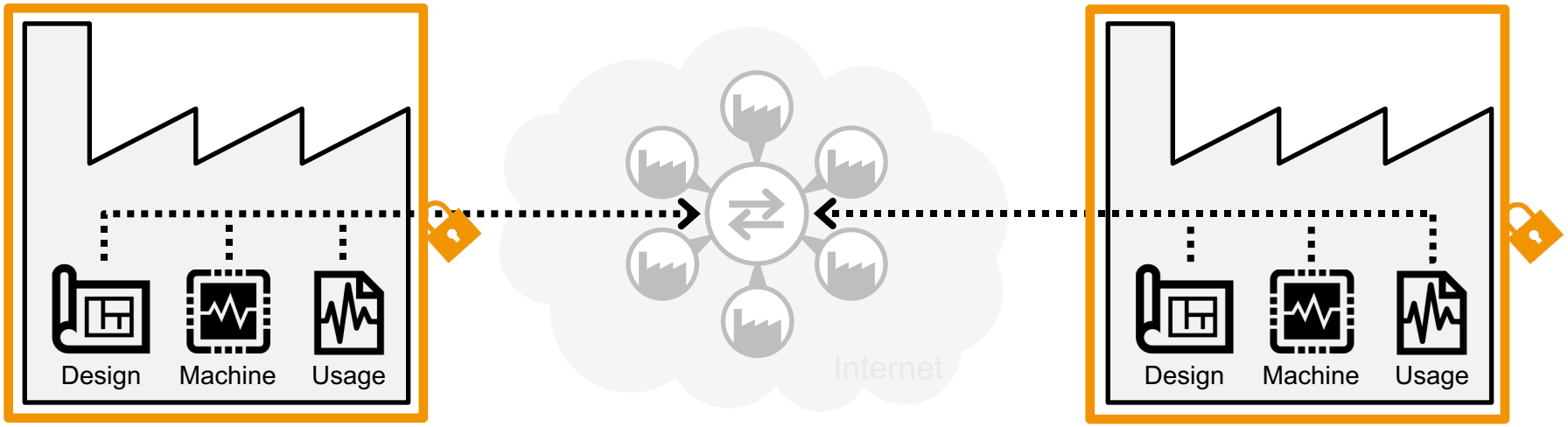
COM SYS | RWTH AACHEN UNIVERSITY

Illustration of an Internet of Production (IoP)



Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Problem Statement: A Lack of Industrial Data Sharing



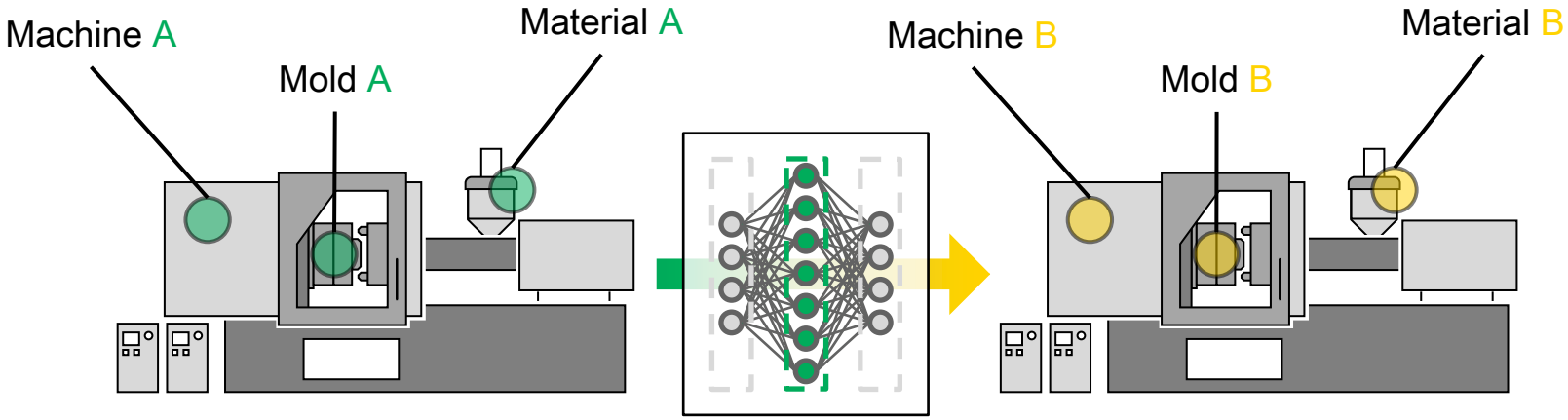
- **Lots of isolated domain-specific knowledge is available**
  - With the potential to improve quality, processes, costs, …
- **No way to privacy-preservingly access this information**
  - Concerns about data leaks, loss of control, …
  - Even a lack of incentives to share such (valuable) data

