Accountable Federated Machine Learning in Government: Engineering and Management Insights

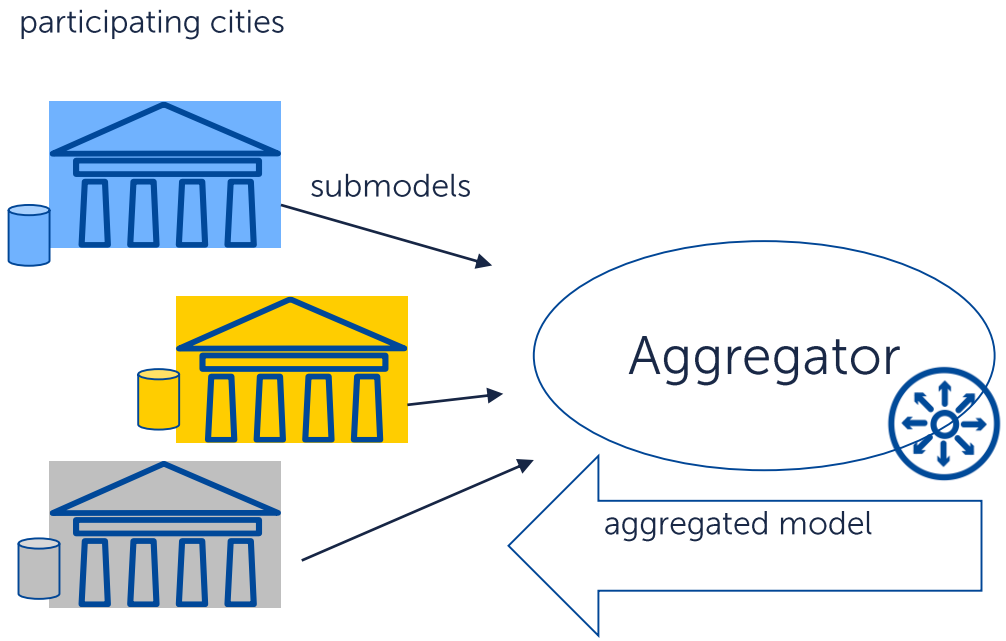
Dian Balta[1], Mahdi Sellami[1], Peter Kuhn[1], Ulrich Schöpp[1], Matthias Buchinger[1],
Nathalie Baracaldo[2], Ali Anwar[2], Heiko Ludwig[2], Mathieu Sinn[2], Mark Purcell[2], Bashar Altakrouri[3]

[1] fortiss GmbH, Research Institute of the Free State of Bavaria for software-intensive systems
[2] IBM Research
[3] IBM Cloud and Cognitive Software

Paper presentation, IFIP EGOV 2021, Granada, Spain

Motivation

Federated Machine Learning (FML) is great...



