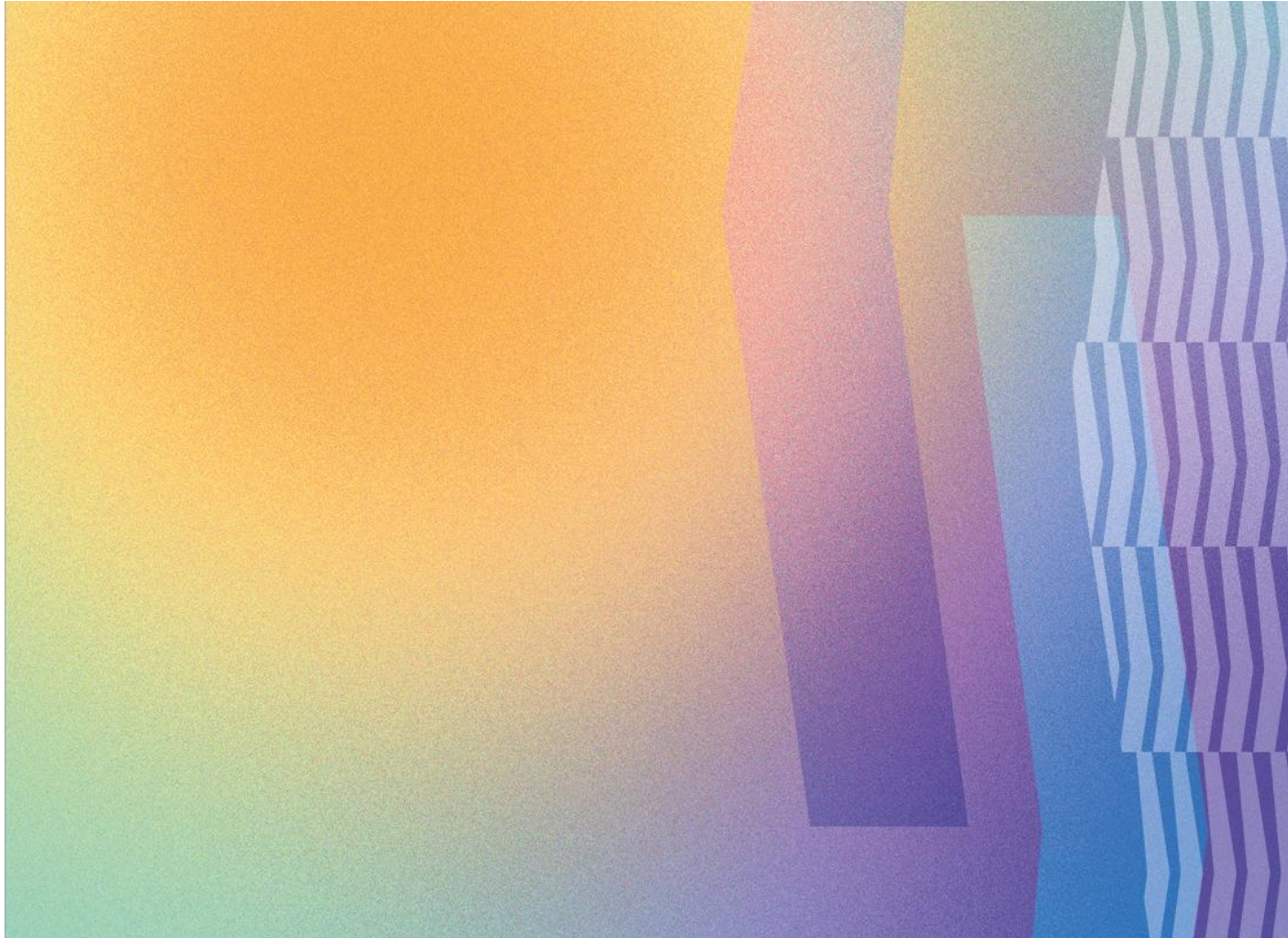


Eine Studie der Begleitforschung zum Technologieprogramm Edge Datenwirtschaft im Auftrag des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR)



PRIVACY-ENHANCING-TECHNOLOGIES FÜR DIE INFORMATIONSSICHERHEIT IN EDGE-CLOUD-ANWENDUNGEN

Impressum

Diese Orientierungshilfe wurde im Auftrag des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) im Rahmen der Begleitforschung zum Technologieprogramm „Edge Datenwirtschaft“ erstellt.

Autor

Nils Jahnke

Sarah Schimankowitz

Fraunhofer-Institut für Software- und Systemtechnik ISST
Dortmund

Herausgeber

Peter Gabriel

Dr. Nicole Wittenbrink

Begleitforschung Edge Datenwirtschaft
Institut für Innovation und Technik (iit)
in der VDI / VDE Innovation + Technik GmbH
Berlin

Datum

Februar 2026

Layout

PRpetuum GmbH

Executive Summary

Edge-Cloud-Systeme ermöglichen Anwendungen, die auf Basis von Daten intelligenter Objekte und Infrastrukturen wirtschaftliche Mehrwerte schaffen und gesellschaftliche Herausforderungen adressieren. Dies bedarf häufig eines Teilens von Daten mit Partnern in etablierten Wertschöpfungsnetzwerken oder entlang des Edge-Cloud-Kontinuums. Eine fundamentale Anforderung ist dabei die Sicherstellung des Schutzes sensibler betrieblicher und personenbezogener Informationen. Während die lokale Datenverarbeitung an der Edge ein grundlegendes Maß an Datenschutz und Informationssicherheit ermöglicht, reicht ein ausschließlicher Rückgriff auf diese Maßnahme oftmals nicht aus, um diese Anforderungen bei gleichzeitiger Erzielung der Mehrwerte datengetriebener Anwendungen zu erfüllen. Beispielsweise besteht häufig die Notwendigkeit, schützenswerte Daten an zentraler Stelle, beispielsweise der Cloud, zu aggregieren, um zu reichhaltigen Erkenntnissen zu gelangen oder die Integrität der verwendeten Daten sicherzustellen. An dieser Stelle rücken Privacy-Enhancing-Technologies (PET) in den Fokus, die Mechanismen umfassen, um Datenschutz, Informationssicherheit und Datensouveränität „by-Design“ in Systemarchitekturen zu integrieren. Bei PET handelt es sich um eine Klasse von individuellen Werkzeugen, die jeweils spezifische Informationssicherheitsanforderungen und -risiken in Edge-Cloud-Systemen adressieren können. Für Praktiker ergibt sich die Herausforderung, auf Basis der spezifischen Bedarfe ihrer Anwendungen und der verfügbaren PET-Werkzeuge passende PET-Strategien zu entwickeln, die eine Realisierung der Edge-Cloud-Anwendung unter Berücksichtigung der Anforderungen und Risiken für die Informationssicherheit ermöglichen.

Diese Orientierungshilfe unterstützt Praktiker bei der Entwicklung eigener PET-Strategien für Edge-Cloud-Anwendungen. Sie bietet Hilfestellungen bei der Identifikation von Informationssicherheitsanforderungen und -risiken, der Auswahl passender PET-Werkzeuge und deren Integration in das Anwendungsdesign. Zentrales Element der Studie ist hierbei die Analyse von PET-Werkzeugen in Edge-Cloud-Anwendungskontexten. Die Orientierungshilfe zeigt, wie PET-Werkzeuge zur Umsetzung von Informationssicherheit beitragen können, welche Voraussetzungen für ihren Einsatz in spezifischen Szenarien geschaffen werden müssen und welche Implikationen sich aus dem Praxiseinsatz der PET-Werkzeuge ergeben. Dazu beruft sich die Orientierungshilfe auf die Erkenntnisse der Early-Adopter von Edge-Cloud-Systemen und PET aus den Projekten des Technologieprogramms „Edge Datenwirtschaft“ des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR). Die Inhalte dieser Orientierungshilfe adressieren insbesondere Systemarchitektinnen und -architekten und Datenschutzbeauftragte, die Datenverarbeitungsprozesse in Edge-Cloud-Systemen datenschutzkonform gestalten müssen.

Ausgehend von der Darstellung möglicher Risiken wie physischen Angriffen und Cyberangriffen, unsicherer Datenhoheit, Insiderbedrohungen und Fehlkonfigurationen sowie Anforderungen wie Datenminimierung, Integrität, Zweckbindung und die Verhinderung von Datenabflüssen „by-Design“ in Edge-Cloud-Anwendungen analysiert diese Orientierungshilfe fünf konkrete PET-Werkzeuge in praxisnahen Anwendungsszenarien:

- Hardware-Schlüssel für die sichere Authentifizierung ohne personenbezogene Daten in der Lebensmittelwirtschaft,

- Federated-Learning für kollaboratives KI-Training ohne Rohdatenweitergabe in der industriellen Fertigung,
- Compute-to-Data zur Ausführung von Analysen in der Umgebung des Dateneigentümers in der industriellen Fertigung,
- Zero-Knowledge-Proofs für datenbasierte Nachweise ohne Offenlegung sensibler Daten in der Energiewirtschaft,
- Trusted-Execution-Environments für vertrauliche Berechnungen in isolierten Hardware-Umgebungen in der Energiewirtschaft.

Zudem präsentiert die Studie vier Handlungsfelder und zugehörige Handlungsempfehlungen für den erfolgreichen Einsatz von PET-Werkzeugen in Edge-Cloud-Anwendungen:

- 1) Aufbau vertrauenswürdiger Partnerökosysteme und Schaffung notwendiger Anreizmechanismen,
- 2) Schaffung betrieblicher Voraussetzungen für den PET-Einsatz inklusive Schulung und Akzeptanzförderung,
- 3) Sicherstellung technischer Validität und Integrationsfähigkeit der PET in den Anwendungskontext,
- 4) Gewährleistung regulatorischer Konformität der PET-gestützten Edge-Cloud-Anwendung.

Im Zuge der steigenden Relevanz von Edge-Cloud-Systemen und dem Teilen von Daten zur Generierung von Datenwertschöpfung bei mindestens gleichbleibenden Anforderungen an Datenschutz und Informationssicherheit wird der Einsatz von PET zu einem entscheidenden Erfolgsfaktor. PET ermöglichen nicht nur die Einhaltung regulatorischer Vorgaben, sondern schaffen die Grundlage für vertrauensbasierte Kooperationen in komplexen Edge-Cloud-Ökosystemen. Unternehmen, die zukünftig gemeinsam datengetriebene Wertschöpfung betreiben wollen, sollten sich aktiv mit PET beschäftigen.

Inhalt

1	Einleitung	4
2	Hintergrund	7
2.1	Edge-Cloud-Systeme	7
2.2	Datenschutz und Informationssicherheit durch Privacy-Enhancing-Technologies	10
3	Der Problemraum – Anforderungen und Risiken für Datenschutz und Informationssicherheit in Edge-Cloud-Anwendungen	17
3.1	Schützenswerte Daten und Informationen in Edge-Cloud-Anwendungen	17
3.2	Spezifische Anforderungen und Risiken für den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen	19
4	Der Lösungsraum – PET-Werkzeuge zur Umsetzung von Datenschutz und Informationssicherheit in Edge-Cloud-Anwendungen	25
4.1	PET-Werkzeuge	25
4.2	PET-Lösungshilfen	28
4.3	Beispiele für den Einsatz von PET-Werkzeugen in Edge-Cloud-Anwendungen	29
4.3.1	Hardware-Schlüssel im Kontext der Qualitätskontrolle in der Lebensmittelwirtschaft	31
4.3.2	Federated-Learning im Kontext der industriellen Fertigung	34
4.3.3	Compute-to-Data im Kontext der industriellen Fertigung	38
4.3.4	Zero-Knowledge-Proofs in der Energiewirtschaft	41
4.3.5	Trusted-Execution-Environments in der Energiewirtschaft	45
5	Handlungsempfehlungen und Ausblick	48
	Anhang A – Detaillierte Übersicht zu PET	56

1 Einleitung

Edge-Computing ermöglicht Rechen- und Speicherprozesse in der Nähe der Datenerzeugung und abseits von zentralisierten Systemen. In Edge-Cloud-Systemen werden Edge- und Cloud-Technologien synergetisch verbunden. Edge und Cloud übernehmen dabei komplementäre Rollen: An der Edge werden Rohdaten aufgenommen und verarbeitet, etwa mittels Methoden der Künstlichen Intelligenz (KI), während in der Cloud die Orchestrierung, die langfristige Speicherung von Analysedaten und die Bereitstellung aggregierter Ergebnisse geleistet wird. Mit Edge-Cloud-Systemen entstehen neue Möglichkeiten, um Daten zu verarbeiten, zu analysieren und zu teilen und somit Geschäftsmodelle mit wirtschaftlichen und gesellschaftlichen Mehrwerten zu erzeugen. Durch die Prozessierung von Daten in lokalen Umgebungen anstatt auf zentralisierten (Cloud-) Ressourcen fördern Edge-Cloud-Systeme zudem grundsätzlich den Datenschutz und die Geheimhaltung.

Der Einsatz von Edge-Cloud-Systemen allein ist jedoch in vielen Fällen nicht ausreichend. Vielmehr entstehen durch die verteilte Datenprozessierung und den Einsatz von KI in Edge-Cloud-Systemen eine Reihe neuartiger datenschutzrechtlicher und informationssicherheitsbezogener Herausforderungen (Sheikh et al., 2025). Zum Beispiel werden oftmals in größerem Umfang potenziell sensible Daten aus der Umwelt und von Interaktionen aufgenommen und analysiert. Weiterhin existiert eine erhöhte Gefahr von physischen Angriffen oder Cyberangriffen auf die dezentralen Edge-Geräte. Zudem können in der Cloud Fehlkonfigurationen oder Fehlverhalten von Menschen zu Datenabflüssen führen. Somit ergibt sich in Edge-Cloud-Systemen ein erhöhter Bedarf hinsichtlich des Schutzes personenbezogener oder geschäftskritischer Daten.