Demands a solution that (a) **addresses the concerns** of companies and (b) eases the **secure exchange** of (valuable) industrial data

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Exemplary Use Case: Injection Molding

- **Common use of resource-consuming empirical testing**
- **Process improvements by utilizing transfer learning**
  - Knowledge sharing (transfer learning) between models of different processes can reduce the necessary amount of training data

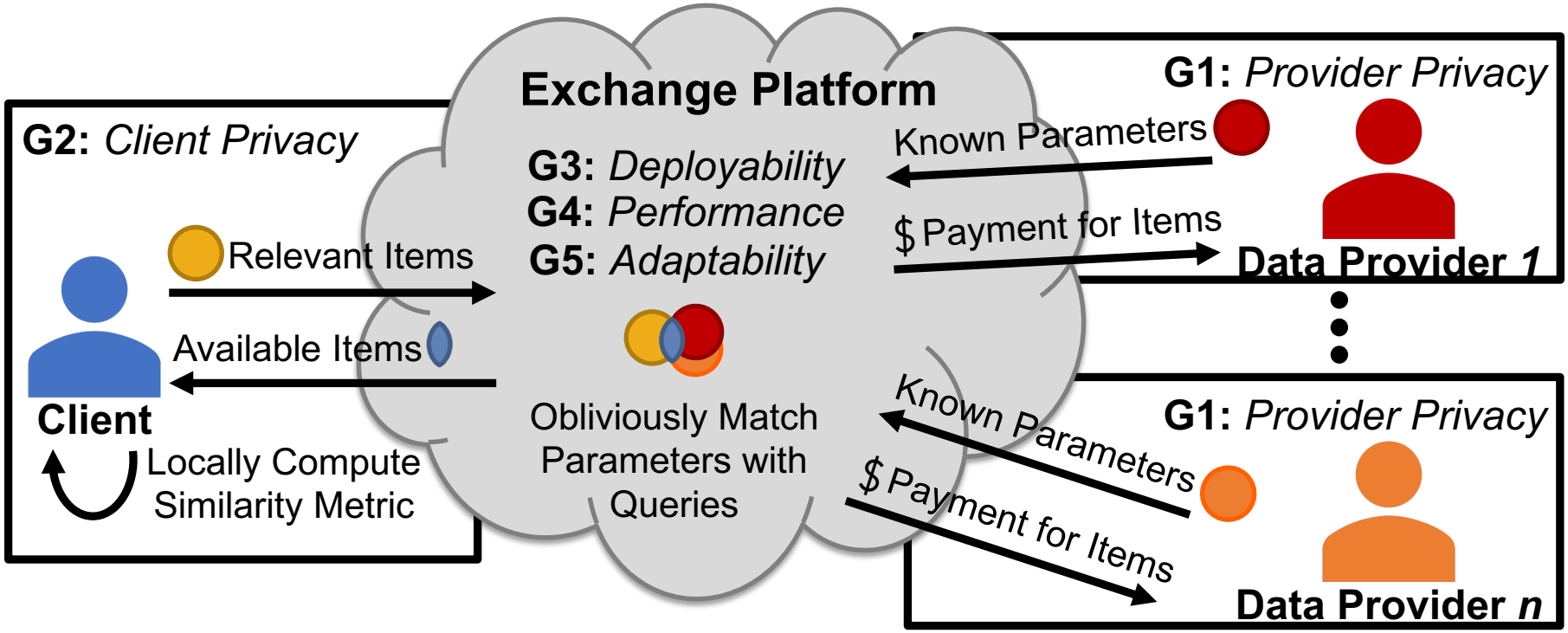


