Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Leveraging Secure Multiparty Computation in the Internet of Things

Marcel von Maltitz, Georg Carle

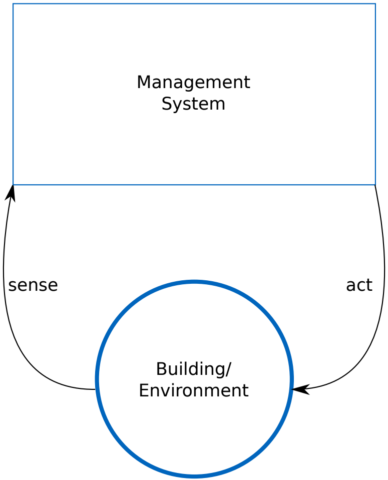
Tuesday 12th June, 2018

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

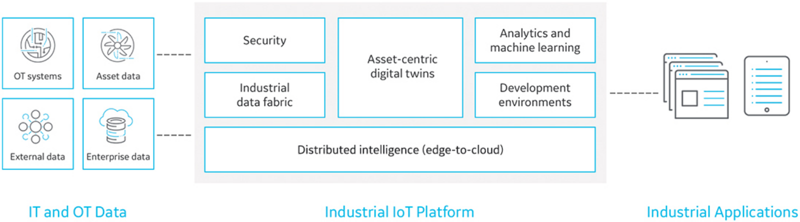
Smart Buildings – Industrial State of the Art

https://www.siemens.com/innovation/en/home/pictures-of-the-future/infrastructure-and-finance/smart-cities-smart-buildings.html

Smart Buildings: Model

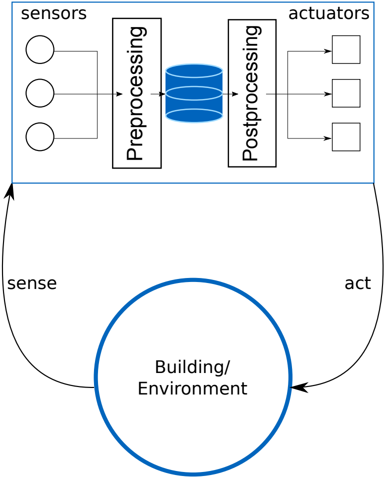


Smart Buildings – Industrial State of the Art



https://www.ge.com/digital/predix-platform-foundation-digital-industrial-applications

Smart Buildings: Model



Smart Buildings: Privacy Criticality

Types of Sensors

- Brightness
- Temperature / Humidity
- CO_2 concentration
- Motion
- Weight (on floor)
- Device usage
- Power consumption
- ...

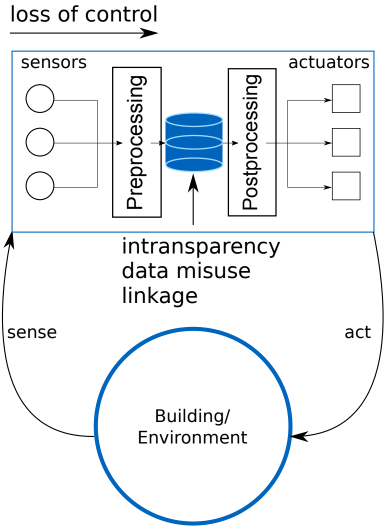
Privacy-criticality

- Location
- Behavioral patterns (cf. [8])

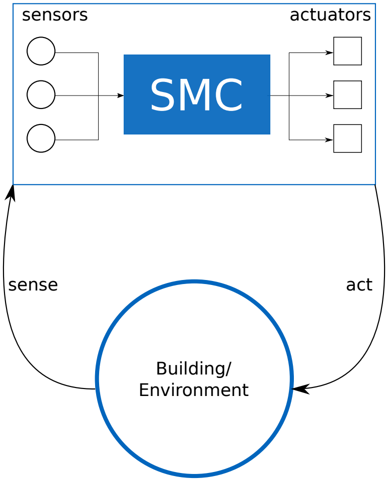
Threats (cf. [5])

- Intransparency of data usage
- Data misuse (other purpose)
- linkage (combination of data for more insights)
- Loss of control (data subjects)