Eine besondere Rolle kommt dabei sogenannten Privacy-Enhancing-Technologies (PET, deutsch: Technologie zum Schutz der Privatsphäre) (Hes & Borking, 1995) zu. Mithilfe von PET können Aspekte des Datenschutzes und der Informationssicherheit bereits durch die Systemgestaltung gewährleistet werden. PET ermöglichen die Nutzung und Analyse von Daten, während sie gleichzeitig die Privatsphäre und Geheimhaltung fördern, das Vertrauen zwischen Partnern der Datenverarbeitungskette stärken und die Einhaltung gesetzlicher Anforderungen wie der Datenschutz-Grundverordnung (DSGVO) unterstützen. Der Begriff „PET“ ist als Oberbegriff verschiedenster technischer Werkzeuge zur Sicherstellung der Privatsphäre zu verstehen, der beispielsweise Ansätze wie Confidential-Computing oder Federated-Learning umfasst, die ihrerseits für spezifische Problemstellungen verwendet werden können.

Für den Einsatz von PET-Werkzeugen sind neben der technischen Umsetzung auch organisatorische (bspw. Rollen, Technologieverständnis, Akzeptanz) und rechtliche Herausforderungen zu klären (Klymenko et al., 2025). Datenverarbeitende Unternehmen müssen daher eine passende PET-Strategie entwickeln, die ihnen ermöglicht, PET-basierte Informationssicherheit in Edge-Cloud-Systemen möglichst effizient und effektiv unter Berücksichtigung der Rahmenbedingungen ihrer Anwendung umzusetzen. Eine PET-Strategie beantwortet folgende Fragestellungen:

- Welches PET-Werkzeug ist konkret dafür geeignet, Daten in meinem Anwendungsfall unter Berücksichtigung von Art, Umfang, Kontext und Zweck der Datenverarbeitung im entworfenen Edge-Cloud-System zu schützen?
- Was sind mögliche Herausforderungen und Limitationen beim Einsatz spezifischer PET-Werkzeuge in Edge-Cloud-Systemen, die in der Gestaltung adressiert werden müssen?

- Wie kann das PET-Werkzeug in Datenverarbeitungsabläufe in Edge-Cloud-Systemen integriert werden, um seine Potenziale für die Informationssicherheit vollständig auszuschöpfen?

Diese Orientierungshilfe befähigt Praktikerinnen und Praktiker, eigene PET-Strategien zur Herstellung von Informationssicherheit in ihren Edge-Cloud-Anwendungen zu entwickeln. Sie charakterisiert spezifische Anforderungen und Risiken der Informationssicherheit in Edge-Cloud-Anwendungen und identifiziert passende PET-Werkzeuge, mit denen sich diese Anforderungen bewältigen lassen. Als zentraler Mehrwert zeigt die Orientierungshilfe zudem auf, welche Umsetzungsvoraussetzungen für den Einsatz von PET-Werkzeuge in realen Anwendungskontexten geschaffen werden müssen und welche Implikationen sich durch deren Einsatz ergeben. Hierzu werden Fallstudien des Einsatzes von PET in realen Edge-Cloud-Anwendungen präsentiert und die Erfahrungen der Early-Adopter weitergegeben. Zudem gibt die Orientierungshilfe Handlungsempfehlungen für die Umsetzung PET-basierter Edge-Cloud-Anwendungen. Die Inhalte dieser Orientierungshilfe richten sich somit insbesondere an Systemarchitektinnen und -architekten von Edge-Cloud-Anwendungen sowie an Datenschutzbeauftragte (Data Protection Officers), die sich in ihren Organisationen mit der Betrachtung von Informationssicherheit in Edge-Cloud-Anwendungen befassen.

Die Orientierungshilfe gestaltet sich wie folgt: Abschnitt 2 erläutert die konzeptuellen Grundlagen dieser Studie – Edge-Cloud-Systeme und PET – als Werkzeuge zur Realisierung von Informationssicherheit. Abschnitt 3 präsentiert den Problemraum, indem die Arten schützenswerter Daten und mögliche spezifische Anforderungen und Risiken für die Informationssicherheit in Edge-Cloud-Systemen herausgearbeitet werden. Der zugehörige Lösungsraum ist in Abschnitt 4 dargestellt. Dieser gibt eine Übersicht über mögliche PET-Werkzeuge, identifiziert existierende Lösungshilfen, die den Entwurf und die Umsetzung von PET-basierten Datenverarbeitungsarchitekturen unterstützen und analysiert praktische Szenarien des Einsatzes von PET-Werkzeugen in Edge-Cloud-Anwendungen. Der abschließende Ausblick gibt Handlungsempfehlungen für Praktikerinnen und Praktiker, die Informationssicherheit durch den Einsatz von PET in eigenen Edge-Cloud-Anwendungsvorhaben sicherstellen möchten (Abschnitt 5).

Die Zusammenarbeit mit den Experten aus den Early-Adopter-Projekten des Technologieprogramms Edge Datenwirtschaft hat maßgeblich dazu beigetragen, praxisnahe Erkenntnisse hinsichtlich der Einbindung von PET-Werkzeugen in Edge-Cloud-Systemen für diese Studie zu analysieren und aufzubereiten. Das Autorenteam möchte sich daher an dieser Stelle noch einmal herzlich und ausdrücklich bei allen Interviewten für ihre Unterstützung bei der Erstellung dieser Orientierungshilfe bedanken:

- Sabine Haag, Robert Bosch GmbH, *Projekt EASY*
- Tobias Schlagenhaut, Robert Bosch GmbH, *Projekt EASY*
- Alexander Tessmer, Universität Osnabrück, *Projekt FRED*
- Marvin Ehaus, Fraunhofer-Institut für Angewandte Informationstechnik FIT, *Projekt DEER*
- Fabian Gast, Institut für Produktionsmanagement, Technologie und Werkzeugmaschinen (PTW) | TU Darmstadt, *Projekt ESCOM*
- Felix Förster, OLI Systems, *Projekt DEER*

Die Verantwortung für den Inhalt dieser Orientierungshilfe liegt ausschließlich bei den Autoren.



Die Orientierungshilfe wurde im Rahmen der Begleitforschung zum Technologieprogramm „Edge Datenwirtschaft“ des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) erstellt. Das Programm umfasst zehn Projekte, die neue Formen von Edge-Cloud-Systemen für wichtige Sektoren der deutschen Wirtschaft entwickeln.

2 Hintergrund

Um Datenschutz und Informationssicherheit in Edge-Cloud-Systemen mittels Privacy-Enhancing-Technologies (PET) herstellen zu können, bedarf es zunächst des notwendigen Grundlagenverständnisses über die Kernkonzepte dieser Problemstellung. Hierzu beschreibt dieser Abschnitt die konzeptuellen Grundlagen von Edge-Cloud-Systemen und der dortigen Datenverarbeitungsprozesse und zeigt auf, warum die Topologie von Edge-Cloud-Systemen die umfassende Betrachtung von Datenschutzaspekten notwendig macht (Abschnitt 2.1). Anschließend erfolgt die grundlegende Darstellung essenzieller Konzepte im Bereich Datenschutz, Informationssicherheit und Risikomanagement und eine Einordnung von PET als Werkzeug zur Umsetzung der Risikoreduktion (Abschnitt 2.2).

2.1 Edge-Cloud-Systeme

Edge-Computing ist ein Konzept für die Ausführung datenbezogener Operationen, das in einer hierarchischen Anordnung verschiedener Datenverarbeitungssysteme Rechenleistung und Speicherplatz nahe dem Ort der Datenerzeugung platziert, um die Menge an Daten, die an die Cloud oder andere zentralisierte Systeme gesendet werden müssen, zu reduzieren. Durch den Einsatz von Edge-Computing ergeben sich geringere Latenzzeiten bei der Datenverarbeitung, eine effizientere Nutzung von Ressourcen und Vorteile bei der Geheimhaltung kritischer Daten. Eine vollständige Abkehr von zentralisierten Cloud-Systemen ist allerdings oftmals nicht sinnvoll, da diese für Aufgaben mit erhöhtem Rechenleistungsbedarf, die langfristige Verfügbarmachung von aggregierten Daten oder die Orchestrierung von Ressourcen benötigt werden.

Um die Vorteile von Cloud und Edge gleichermaßen zu nutzen, werden deren Komponenten in Edge-Cloud-Systemen miteinander kombiniert. Edge-Cloud-Systeme sind hybride Rechnerarchitekturen, die auf verschiedenartige Ressourcen – üblicherweise Rechenleistung, Speicher und Netzwerkressourcen – des sogenannten Cloud-Edge-Kontinuums zurückgreifen. Die Bandbreite dieser Ressourcen erstreckt sich dabei von Geräten des Internet-of-Things (IoT) bis hin zur Public-Cloud-Infrastruktur. Sowohl in der wissenschaftlichen als auch in der praxisnahen Literatur wurden verschiedene Versuche zur Einteilung des Edge-Cloud-Kontinuums unternommen.

In dieser Publikation wird das Edge-Cloud-Kontinuum in vier Ebenen eingeteilt, die anhand ihrer Distanz zum Ort der Datenerzeugung angeordnet werden (s. Abbildung 1). Diese Ebenen unterscheiden sich zusätzlich einerseits hinsichtlich der verfügbaren Rechen- und Speicherkapazitäten sowie andererseits hinsichtlich der für die jeweilige Ebene verantwortlichen Akteure.

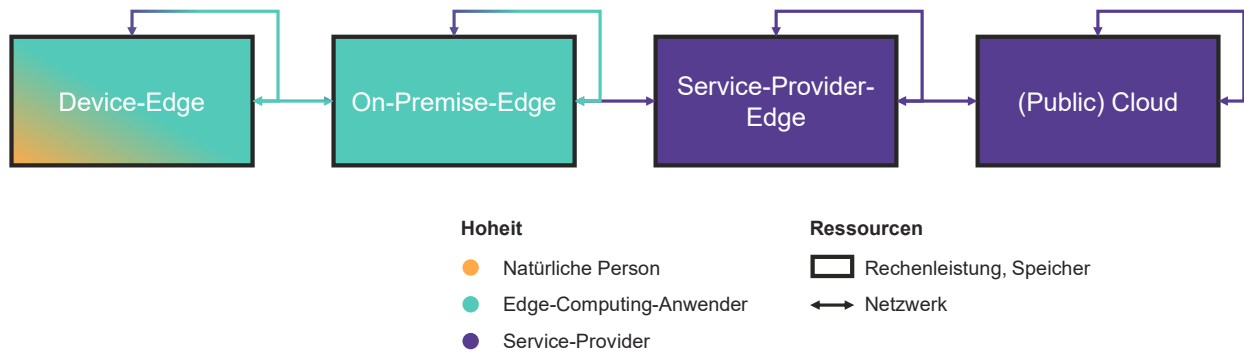


Abbildung 1: Ebenen des Edge-Cloud-Kontinuums für Edge-Cloud-Systeme

Die *Device-Edge* umfasst einerseits sogenannte „Constrained-Devices“, also microcontrollerbasierte Geräte mit begrenzter Speicherkapazität, Rechenleistung und Leistungsaufnahme aus dem Bereich des Internet-of-Things (IoT), die oftmals anwendungsspezifisch entwickelt werden. Andererseits umfasst diese auch „intelligenter“ Geräte, die über umfassendere technische Kapazitäten verfügen und anwendungsunabhängige Rechenleistung bereitstellen. Beispiele hierfür sind Smartphones und Tablets. Die Verantwortung für den Betrieb der Device-Edge unterliegt entweder natürlichen Personen, beispielsweise wenn diese Applikationen auf ihrem Smartphone nutzen, oder im Falle von industriellen Anwendungen den entsprechenden Unternehmen. Die *On-Premise-Edge* umfasst Server-Hardware, die in konventionellen, physisch abgesicherten Rechenzentren oder in modularen Rechenzentrumseinheiten in der Nähe von oder in Bürogebäuden und Fabriken untergebracht ist. Diese Ressourcen gehören in der Regel einem einzelnen Anwenderunternehmen, das diese auch betreibt. Mit der *Service-Provider-Edge* rücken Cloud-Service-Provider oder Telekommunikationsanbieter Mechanismen des Cloud-Computing näher an die Anwendenden. Entsprechende Ressourcen befinden sich etwa in Funkmasten, Netzwerkknoten oder städtischen Ballungsräumen und damit weiterhin in unmittelbarer Nähe zur Datenerzeugung. Entsprechende Services, die auf standardisierter Hardware und Software basieren, können jedoch von verschiedenen Kunden gebucht werden. Die *(Public) Cloud* stellt potenziell endlos skalierbare Rechen- und Speicherressourcen an zentralisierten Orten als Serviceleistung zur Verfügung.

Die Verbindung zwischen den einzelnen Speicher- und Rechenressourcen im Edge-Cloud-Kontinuum geschieht über Netzwerkverbindungen, die ebenfalls durch verschiedene Akteure betrieben werden. Im Bereich von Device-Edge und On-Premises-Edge können diese einerseits durch Edge-Computing-Anwendende in Form von WiFi, 5G-Campusnetzen oder Ethernet-Verbindungen bereitgestellt werden. Andererseits werden insbesondere bei Anwendungen in abgelegenen Regionen oder bei beweglichen Objekten Dienste der (Mobilfunk-) Netzbetreiber (4G/5G) und Internet-Service-Provider genutzt. Die Dienste dieser Anbieter werden ebenso benötigt, um Daten über weitere Distanzen zur Service-Provider-Edge oder Public-Cloud zu transportieren. Für direkte Netzwerkverbindungen, die das öffentliche Internet umgehen, können sogenannte Interconnection-Services genutzt werden.

Datenverarbeitung in Edge-Cloud-Systemen

Bei der Realisierung von datengetriebenen Anwendungen übernehmen die einzelnen Ebenen eines Edge-Cloud-Systems spezifische Aufgaben entlang der Datenverarbeitungskette. Zur Gewinnung von Daten können Device-Edge und On-Premises-Edge Daten in großen Mengen, mit hoher Geschwindigkeit und mit geringer Ausfallwahrscheinlichkeit aus der verbundenen Sensorik

erfassen. Beide Ebenen werden ebenso zur Datenaufbereitung herangezogen. Device-Edge und On-Premises-Edge sorgen für eine lokale Anonymisierung oder Pseudonymisierung der Daten. Weiterhin können sie gemeinsam mit der Service-Provider-Edge Daten reduzieren, um den Datentransfer in die Cloud zu ermöglichen oder die Effizienz eines datengesteuerten Systems zu verbessern.

