Towards Collaborative Predictive Maintenance Leveraging Private Cross-Company Data

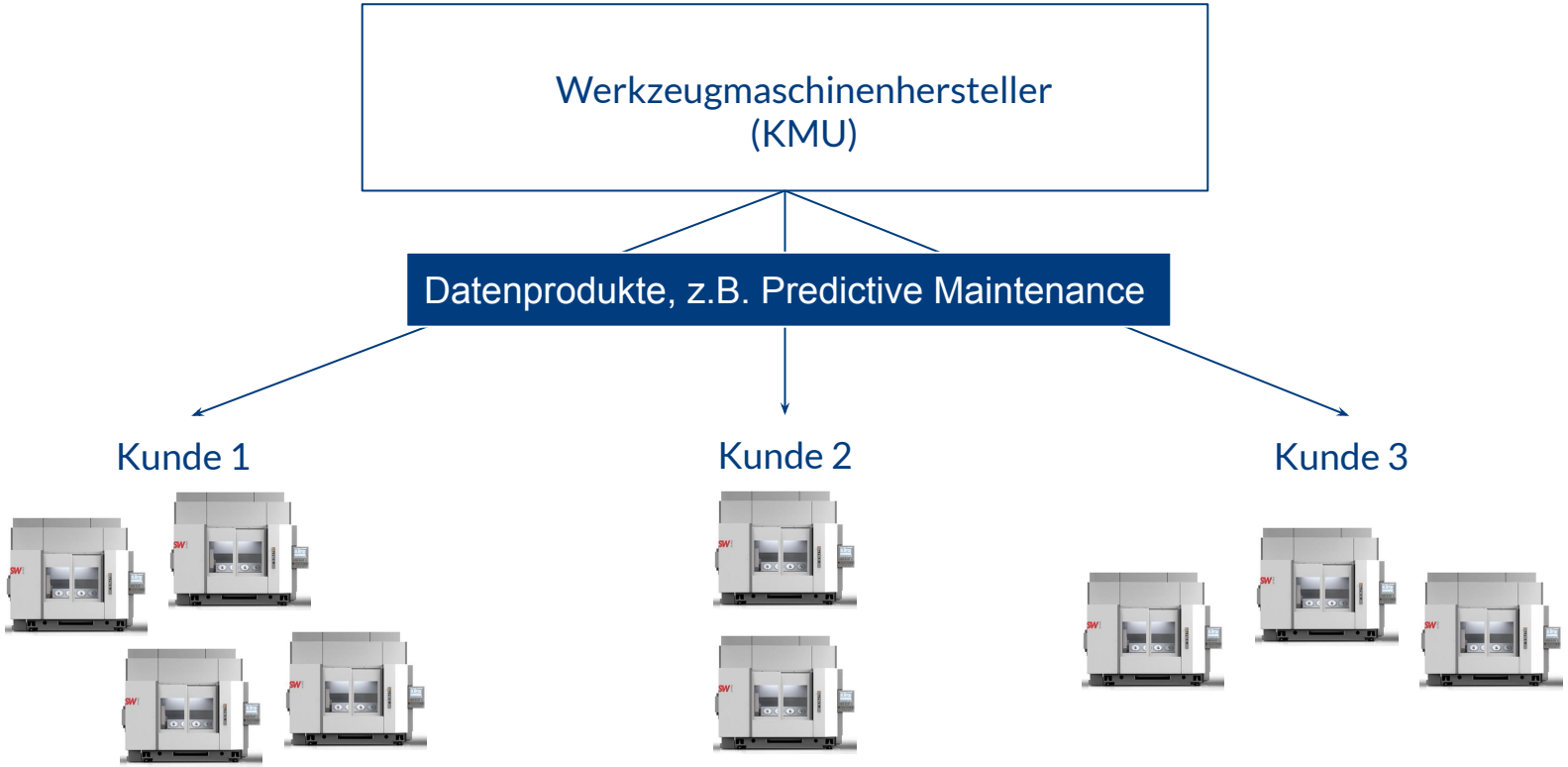
Autoren: Marisa Mohr, Christian Becker, Ralf Möller, Matthias Richter

inovex

UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR INFORMATIONSSYSTEME

European Women in Mathematics

Datenprodukte im IIoT



KOSMoS

Bundesministerium für Bildung und Forschung

Kollaborative Smart Contracting Plattform für digitale Wertschöpfungsnetze

Maschinenhersteller	Enabler	Forschungsinstitute

Schütte · ASYS GROUP · SW Technology People

ONDIDS Apps und Webs für Ihre Prozesse · inovex · DATARELLA

Hochschule Furtwangen University HFU · Frankfurt School Blockchain Center · Universität Stuttgart Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen ISW

Ein **System** für den **sicheren** und **semitransparenten** Austausch von **produktionsbeschreibenden** Informationen zwischen **kooperierenden** Firmen hilft, neue **datengetriebene Geschäftsmodelle** zu ermöglichen.

