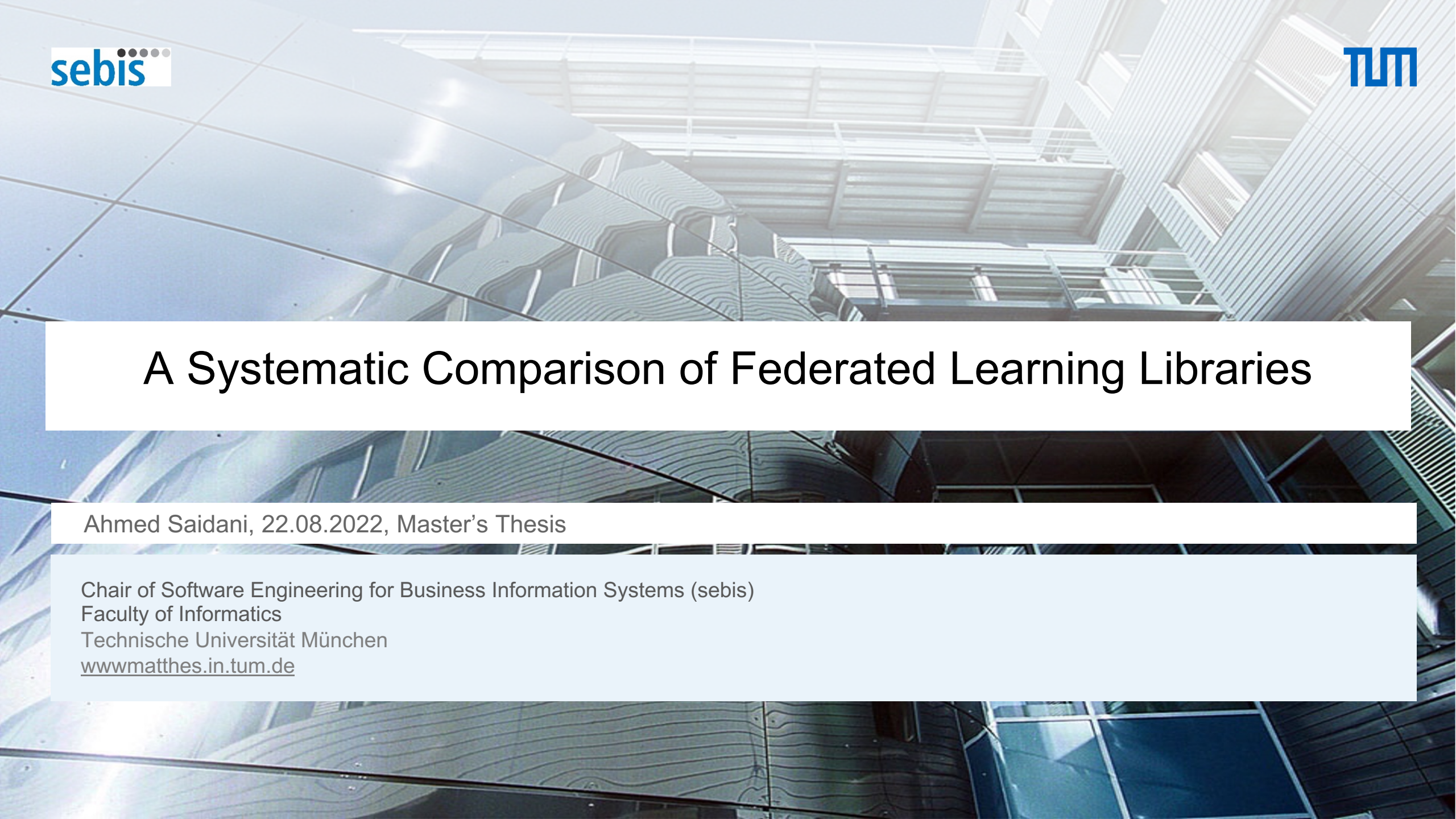


A Systematic Comparison of Federated Learning Libraries

Ahmed Saidani, 22.08.2022, Master's Thesis

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

Background
- Federated Machine Learning Process
- Problem Statement

Research Approach
- Research Questions
- Current State of Research
- Research Design