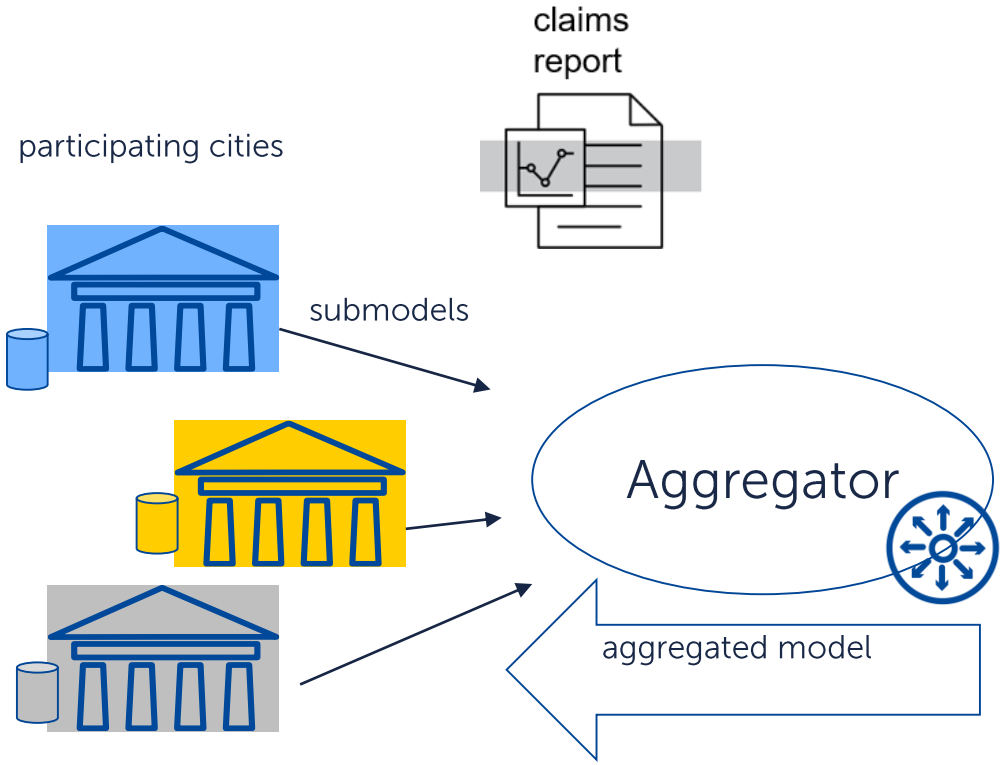
... unless, the world is not perfect

- Do we trust the FML protocol, its execution & the fulfilment of quality guarantees?
- What about the process of data pre-processing?
- How can we provide a verifiable claim about the FML supported by tamper-proof evidence to a third party?

Motivation

Accountability as a possible solution

- formalized workflows
- in distributed datalog
- for verifiable claims
- regarding guarantees of protocols
- in an asynchronous & incremental manner



Theoretical Background

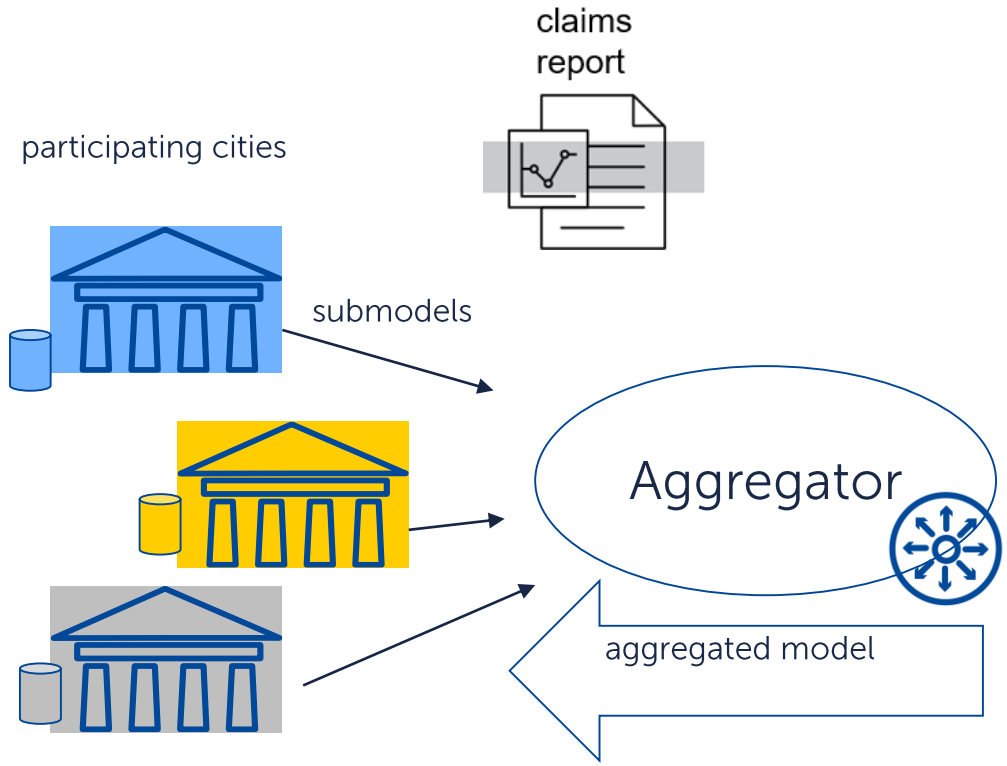
Federated Machine Learning

"Each client's raw data is stored locally and not exchanged or transferred"

(Kairouz et al., 2019)

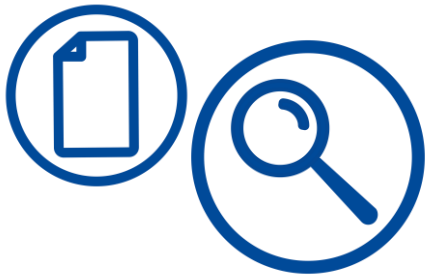
Accountability

Creating verifiable claims towards trustworthy FML, where trustworthiness is an argument that aims at explaining the design of a system



