Benchmarking Federated Learning in the SME Industry Context

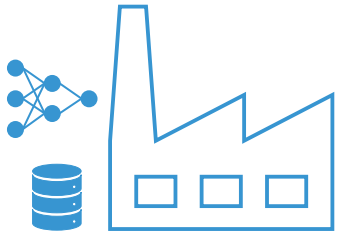
Evaluation concerning Privacy, Complexity and Performance with an Application to real-world Image Classification Problem

Anna Hensel, master's thesis

KARLSRUHE SERVICE RESEARCH INSTITUTE (KSRI)
INSTITUTE OF INFORMATION SYSTEMS AND MARKETING (IISM)

SMEs* often have related machine learning use cases, each facing several problems concerning classical ML


[7]

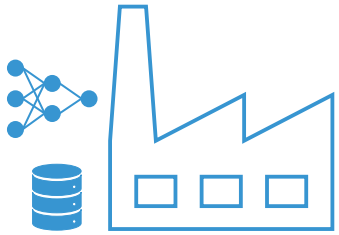


* SME: small medium-sized enterprise (dt. KMU)

SMEs* often have related machine learning use cases, each facing several problems concerning classical ML


[7]

Problems: too little data, lack of experience
→ poor performance



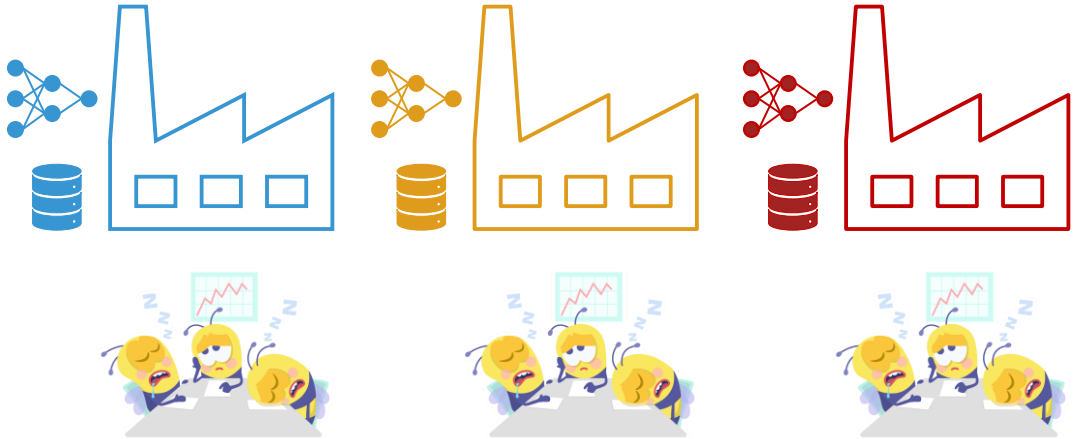
* SME: small medium-sized enterprise (dt. KMU)

SMEs* often have related machine learning use cases, each facing several problems concerning classical ML


[7]

One model per company

Problems: too little data, lack of experience
→ poor performance



* SME: small medium-sized enterprise (dt. KMU)

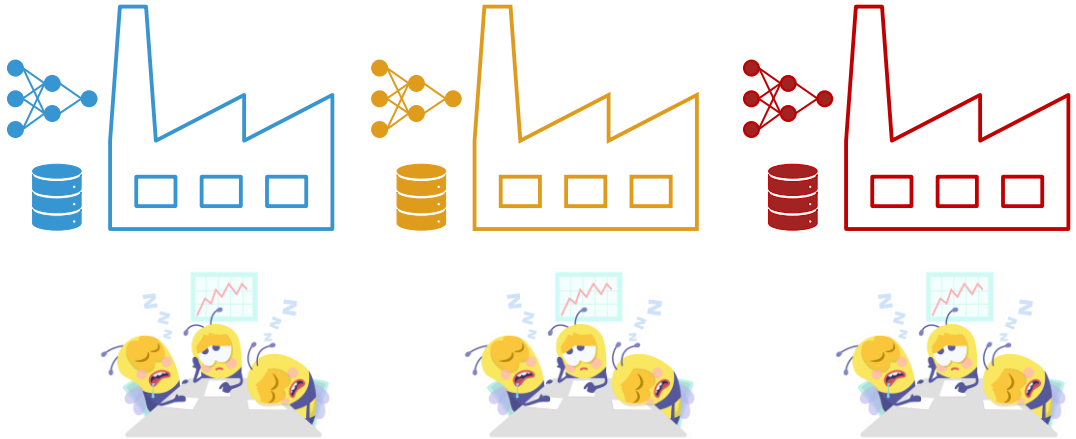
Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

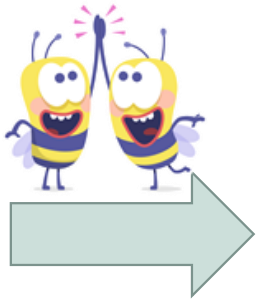
SMEs* often have related machine learning use cases, each facing several problems concerning classical ML

[7]