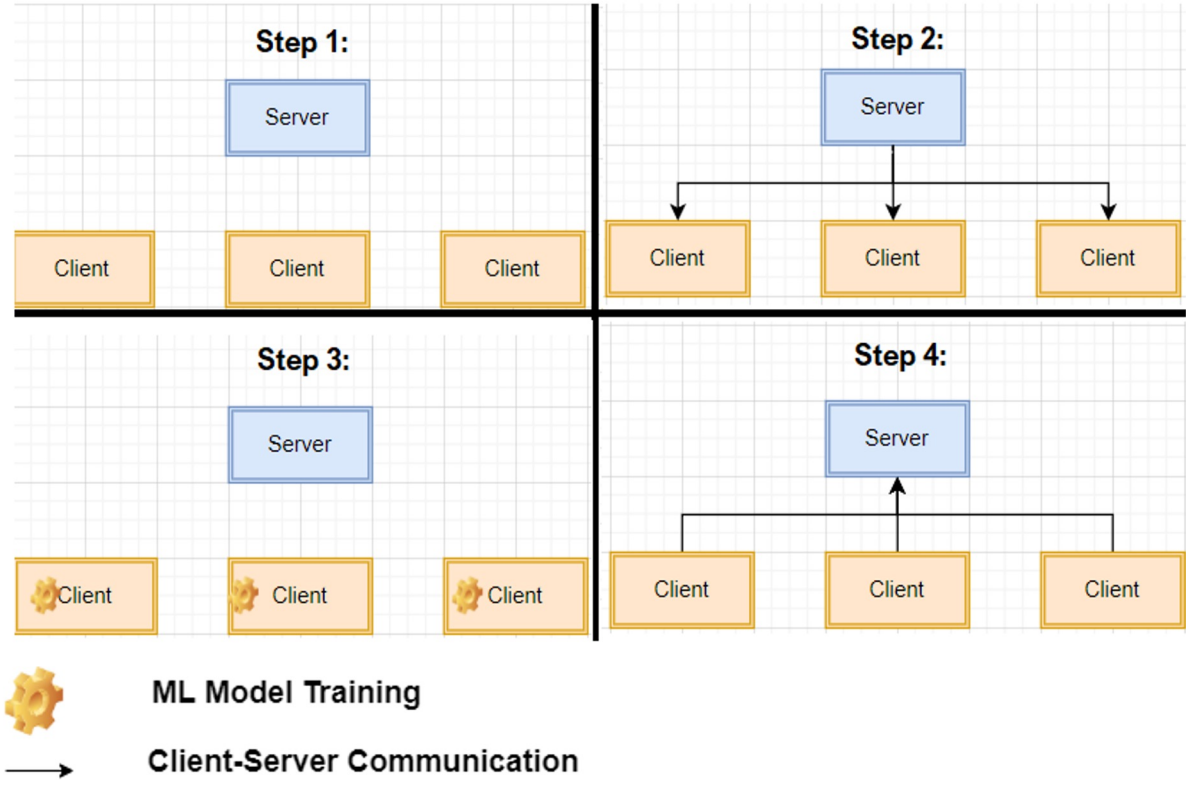
Qualitative Research Methodologies
- Literature Review & Document Analysis
- Expert Interview

Libraries Comparison
- Architecture
- Functionalities

Quantitative Research Methodologies
- Benchmarking Tool Development
- Benchmarking Tool Architecture
- Evaluation Method

Time Schedule

Background
Federated Machine Learning Process



Step 1: Server chooses the machine learning model

Step 2: Server communicates model to clients

Step 3: Clients train model with their data locally

Step 4: Clients transmit the gradient update but not data to server to generate a global updated gradient

Background
Problem Statement

TensorFlow Federated

FATE

PaddleFL

Flower

PySyft

FedML

- **Different federated learning libraries**
- **Different capabilities & limitations**
- **Lack of literature evaluating and benchmarking the libraries**
- **Libraries differ in terms of functionality and overall quality (performance, scalability, security …)**
- **The choice of the library could be challenging for practitioners who do not have enough experience with different libraries**

Research Approach

Research Questions

RQ1 What are the different federated libraries available, and how do they differ in terms of functionality?