Herausforderung

- **Verfügbare Trainingsdaten** bestimmen die Genauigkeit eines datengetriebenen Modells
- Daten müssen Ausfall-Muster enthalten
- **Relativ seltenes Auftreten von Maschinenausfällen**
- Absichtliche Degradierung von Maschinen zur Sammlung von Trainingsdaten ist unverantwortlich

Lösungsvorschlag und Contribution

- Zusammenführen von Trainingsdaten über Unternehmen hinweg
- Einsatz von **Blockchain** und **Federated Learning** zur Wahrung der Privatsphäre von Daten

Contribution (Work-In-Progress-Paper):

- Kombination und Anwendung von Forschungsergebnissen
- Vorbereitung der Architektur für ein kollaboratives Modell zur vorausschauenden Wartung mit unternehmensübergreifenden Daten
- **Erprobung in KMUs**

Collaborative Predictive Maintenance

Herausforderungen bei der Kombination von Datenquellen:

1. Datenmanipulation (z.B. zur Sabotage von Modellvorhersagen)
2. Transparente Dokumentation der Wartungen
3. Gemeinsames Training von Modellen für die vorausschauende Wartung ohne Offenlegung von Geschäftsinformationen

1. Blockchain: Schutz gegen Manipulation

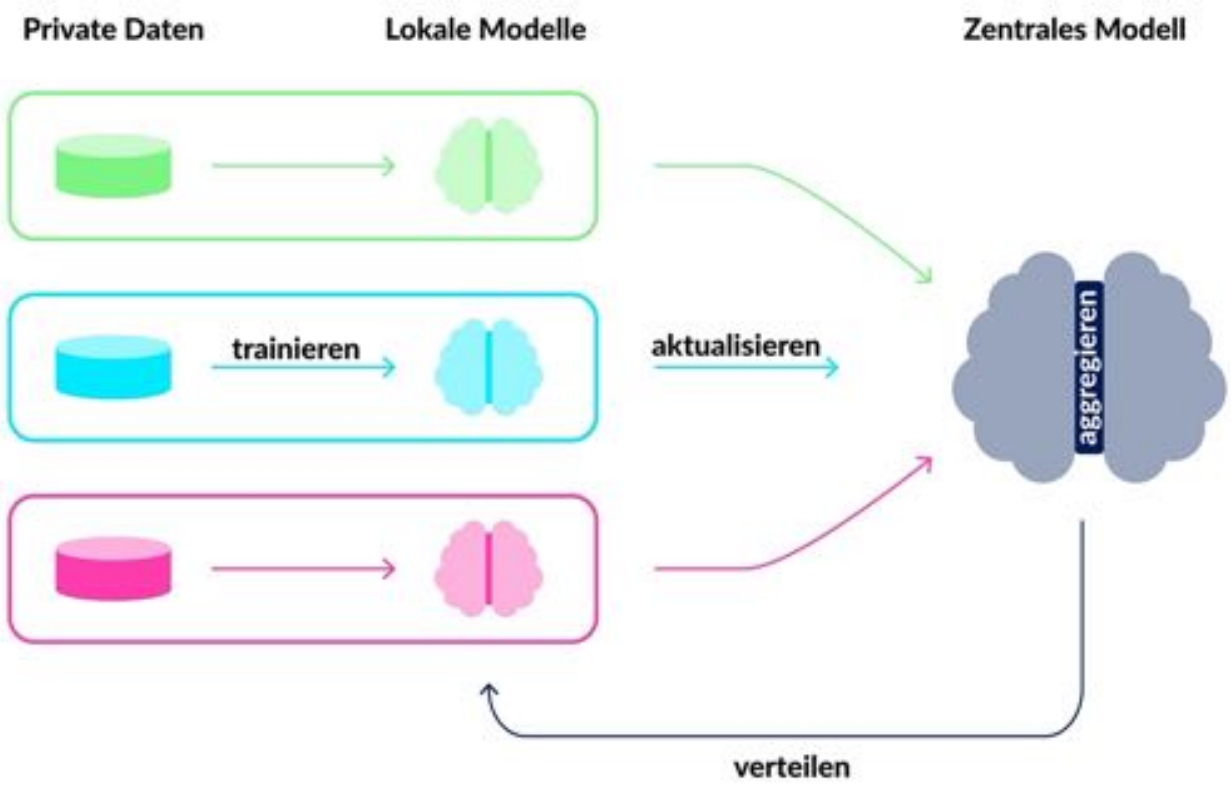
- Daten dort signieren, wo sie aufgezeichnet werden
- Kommerzielle Systeme sind i.d.R. zwischen verschiedenen Herstellern inkompatibel
- Installation eines Mikrocontrollers zwischen Sensor und nachgeschaltetem System (Korb et al., ISW Stuttgart)
- Implementierung einer **Blockchain** für ein geeignetes Signierverfahren