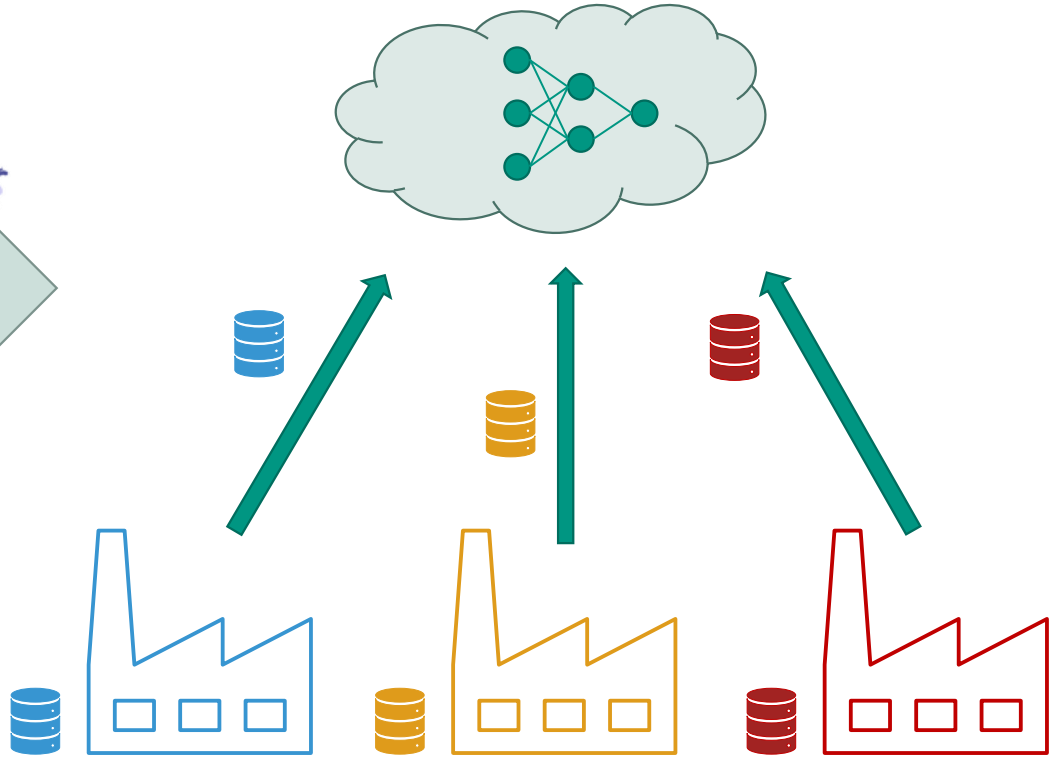
One model per company

Problems: too little data, lack of experience
→ poor performance





All data model



* SME: small medium-sized enterprise (dt. KMU)

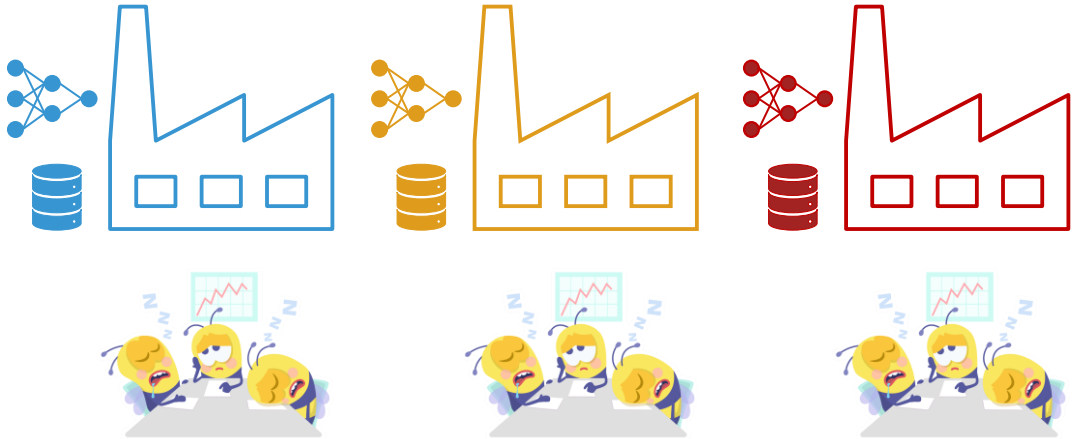
Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

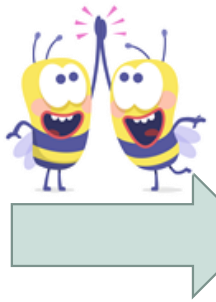
SMEs* often have related machine learning use cases, each facing several problems concerning classical ML

[7]

One model per company

Problems: too little data, lack of experience
→ poor performance





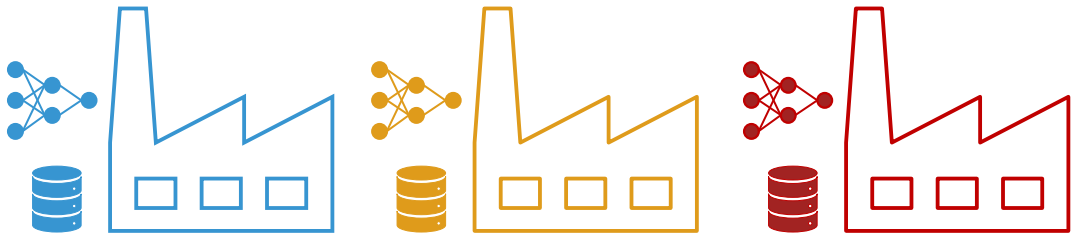
All data model

Huge privacy problem as companies data is sent to a central node

* SME: small medium-sized enterprise (dt. KMU)