RQ2 What are the metrics relevant for the benchmarking of the different federated learning libraries?

RQ3 How could a modular software application that benchmarks the different federated learning libraries using the metrics be developed ?

Thesis Title

A Structured Comparison of Federated Learning Libraries

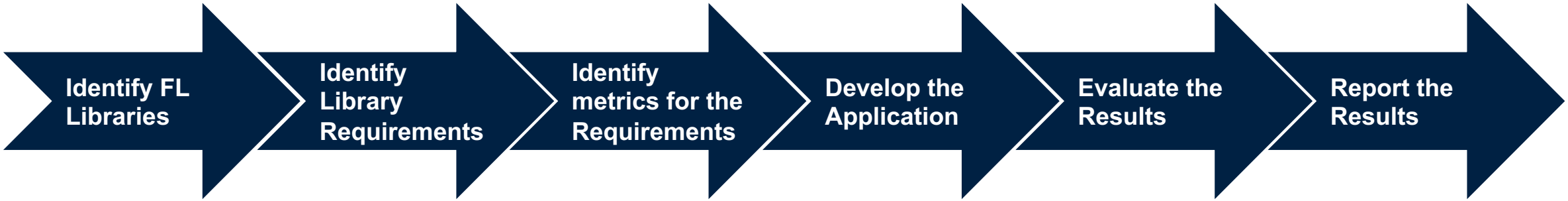
Research Approach

Current state of Research

- Research is centered around bottlenecks in Federated machine learning [1]
- 14 different libraries in total
- Most of Libraries are not production ready or have too limited utilities
- 6 Libraries have enough community support and are actively developed
- 12 benchmarking publications in the field of Federated Machine Learning
- 11 benchmark the different FL algorithm
- Only one compare and benchmark the libraries [4]
  - Only compares 5 libraries
  - Offers a high level qualitative comparison
  - Specific to IoT
  - Only compares accuracy and overall performance of the libraries
- No overview over the functionality and the quality of the different libraries

Sources: 1. Kairouz, P., et al.. Advances and Open Problems in Federated Learning. Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1–210, (2021).
Kholod, I., Yanaki, E., Fomichev, D., Shalugin, E., Novikova, E., Filippov, E., & Nordlund, M.: Open-source federated learning frameworks for IoT: A comparative review and analysis. Sensors, 21(1), 167. (2020).

Research Approach
Research Design



- Literature Review & Document Analysis:
  - Research the different FL Library (e.g FATE, FedML …)
  - Research the different FL mechanisms (e.g Aggregation algorithms, Privacy mechanisms…)
  - Compare FL Library Functional and qualitative Non-Functional Requirements (e.g Functionality, Scalability, Performance…)
- Expert interviews:
  - Identify the different FL Library Functional and Non-Functional Requirements (e.g Functionality, Scalability, Performance…)
  - Identify the different metrics for the Requirements (e.g Number of Supported Clients, the Runtime of the Client…)
- Design Research Methodology:
  - Design & Develop Application
  - Conduct Experiment (quantitative comparison of NFR)
  - Evaluate Results

Qualitative Research Methodologies

Literature Review & Document analysis

- **Process:**
  - Review of the academic literature
  - Review of the libraries' documentation
- **Goals:**
  - Identify the different federated learning mechanisms (aggregation algorithms, data partitioning, privacy mechanisms …)
  - Identify the Federated Learning libraries
  - Identify the functionalities, features, and maturity of the libraries
- **Artifact**
  - An overview of the different federated learning mechanisms
  - A list of all the FL libraries', their functionalities, features, and maturity