  - However: Most effective dataset(s) not necessarily locally available

In need of **privacy-preserving** approach to exchange process parameters between **mutually distrustful companies**

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Design Goals: Creating a Privacy-Preserving Exchange

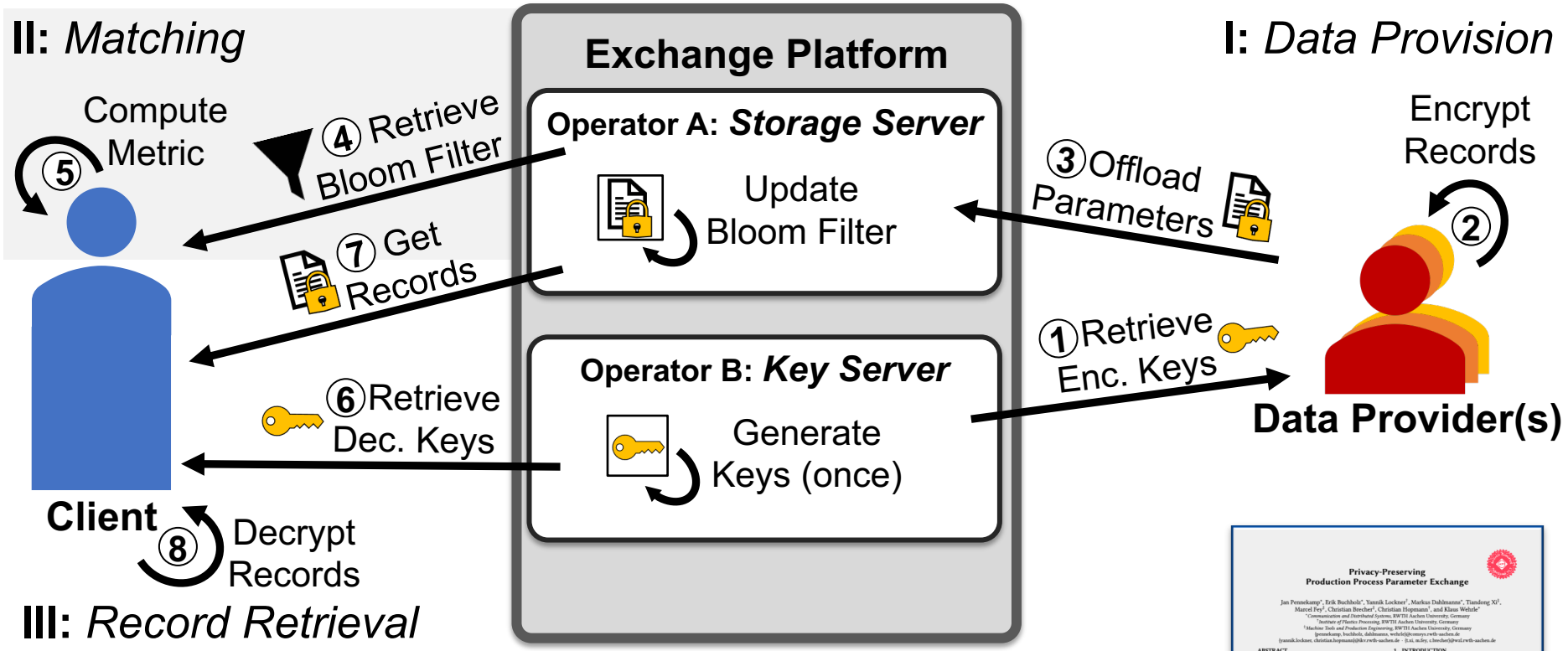


- **Related work is not suitable**
  - Either focus on client privacy or provider privacy
  - Sophisticated approaches do not scale to industry needs