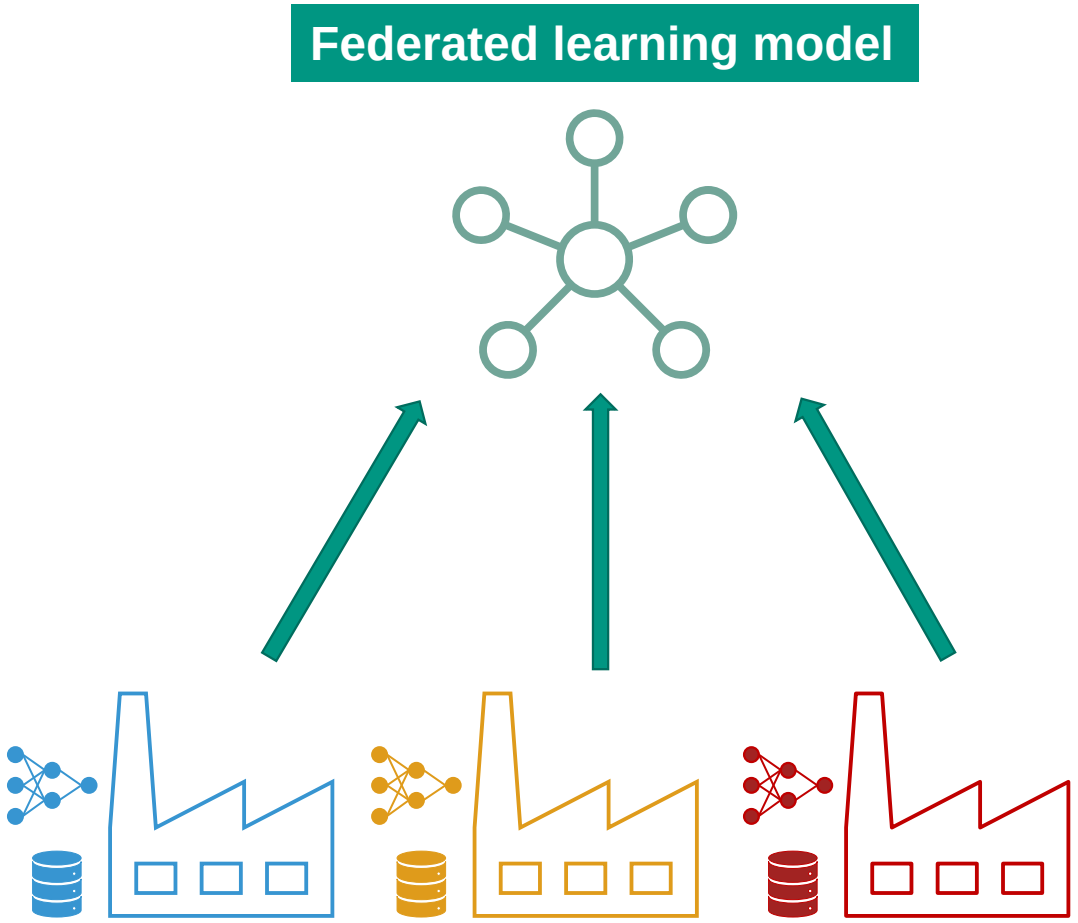
Federated learning allows for decentralized machine learning potentially mitigating privacy issues

Federated learning model



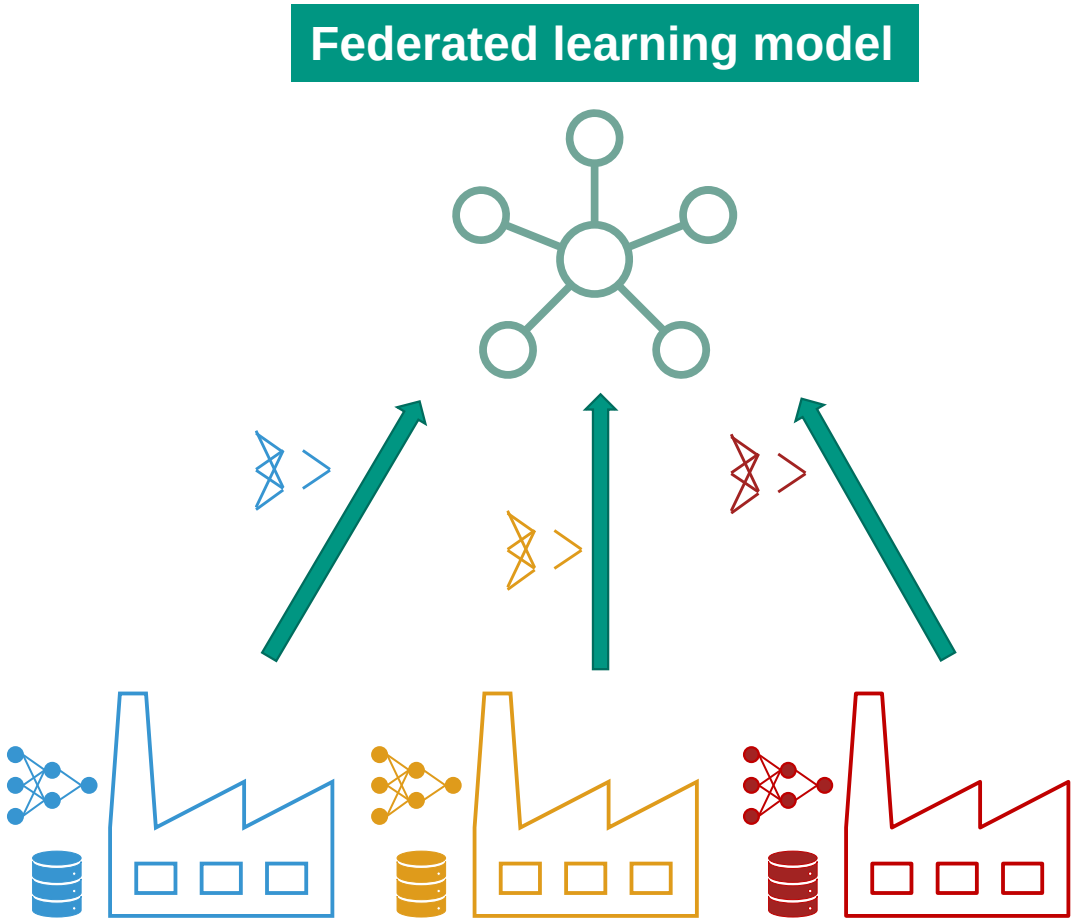
[2]

Federated learning allows for decentralized machine learning potentially mitigating privacy issues