Source: Literature review process, Evidence partners website, https://www.evidencepartners.com/products/distillersr-systematic-review-software

Libraries Comparison

Architecture

	PySyft	**Flower**	**FATE**	**TensorFlow Federated**	**FedML**
Data Partitioning	vert/hori	vert/hori	vert/hori	hori	vert/hori
Privacy & Security	HE,MPC,DP	SecAgg	HE,RSA,Diffe-Hellman	DP	secret sharing, key agreement, digital signature, and public key infrastructure
Communication scheme	gRPC	gRPC	-	Custom Protocol	MPI,MQTT,gRPC …
Strategy	FedAVG (maybe others)	FedAVG	FedAVG	FedAVG, FedSGD	FedAVG, FedNOV,. FedNAS….
Model	NN/RNN/CNN LR/PR/LogR K-mean	NN/RNN/CNN LR/PR/LogR K-mean	NN/RNN/CNN LR/PR/LogR K-mean	NN/RNN/CNN	NN/RNN/CNN LR/PR/LogR K-mean

Libraries Comparison

Functionalities

	PySyft	**Flower**	**FATE**	**TensorFlow Federated**	**FedML**
standalone simulation	yes	yes	yes	yes	yes
distributed computing	yes	yes	yes	yes	yes
on-device training	no	yes	no	no	yes
topology customization	yes	no	no	no	yes
exchange message customization	yes	yes	no	no	yes
SplitNN (split learning)	yes	no	no	no	yes

Source: He, C., et al. "Fedml: A research library and benchmark for federated machine learning." arXiv preprint arXiv:2007.13518 (2020).

Qualitative Research Methodologies

Expert Interview

- **Process:**
  - Conduct a series of semi-structured interviews with Federated Learning experts
- **Goals:**
  - Identify the Functional (Qualitative) and Non-Functional (Qualitative & Quantitative) Requirements Federated Learning libraries
  - Identify the Metrics to Benchmark the Non-Functional Requirements
- **Artifact**
  - A list of the most important FR and NFR for FL libraries, and the metrics to benchmark them

Source: Expert Interview Picture, Bryony Gibson Consulting website, https://www.bryonygibson.com/expert-interview-tips-for-employers/