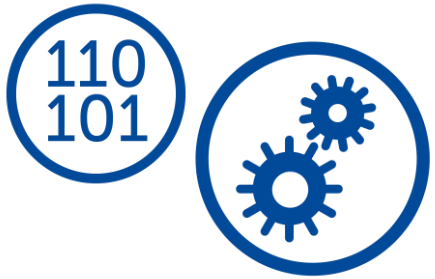
Research Approach

Qualitative analysis approach to explorative research



Hermeneutic literature review

- to develop our understanding of the concepts of accountability [19, 34, 35]
- and FML [16, 17, 36, 37]
- and derived implications from a standardization perspective [28, 29]



Prototype development

- data and a list of challenges from a research project on online citizen participation
- Application of natural language processing (NLP)
- Implementation of FML by representing different cities as different parties

Results

AFML sounds cool, but how should I approach it?

Engineering

Build an AFML system

Management

Administer an AFML system

Results

Engineering

Feasibility Evaluation for FML

Dimension	Characteristics		
data partitioning	horizontal	vertical	hybrid
ML model	linear model	decision tree	neural network
training data input	featured	raw	
training data output	structured	unstructured	
data federation	cross-silo	cross-device	
privacy preservation	differential privacy	cryptographic techniques	
network topology	centralized	decentralized	
federation need	economic incentive	regulation	
technology grade	research	industry	

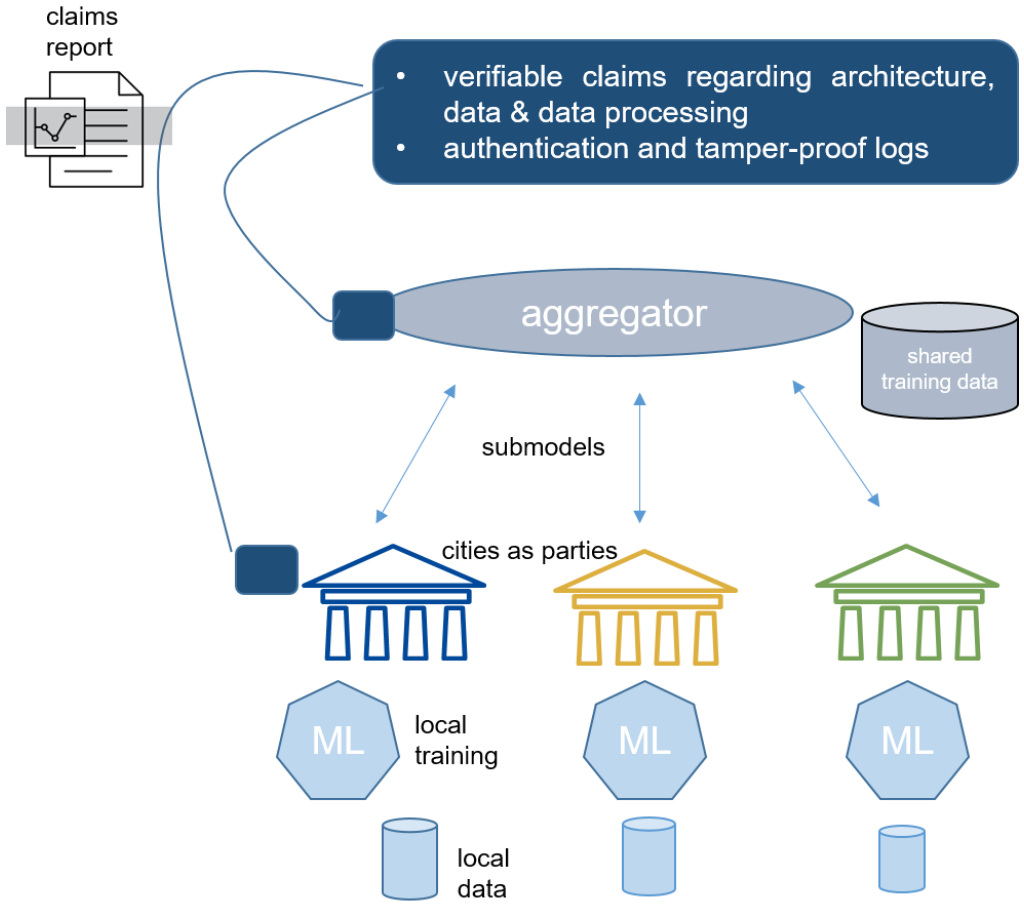
Results

Architecture of AFML

- *data partitioning would be rather horizontal,*
- *data federation would be cross-silo,*
- *network typology would be rather centralized*
- *and considered technologies should be industry or near-industry grade*