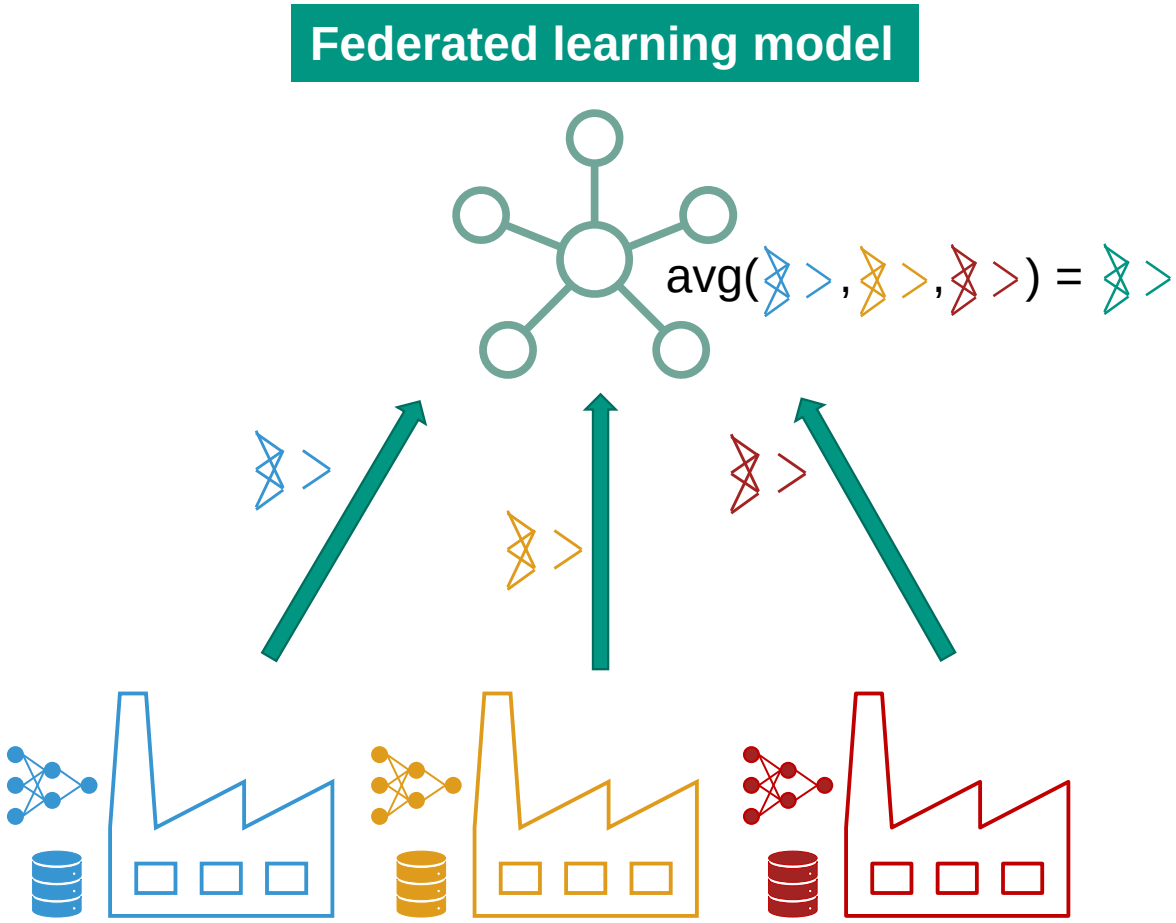
[2]

Federated learning allows for decentralized machine learning potentially mitigating privacy issues



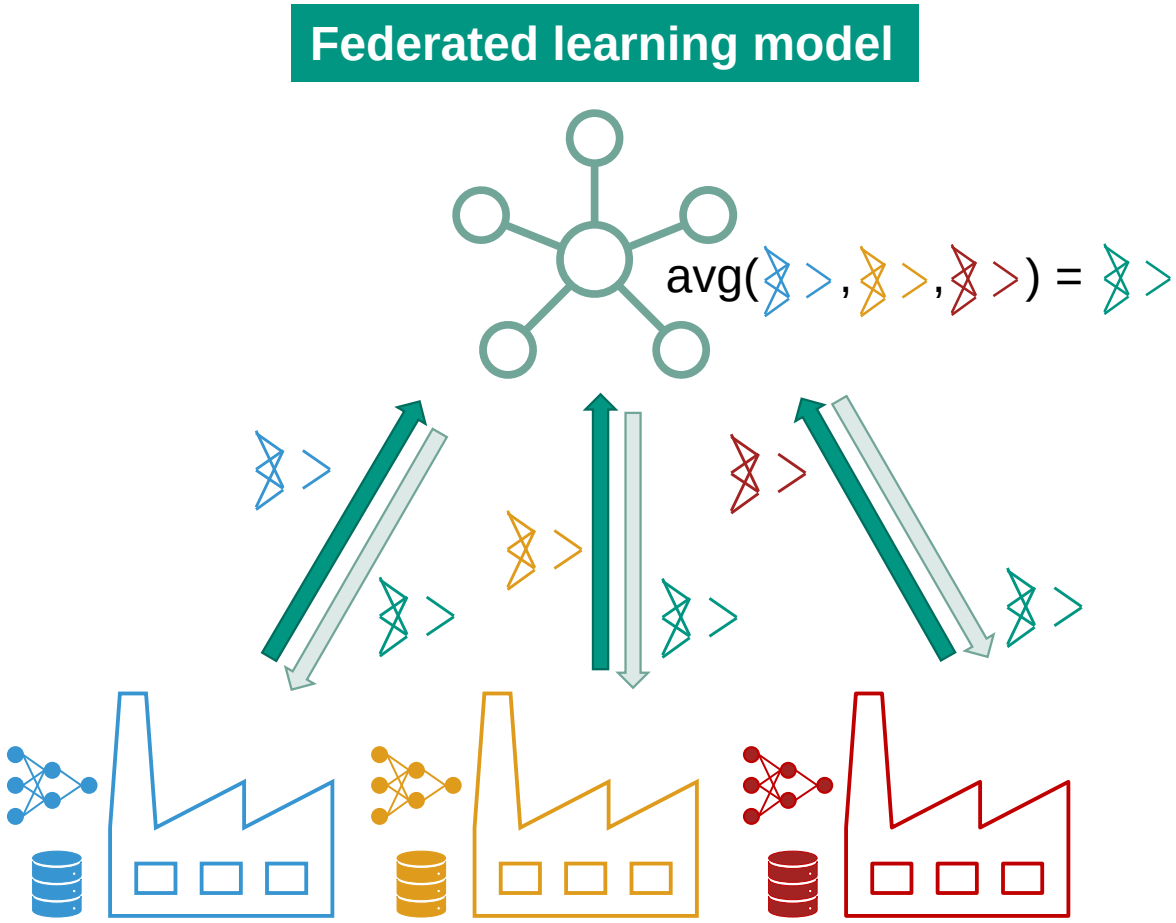
[2]