Smart Buildings: Privacy Criticality



Smart Buildings: Application for Secure Multiparty Computation



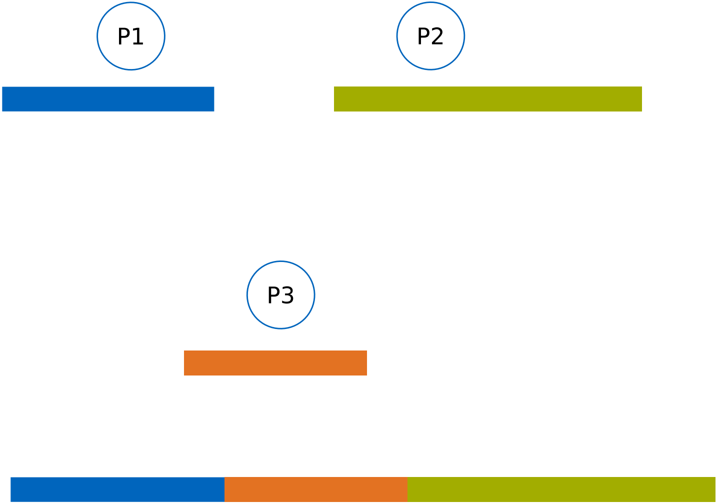
Secure Multiparty Computation

Definition (cf. [6])

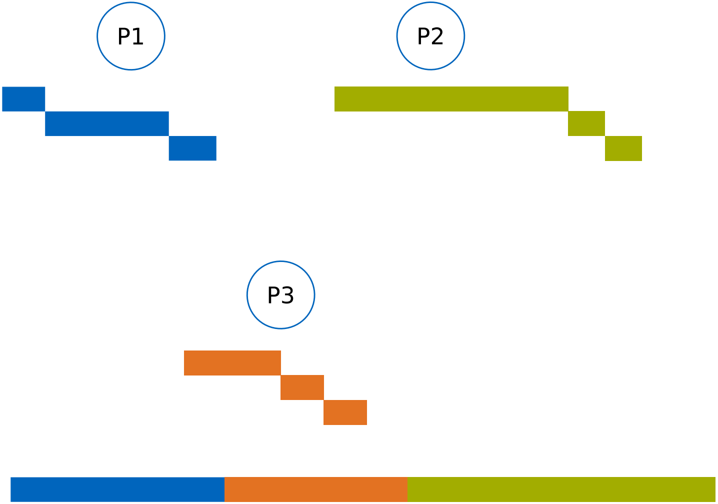
Given n parties $P_1, \ldots, P_n$. Each party P_i holds a secret value x_i.
Secure Computation of $y = f(x_1, \ldots, x_n)$ is performed if two conditions are satisfied:

- Correctness: the correct value of y is computed
- Privacy: y is the only new information that is released