Develop an applicable design

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Design: Bloom filter-based Parameter Exchange (BPE)




Privacy-Preserving Production Process Parameter Exchange

- See the paper for details on the notation, protocol specifics, and our security assumptions (for the server operators)

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

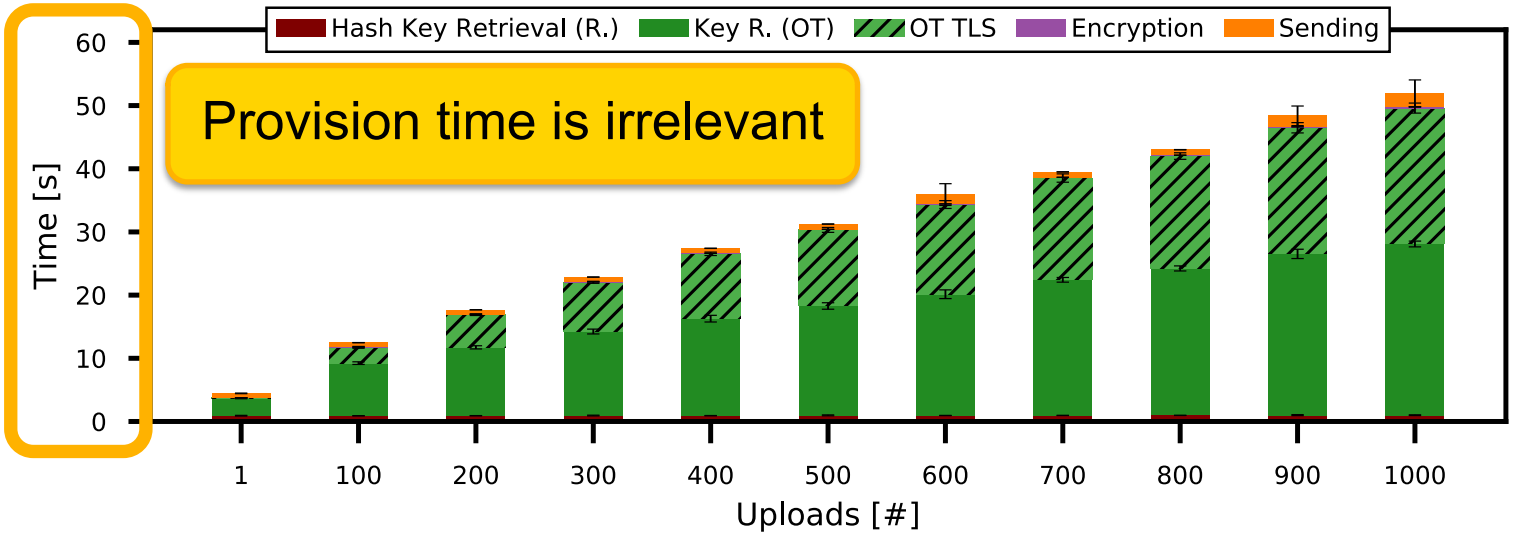
Performance Evaluation of BPE

- **4-fold approach to underline applicability & universality**
  1) Building block evaluation (Section 7.2)
     - Investigate individual components and network as well as scaling effects
  2) A random artificial scenario (Section 7.3)
     - Demonstrating our design's feasibility when combining the building blocks
  3) A real-world use case in the domain of injection molding (Section 7.4)
     - Exchanging production process parameters of toy bricks
     - Here: Identifying suitable parameters is allowed take up to several weeks
       - This includes the time for querying process parameters from our exchange and running the required transfer learning algorithm
  4) A second use case in the domain of machine tools (Section 7.5)
     - Underlining the universality of our parameter exchange