Korb, T.; Michel, D.; Riedel, O.; Lechler, A.: Securing the Data Flow for Blockchain Technology in a Production Environment. IFAC-PapersOnLine, 52(10):125–130, January 2019.

2. Blockchain: Transparente Dokumentation

- **Konsensus**: Alle Teilnehmer sind synchronisiert und validieren Transaktionen
- Transparentes Wartungsprotokoll auf der Grundlage von Fehlermeldungen und Wartungseinträgen
- Das Tupel eines Eintrags wird kryptographisch gehasht und der Hash wird in die Blockchain geschrieben
- Echtheit der Einträge, unberechtigte Manipulation und Vertrauen

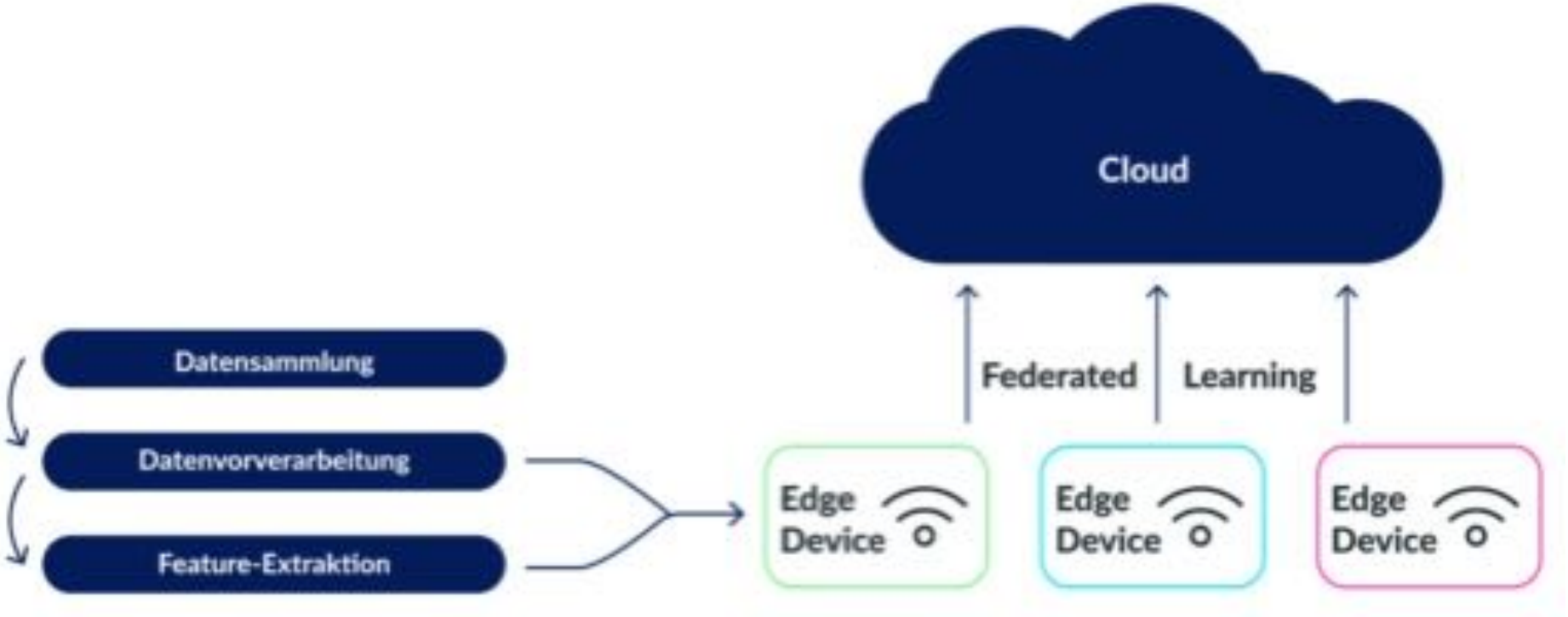
3. Federated Learning mit privaten Daten