Accountability

- is paramount to fully overcoming legislative and jurisdictional constraints in federated machine learning -> verifiable claims and claims report



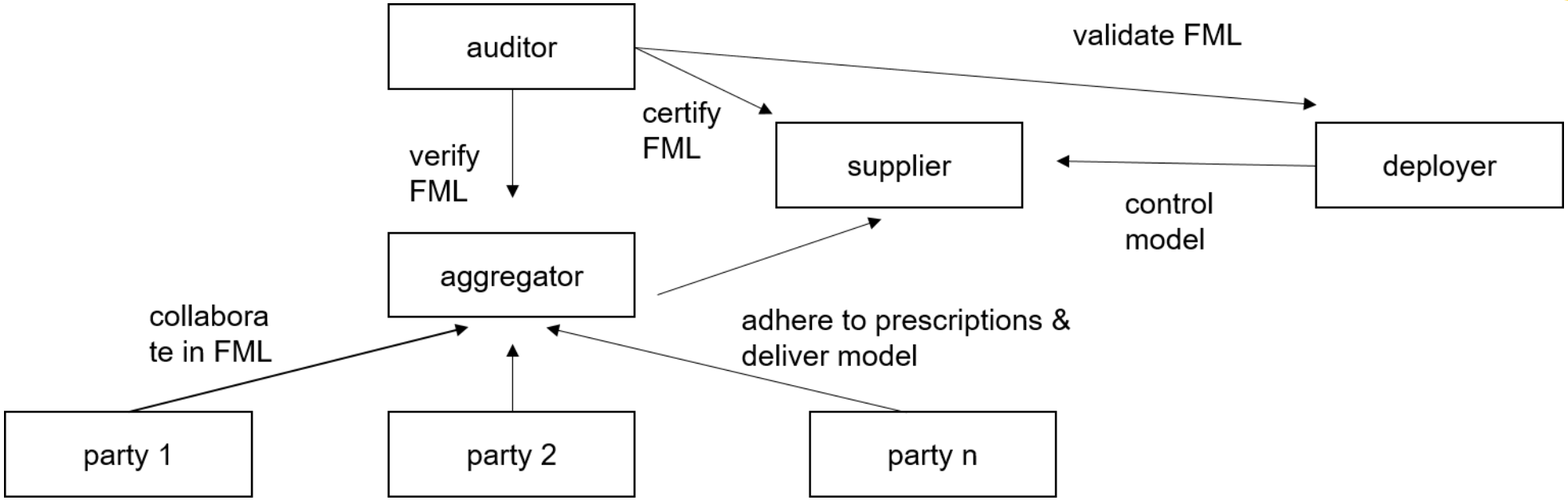
Results

Management:

Actors in AFML

Trust between parties is based on evidence

How to establish accountability?



Examplary application

Case: Citizen participation

- Ideas for new districts, novel mobility concepts etc.
- Categorization of ideas using AFML

Dimension	Characteristics		
data partitioning	horizontal	vertical	hybrid
ML model	linear model	decision tree	neural network
training data input	featured	raw	
training data output	structured	unstructured	
data federation	cross-silo	cross-device	
privacy preservation	differential privacy	cryptographic techniques	
network topology	centralized	decentralized	
federation need	economic incentive	regulation	
technology grade	research	industry	

Discussion

	Administration	Modeling	Processing	Communication & Interaction	Security & Privacy
Organizational/ Managerial	governance of incentives vs. regulations	**lifecycle blueprint**	**FML training integration**	**enterprise infrastructure integration**	compliance
Semantic	claim report semantics	trust semantics	explain-ability	data & model metadata	**guarantees for attacks and threats**
Technical / Syntactic	**evidence granularity & tamper-proof guarantees**	common accountability criteria	toolchain	tool & model interoperability	**cryptography & differential privacy, ID mgmt**

Conclusion

- Federated Machine learning is technique to collaboratively train models without transferring data to a centralized location
- Accountability
- Engineering

Thank you!

Any questions?

Peter Kuhn
pkuhn@fortiss.org
@nhuKreteP