Um Informationen aus den verfügbaren Daten zu erhalten, müssen diese in Rahmen von (KI-) Analyseverfahren kombiniert und ausgewertet werden. Für Anwendungen, die eine Bereitstellung von Informationen in Echtzeit benötigen (z.B. Maschinensteuerung oder autonomes Fahren), können Analyseanwendungen unter Berücksichtigung von Ressourcenbeschränkungen an der Edge-Ebene durchgeführt werden. Mit Anstieg des Speicher- und Rechenbedarfs sowie der Menge an Datenquellen, werden üblicherweise zentralisiertere Ressourcen wie die Service-Provider-Edge oder die Public-Cloud zur Informationsgewinnung genutzt.

Die gewonnenen Informationen müssen entlang des Edge-Cloud-Kontinuums für die Nutzung durch Menschen und Maschinen verfügbar gemacht werden. Die Edge-Ebene kann als Relaispunkt für die Informationsbereitstellung dienen und ausgewählte Informationen von Cloud-Diensten an bestimmte Geräte und Nutzende verteilen. Andersherum können Informationen von der Edge an Cloud-Dienste weitergegeben werden, um diese Informationen auf globaler Ebene verfügbar und nutzbar zu machen. Die bereitgestellten Informationen müssen im betrieblichen Kontext für Entscheidungen verwendet werden, um ihre geschäftliche Wirkung zu erzielen. Edge-Computing ermöglicht die unterbrechungsfreie Nutzung von Informationen durch Maschinen und Personen, indem Daten lokal verfügbar gemacht werden. Die Cloud-Ebene in Edge-Cloud-Systemen kann Informationen hingegen für globale Entscheiderinnen und Entscheider nutzbar machen.

Edge-Cloud-Systeme in der Datenwirtschaft

Während viele Unternehmen bereits Edge-Cloud-Systeme für interne Zwecke einsetzen, ist für verschiedene Anwendungen in der Datenwirtschaft eine auf ein einzelnes Unternehmen bezogene Verarbeitung von Daten nicht mehr ausreichend. Stattdessen werden verstärkt kollaborative Geschäftsmodelle verfolgt, in denen Daten oder Informationen über verschiedene Parteien hinweg geteilt werden müssen. Hierzu gehören Anwendungen, in denen Daten im Rahmen von Auftragsanalysen durch einen Dienstleister mit entsprechenden Kompetenzen durchgeführt werden oder Anwendungen, in denen Daten an zentraler Stelle für Monitoring und Steuerung verfügbar gemacht werden. Ein Beispiel hierfür sind Prozesse in der Logistik, in denen Warenzustände über die gesamte Lieferkette verfolgt werden und diese Waren bei Nichteinhaltung von Grenzwerten entsorgt werden müssen. Weiterhin können Anforderungen hinsichtlich des Erreichens von regulatorischer Konformität, der Beweisführung und der Präsentation verifizierbarer Informationen für Dritte ein Teilen von Daten mit weiteren Parteien erforderlich machen. Nicht zuletzt ist eine Datenübertragung für die Entwicklung des Produkts, die Generierung von Erkenntnissen oder im Sinne des Wissenstransfers, beispielsweise zum kollaborativen Training von KI-Modellen, denkbar. In diesen Fällen kommt Edge-Cloud-Systemen weiterhin die Aufgabe der Datenaufnahme, -aufbereitung und -verfügbarmachung zu. Zur vollständigen Werterfüllung müssen die an zentrale Punkte weitergegebenen oder geteilten Daten oftmals weiterhin geschäftlich sensible oder personenbeziehbare Inhalte enthalten, denen jedoch die Schutzbedarfe der datengebenden Organisationen oder der betroffenen Personen entgegenstehen.

2.2 Datenschutz und Informationssicherheit durch Privacy-Enhancing-Technologies

Ausgehend von den allgemeinen Rechten von natürlichen Personen auf den Schutz ihrer Privatsphäre und von Unternehmen hinsichtlich des Schutzes von Geschäftsgeheimnissen ergeben sich im digitalen Raum Ansprüche an den Schutz von Daten und die sichere Verarbeitung und Verwahrung von Informationen. Datenschutz bedeutet, die existierenden Rechte, Verpflichtungen und Freiheiten der betroffenen Personen in Bezug auf die Sammlung, Speicherung, Nutzung, Veröffentlichung, Weitergabe und Löschung von solch sensiblen Informationen einzuhalten und sicherzustellen. Hierbei stehen also neben dem Schutz von Daten als immateriellem Vermögenswert auch die Bedürfnisse der Betroffenen im Vordergrund. Ziel des Datenschutzes ist die Sicherstellung der legitimen Verwendung von Daten über den gesamten Datenlebenszyklus hinweg. Im Rahmen dieser Orientierungshilfe werden neben den aus Sicht der Privatsphäre natürlicher Personen schützenswerten Daten auch aus betrieblicher Sicht schützenswerte Informationen berücksichtigt.

Risiken für den Datenschutz und die Informationssicherheit bezeichnen allgemein die möglichen Auswirkungen, die sich aus einem Informationsdefizit hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie der Einhaltung von datenschutzrechtlichen Vorschriften ergeben (ISO, 2024). Um diese Unsicherheiten zu identifizieren, zu analysieren und zu adressieren, muss ein Risikomanagement für den Datenschutz und die Informationssicherheit umgesetzt werden. Das Risikomanagement ist dabei üblicherweise in das breitere Risikomanagement-Framework einer Organisation eingebettet. Ein Management von Datenschutzrisiken beinhaltet vorrangig folgende Tätigkeiten (ISO, 2024):

- Entwickeln des notwendigen Verständnisses für den Anwendungskontext und Anwendungsfall inklusive Analyse der Datenschutzerfordernungen,
- identifizieren, analysieren und evaluieren der Risiken im Hinblick auf die zu schützenden Daten und Informationen,
- entwickeln und umsetzen von angemessenen Gegenmaßnahmen, um Risiken zu vermeiden oder zu verringern,
- kommunizieren und Rücksprache halten zu Risiken und Gegenmaßnahmen mit den betroffenen Stakeholdern,
- kontinuierliches Monitoring und Prüfen der Risiken und Gegenmaßnahmen.

Diese Arbeit fokussiert sich insbesondere auf die ersten drei Aspekte des Risikomanagements. Im Folgenden werden daher zunächst allgemeine Modelle beschrieben, die eine Ableitung von Anforderungen an den Datenschutz und die Informationssicherheit sowie die Identifikation möglicher Risiken unterstützen. Anschließend erfolgt die konzeptuelle Einordnung von Privacy-Enhancing-Technologies (PET) als Werkzeug, um diese Anforderungen zu erfüllen und mögliche Risiken „by-Design“ zu minimieren.

Identifizierung von Anforderungen an den Datenschutz und die Informationssicherheit

Ein erster notwendiger Aspekt des Risikomanagements stellt die Generierung eines ausreichenden Wissens über die Anwendung, die verwendeten oder generierten schützenswerten Daten und Informationen sowie der möglichen Anforderungen an deren Schutz dar. Während sich die schützenswerten Daten und Informationen aus dem konkreten Anwendungskontext heraus erge-

ben, können verbundene Anforderungen generell aus den in Tabelle 1 beschriebenen Perspektiven entstammen und entsprechend aus einer Reihe von Faktoren motiviert werden. Diese Faktoren sind dort entsprechend ihrer Granularität angeordnet. Rechtliche und regulatorische Faktoren setzen den allgemeinen Rahmen, in dem Datenverarbeitungsaktivitäten stattfinden dürfen. Vertragliche Faktoren definieren zusätzliche, darüberhinausgehende Ansprüche und Verpflichtungen an die beteiligten Parteien. Anwendungsfaktoren beziehen sich auf konkrete technische und organisatorische Elemente, um den Datenschutz und die Informationssicherheit in der Praxis zu gewährleisten.

Rechtliche und regulatorische Faktoren	Vertragliche Faktoren	Anwendungsfaktoren	Weitere Faktoren
- Internationale, nationale oder lokale Gesetze	- Vereinbarungen zwischen den Beteiligten	- Eigenschaften der anvisierten Anwendung	- Individuelle Anforderungen an die Privatsphäre durch die Betroffenen
- Gerichtliche Entscheidungen	- Existierende Unternehmensregeln und -richtlinien	- Industriespezifische Richtlinien oder Best-Practices	- Interne Kontrollsysteme
- Vereinbarungen mit Gewerkschaft oder Betriebsrat		- Reputationsfaktoren	

Tabelle 1: Herkunft von Datenschutzerfordernungen nach ISO/IEC 29100:2024 (ISO, 2024)

Rechtliche und regulatorische Vorschriften resultieren vor allem aus der Datengesetzgebung. Die Europäische Union formuliert als Vorreiterin in der Datengesetzgebung umfassende Anforderungen an den Schutz von (personenbezogenen) Daten. Zentrales Instrument ist die Datenschutzgrundverordnung DSGVO (European Parliament & Council of the European Union, 2016), die zunächst sieben Prinzipien für die Verarbeitung von personenbezogenen Daten aufstellt (Art. 5) und basierend auf diesen Prinzipien unter anderem technische Verpflichtungen an die Realisierung von Datenschutz (Art. 25) formuliert. Neben der DSGVO beschreiben zudem die KI-Verordnung (AI-Act, European Parliament und Council of the European Union (2024)) und das Datengesetz (Data-Act, European Parliament und Council of the European Union (2023)) potenzielle zusätzliche Anforderungen an den Schutz von Daten und Informationen. Die KI-Verordnung verweist dabei einerseits auf die Prinzipien der DSGVO. Sie nennt aber auch den Einsatz von PET explizit, um Algorithmen auf Daten anzuwenden und KI-Systeme zu trainieren, ohne dass Daten zwischen den Parteien übermittelt oder kopiert werden müssen (ErwG. 39). Der Data Act soll den Zugang zu Rohdaten und vorverarbeiteten Daten aus vernetzten Produkten und Diensten vereinfachen. Dabei ergibt sich ein Spannungsfeld zwischen der Weitergabe von Daten und dem Schutz vor unrechtmäßiger Offenlegung von Informationen und den damit verbundenen Geschäftsgeheimnissen. Auch das Datengesetz nennt sogenannte technische Schutzmaßnahmen als Mittel, um den unerlaubten Zugriff auf Daten und Metadaten einzuschränken und gleichzeitig der Verpflichtung zur Bereitstellung von Daten nachzukommen. Zudem sind auch branchenspezifische sowie internationale Gesetzgebungen zu betrachten, die gewisse Anforderungen an den grenzübergreifenden Fluss von Daten definieren.

In der Umsetzung dieser Vorgaben helfen bereits umfassend verfügbare gerichtliche Entscheidungen, die die Auslegung der DSGVO präzisieren. Da die neuen Datengesetzgebungen (AI-Act und Data-Act) allerdings zum Zeitpunkt der Studiererstellung noch nicht vollständig anwendbar sind, kann erst in den kommenden Jahren mit gerichtlichen Entscheidungen in Bezug auf mögliche Streitgegenstände gerechnet werden.

Weitere nennenswerte Anforderungen können aus bestehenden Vereinbarungen oder akuten Interessen der Beschäftigtenvertretungen entstammen. Beispiele für aus dieser Sicht kritische Anwendungen stellen Videoüberwachung, Aufzeichnung von Aktivitäten oder Tracking von Betriebsmitteln dar. Auch wenn die Datenaufnahme nicht dem Zweck der Mitarbeitendenüberwachung gilt, ist es im Interesse der Beschäftigten, die Anforderungen an den Schutz der Privatsphäre zu erfüllen.

Vertragliche Vereinbarungen sind der zweite Bereich, aus dem Schutzansprüche an die Datenverarbeitung formuliert werden. Hierbei sind vertragliche Vereinbarungen zwischen verschiedensten Akteuren denkbar. Beispiele sind Vereinbarungen zwischen den Anwendungsnutzenden oder Unternehmen mit den von ihnen genutzten Serviceanbietern oder Auftragsverarbeitern, beispielsweise Cloud-Service-Providern. Zudem sind Vereinbarungen über bilaterale Datenflüsse zwischen Unternehmen (sogenannte Datennutzungsverträge) Dokumente, in denen Anforderungen an die Datenverarbeitung und Informationsnutzung genannt werden.

Weitere Anforderungen an die Privatsphäre können aus den existierenden Richtlinien und Regeln der Organisation entstammen. So formulieren Organisationen Ansprüche an sich selbst, wie Daten zu verarbeiten und Informationen zu handhaben sind und welche Aspekte bei der Entwicklung von Datenarchitekturen berücksichtigt werden müssen. Hierzu können ebenso Ansprüche an die eigene Datensouveränität, d. h. die Kontrolle über Daten auch nach deren Transfer, gehören.

Als dritter Herkunftsbereich für Anforderungen gelten Anwendungsfaktoren. Diese beschreiben Rahmenbedingungen, die sich aus dem spezifischen Anwendungskontext, der Anwendungszielsetzung, den Anwendungsmerkmalen sowie aus den Erwartungen der Anwendungs-Stakeholder ergeben. Solche Anwendungsfaktoren können entsprechend je nach Anwendung, Branche und Unternehmen sehr unterschiedlich ausfallen. Beispielsweise existieren je nach Branche unterschiedliche Standards und Richtlinien, die durch entsprechende Applikationen erfüllt werden müssen. Die aus diesen Faktoren entstammenden Anforderungen beschreiben dabei oftmals das „Wie“, während die vorangegangenen Kategorien formulieren, „Was“ gewährleistet werden soll. Hierbei sollte auch bedacht werden, welche negativen Implikationen die Nichteinhaltung gegebener Standards oder technischer Maßnahmen beispielsweise im Hinblick auf die Reputation des Unternehmens und die Nutzung der Anwendung haben könnten (Janakiraman et al., 2018).