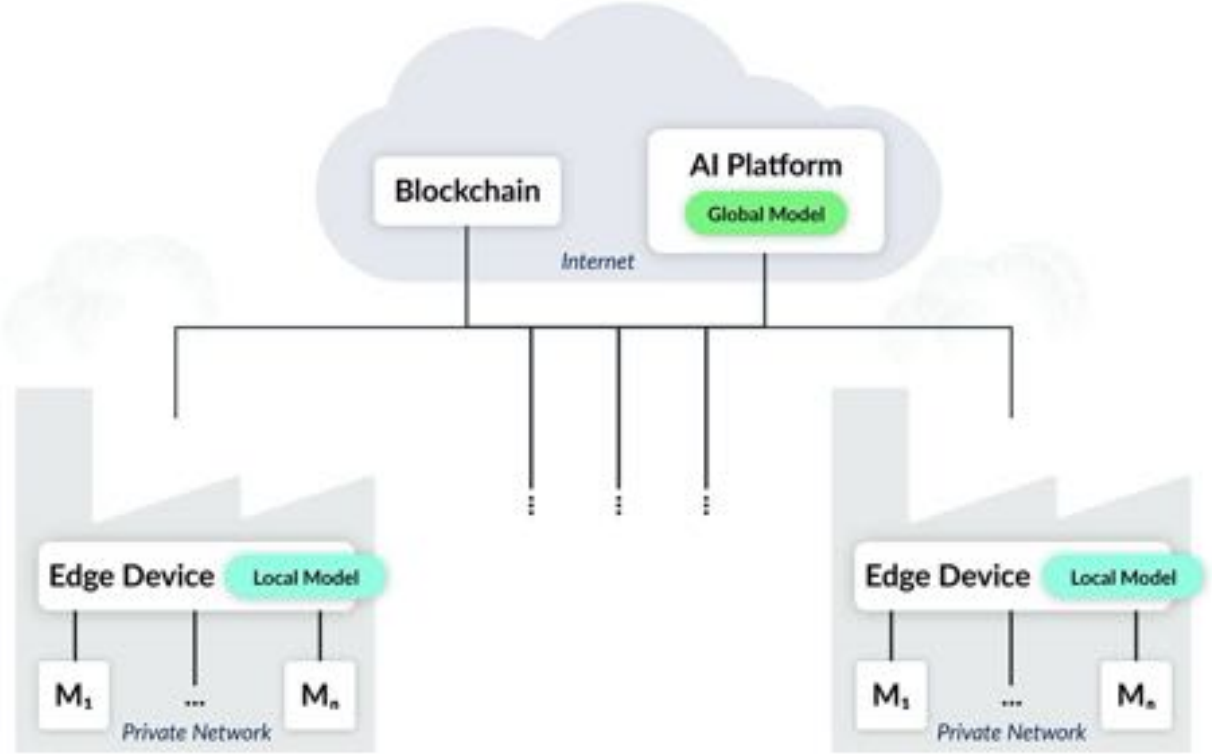
3. Privacy in Machine Learning

- Trainingsdaten können aus dem Modell rekonstruiert werden: Verbreiten von geheimen Betriebs- und Produktionsdaten
- Verwendung von **Differential Privacy** im Training verhindert Rekonstruktion

Vernetzung von KMU



Federated Learning in KOSMoS



Diskussion

- Einfache Anwendbarkeit?

  Experten/Data Scientists werden benötigt. Es nicht das Ziel Maschinenbediener zum Data Scientist zu machen.

- “Falsche” Maschinen verfälschen das kollaborative Modell

  Große Verantwortung des Curators -> Offenes Problem in der Forschung

- Gefahr, dass mathematische/physikalische Modelle besser performen

  PoC; Erprobung, wann sinnvoll/wann nicht

- Welches FL-Framework?

  Keine passenden open source Frameworks -> eigene Implementierung verwenden

- … ?

Vielen Dank

Marisa Mohr

marisa-mohr.de

@ marisa.mohr@inovex.de

@ mohr@ifis.uni-luebeck.de

Christian Becker

@ christian.becker@inovex.de

www.kosmos-bmbf.de