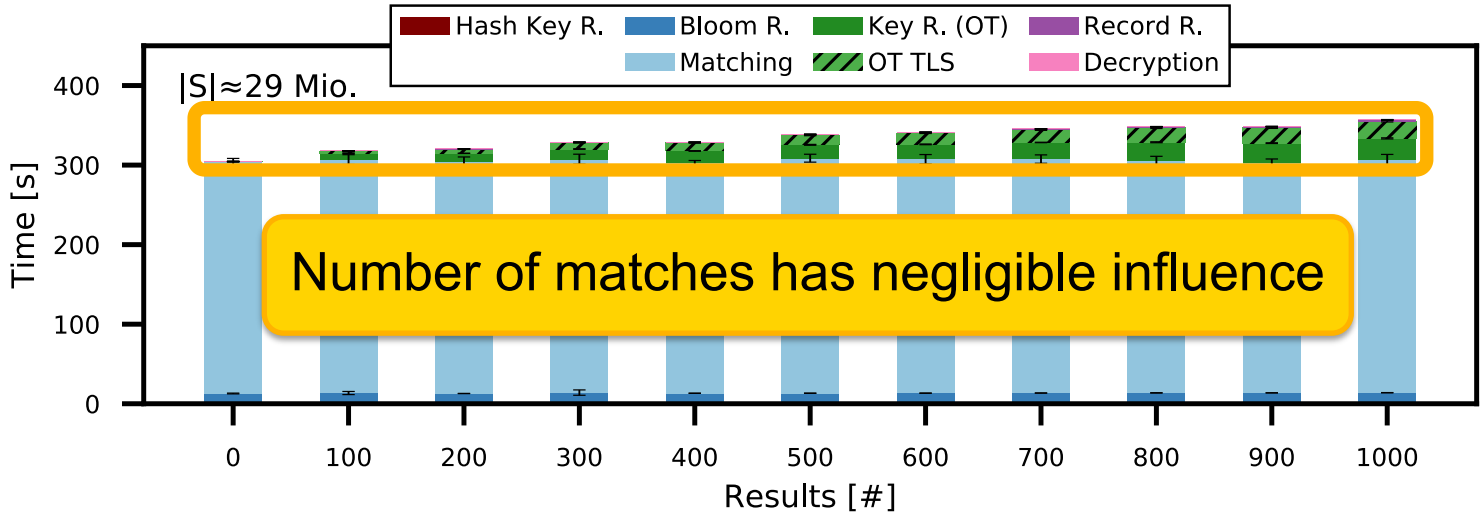
Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Provision and Querying in BPE