Viertens existieren weitere allgemeine Faktoren, die eine Rolle bei der Ableitung von Anforderungen an den Datenschutz und die Informationssicherheit spielen. Besonders zu berücksichtigen sind die individuellen Privatsphäre-Erwartungen der betroffenen Personen. So können Betroffene zusätzliche, gegebenenfalls nicht in den AGB einer Lösung vereinbarte, Erwartungen besitzen. Weiterhin werden AGB nur von etwa einem Viertel der betroffenen Personen überhaupt vollständig gelesen (Gerber et al., 2018). Die persönliche Einstellung gegenüber Privatsphäre und die Einschätzung wahrgenommener Risiken hängen von vielen Einflussgrößen ab, darunter dem Zweck der Transaktion und deren subjektiven Vorteilen, dem technischen Verständnis, dem Vertrauen in den Datenverarbeiter, frühere Erfahrungen und dem Selbstvertrauen der Bereitstellenden (Gerber et al., 2018). Darüber hinaus können interne Kontrollsysteme die konkreten Datenschutzmaßnahmen beeinflussen. Bestandteile solcher Kontrollsysteme sind beispielsweise die Datengovernance, das Risikomanagement oder weitere im Rahmen von Auditierung und Zertifizierung vereinbarte Schutzmaßnahmen des Unternehmens.

Identifizierung von Risiken für den Datenschutz und die Informationssicherheit

Zur Identifizierung von Risiken für den Datenschutz und die Informationssicherheit können mehrere dedizierte Ansätze verfolgt werden. Zwei populäre Ansätze sind der Asset-basierte Ansatz und der ereignisbasierte Ansatz (ISO, 2022). Beim Asset-basierten Ansatz sind Organisationswerte der Ausgangspunkt der Betrachtungen und es wird geprüft, welche Bedrohungen und Schwachstellen diese Assets beschädigen können. Zu den Vermögenswerten zählen neben den schützenswerten Daten und Informationen auch die Systeme und Softwareanwendungen, die eingesetzte Hardware sowie weitere Faktoren wie die Reputation, die durch Probleme beim Datenschutz oder in der Informationssicherheit beschädigt werden kann. Nachdem die schützenswerten Assets identifiziert wurden, sind relevante Bedrohungen für Datenschutz und Informationssicherheit zu identifizieren. Bedrohungen können sich beispielsweise aus der Organisation, den Prozessen, der Systemkonfiguration, der eingesetzten Hardware und Software oder durch Dritte ergeben. Der ereignisbasierte Ansatz der Risikoidentifizierung fokussiert auf die Analyse von (zuvor definierten) Ereignissen, die eine Auswirkung auf den Schutz von Daten oder die Sicherheit von Informationen besitzen. Solche Ereignisse umfassen beispielsweise die Nutzung von sensiblen Daten über den Anwendungszweck hinaus, die umfassende Überwachung von Individuen oder die mangelnde Transparenz über die Datennutzung. Zu diesen Ereignissen werden Szenarien gebildet, um Konsequenzen besser abschätzen zu können. Während der Asset-basierte Ansatz eher eine technische Perspektive einnimmt, ist der ereignisbasierte Ansatz insbesondere für Überlegungen auf der Management-Ebene geeignet. Beide Ansätze können auch miteinander kombiniert werden.

Mögliche allgemeine Risiken beinhalten unter anderem den nicht-autorisierten Zugriff, die nicht autorisierte Veränderung oder den Verlust beziehungsweise Diebstahl schützenswerter Daten. Darüber hinaus können sich weitere Risiken aus der Datenverarbeitung ergeben. Dazu gehören die Erhebung von schützenswerten Daten über deren Anwendungszweck hinaus, die unangemessene Verknüpfung personenbezogener Daten, die Missachtung rechtlicher Vorschriften, die limitierte Transparenz in der Datenverarbeitung oder das Teilen von sensiblen Daten mit Dritten ohne die Einwilligung der Betroffenen (DIN, 2020).

Privacy-Enhancing-Technologies

Im Zuge der immer umfassenderen Entwicklung der Datenwirtschaft ergibt sich ein stetig steigender Bedarf nach Werkzeugen, die eine datenschutzkonforme Verarbeitung von Daten ermöglichen und die Informationssicherheit verbessern. Wenngleich die Marktforschungsorganisation Gartner erwartet, dass 2025 etwa 60 Prozent der Großunternehmen zumindest eine Privacy-Enhancing-Technology (PET) einsetzen, ist der PET-Markt noch vergleichsweise jung (Noble, 2023). Zurzeit existieren daher weder eine feste Definition des Konzepts „PET“ noch Einigkeit darüber, welche technischen Maßnahmen konkret als PET zu klassifizieren sind. Diese Studie versteht PET-Werkzeuge im Sinne der Agentur der Europäischen Union für Cybersicherheit generell als „Software- und Hardware-Lösungen, d. h. Systeme, die technische Prozesse, Methoden oder Kenntnisse umfassen, um bestimmte Datenschutzfunktionen zu erreichen oder Risiken für die Privatsphäre einer Person oder einer Gruppe von natürlichen Personen abzuwehren“ (Schiffner, 2015b, S. 9). Während diese Definition insbesondere den Schutz personenbezogener Daten hervorhebt, sind PET auch in der Lage, die Sicherheit aus geschäftlicher Sicht schützenswerter Informationen zu verbessern. Im Zusammenhang mit PET wird oft auch der Begriff Privacy-Preserving-Technology (PPT, deutsch: Technologie zur Bewahrung der Privatsphäre) synonym ver-

wendet. Unter den Schirm der PET fallen auch Konzepte des Privacy-Preserving-Machine-Learning (Xu et al., 2021), bei dem Techniken zum Schutz der Privatsphäre in Machine-Learning-Prozesse integriert oder spezielle KI-Algorithmen verwendet werden.

PET werden gezielt eingesetzt, um den Schutz sensibler Daten und Informationen ab einem bestimmten Punkt in der Datenverarbeitungskette sicherzustellen. Ihre konkrete Einbindung kann dabei in der Erhebung, der Verarbeitung oder in der Analyse und Weitergabe von Daten erfolgen. PET können als einzelne technische Lösung in Datenverarbeitungsarchitekturen integriert oder in Kombination miteinander verwendet werden. Für viele datengetriebene Kooperationsmodelle ist eine solche Kombination verschiedener PETs zur Erfüllung komplexer Anforderungen essenziell. Entsprechend existiert keine universell einsetzbare PET. Der optimale Schutz erfordert stattdessen eine kontextbezogene Auswahl und ggf. Integration mehrerer Technologien, die sich nach den zu erreichenden Zielen, möglichen Herausforderungen sowie den technischen und organisatorischen Rahmenbedingungen richtet (ISACA, 2024) – also eine passende PET-Strategie.

Neben dem erhöhten Schutz sensibler Daten und Informationen ist der Einsatz von PET mit weiteren Vorteilen verbunden: Sie stärken das Vertrauen von Nutzenden und Partnern in die Datenverarbeitung, ermöglichen rechtssicherere Kollaborationen und erlauben datengetriebene Innovationen unter Wahrung von Datensouveränität. Zudem reduzieren ausgewählte PET die Abhängigkeit von vertrauenswürdigen Intermediären und machen Art und Umfang des Datenschutzes messbar. Allerdings erhöhen PET den technischen Implementierungsaufwand von Datenarchitekturen, benötigen oftmals spezialisierte Expertise und setzen ein hohes Technologieverständnis voraus. Durch ihren Einsatz ergeben sich teilweise Performance-Einbußen sowie höhere Aufwände und Kosten, für die Nutzende nur selten aufkommen möchten. Zudem ist es weiterhin notwendig, die Datenarchitekturen durch zusätzliche organisatorische und technische Aspekte zu stärken.

Die Charakteristika von PETs lassen sich anhand mehrerer funktionaler Kriterien unterscheiden (Heurix et al., 2015). Eine Übersicht über diese Kriterien ist in Abbildung 2 abgebildet.

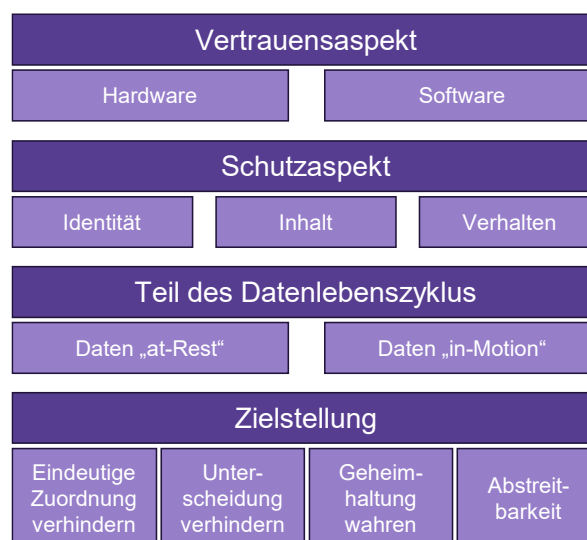


Abbildung 2: Taxonomie von PET in Anlehnung an Heurix et al. (2015)

An erster Stelle steht dabei der Vertrauensaspekt beziehungsweise der eingesetzte Schutzmechanismus. Hardware-basierte PET erzielen ihren Schutzaspekt primär durch spezialisierte phy-

sische Architekturen (ergänzt durch Softwarebibliotheken), die Daten und Code während der Datenprozessierung von der Umwelt isolieren und schützen. Software-basierte PET stützen sich vorwiegend auf mathematische oder kryptografische Verfahren, um Datenschutz zu gewährleisten.

PET fokussieren zudem auf einen oder mehrere Aspekte des Schutzes von Daten. Die Aspektdimension unterscheidet zwischen drei Hauptkategorien: Identität, Inhalt und Verhalten. Ein Schutz der Identität bezieht sich auf das Verbergen oder Maskieren der aktiv oder passiv involvierten Entitäten. Aktive Entitäten stellen Daten über sich selbst bereit, während passive Entitäten von einer Drittpartei verwaltet werden. Der Schutzaspekt „Inhalt“ bezieht sich auf die Daten oder Informationen, die während der Inanspruchnahme eines Services erstellt und in deren Nachgang verwaltet werden. Daten zum Verhalten umfassen die Aktionen der betroffenen Personen bei der Datengenerierung. Der Schutz dieser Daten ist relevant, wenn der Dateninhalt bereits verborgen ist, aber Zugriffsmuster oder Metadaten sensible Informationen über den Nutzenden offenbaren können.

Die Dimension „Datenlebenszyklus“ beschreibt, welche Daten durch eine PET adressiert und geschützt werden. PET können grundsätzlich entlang des gesamten Datenlebenszyklus eingesetzt werden. Auf Basis der unterschiedlichen Funktionsweisen werden vor allem zwei grundlegende Status von Daten unterschieden: Daten „at-Rest“ und Daten „in-Motion“. Daten „at-Rest“ beziehen sich auf Daten beziehungsweise Informationen, die in Speichern wie Datenbanken oder Dateisystemen liegen. Verfahren, die auf den Schutz dieser Daten abzielen, stellen sicher, dass Unbefugte, die Zugriff auf diese Daten erlangen, die Privatheit nicht verletzen können. Daten „in-Motion“ umfassen im Rahmen dieser Publikation Daten beziehungsweise Informationen während der Übertragung von einer Partei zu einer anderen Partei sowie während ihrer Verarbeitung.

Die Zielstellung einer PET definiert, was die PET tun soll. Sie legt gleichzeitig die Mittel fest, die zum Schutz der Privatsphäre und Gewährleistung der Informationssicherheit verfolgt werden. Die Verhinderung einer eindeutigen Zuordnung von Daten zu Personen beschreibt das Ziel, einzelne Entitäten nicht mit weiteren Daten, wie Transaktionen oder Dateneinträgen, verknüpfen zu können. Somit können Dritte nicht feststellen, ob gewisse Entitäten zu einem größeren Verbund gehören. Ein weiteres Ziel ist die Verhinderung der Unterscheidbarkeit zwischen zwei Entitäten. Somit ist es möglich, eine Entität in einer größeren Menge von Entitäten zu verbergen. Beispielsweise wird dies erreicht, indem die Attribute in einer Tabelle so verändert oder geclustert werden, dass keine Rückführung auf eine einzelne Person möglich ist. Die Wahrung der Geheimhaltung beziehungsweise Gewährleistung von Vertraulichkeit bezieht sich auf die Anforderung, Daten vor unbeabsichtigter Offenlegung zu schützen. Zuletzt beschreibt „Abstreitbarkeit“ die Fähigkeit, dass ein Beteiligter gegenüber Dritten glaubhaft bestreiten kann, an einer bestimmten Kommunikation oder Transaktion mitgewirkt zu haben, selbst wenn der unmittelbare Gegenpart in der Situation von der Echtheit überzeugt war. Beispiele hierfür sind Gruppenmechanismen, in denen „jemand aus der Gruppe“ eine entsprechende Tätigkeit durchgeführt hat.

Die Ausführungen in diesem Abschnitt zeigen auf, welche Arten von Anforderungen für den Datenschutz und die Informationssicherheit allgemein auftreten und wie verbundene Risiken identifiziert werden können. Zudem wurde dargelegt, wie PET generell als Werkzeug eingesetzt werden können, um angemessene Maßnahmen zur Verringerung von Risiken zu unterstützen. Im Kontext von Edge-Cloud-Anwendungen existieren jedoch eine Reihe spezifischer Rahmenbedingungen, wie etwa die umfassende Generierung von Daten aus der Umwelt, die beschränkte lokale Rechenleistung und die verteilte Datenprozessierung, mit denen spezifische Anforderungen



und Risiken für den Datenschutz und die Informationssicherheit einhergehen. Um diese Herausforderungen mittels PET anzugehen, bedarf es derzeit weiterer Hilfsmittel.