Federated learning allows for decentralized machine learning potentially mitigating privacy issues



[2]

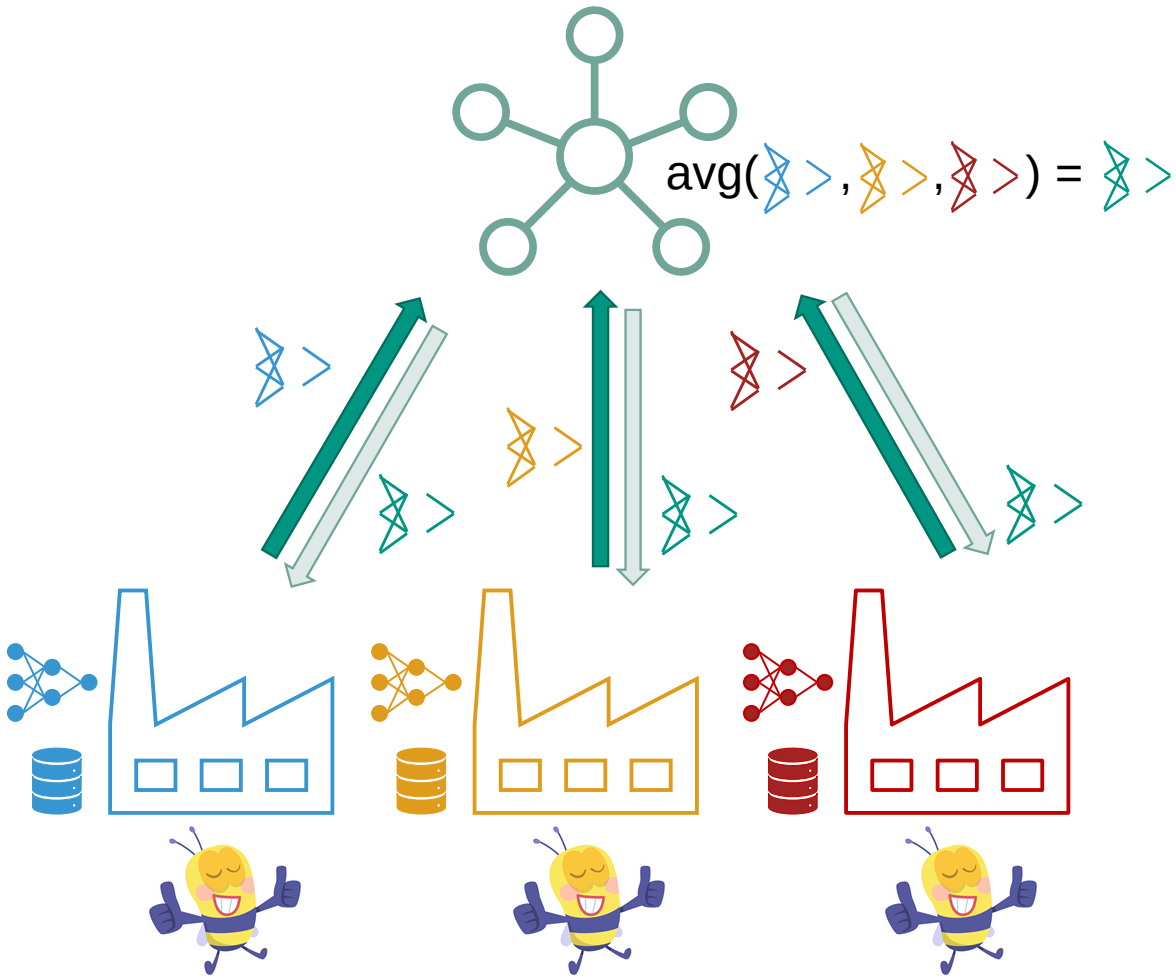
Federated learning allows for decentralized machine learning potentially mitigating privacy issues



[2]

Federated learning allows for decentralized machine learning potentially mitigating privacy issues