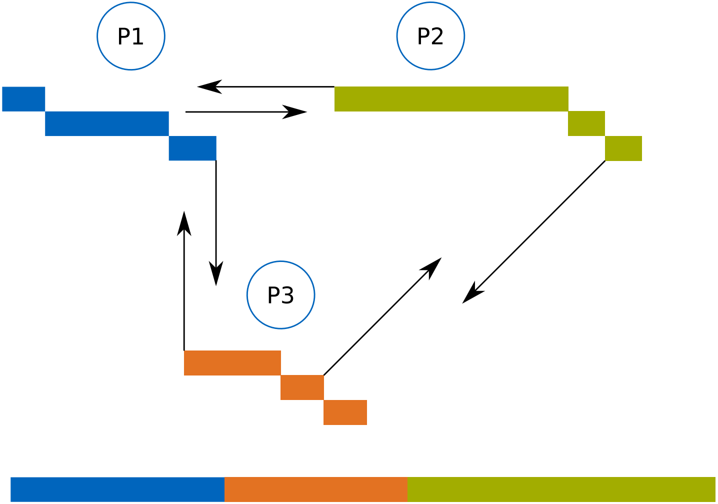
Secure Multiparty Computation: Example



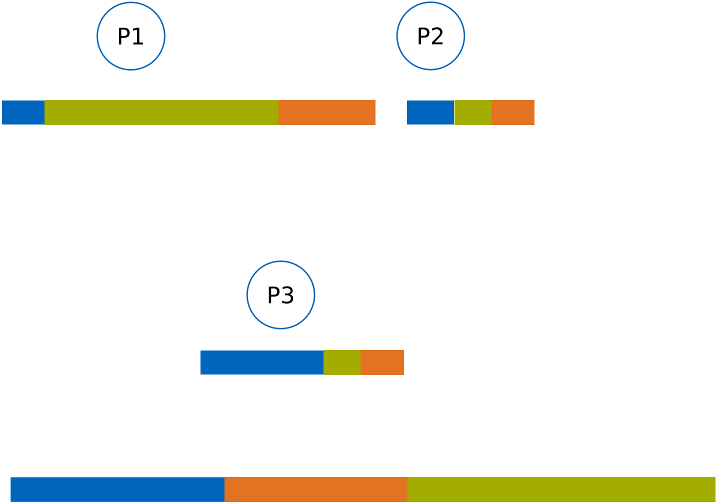
Secure Multiparty Computation: Example



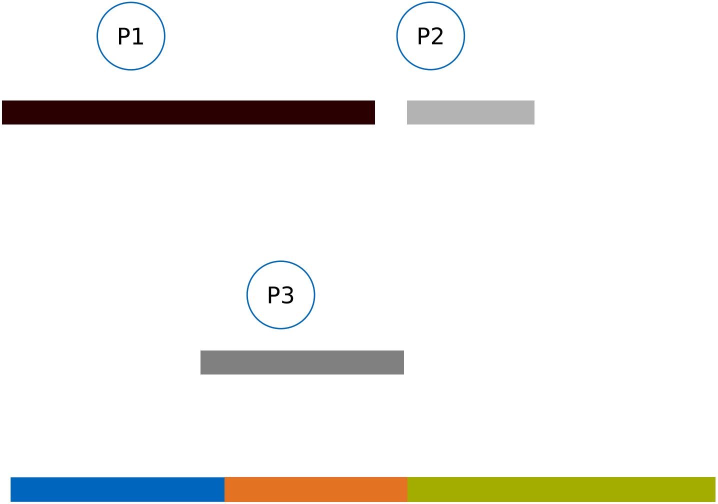
Secure Multiparty Computation: Example



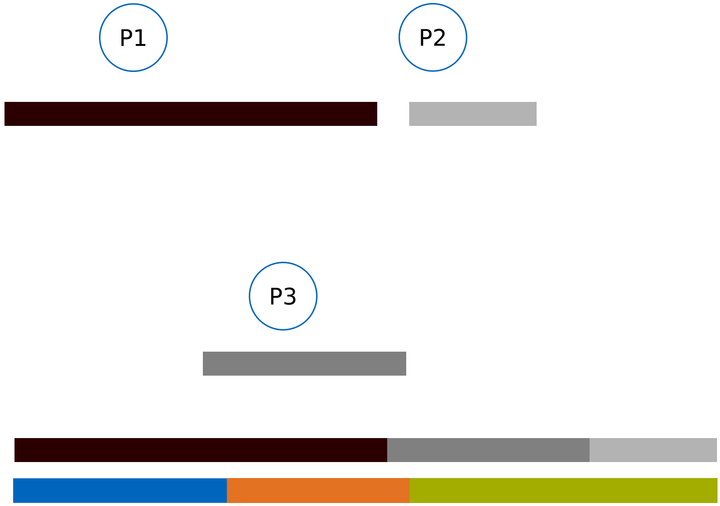
Secure Multiparty Computation: Example



Secure Multiparty Computation: Example

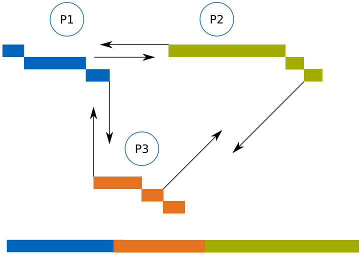


Secure Multiparty Computation: Example

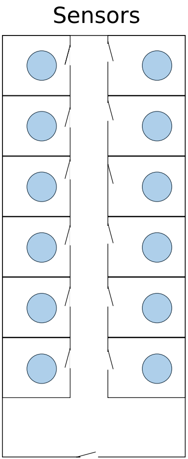


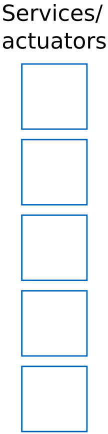
Secure Multiparty Computation: Previous Applications

- (Double) auctions [2]
- EU emission trading scheme (CO_2 trading) [9]
- KPI ranking among companies [1]
- Network anomaly and outage detection [4, 7]
- Federated learning (distributed machine learning) [3]