3 Der Problemraum – Anforderungen und Risiken für Datenschutz und Informationssicherheit in Edge-Cloud-Anwendungen

Der Schutz von Daten und die Gewährleistung von Informationssicherheit in Edge-Cloud-Systemen beinhalten besondere Herausforderungen, die über allgemeine Problemstellungen datengetriebener Anwendungen hinausgehen. Dieser Abschnitt schafft ein Verständnis darüber, welche Herausforderungen konkret bestehen. Er geht auf den Kontext und die Kernursachen ein. Dazu wird zunächst dargelegt, welche Arten von schützenswerten Daten und Informationen in Edge-Cloud-Systemen generiert werden (Abschnitt 3.1). Anschließend werden zentrale Anforderungen für den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen dargestellt und relevante Risiken beschrieben (Abschnitt 3.2). Durch die Vielfalt der schützenswerten Daten und Informationen sowie der zugehörigen Anforderungen und Risiken ergibt sich ein komplexer und hochdimensionaler Problemraum. Die umfassende Analyse dieses Problemraums im Zuge eigener Edge-Cloud-Systementwicklungen stellt die Grundlage dar, um passende Privacy-Enhancing-Technology (PET)-Werkzeuge zur Umsetzung von Datenschutz und Informationssicherheit identifizieren zu können.

3.1 Schützenswerte Daten und Informationen in Edge-Cloud-Anwendungen

Durch die direkte Erfassung und Integration von Daten physischer Geräte, Anwendungen und ihrer Umwelt werden dedizierte Arten von schützenswerten Daten und Informationen in Edge-Cloud-Systemen generiert. Diese können sich beispielsweise stark von den erfassten personenbezogenen Daten in formularbasierten Anwendungen unterscheiden. Tabelle 2 bietet eine Übersicht schützenswerter personenbezogener Daten und Informationen, die in der Folge in den Kontext von Edge-Cloud-Systemen eingeordnet werden.

Schutzbedürftige Personendaten	Schutzbedürftige Unternehmensdaten und -informationen
<ul style="list-style-type: none"> - Identifikatoren - Weitere Charakteristika, die Personen unterscheiden können - Pseudonymisierte Daten, die auf eine Person bezogen werden können - Metadaten und Bewegungsdaten - Nicht angefragte, zufällig generierte Personendaten 	<ul style="list-style-type: none"> - Geistiges Eigentum - Daten aus Kundenbeziehungen - Nicht-öffentliche Finanzkennzahlen und statistische Daten - Daten, die auf Basis weiterer branchenspezifischer Vorschriften geschützt werden müssen

Tabelle 2: Übersicht der Typen schutzbedürftiger Daten und Informationen

Schutzbedürftige Personendaten

Ein umfassender Schutz von personenbezogenen Daten ist in der Datenschutz-Grundverordnung (DSGVO) vorgeschrieben. Als personenbezogene Daten gelten alle Daten, die sich auf natürliche Personen beziehen oder die mit angemessenem Aufwand auf diese Personen beziehbar sind.

An erster Stelle sind hier Identifikatoren zu nennen, die eine natürliche Person eindeutig identifizieren können. Klassische Beispiele für Identifikatoren sind Reisepassnummern oder mobile Rufnummern. In Edge-Cloud-Anwendungen sind weitere Identifikatoren von Relevanz. Dazu gehören insbesondere Gerätekennungen, die eindeutig einer natürlichen Person zugeordnet werden können. Beispiele für solche Kennungen sind IMEI/IMSI, MAC- und Bluetooth-IDs, IP-Adressen, Kfz-Kennzeichen oder Badge-Nummern. Zudem werden in einer Reihe von Edge-Cloud-Anwendungen biometrische Identifikatoren generiert und genutzt. Solche Identifikatoren entstehen vor allem in Szenarien wie der Kameraüberwachung mit Kennzeichen- oder Gesichtserkennung, Zugangskontrollsystemen und Zeiterfassungsterminals oder Wearables.

Darüber hinaus existieren weitere Datenattribute, die nicht direkt einer Person zugeordnet werden, aber in bestimmten Kontexten und auf Basis weiterer verfügbarer Daten oder der Kombination von Datenattributen Aufschluss über eine Person geben können. Hierzu gehören beispielsweise Bearbeitungsvorgänge an Maschinen, die unter Kenntnis des Schichtplans individuellen Personen zugeordnet werden können.

Zur Arbeit mit personenbezogenen Daten, werden in Edge-Cloud-Systemen verschiedene Techniken zur Pseudonymisierung eingesetzt. Daten gelten als pseudonymisiert, wenn die mit dem Pseudonym verbundenen Attribute nicht ausreichen, um die sich dahinter verbergende Person zu identifizieren und die Pseudonymisierung nicht ohne unverhältnismäßigen Aufwand rückgängig gemacht werden kann. Werden die an der Edge pseudonymisierten Daten jedoch an zentraler Stelle, beispielsweise der Cloud, mit anderen Daten zusammengeführt, kann durch die größere Menge an Attributen eine Identifikation möglich sein. Dies ist umso wahrscheinlicher, je mehr Attribute mit einem Pseudonym verbunden werden.

In Edge-Cloud-Systemen werden häufig umfangreiche Metadaten generiert. Metadaten entstehen während der Verarbeitung, Übertragung und Speicherung von Daten zwischen Endgeräten (Edge), Zwischenknoten (Fog/Edge-Server) und der Cloud und liefern Kontextinformationen, die für die Steuerung, Auswertung und Sicherheit in Edge-Cloud-Systemen entscheidend sind. Metadaten umfassen beispielsweise den Ort der Datenerzeugung bei beweglichen Objekten wie Smartphones oder autonomen Fahrzeugen, Zeitstempel der Datenübermittlung oder Zugriffsdaten bei Datenabruf in der Cloud. Auch Metadaten können sensible Informationen enthalten.

Zuletzt sollte auch die Möglichkeit der Generierung nicht angefragter, jedoch zufällig generierter Personendaten beachtet werden. Hierunter werden personenbezogene Daten verstanden, die während der Laufzeit der Anwendung erzeugt werden, ohne dass die Aufnahme dieser Daten im Anwendungsdesign beabsichtigt wurde. Zum Beispiel können Audio- und Videoaufnahmen unbeabsichtigte sensible Inhalte aufnehmen, wenn sich Personen unbefugt oder zufällig in den Aufnahmebereichen aufhalten oder erstellte Fehlerlogs zu Maschinenzuständen von den Bedienenden mit personenbezogenen Daten befüllt werden.

Schutzbedürftige Unternehmensdaten und -informationen

Auch sensible Unternehmensdaten und -informationen sollten in Edge-Cloud-Systemen geschützt werden. Als sensibel werden alle Daten oder Informationen verstanden, deren Offenlegung wirtschaftliche, rechtliche oder strategische Schäden für die Organisation oder deren Geschäftspartner verursachen könnte. Mögliche Schäden sind unter anderem der Verlust von Umsatz, Reputationsschäden, regulatorische Strafen, die Erzeugung von Erpressbarkeit, das Pausieren von Wertschöpfungsprozessen sowie die in der Folge einer Offenlegung notwendige Untersuchung und deren Kosten.

Eine äußerst schützenswerte Kategorie stellen Daten dar, die *geistiges Eigentum* beschreiben. Zum geistigen Eigentum zählen vor allem Informationen, die sich auf die Produkte einer Unternehmung beziehen. Darunter fallen technische Dokumentationen, Konstruktionspläne oder Software-Quellcode. Zusätzlich gehören Geschäftsgeheimnisse wie Produktionsprozesse und Arbeitsweisen, Preismechanismen, Marktforschungen oder unveröffentlichte Forschungsergebnisse zu schützenswertem geistigem Eigentum. Solche Geschäftsgeheimnisse sind nach der EU-Trade-Secrets-Richtlinie und vergleichbaren internationalen Gesetzen geschützt, sofern angemessene Geheimhaltungsmaßnahmen getroffen werden. In Edge-Cloud-Anwendungen werden solche Daten unter anderem im Bereich der industriellen Produktion genutzt. Beispielsweise werden zur Zustandsüberwachung Maschinenparameter erhoben, die Aufschluss über Produktionsprozesse oder Teilegeometrien geben können.

Weiterhin stellen Daten, die Informationen zu Unternehmenskunden beinhalten, eine schützenswerte Kategorie dar. Dies betrifft nicht nur das geistige Eigentum der Kunden, sondern auch Elemente wie Vertragsdetails, Servicehistorien, Kommunikationsinhalte und Nutzungsdaten. Solche Daten werden oftmals durch bilaterale Verträge wie beispielsweise Geheimhaltungsvereinbarungen geschützt. Dritte Parteien könnten solche Daten nutzen, um wirtschaftliche Vorteile zu generieren oder mögliches Fehlverhalten der Kunden aufzudecken. Auch hier sind Daten aus Maschinen und Anlagen ein relevantes Beispiel. So könnten beispielsweise Auftragsfertiger Teilegeometrien ihrer Kundinnen und Kunden an Servicedienstleister offenlegen.

Für Unternehmen sind zudem interne Finanzinformationen sowie weitere statistische Informationen, wie beispielsweise Umsatzprognosen, Kostenstrukturen, Investitionspläne oder Daten zu Mergers & Acquisitions, von strategischer Bedeutung. Ihre Offenlegung kann zu Marktmanipulationen, Insiderhandel oder Wettbewerbsnachteilen führen. In Edge-Cloud-Systemen sind solche Daten potenziell gefährdet, wenn erfasste Produktionskennzahlen oder Energieverbrauchsdaten Rückschlüsse auf die wirtschaftliche Lage zulassen.

Nicht zuletzt existieren branchenspezifische Vorgaben, die zusätzliche Anforderungen an den Schutz von bestimmten Unternehmensdaten und -informationen stellen und deren Aggregation verbieten. Dies gilt insbesondere für kritische Infrastrukturen, die Finanzwirtschaft oder den Medizinbereich. Auch hier können existierende Richtlinien eine Relevanz für Datentransfers und Datenanalysen in Edge-Cloud-Systemen besitzen.

3.2 Spezifische Anforderungen und Risiken für den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen

Zusätzlich zu den allgemeinen Anforderungen und Risiken für den Datenschutz und die Informationssicherheit, die sich aus den Anwendungskontexten ergeben, beinhaltet die Umsetzung einer Anwendung als Edge-Cloud-System weitere, teilweise darüber hinausgehende Herausforderungen. Zum Beispiel resultieren aus der Kombination verschiedener Komponenten entlang des Edge-Cloud-Kontinuums zusätzliche Risiken für die Informationssicherheit. Andererseits trägt auch die Verteilung der Datenverarbeitung über verschiedene Partner entlang der Datenwertschöpfungskette zu besonderen Risiken und Anforderungen bei. Mögliche Risiken und Anforderungen an den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen sind in Abbildung 3 dargestellt und werden folgend erläutert.

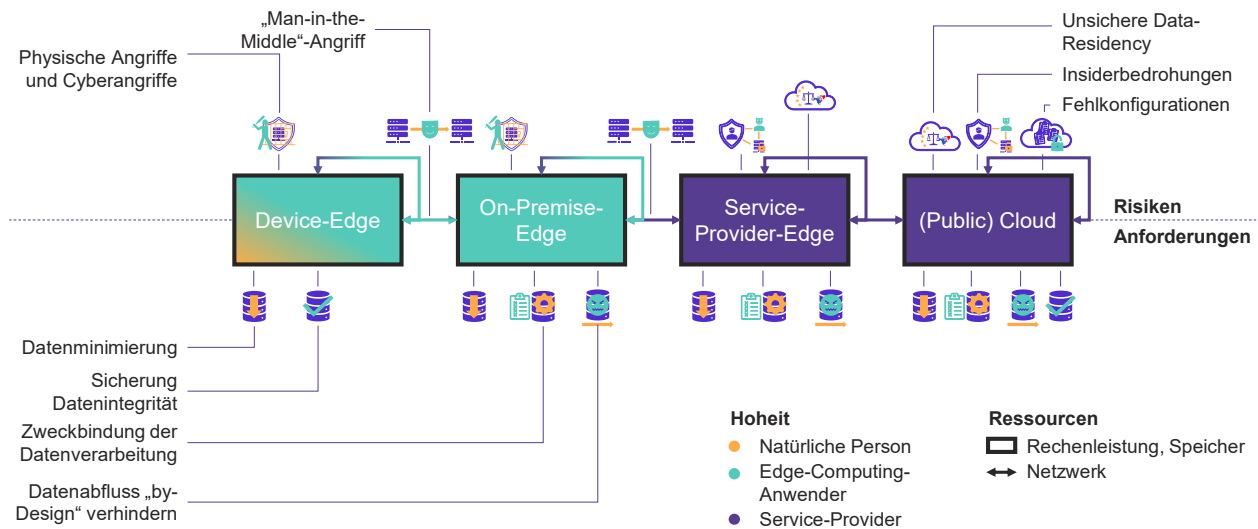


Abbildung 3: Risiken und Anforderungen für den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen

Erhöhte Angriffsfläche für physische Angriffe und Cyberangriffe

Die Betreiber großer Rechenzentren, die zumeist auch Cloud-Service-Provider im Rahmen von Co-Location-Angeboten unterstützen, etablieren umfassende Sicherheitskonzepte, die insbesondere den Zugang zu den physischen Rechenressourcen regeln und einschränken. Dort eingesetzte Mechanismen umfassen unter anderem Maßnahmen wie Zugriffskontrollen, Videoüberwachung und bauliche Schutzvorrichtungen. Mit dem Einsatz von Edge-Geräten werden Rechenressourcen dezentral an Standorten, die oft einfacher zugänglich und schwieriger überwachbar sind, platziert (Chang & Wu, 2021). Die physische Zugänglichkeit von Edge-Geräten ist entsprechend niedragschwelliger als in zentralen Rechenzentren. Durch diese eingeschränkte physische Absicherung ergeben sich verschiedene Risiken. Einerseits sind Edge-Geräte anfällig für Diebstahl und absichtliche und unbeabsichtigte Beschädigungen, beispielsweise durch Unfälle, Wetterereignisse oder Fehlbedienungen. Wird ein Edge-Knoten physisch zerstört, kann dies zu Dienstunterbrechungen führen. Weiterhin ergibt sich die Gefahr physischer Manipulationen, bei denen Angreifende die Hardware modifizieren, Schadsoftware installieren oder lokale Datenträger extrahieren und Daten auslesen können, um Zugriff auf sensible Informationen zu erhalten. Zudem können Edge-Geräte zum Einfallstor werden, wenn Angriffe auf ein Edge-Gerät auf weitere verbundene Netze ausgedehnt werden und sich die Täter lateral ausbreiten, bis kritische Systeme kompromittiert sind (Sheikh et al., 2025). Angreifende können beispielsweise Backdoors platzieren und diese dann später von außen aktivieren. Befördert werden diese Möglichkeiten durch die Situation, dass viele Edge-Geräte über keine sichere Hardware-Roots-of-Trust verfügen und selten mit manipulationssicheren Gehäusen oder „Selbsterstörungsmechanismen“ ausgerüstet sind.