Quantitative Research Methodologies

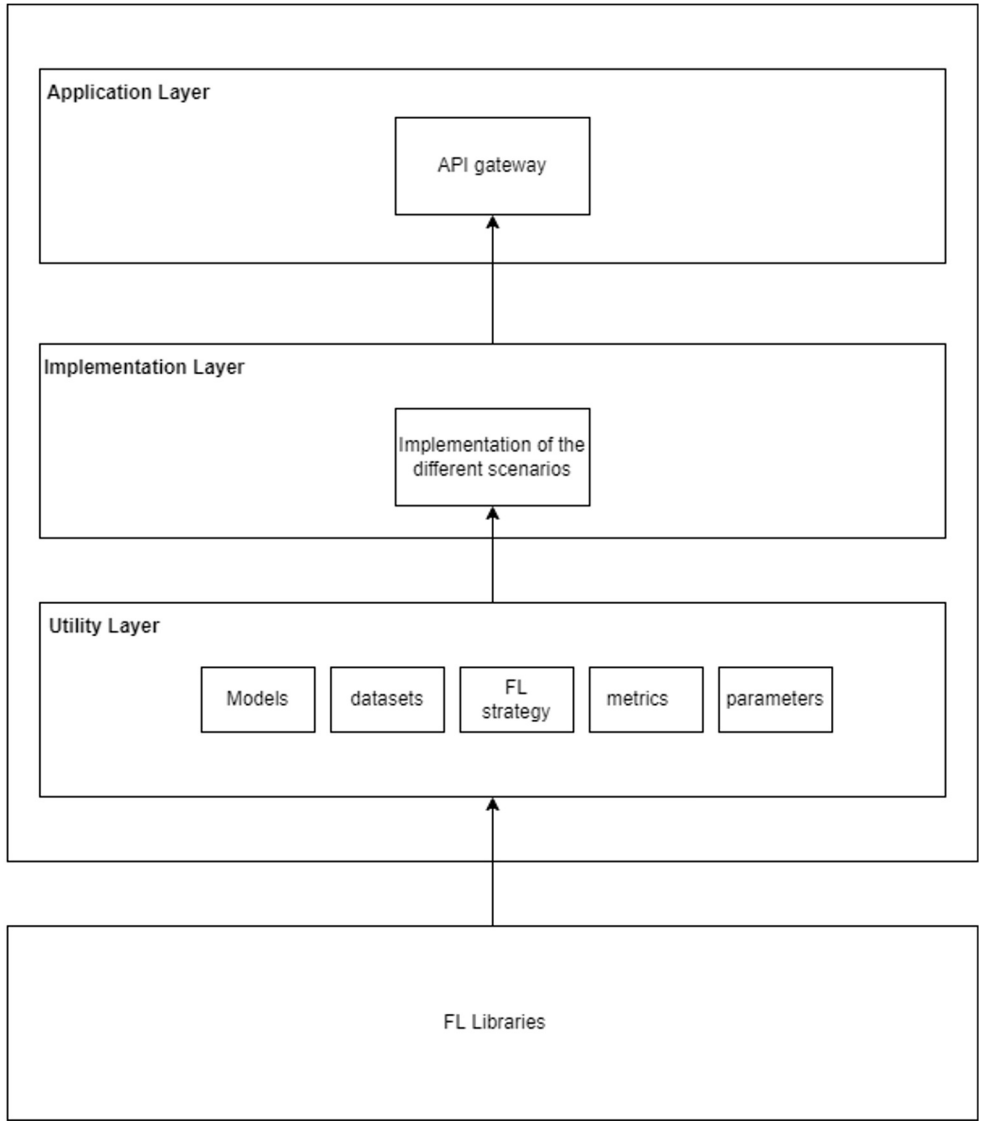
Benchmarking Tool Development

- **Process:**
  - Use the Design Research Methodology to develop the tool
- **Goals:**
  - Develop a modular benchmarking suite to benchmark the different libraries
- **Artifact**
  - A tool to benchmark the different libraries

Source: Benchmark Icon, Icon Library website, https://icon-library.com/icon/benchmark-icon-13.html

Quantitative Research Methodologies

Benchmarking Tool Architecture



- **Application Layer:**
  - API Gateway
- **Utilities Layer:**
  - Abstract Implementation of the ML models (with different hyperparameters) and FL algorithms
  - Implementation of the metrics
  - Reference datasets
- **Implementation Layer:**
  - Implementation of different models with different libraries
- **FL Libraries:**
  - Actual FL Libraries