Federated learning model

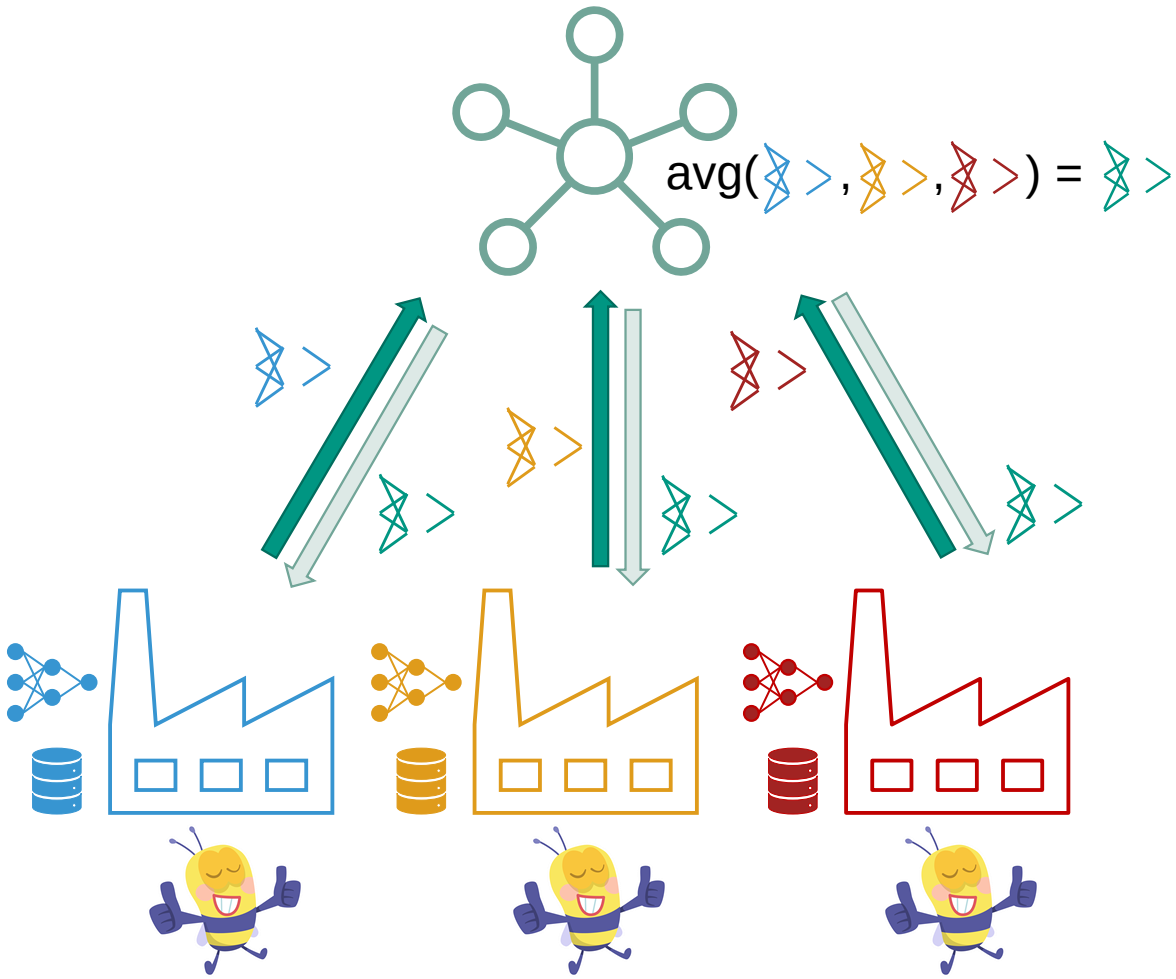


- Local training and model sharing preserves **privacy**
- Enables joint use of data of several companies → unlocks **performance** potential
- **Complexity** due to model sharing and update communication

[2]

Federated learning allows for decentralized machine learning potentially mitigating privacy issues

Federated learning model



Research Questions and Contributions:

1. Under what conditions is federated learning (not) useful for SMEs in an industrial context?

2. How does federated learning compare to *one model per company* and *all data model*? What do SMEs need to consider in terms of *privacy*, *complexity* and *performance*?

3. Implementation of a benchmarking pipeline to empirically investigate and simulate federated learning in relation to *one model per company* and *all data model*.

Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

Complexity

Performance

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Complexity

Performance

Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:

- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Performance

Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:

- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity

Organizational Complexity

Implementation Complexity

Performance

Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:
- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity
- Number of communication rounds [2] / iterations / communicated bits [5] not relevant in SME setting as much less clients

Organizational Complexity

Implementation Complexity

Performance

Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:

- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity

- Number of communication rounds [2] / iterations / communicated bits [5] not relevant in SME setting as much less clients

Organizational Complexity

- FL: setting up network complexity, contracts, legal issues, sharing costs, …
- The more companies the harder to organize

Implementation Complexity

Performance

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:
- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity
- Number of communication rounds [2] / iterations / communicated bits [5] not relevant in SME setting as much less clients

Organizational Complexity
- FL: setting up network complexity, contracts, legal issues, sharing costs, …
- The more companies the harder to organize

Implementation Complexity
- FL: reduced/shared modelling complexity
- One model per company: set up and implement own model

Performance

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:
- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity
- Number of communication rounds [2] / iterations / communicated bits [5] not relevant in SME setting as much less clients

Organizational Complexity
- FL: setting up network complexity, contracts, legal issues, sharing costs, …
- The more companies the harder to organize

Implementation Complexity
- FL: reduced/shared modelling complexity
- One model per company: set up and implement own model

Performance

⊕ All data model

Federated learning

⊖ One model per company

Privacy, complexity and performance are important dimensions for the evaluation of federated learning use cases for SMEs

Privacy

⊕ One model per company

Federated learning

⊖ All data model

Critical aspects:
- Company sends weights to central node [2]
- Weights reflect company data

→ Adversarial attacks from “malicious client” or “malicious server” possible [8]
  - Sample reconstruction
  - Information inference

Complexity

Computational Complexity
- Number of communication rounds [2] / iterations / communicated bits [5] not relevant in SME setting as much less clients

Organizational Complexity
- FL: setting up network complexity, contracts, legal issues, sharing costs, …
- The more companies the harder to organize

Implementation Complexity
- FL: reduced/shared modelling complexity
- One model per company: set up and implement own model

Performance

⊕ All data model

Federated learning

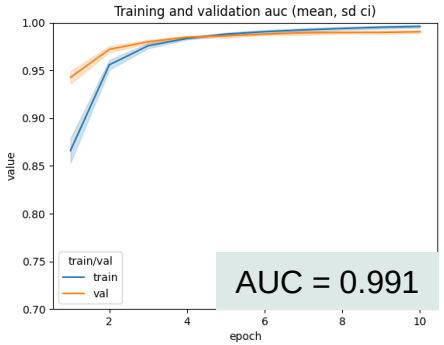
⊖ One model per company

Performance measure to enable **comparability** between and within companies
- Accuracy [2, 6]
  - Threshold needed
  - Unbalancedness
- AUC [9]
  - Abstracts from balancedness
  - Quality of score (no threshold needed)