Gefahr durch „Man-in-the-Middle“-Angriffe

Ein weiteres Risiko stellt die Vulnerabilität von Edge-Cloud-Systemen gegenüber Netzwerkangriffen dar. In Edge-Cloud-Systemen existieren verschiedenste Kombinationen lokaler Netzwerkkomponenten (LAN: Ethernet, WLAN, 5G-Campusnetze) und Weitverkehrsnetzen (WAN) zur Vernetzung einer Vielzahl von Geräten, Speicher- und Netzwerkkomponenten, sowie den entsprechenden Diensten in horizontaler und vertikaler Richtung. Insbesondere die lokale Ebene ist dabei anfällig für Angriffe. Ein relevantes Angriffsmuster sind sogenannte „Man-in-the-Middle“-

Angriffe. Bei einem „Man-in-the-Middle“-Angriff platzieren sich die Angreifenden zwischen zwei kommunizierenden Parteien, um Daten abzufangen, zu verändern oder zu manipulieren, ohne dass die betroffenen Parteien dies bemerken. Neben den Dateninhalten können bereits erfasste Metadaten relevante Informationen über die Nutzenden preisgeben. Durch eine Datenmanipulation kann zudem das Systemverhalten kompromittiert werden. Konkrete Risiken in Edge-Cloud-Systemen ergeben sich einerseits durch die vielen verteilten Standorte und unterschiedlichen Netzwerktypen, die die Angriffsfläche vergrößern. Zudem erhöht sich das Risiko durch den Einsatz von IoT-Geräten. Diese verfügen häufig nur über begrenzte Sicherheitsmechanismen und sind daher bei falschen Konfigurationen besonders anfällig für Angriffe (Ali & Al-Sharafi, 2025).

Herausforderungen durch unsichere Data-Residency

Die Nutzung von Cloud-Services und weiteren zentralisierten Diensten von Drittparteien im Rahmen von Edge-Cloud-Systemen bietet Unternehmen hohe Flexibilität und Skalierbarkeit sowie geringe Kosten bei der Datenverarbeitung, birgt aber auch spezifische Datenschutz- und Sicherheitsrisiken. Eines dieser Risiken ist die unsichere Data-Residency (Datenhoheit). Data-Residency umfasst die physische Lokalisierung von Daten in der Cloud und deren rechtliche Zugriffsmöglichkeiten. Gerade europäische Unternehmen müssen sicherstellen, dass personenbezogene Daten die Anforderungen der DSGVO erfüllen und nicht ohne Genehmigung in andere Jurisdiktionen übermittelt werden (European Commission, 2023). Insbesondere bei der Nutzung außereuropäischer Dienstleister muss darauf vertraut werden, dass personenbezogene oder weitere sensible Daten nur auf den vereinbarten Servern im europäischen Raum verarbeitet und gespeichert werden. Dies kann Konflikte mit Gesetzgebungen weiterer Regionen auslösen. An erster Stelle ist hier der US-amerikanische CLOUD-Act (115th Congress [2017-2018], 2018) zu nennen. Dieser erlaubt US-Strafverfolgungsbehörden Zugang zu den in den Clouds USA-ansässiger Dienstleister gespeicherten Daten, auch wenn diese (beispielsweise von Nicht-US-Tochtergesellschaften) in Europa verarbeitet werden. Ein Zugriff ist beispielsweise zu Zwecken der Strafverfolgung oder auch bei Bedenken der nationalen Sicherheit möglich. Daher treiben diese Anbieter derzeit neue, auf Souveränität ausgelegte Angebote in Europa voran. Eine Datenweitergabe auf juristischen Druck kann jedoch auch bei Nutzung dieser Angebote nicht ausgeschlossen werden.

Gefahr durch Insiderbedrohungen

Ein weiteres Risiko auf Seiten der Cloud-Services-Provider oder anderer Drittparteien sind Insiderbedrohungen (Chang & Wu, 2021). Unter Insidern werden Personen verstanden, die eine Position innerhalb eines Serviceanbieters innehalten oder innehatten. Dies können entweder interne Mitarbeitende oder Dienstleister sein, die durch ihren Insider-Status rechtmäßigen Zugriff auf sensible und kritische Daten haben. Solche Personen sind in der Lage, beabsichtigt oder unbeabsichtigt auf sensible Daten beziehungsweise Informationen zuzugreifen und diese zu manipulieren. Oftmals existieren für solche Vorgänge keine direkten Erkennungsmechanismen.

Erhöhtes Risiko für Fehlkonfigurationen

Nicht zuletzt sind auch Fehlkonfigurationen eine relevante Ursache für Datenlecks in der Cloud. Fehlkonfigurationen können sowohl den gesamten Cloud-Mandanten, d.h., das gesamte Kundenkonto, als auch einzelne Cloud-Dienste, wie Analyse- oder Speicherdienste, betreffen. Zu den

bekanntesten Fehlkonfigurationen zählen falsch gesetzte Zugriffsrechte, offen zugängliche Speicherservices oder unzureichend gesicherte Secrets (digitale Zugangsdaten für nicht-menschliche Benutzer) und Benutzerkonten. In bisher bekannten Vorfällen wurden unter anderem personenbezogene Daten, Finanzinformationen oder Gesundheitsdaten öffentlich zugänglich gemacht (Chang & Wu, 2021). Beispielsweise legte Verizon Daten von ca. 6 Millionen Kunden in einen öffentlichen AWS-S3-Speicher¹, während Decathlon etwa 9 GB Daten, darunter sensible Personendaten, durch einen falsch konfigurierten ElasticSearch-Server² preisgab. Während die betroffenen Unternehmen diese Situationen zumeist als das Fehlverhalten einzelner Mitarbeitender beschreiben, erhöhen die Komplexität moderner Cloud-Plattformen und das Fehlen einheitlicher, durchgängiger Konfigurationsstandards generell das Risiko für entsprechende Vorfälle.

Neben den spezifischen, für Edge-Cloud-Systeme relevanten Datenschutzrisiken äußern Organisationen zudem allgemeine Anforderungen an ihre Informationssicherheit, die sich aus den rechtlichen, geschäftlichen und gesellschaftlichen Rahmenbedingungen sowie aus den individuellen Eigenschaften des Geschäftsmodells und der zugrundeliegenden Architektur ergeben können.

Anforderung der Minimierung von Daten und Informationen

Die Datenminimierung ist ein Grundsatz für die Verarbeitung personenbezogener Daten, der einerseits in der DSGVO (Art. 5) als grundlegendes Prinzip formuliert wird. Andererseits kann sich eine Minimierung auch auf die Verarbeitung von unternehmensbezogenen Informationen beziehen. Datenminimierung bedeutet generell, nur solche Daten zu erheben, zu verarbeiten und zu teilen, die für den Zweck der Anwendung angemessen und tatsächlich notwendig sind (ISACA, 2024). In Edge-Cloud-Systemen gewinnt dieses Prinzip an Bedeutung, da Daten üblicherweise verteilt erhoben und verarbeitet werden und ein Transfer von Daten über verschiedene Knoten entlang des Edge-Cloud-Kontinuums notwendig ist. Neben der Einhaltung regulatorischer Konformität sorgt Datenminimierung für eine Reduktion der Angriffsfläche, da im Falle von Sicherheitsvorfällen weniger Informationen offengelegt werden können. Weiterhin wird der Umfang möglicher Zweckentfremdung durch Partner entlang der Datenverarbeitungskette reduziert. Entsprechend kann nach einer durchgeführten Minimierung der Daten auch die Verarbeitung durch weniger vertrauenswürdige Drittparteien möglich sein. Ein positiver Nebeneffekt von Datenminimierung ist zudem, dass sie die technische Komplexität durch Verringerung des Speicherbedarfs oder der Netzwerklast reduziert und somit Energie einsparen kann. Schlussendlich kann die Minimierung von Daten und Informationen nicht nur eine Anforderung der betroffenen Personen oder datengebenden Organisationen sein, sondern auch der Datenverarbeiter, um eine einfachere Verarbeitung zu ermöglichen. Beispielsweise können so notwendige Schutzmaßnahmen reduziert werden.

Bedarf zur Sicherung der Daten- und Informationsintegrität

Auch die Sicherstellung von Integrität und Vertraulichkeit ist ein in der DSGVO formulierter Grundsatz zur Verarbeitung personenbezogener Daten. Datenintegrität bezeichnet die durchgehende

¹ <https://www.cbsnews.com/philadelphia/news/verizon-data-leaked-online/>

² <https://www.computerweekly.com/news/252479101/Sports-retailer-Decathlon-left-employee-data-exposed>

Genauigkeit, Vollständigkeit und Qualität von Daten entlang der gesamten Datenverarbeitungskette. Für die Verarbeitung personenbezogener Daten ist Datenintegrität ein wichtiges Kriterium. Wenn Daten die Merkmale einer natürlichen Person nicht korrekt widerspiegeln, können sich daraus erhebliche Nachteile für diese Personen ergeben. Beispiele hierfür sind unangemessene Behandlungen bei falschen Gesundheitsdaten oder monetäre Nachteile bei der Berechnung der Kreditwürdigkeit. Integrität ist auch bei der Weitergabe von unternehmensbezogenen Informationen wichtig, beispielsweise wenn auf IoT-Daten basierend Abrechnungen in Subskriptionsmodellen erfolgen sollen oder Aufträge basierend auf Verfügbarkeiten und Kosten von Ressourcen verteilt werden. In Edge-Cloud-Systemen spielt die Integrität von Informationen eine besondere Rolle, da Daten zum einen von Sensoren und Aktoren direkt aus der Umwelt aufgenommen werden und andererseits über eine Reihe von Partnern hinweg verarbeitet werden (Adam et al., 2024). Für autonom agierende Objekte und Systeme muss daher sichergestellt werden, dass diese wie erwartet agieren. Bei der Verarbeitung von Daten über Partner hinweg muss zudem oftmals prüfbar sein, dass Daten während der Verarbeitung oder des Transfers nicht manipuliert wurden. Wie die Datenminimierung ist auch die Datenintegrität oftmals eine Anforderung von betroffenen Personen, datengebenden Organisationen und Datenverarbeitern.

Notwendigkeit der Zweckbindung der Datenverarbeitung und Informationsnutzung

Unter der Zweckbindung der Datenverarbeitung wird verstanden, dass Daten ausschließlich für den festgelegten und legitimen Zweck erhoben und weiterverarbeitet werden dürfen (ISACA, 2024). Die Zweckbindung ist ebenfalls ein Prinzip, das in der DSGVO formuliert wird. Zentraler Inhalt ist, dass personenbezogene Daten nicht mit einer mit dem Zweck nicht zu vereinbarenden Art und Weise verarbeitet werden dürfen. Auch für schützenswerte unternehmensbezogene Informationen muss sichergestellt werden, dass diese von den Datenverarbeitern ausschließlich für die vereinbarten Zwecke genutzt werden. Für Daten mit Personenbezug ist dies entscheidend, da Daten ansonsten für oftmals problematische Zwecke verwendet werden könnten. Beispielsweise könnten Gesundheitsdaten für Versicherungsrisikobewertungen oder Marketingzwecke missbraucht werden. Für die Verarbeitung sensibler Informationen ist die Zweckbindung unter anderem wichtig, um Geschäftsgeheimnisse zu schützen und Wettbewerbsnachteile zu vermeiden. So könnten beispielsweise Auftrags- und Auslastungsdaten, die eigentlich zur Optimierung der Lieferkette gedacht sind, im Zuge von Preisverhandlungen als unfairer Wettbewerbsnachteil verwendet werden. Beispiele für die Notwendigkeit einer Zweckbindung der Datenverarbeitung im Rahmen von Edge-Cloud-Anwendungen sind Dienste, die personenbezogene Fahrzeugdaten aufnehmen und diese nicht für Versicherungsdienste verfügbar machen sollten, oder „Pay-per-Use“-Geschäftsmodelle, in denen an der Edge aufgenommene Verbrauchsdaten ausschließlich für Abrechnungszwecke genutzt werden sollen. Herkömmlich wird die Zweckbindung der Datenverarbeitung über organisatorische und vertragliche Konzepte wie Datenklassifizierungen, Berechtigungen und Speicherfristen gelöst. Solche Gestaltungsmaßnahmen stehen in engem Zusammenhang mit dem Begriff der Datensouveränität, also der Fähigkeit der datengebenden Organisationen, über die Nutzung der Daten und Informationen während des gesamten Verarbeitungsprozesses, einschließlich der Nutzung durch Drittparteien, zu entscheiden (Scherenberg et al., 2024).

Bedürfnis, Datenabflüsse „by-Design“ zu verhindern

Oftmals genügen Datennutzungsverträge und ergänzende organisatorische Maßnahmen, um datengebende Organisationen und betroffene Personen davon zu überzeugen, dass die Zweckbindung der Datenverarbeitung eingehalten wird. Wenn jedoch nur geringes Vertrauen in die datenverarbeitende Partei besteht oder diese starke Anreize hätte, die erhaltenen Daten für weitere Zwecke zu verwenden, reichen solche Maßnahmen nicht aus. Stattdessen besitzen die datengebenden Organisationen die Anforderung, Datenabflüsse und Informationsnutzung für nicht definierte Zwecke bereits durch die Anwendungsarchitektur zu verhindern. Entsprechende Maßnahmen des „Privacy-by-Design“ stellen auf technischem Weg sicher, dass Daten nur vordefinierte Wege nehmen können (Schiffner, 2015a). Die Implementierung solcher technischen Gestaltungsmechanismen ist insbesondere in Edge-Cloud-Systemen sinnvoll, in denen ein höherer Gestaltungsspielraum hinsichtlich des Orts der Datenverarbeitung, der Auswahl der Komponenten und Partner und der zu erhebenden und verarbeitenden Daten existiert. Beispielsweise kann ein hoher Anteil der Daten bereits lokal, d. h. in der Kontrollumgebung der betroffenen Personen oder datengebenden Organisationen verarbeitet werden. Sofern Datenabflüsse „by-Design“ verhindert werden können, ergeben sich höhere Erfolgchancen bei der Umsetzung von Anwendungen, die auf kritische Daten externer Parteien zurückgreifen.