Provision



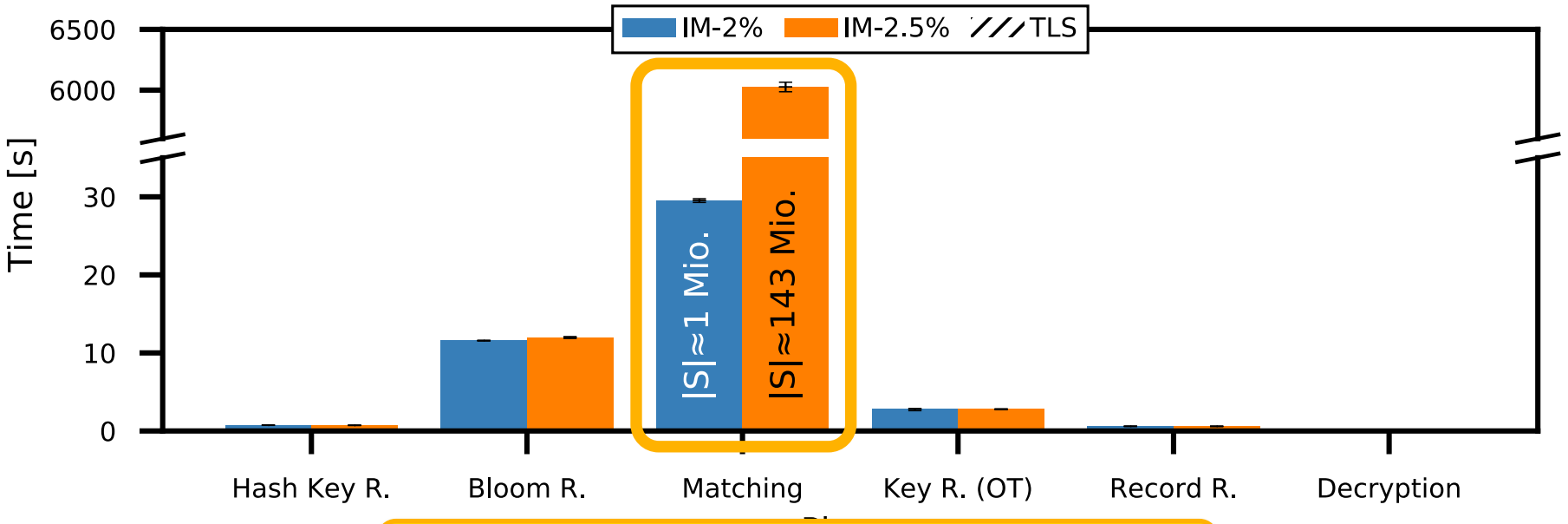
Querying



Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Real-World Performance in Injection Molding

- **Candidate set *S* can grow significantly (metric-driven)**
  - 21 identifying parameters to obtain vectors with 28 detailed entries
  - Apply a “binning” to 2 digits per parameter
  - IM-**x**%: Use a relative offset of **x**% for each parameter



Client runtime dominates our approach

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Curious? Additional Content!

- **Security discussion (Section 8.1)**
- **Second design variant PPE (Section 8.2)**
  - Utilizing PSIs instead of Bloom filters to improve provider privacy (no Bloom filter-induced leakage of the indexed indices)
- **Universality of our parameter exchange (Section 7.5)**
  - Second use case in the domain of machine tools

Source code

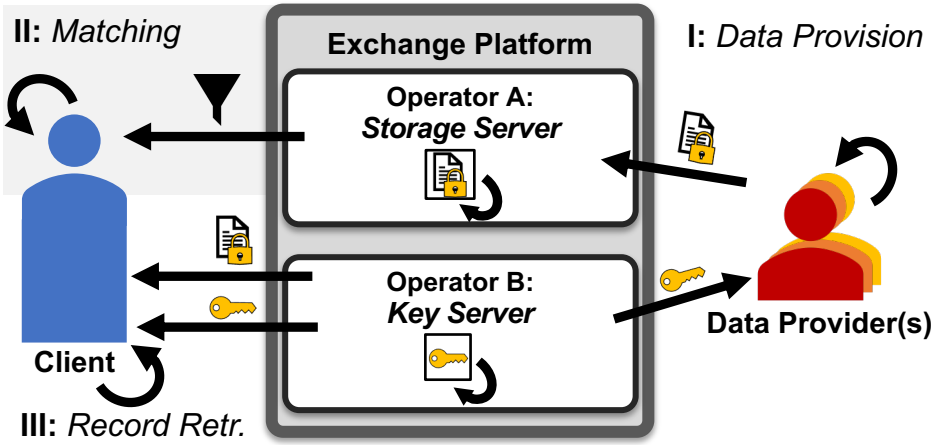


For details, check the paper

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Conclusion: BPE – A Privacy-Preserving Exchange

- **Approaches for industrial data exchanges are missing**
  - Lots of potential is wasted (in terms of quality, costs, …)
- **Real-world applicable privacy-preserving parameter exchange**
  - For industry needs
  - Scalable & universal



- **Demonstrated BPE with two real-world use cases**
- **Account for the needs of tomorrows industrial landscape**
  - Considering both client and provider privacy to address any concerns

Thank you for your attention!

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de