All data model

FL model per company

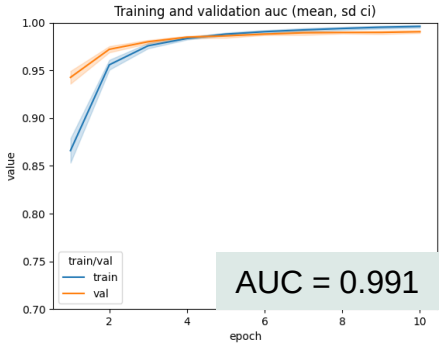
One model per company



- The all data model can be seen as an upper bound

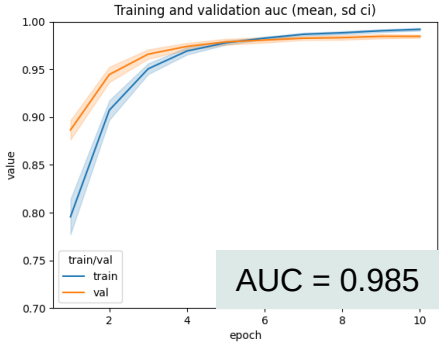
Digital Service Innovation
Karlsruhe Service Research Institute
Institute of Information Systems and Marketing

All data model

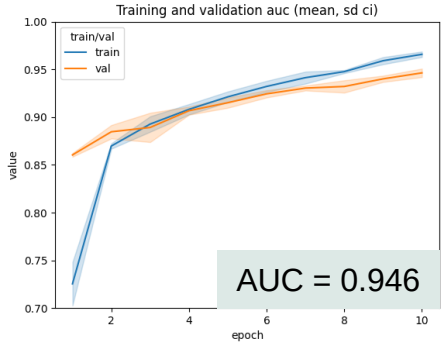


FL model per company

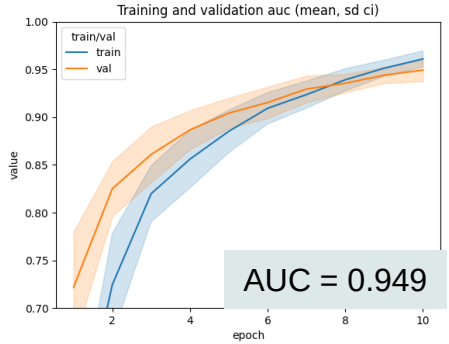
One model per company



Company 1
50% of all data, balanced



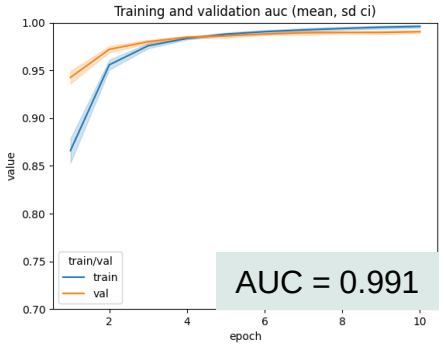
Company 2
25% of all data, unbalanced



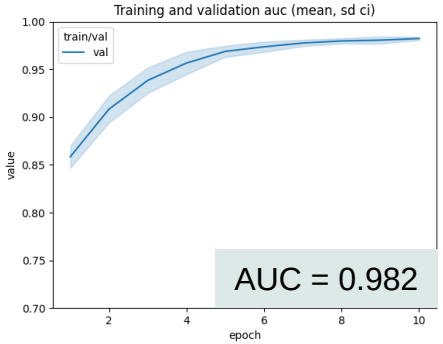
Company 3
25% of all data, unbalanced

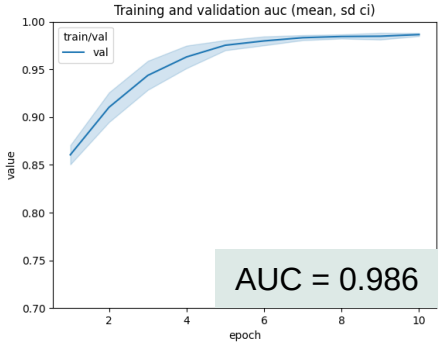
- The all data model can be seen as an upper bound
- One model per company can be seen as a lower bound