4 Der Lösungsraum – PET-Werkzeuge zur Umsetzung von Datenschutz und Informationssicherheit in Edge-Cloud-Anwendungen

Ausgehend von den in Abschnitt 3 (Problemraum) dargestellten Anforderungen und Risiken für den Datenschutz und die Informationssicherheit in Edge-Cloud-Anwendungen unterstützt dieser Abschnitt den Entwurf Privacy-Enhancing-Technology (PET)-basierter Lösungsansätze, um diesen Herausforderungen zu begegnen. Der Abschnitt gibt zunächst eine Übersicht über generell mögliche PET-Werkzeuge, um Datenschutz und Informationssicherheit technisch umzusetzen (Abschnitt 4.1). Danach werden existierende, allgemeine Lösungshilfen vorgestellt, die die Anforderungsanalyse und das Systemdesign, die Pilotierung und Umsetzung sowie die Evaluierung und Tests von PET-Werkzeugen in realen Anwendungsszenarien unterstützen (Abschnitt 4.2). Anschließend zeigt dieser Abschnitt praktische Anwendungsszenarien des Einsatzes von PET-Werkzeugen auf, um die Anforderungen an den Datenschutz und die Informationssicherheit in Edge-Cloud-Anwendungen verschiedener Industriezweige zu erfüllen (Abschnitt 4.3). Die präsentierten Strategien basieren auf den Praxiserkenntnissen der Arbeiten im Rahmen von Förderprojekten des BMFTR-Technologieprogramms „Edge Datenwirtschaft“. Die PET-Strategien werden in ihrem jeweiligen Anwendungskontext dargestellt und deren spezifische Umsetzungsbedingungen und Implikationen aus der Sicht der Early-Adopter beschrieben. Sie geben somit Aufschluss darüber, wie PET im Praxiskontext von Edge-Cloud-Systemen eingesetzt werden können und welche Rahmenbedingungen dabei zu beachten sind. So liefern sie wertvolle Informationen für Unternehmen bei der Entwicklung eigener PET-Strategien.

4.1 PET-Werkzeuge

Zur technischen Gewährleistung des Schutzes von Daten und Informationen im Allgemeinen sowie zur Realisierung der spezifischen Anforderungen in Edge-Cloud-Systemen ist potenziell der Einsatz verschiedener PET denkbar. Abbildung 4 zeigt die derzeit überwiegend eingesetzten PET, geordnet nach dem Vertrauensaspekt, über den Datenschutz und Informationssicherheit erzeugt werden, sowie dem typischen Verwendungsbereich der PET entlang des Datenlebenszyklus. Die Typen von PET-Werkzeugen werden im Folgenden kurz dargestellt. Eine ausführlichere Erläuterung der gelisteten PET findet sich im Anhang zu dieser Studie.

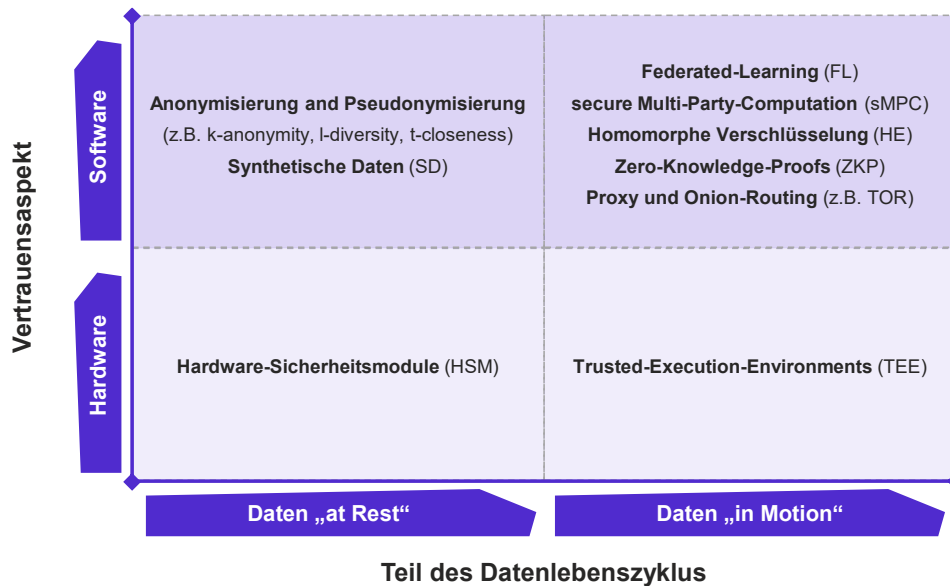


Abbildung 4: Übersicht populärer PET

Anonymisierung und Pseudonymisierung

Mittels einer Anonymisierung werden Attribute aus Datensätzen entfernt oder generalisiert, um eine Identifizierung zu verhindern und die Ununterscheidbarkeit von Entitäten herzustellen. Effektiv anonymisierte Daten gelten nicht mehr als personenbezogen. Typische Ansätze der Pseudonymisierung sind k-Anonymität, l-Diversität und t-Nähe. Bei der Pseudonymisierung werden beispielsweise Identifikatoren in Datensätzen durch Pseudonyme ersetzt. Durch die Möglichkeit zur Re-Identifikation gelten pseudonymisierte Daten weiterhin als personenbezogen. Beide Ansätze werden meist auf Daten „at-Rest“ angewendet.

Synthetische Daten

Synthetische Daten sind maschinell generierte Daten, die die statistischen Eigenschaften der Grundgesamtheit nachahmen und die Privatsphäre der Datenerzeuger wahren. Dafür werden heute vermehrt Machine-Learning-Verfahren eingesetzt, die die zugrunde liegende Verteilung lernen und daraus neue Daten erzeugen. Synthetische Daten können vollständig synthetisch (alle Variablen werden durch ein Modell generiert), teilweise synthetisch (nur einige Variablen werden synthetisiert) oder hybrid (aus dem realen Satz und einem vollständig synthetischen Satz generiert) sein.

Federated-Learning

Federated-Learning ist ein kollaborativer Ansatz des maschinellen Lernens. Ein globales KI-Modell wird initial durch einen zentralen Server bereitgestellt und auf verschiedene Knoten/Clients (z.B. Server, Edge-Geräte, Smartphones) verteilt. Diese trainieren das Modell lokal mit eigenen Daten und übertragen lediglich aktualisierte Modellparameter an den zentralen Server. Der Server aggregiert diese Werte, aktualisiert das globale Modell und gibt das aktuelle globale Modell an die Clients zurück.

Secure Multi-Party-Computation

Secure Multi-Party-Computation ist ein kryptografischer Ansatz, der es mehreren, sich gegenseitig misstrauenden Parteien ermöglicht, gemeinsam Berechnungen durchzuführen, ohne dabei ihre jeweiligen Eingabedaten offenzulegen. Zur Umsetzung von Secure Multi-Party-Computation werden die Inputs der Beteiligten zerlegt und auf die anderen Parteien verteilt, sodass keine Partei allein auf alle Informationen zurückgreifen kann. Die Parteien führen anschließend ihre individuellen Berechnungen durch und fügen das Berechnungsergebnis am Ende zusammen. Das Verfahren benötigt eine Mindestanzahl an teilnehmenden Parteien. Weitere derzeitige Herausforderungen sind die niedrige Performance und die Beschränkung auf dedizierte Rechenverfahren.

Homomorphe Verschlüsselung

Homomorphe Verschlüsselung ist ein kryptografisches Verfahren, das die Durchführung von Berechnungen auf verschlüsselten Daten erlaubt, ohne diese entschlüsseln zu müssen. Die vollständige homomorphe Verschlüsselung ermöglicht die Ausführung beliebiger mathematischer Operationen direkt auf dem Verschlüsselungstext. Nach Abschluss der Berechnungen kann das verschlüsselte Ergebnis entschlüsselt werden, um das reale Ergebnis zu erhalten. Homomorphe Verschlüsselung lässt sich insbesondere für Berechnungen nutzen, die sich als Polynomfunktionen ausdrücken lassen, sowie für ausgewählte KI-Anwendungen. Zu den derzeitigen Einschränkungen gehören ein erhöhter Rechenaufwand und Berechnungsungenauigkeiten (Stock et al., 2022).

Zero-Knowledge-Proofs

Zero-Knowledge-Proofs sind ein kryptografisches Konzept, das es einer Partei (Prover) ermöglicht, einer anderen Partei (Verifier) die Gültigkeit einer Aussage zu beweisen, ohne die zugrundeliegenden Daten bereitstellen zu müssen. Zur Erstellung von Zero-Knowledge-Proofs existieren interaktive Verfahren, die mehrfache Kommunikation zwischen Prover und Verifier erfordern, sowie nicht-interaktive Verfahren, bei denen ein einmaliger Beweis erbracht werden kann (Lavin et al., 2024). Etablierte Einsatzbereiche von Zero-Knowledge-Proofs sind insbesondere das Identitätsmanagement und die Finanzwirtschaft.

Proxys und Onion-Routing

Proxy-Server und Onion-Router steuern Anfragen und Kommunikation zwischen verschiedenen Parteien. Ein Proxy-Server vermittelt zwischen Client und Zielsystem, leitet Anfragen weiter und Antworten zurück und kann dabei die Identität der Quelle (z. B. IP-Adresse) verschleiern. Für den Privatsphärenschutz sind vor allem anonyme Proxys und hoch-anonyme Proxys relevant. Anonyme Proxys verbergen die IP-Adresse der Nutzenden, während hoch-anonyme Proxys darüber hinausgehend verschleiern, dass sie selbst als Proxy fungieren.

Onion-Routing ist eine Netzwerktechnik, die bidirektionale Kommunikation über eine Kette von Relays (Onion-Router) leitet, um Absender und Ziel voneinander zu entkoppeln. Ziel ist es, sowohl den Inhalt der Kommunikation als auch die Kommunikationspartner vor Überwachung zu schützen. Die Nachrichten werden dazu vom Client schichtweise verschlüsselt, analog zu den Schalen einer Zwiebel. Jeder Onion-Router in der Verbindungskette entfernt ausschließlich seine eigene Schicht und leitet die Nachricht entsprechend weiter. Ein einzelner Onion-Router kennt

somit nur den unmittelbaren Vorgänger und den Nachfolger und hat weder Zugriff auf die vollständigen Inhalte noch auf die gesamte Route.

Hardware-Sicherheitsmodule

Hardware-Sicherheitsmodule generieren, speichern und verwalten kryptografische Schlüssel in manipulationssicherer Hardware und bieten Funktionen für die Verschlüsselung und Entschlüsselung von Daten und die Erzeugung von digitalen Signaturen. Sie leisten somit einen Beitrag, um geistiges Eigentum und sensible Daten vor unerlaubten Zugriffen zu schützen. Die Schlüssel entstehen und verbleiben im Kryptoprozessor, Zugriffe auf diese Schlüssel erfolgen über definierte APIs, und physische Angriffe werden verhindert oder durch Löschung sensibler Daten abgewehrt. Hardware-Sicherheitsmodule werden vor allem in Bereichen mit hohen Compliance-Anforderungen eingesetzt und oftmals mit anderen PET kombiniert.

Trusted-Execution-Environments

Trusted-Execution-Environments sind Hardware-Architekturen, die es ermöglichen, Anwendungen isoliert vom restlichen System auszuführen. Dazu nutzen sie spezialisierte CPU-Lösungen, die verhindern, dass auf den Speicherbereich zugegriffen werden kann. Sie schaffen eine vertrauenswürdige Bearbeitungsumgebung, in der Daten und Prozesse vor unautorisiertem Zugriff, Manipulation oder Überwachung geschützt sind, selbst wenn der Host oder das zugrunde liegende Betriebssystem kompromittiert wurden. Auch Betreiber der Umgebungen können die Daten nicht einsehen. Mittels Remote-Attestation können Nutzende zudem die Integrität und Authentizität des Codes und der Daten überprüfen.

4.2 PET-Lösungshilfen

Derzeit existiert bereits eine Reihe von Publikationen, die Praktiker bei der Auswahl, Gestaltung und Umsetzung von PET zur Sicherung von Datenschutz und Informationssicherheit, unabhängig vom Anwendungskontext, unterstützen können. Eine Übersicht dieser im Folgenden als Lösungshilfen bezeichneten Ressourcen ist in Tabelle 3 dargestellt. Konkret geben die Publikationen Handreichungen, die in den Bereichen Anforderungsanalyse und Systemgestaltung („Wann kann welche PET wie unterstützen?“), Pilotierung und Umsetzung („Wie kann eine PET-Anwendung implementiert werden?“) und der Evaluierung von PET („Anhand welcher Kriterien kann eine PET bewertet werden?“) wertvolle Unterstützung leisten können.

Eine Handvoll Lösungshilfen gibt einen ausführlichen Überblick über einzelne PET, die über die Beschreibungen im vorangegangenen Abschnitt hinausgehen. Diese Übersichten stehen dabei in verschiedenen Kontexten wie etwa Privacy-by-Design, Data Protection Engineering oder der Erfüllung existierender Datenschutzvorschriften. Darüber hinausgehend zeigt ENISA (2022), welche weiteren Technologien gewinnbringend eingesetzt werden können, um PET-Anwendungen zu realisieren. Das Centre for Data Ethics and Innovation (2021) liefert zudem einen Entscheidungsbaum, mit dem passende PET für allgemeine Schutzbedarfe identifiziert werden können.