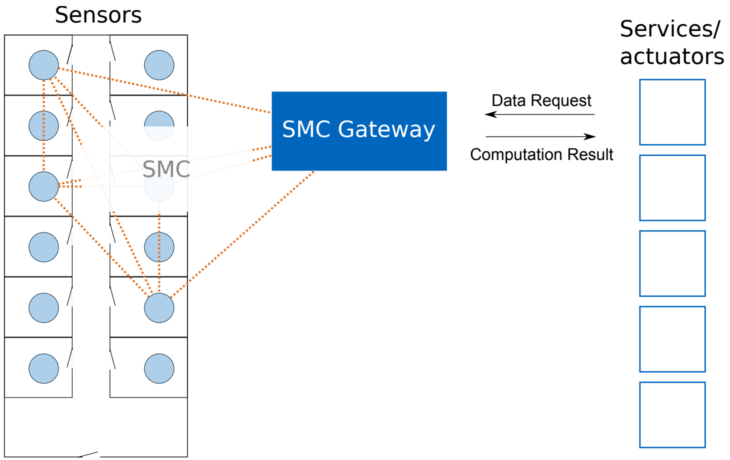


Leveraging SMC in the IoT: Design

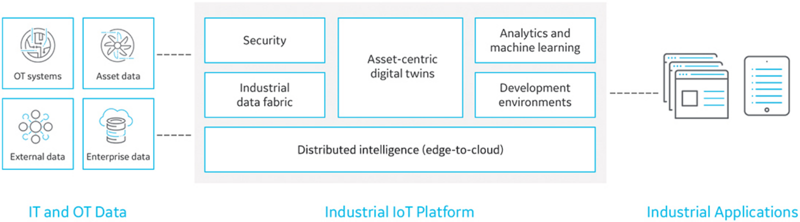




Leveraging SMC in the IoT: Design

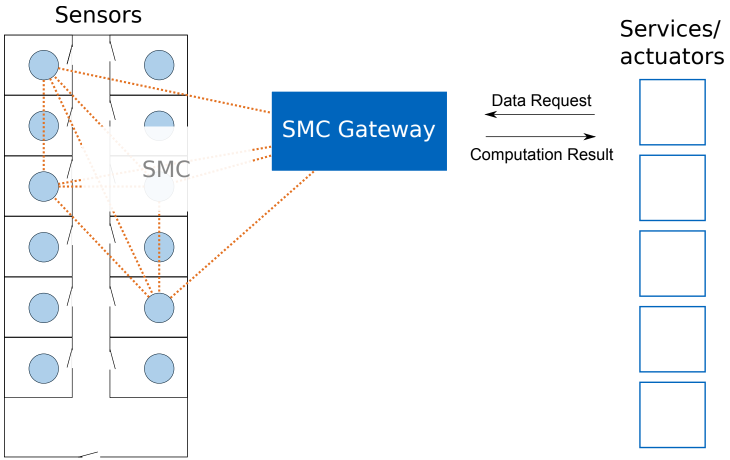


Leveraging SMC in the IoT: Design



https://www.ge.com/digital/predix-platform-foundation-digital-industrial-applications

Leveraging SMC in the IoT: Design



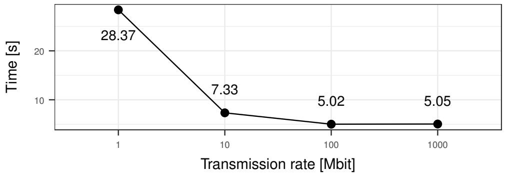
Leveraging SMC in the IoT: Addressed Challenges

A Performance and Resource Consumption Assessment of Secure Multiparty Computation.

M. von Maltitz and G. Carle. (2018, submitted)

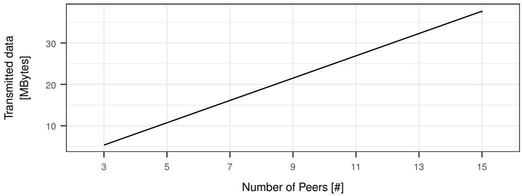
Parameters

- #Nodes
- CPU #cores and frequency
- network latency
- transmission rate
- packet loss
- parallelization



Variables

- Execution time
- CPU consumption
- Memory allocation (stack, heap)
- Bandwidth usage



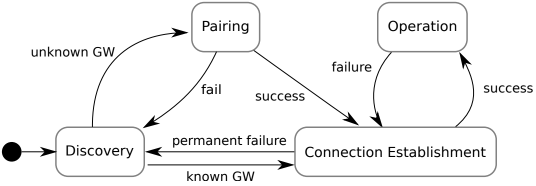
Leveraging SMC in the IoT: Addressed Challenges

A Management Framework for Secure Multiparty Computation in Dynamic Environments.