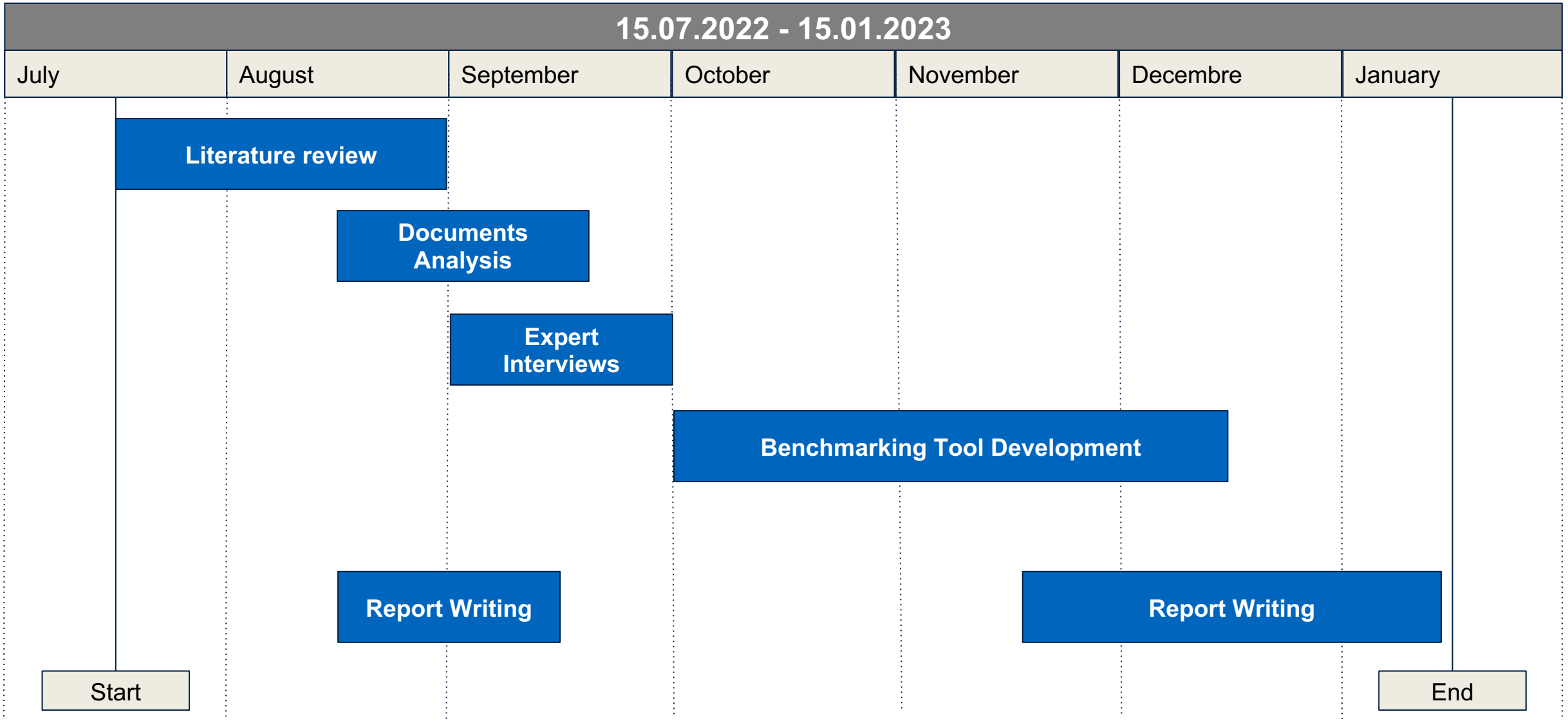
Source: Sixu, H. et al. "The oarf benchmark suite: Characterization and implications for federated learning systems." ACM Transactions on Intelligent Systems and Technology (TIST) 13.4 :p. 1-32.(2022)

Quantitative Research Methodologies
Evaluation Method

- **Process:**
  - Benchmark the NFR for FL libraries using the Benchmarking tool
- **Goals:**
  - Conduct the benchmarking of the different libraries
- **Artifact**
  - Results of the libraries' benchmarks

Source: Benchmark Icon, Flat Icon website, https://www.flaticon.com/de/kostenloses-icon/benchmark_1924809

Time Schedule



Ahmed Saidani
ge72vej@mytum.de

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.
Fax +49.89.289.17136

wwwmatthes.in.tum.de

References

1. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S: Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1-210.(2021).
2. Hu, S., Li, Y., Liu, X., Li, Q., Wu, Z., He, B.: The OARF Benchmark Suite: Characterization and Implications for Federated Learning Systems, ACM Transactions on Intelligent Systems and Technology, Vol. 13, No. 4, Article 63 (2020).
3. Caldas, S., Duddu, S. M. K., Wu, P., Li, T., Konečný, J., McMahan, H. B., ... & Talwalkar, A. . Leaf: A benchmark for federated settings. arXiv preprint arXiv:1812.01097. (2018).
4. Kholod, I., Yanaki, E., Fomichev, D., Shalugin, E., Novikova, E., Filippov, E., & Nordlund, M. . Open-source federated learning frameworks for IoT: A comparative review and analysis. Sensors, 21(1), 167.(2020)