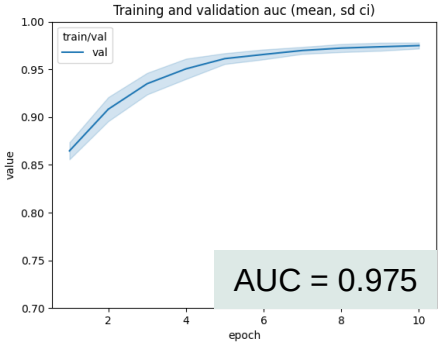
All data model



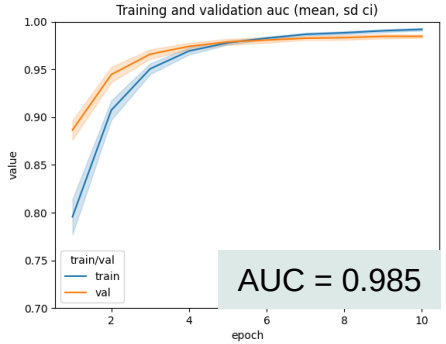
FL model per company

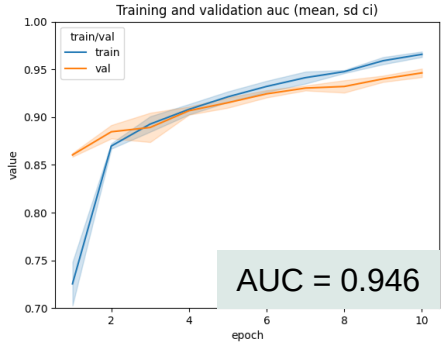


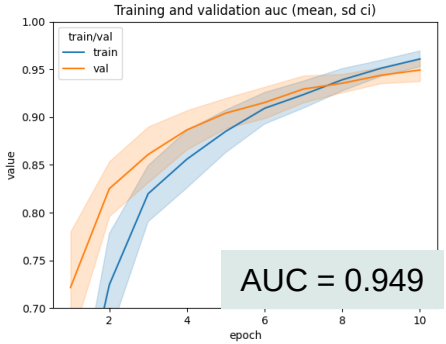




One model per company







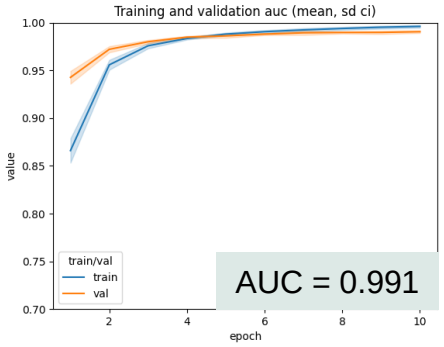
Company 1
50% of all data, balanced

Company 2
25% of all data, unbalanced

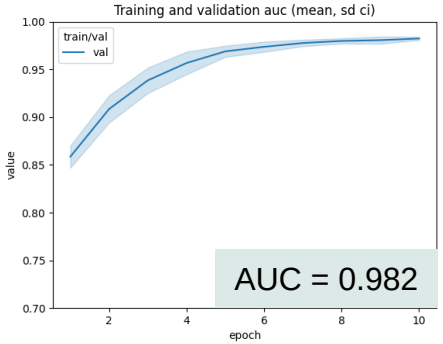
Company 3
25% of all data, unbalanced

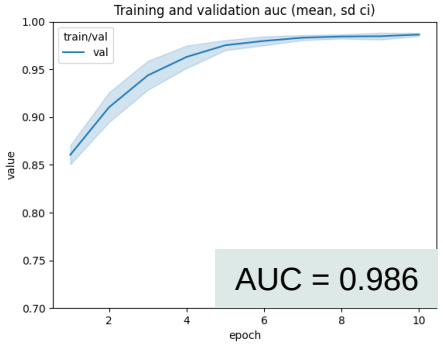
- The all data model can be seen as an upper bound
- One model per company can be seen as a lower bound
- Companies with insufficient data profit more from the federated model

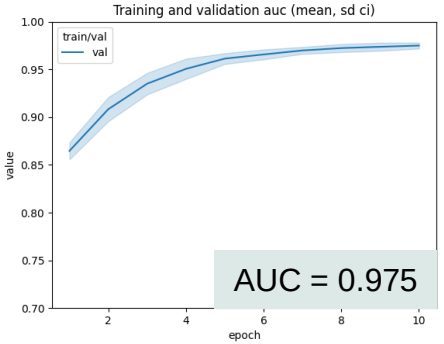
All data model



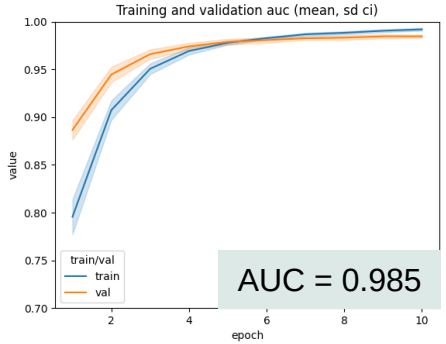
FL model per company

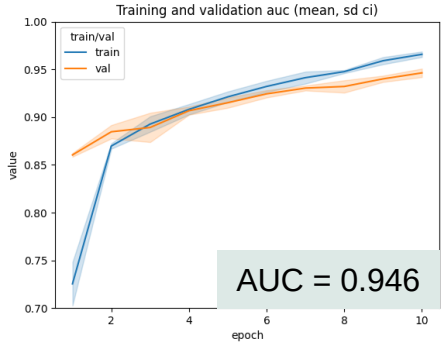


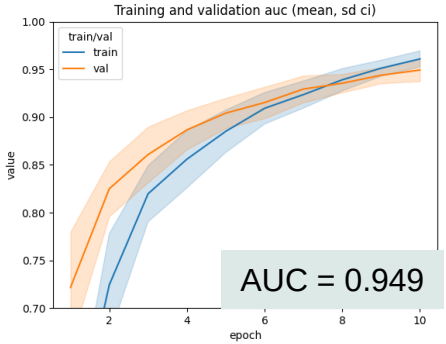




One model per company







Company 1
50% of all data, balanced

Company 2
25% of all data, unbalanced

Company 3
25% of all data, unbalanced

- The all data model can be seen as an upper bound
- One model per company can be seen as a lower bound
- Companies with insufficient data profit more from the federated model
- For companies with sufficient data there is little incentive to take part in FL setting

Discussion topics

Measuring Performance

Do you know an alternative measure to AUC which suits to my industry/SME setting?

Measuring Incentives

Idea: Shapley Value with AUC as contribution measure
Do you have experience with it?
How to interpret the result?

Measuring Complexity

What kind of complexity does really matter for SMEs regarding my setting?

Thank you for your attention!

anna.hensel@student.kit.edu

Karlsruhe Service Research Institute (KSRI)
Institute of Information Systems and Marketing (IISM)
Kaiserstr. 89 | Building 05.20
D-76133 Karlsruhe

www.ksri.kit.edu / https://dsi.iism.kit.edu/

@ksri_kit

Sources

1. Bonawitz et al. 2019
2. McMahan et al. 2017
3. Murakonda et al. 2020
4. Konečný et al. 2016
5. Sattler et al. 2021
6. Yang et al. 2019
7. Schlagenhauf 2021
8. Enthoven and Al-Ars 2021
9. Hanley and McNeil 1982