M. von Maltitz, S. Smarzly, H. Kinkelin, and G. Carle (NOMS 2018, DOMINOS Workshop)

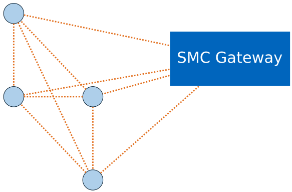
Peer Orchestration

- Discovery
- Pairing
- Recovery



Session Management

- Session Creation
- Peer allocation
- Monitoring
- Recovery



Leveraging SMC in the IoT: Addressed Challenges

Access control and Accountability for Secure Multiparty Computation.

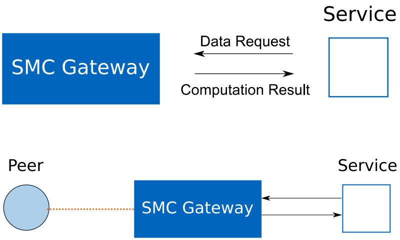
M. von Maltitz, D. Bitzer, and G. Carle. (2018, submitted)

Client Interaction

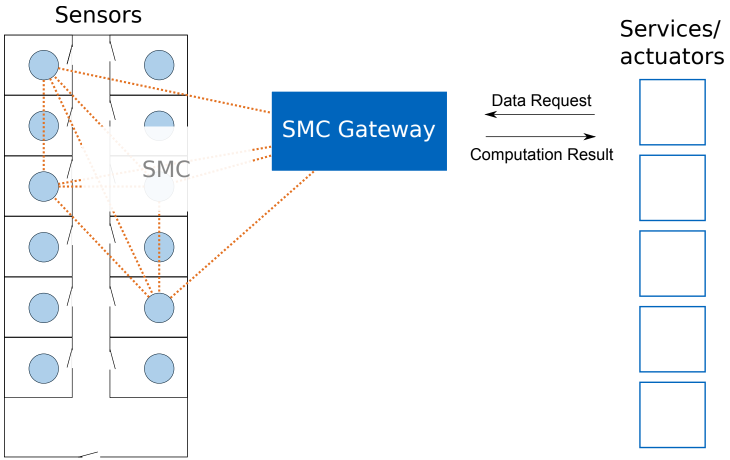
- Request and query formats
- Request generation
- Access control and authorization
- Request $\rightarrow$ session translation
- Result validation

Peer-side privacy protection

- Transparency of requests
- Intervenability upon computation
- Accountability of performed requests/ computations



Leveraging SMC in the IoT: Addressed Challenges



Bibliography

[1] D. Bogdanov, R. Talviste, and J. Willemson.
Deploying secure multi-party computation for financial data analysis.
Financial Cryptography, pages 57 – 64, 2012.

[2] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft.
Secure multiparty computation goes live.
In *Lecture Notes in Computer Science*, volume 5628 LNCS, pages 325–343, 2009.

[3] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth.
Practical Secure Aggregation for Privacy Preserving Machine Learning.
In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, volume 2017, pages 1175–1191, 2017.

[4] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos.
SEPIA: Privacy-preserving Aggregation of Multi-domain Network Events and Statistics.
Proceedings of the 19th USENIX Conference on Security, page 15, 2010.

[5] H. Chan and A. Perrig.
Security and privacy in sensor networks.
Computer, 36(10):103–105, 2003.

[6] R. Cramer, I. B. Damgard, and J. B. Nielsen.
Secure Multiparty Computation and Secret Sharing.
Cambridge University Press, New York, NY, USA, 2015.

[7] M. Djatmiko, D. Schatzmann, X. Dimitropoulos, A. Friedman, and R. Boreli.
Collaborative Network Outage Troubleshooting with Secure Multiparty Computation.
IEEE Communications Magazine, (November):78–84, 2013.

Bibliography

[8] A. Ridi, C. Gisler, and J. Hennebert.
A survey on intrusive load monitoring for appliance recognition.
Proceedings - International Conference on Pattern Recognition, pages 3702–3707, 2014.

[9] M. Zanin, T. T. Delibasi, J. C. Triana, V. Mirchandani, E. Álvarez Pereira, A. Enrich, D. Perez, C. Paşaoğlu, M. Fidanoglu, E. Koyuncu, G. Guner, I. Ozkol, and G. Inalhan.
Towards a secure trading of aviation CO2 allowance.
Journal of Air Transport Management, 56:3–11, 2016.