Accountable Federated Machine Learning in Government: Engineering and Management Insights

Dian Balta\textsuperscript{1}, Mahdi Sellami\textsuperscript{1}, Peter Kuhn\textsuperscript{1}, Ulrich Schöpp\textsuperscript{1}, Matthias Buchinger\textsuperscript{1}, Nathalie Baracaldo\textsuperscript{2}, Ali Anwar\textsuperscript{2}, Heiko Ludwig\textsuperscript{2}, Mathieu Sinn\textsuperscript{2}, Mark Purcell\textsuperscript{2}, Bashar Altakrouni\textsuperscript{3}

\textsuperscript{1} fortiss GmbH, Research Institute of the Free State of Bavaria for software-intensive systems
\textsuperscript{2} IBM Research
\textsuperscript{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

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>data partitioning</td>
<td>horizontal, vertical, hybrid</td>
</tr>
<tr>
<td><strong>ML model</strong></td>
<td>linear model, decision tree, neural network</td>
</tr>
<tr>
<td>training data input</td>
<td>featured, raw</td>
</tr>
<tr>
<td>training data output</td>
<td>structured, unstructured</td>
</tr>
<tr>
<td>data federation</td>
<td>cross-silo, cross-device</td>
</tr>
<tr>
<td>privacy preservation</td>
<td>differential privacy, cryptographic techniques</td>
</tr>
<tr>
<td>network topology</td>
<td>centralized, decentralized</td>
</tr>
<tr>
<td><strong>federation need</strong></td>
<td>economic incentive, regulation</td>
</tr>
<tr>
<td>technology grade</td>
<td>research, industry</td>
</tr>
</tbody>
</table>
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

- auditor
  - verify FML
  - certify FML
- supplier
  - adhere to prescriptions & deliver model
- deployer
  - validate FML

- aggregator
  - collaborate in FML
  - control model

- party 1
- party 2
- party n

Trust between parties is based on evidence

How to establish accountability?
Exemplary application

Case: Citizen participation

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

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>data partitioning</td>
<td>horizontal</td>
</tr>
<tr>
<td>ML model</td>
<td>linear model</td>
</tr>
<tr>
<td>training data input</td>
<td>featured</td>
</tr>
<tr>
<td>training data output</td>
<td>structured</td>
</tr>
<tr>
<td>data federation</td>
<td>cross-silo</td>
</tr>
<tr>
<td>privacy preservation</td>
<td>differential privacy</td>
</tr>
<tr>
<td>network topology</td>
<td>centralized</td>
</tr>
<tr>
<td>federation need</td>
<td>economic incentive</td>
</tr>
<tr>
<td>technology grade</td>
<td>research</td>
</tr>
</tbody>
</table>
## Discussion

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