Hilfestellungen bei der Pilotierung und Umsetzung von PET werden vor allem mittels der Darstellung von PET-Anwendungsfällen geleistet. Beispiele hierfür sind die Arbeiten des Centre for Data Ethics and Innovation (2021), der United Nations (2023) sowie von Noble (2023), wobei letztere auf den Einsatz von PET für Behörden beziehungsweise im öffentlichen Sektor fokussieren.

Noble (2023) gibt zudem eine Übersicht über relevante Standards im Kontext der PET-Umsetzung.

Für die Evaluierung und das Testen von PET-Werkzeugen präsentiert das Future of Privacy Forum (2024) eine Zusammenfassung existierender Testumgebungen. Noble (2023) gibt im Rahmen der Darstellung von PET-Anwendungen Hinweise auf einzelne Evaluierungsaspekte von PET. Zur Entwicklung eines eigenen Kriterienkatalogs zur Analyse von PET-Technologien formuliert ENISA (2016) ein Rahmenwerk, das verschiedenste Kriterien und Indikatoren beinhaltet.

Lösungshilfe	Inhalt	Anforderungs- analyse und Systemdesign	Pilotierung und Umsetzung	Evaluierung und Tests
Klymenko et al. (2025)	Detaillierte Übersicht zu PET; Handlungsempfehlungen zum Umsetzen von Privacy-By-Design	x		
OECD (2023)	Übersicht zu PET sortiert nach ihrem Einsatzzweck (Datenverschleierung, verschlüsselte Datenverarbeitung, föderierte Analysen, Tools zur Datenkontrolle)	x		
ENISA (2022)	Übersicht zu PET im Kontext des „Data-Protection-Engineering“; Erläuterung ergänzender Technologien zur technischen Umsetzung von Datenschutz	x		
ISACA (2024)	Übersicht zu PETs mit Fokus auf Standards und die Erfüllung von regulatorischen Datenschutzvorschriften	x		
Centre for Data Ethics and Innovation (2021)	Entscheidungsbaum zur Auswahl passender PET; Übersicht über PET-Use Cases	x	x	
United Nations (2023)	Übersicht zu PET; PET-Use Cases für behördliche Zwecke	x	x	
Future of Privacy Forum (2024)	Übersicht zu regulatorischen Aktivitäten, Studien und Testumgebungen mit Bezug zu PET	x	x	x
Noble (2023)	Übersicht zu PET und deren Gegenüberstellung; Übersicht über Standards mit Bezug zu PET; PET-Use-Cases im öffentlichen Sektor	x	x	x
ENISA (2016)	Rahmenwerk zur Analyse von PET basierend auf verschiedenen Kriterien und Indikatoren			x

Tabelle 3: Übersicht der Lösungshilfen für die Entwicklung von PET-gestützten Anwendungen

4.3 Beispiele für den Einsatz von PET-Werkzeugen in Edge-Cloud-Anwendungen

Über die zuvor präsentierten allgemeinen Lösungshilfen hinausgehend analysiert dieser Abschnitt PET-Werkzeuge in verschiedenen Anwendungskontexten, um die in Abschnitt 3 beschriebenen Risiken für den Datenschutz und die Informationssicherheit in Edge-Cloud-Systemen zu minimieren und den damit verbundenen Anforderungen der betroffenen Personen und datenbereitstellenden Organisationen gerecht zu werden. Die hier vorgestellten Erkenntnisse basieren auf Forschungs- und Entwicklungsarbeiten, die im Rahmen von Förderprojekten des BMFTR-Technologieprogramms „Edge Datenwirtschaft“ durchgeführt wurden und den dort vorhandenen

Lösungsraum abdecken. Die vorgestellten PET-Werkzeuge umfassen neben der eigentlichen technischen Implementierung der PET auch die Integration der Technologie in den Anwendungskontext mitsamt der verbundenen organisatorisch-strukturellen und kulturellen Konsequenzen. Die PET-Werkzeuge werden in ihrem praktischen Anwendungskontext präsentiert und durch die Early-Adopter der Technologie in diesem Kontext evaluiert. Tabelle 4 stellt die in diesem Abschnitt präsentierten PET-Lösungsstrategien mit den durch diese adressierten Anforderungen und Risiken für den Datenschutz und die Informationssicherheit gegenüber.

Vorrangig adressierte Anforderungen und Risiken für den Datenschutz und die Informationssicherheit	PET-Werkzeug	Beispielhafter Anwendungsbereich im Programm Edge Datenwirtschaft
Datenminimierung, Physische und Cyberangriffe	Hardware-Schlüssel (4.1)	Lebensmittelwirtschaft
Datenminimierung, Physische und Cyberangriffe	Federated-Learning (4.2)	Industrielle Fertigung
Zweckbindung, Datenabfluss „by-Design“ verhindern, Unsichere Data-Residency, Insiderbedrohungen, Fehlkonfigurationen	Compute-to-Data (4.3)	Industrielle Fertigung
Datenminimierung, Datenintegrität	Zero-Knowledge-Proofs (4.4)	Energiewirtschaft
Zweckbindung, Datenintegrität, Datenabfluss „by-Design“ verhindern, Insiderbedrohungen	Trusted-Execution-Environments (4.5)	Energiewirtschaft

Tabelle 4: PET-Werkzeuge und adressierte Anforderungen und Risiken für den Datenschutz

Die Beschreibung der einzelnen PET-Werkzeuge in den folgenden Abschnitten erfolgt nach einem einheitlichen Schema. Zunächst wird das PET-Werkzeug und seine Motivation im Rahmen des konkreten Einsatzbereichs dargestellt. Konkret werden die Herausforderungen für den Datenschutz und die Informationssicherheit sowie weitere Anforderungen erläutert, die sich aus den Anliegen der Stakeholder im Anwendungskontext ergeben. Darüber hinaus wird die technische Funktionsweise des PET-Werkzeugs dargelegt und die für die Umsetzung der PET im Anwendungskontext erforderlichen Rollen beschrieben. Anschließend werden die für den jeweiligen Kontext notwendigen Umsetzungsvoraussetzungen des PET-Werkzeugs betrachtet und der Aufwand zur Leistung dieser Umsetzungsvoraussetzungen im individuellen Kontext aus Sicht der Praktikerinnen und Praktiker bewertet³. Die Umsetzungsvoraussetzungen gliedern sich in folgende Kategorien:

- *Organisatorische Voraussetzungen* umfassen beispielsweise den Aufbau der Organisationsstrukturen, die Schaffung von Anreizen, die Festlegung von Rollen und Verantwortlichkeiten und die Etablierung von Partnerschaften.
- *Technische Voraussetzungen* umfassen beispielsweise die technische Spezifizierung oder den Aufbau, die Integration und die Wartung der Gesamtlösung in Bezug auf die verwendete Hardware und Software.

³ Die Bewertung durch die Early-Adopter erfolgte auf Basis einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“. Die Bewertung gibt ausschließlich einen Eindruck über die relative Komplexität der Umsetzungsvoraussetzungen je Anwendungskontext aus Sicht der Anwender und kann nicht über die vorgestellten Anwendungen hinweg generalisiert werden.

- *Voraussetzungen an Kompetenzen und Verständnis* umfassen beispielsweise die Schaffung des Wissens über das PET-Werkzeug oder die Herstellung von Vertrauen in die eingesetzte Technologie.
- *Voraussetzungen für den Betrieb und die Integration* umfassen beispielsweise die Anpassung laufender Prozesse oder die Herstellung von Kompatibilität mit existierenden Protokollen und Diensten.
- *Rechtliche Voraussetzungen* umfassen beispielsweise die rechtliche Sicherstellung des Technologieeinsatzes im Anwendungskontext und dessen angemessene Dokumentation.

Abschließend werden die beabsichtigten und unbeabsichtigten Implikationen, die durch den Einsatz der PET in ihrem Anwendungskontext hervorgerufen werden, analysiert. Implikationen können sich beispielsweise im Hinblick auf die zukünftige Zusammenarbeit verschiedener Rollen, die langfristigen Kosten und Aufwände oder den Ressourcenverbrauch ergeben. *Befähiger* werden in diesem Kontext als positive Implikationen verstanden, die einen Einsatz der PET zusätzlich motivieren können. Als *Beschränker* werden Implikationen bezeichnet, die einer breiten Adoption der Technologie entgegenstehen könnten.

4.3.1 Hardware-Schlüssel im Kontext der Qualitätskontrolle in der Lebensmittelwirtschaft

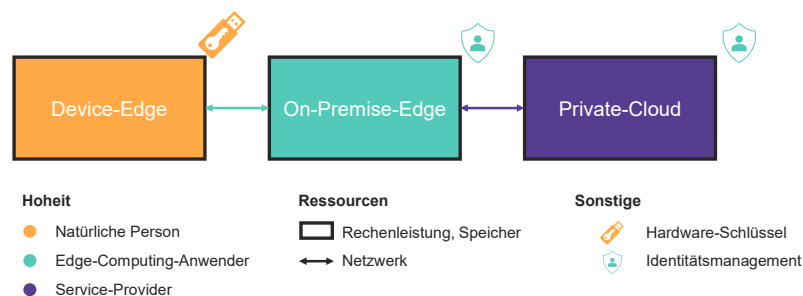


Abbildung 5: Schematische Darstellung – Hardware-Schlüssel in der Lebensmittelwirtschaft

In Edge-Cloud-Systemen dienen Hardware-Schlüssel dazu, eine sichere Authentifizierung von Anwendenden der Edge-Geräte zu erreichen, ohne personenbezogene Daten, die sich bei üblichen Anmeldeverfahren mittels Benutzername und Passwort ergeben, aufnehmen zu müssen. Hardware-Schlüssel sind eine Form von Hardware-Sicherheitsmodulen. In der konkreten Anwendung (s. Abbildung 5) nutzen Qualitätsprüfende einer beauftragten Dienstleistungsfirma Edge-Computing-basierte Scanner-Systeme (Device-Edge) zur Prüfung der Qualität von Obst und Gemüse eines Lebensmittelunternehmens an bestimmten Stationen der Lebensmittellieferkette, beispielsweise nach der Ernte in der Lebensmittelabpackung. Anschließend werden die Qualitätsdaten zur langfristigen Dokumentation an Softwaresysteme des Lebensmittelunternehmens übertragen. Die Softwaresysteme werden entweder in der Private-Cloud oder On-Premise-Edge bereitgestellt. Die erhobenen Daten können von dort aus weiteren Berechtigten entlang der Lieferkette zur Verfügung gestellt werden. Der Schutz von Personendaten wird dabei insbesondere vom Lebensmittelunternehmen gefordert, um ein möglichst einfaches Datenhandling zu ermöglichen. In der beschriebenen Anwendung der Lebensmittelwirtschaft ist es weiterhin wichtig, dass die Beschäftigten des Dienstleisters einfach in die Authentifizierungsmethode eingebunden werden können. Zudem sollten die Authentifizierungsmethode in das existierende Identitätsmanagementsystem des Lebensmittelherstellers integrierbar sein und die Authentifizierungsaufwände für

die Nutzenden niedrig bleiben. Weiterhin sollte die Authentifizierung auch in Bereichen mit beschränktem Netzwerkzugriff, wie er in der Landwirtschaft häufig vorkommt, funktionieren.

Zur konkreten Umsetzung werden zunächst die entsprechenden Hardware-Schlüssel durch die Administratoren eingerichtet. Zur Integration von Server und Hardware-Schlüssel wird der Standard WebAuthn⁴ verwendet. Durch ein kryptografisches Verfahren (Challenge-Response-Verfahren) wird sichergestellt, dass der Schlüssel eindeutig zugeordnet werden kann und die Anmelde-daten nicht vom Hardware-Schlüssel auslesbar und damit auch nicht für Dritte zugänglich sind. Mit dem Schlüssel kann fortan eine robuste Zugriffssteuerung auf unterschiedlichen Ebenen, von der Device-Edge über On-Premise-Edge bis zur Cloud, ohne personenbezogene Daten durchgeführt werden. Diese Hardware-Schlüssel werden anschließend an den Dienstleister gegeben, der diese den entsprechenden Mitarbeitenden bereitstellt. Die Mitarbeitenden nutzen den Hardware-Schlüssel anschließend, um sich mit dem Scanner-System am damit verbundenen Qualitätsmanagementsystem über eine Weboberfläche zu authentifizieren. Das Qualitätsmanagementsystem kann dabei, je nach Rahmenbedingungen, an der Edge, in der Cloud oder verteilt betrieben werden.

Umsetzungsvoraussetzungen

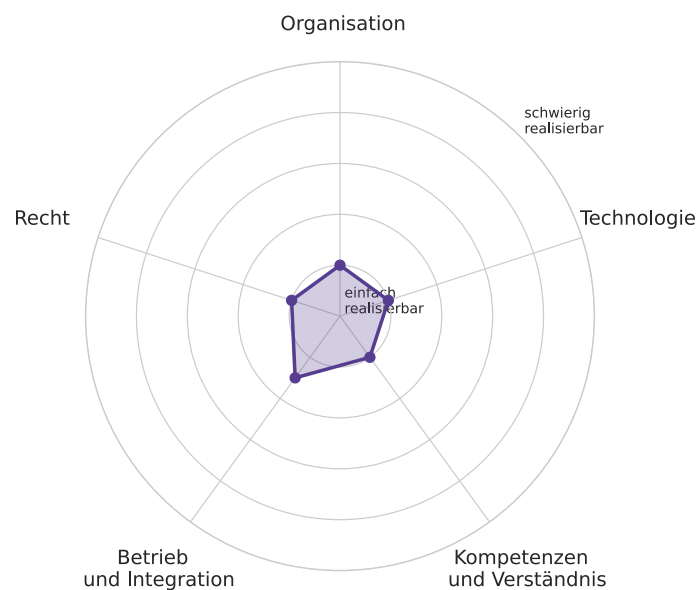


Abbildung 6: Evaluierung der Umsetzungsvoraussetzungen – Hardware-Schlüssel in der Lebensmittelwirtschaft | Subjektive Bewertung der relativen Komplexität der Umsetzungsvoraussetzungen durch die Early-Adopter der PET im gegebenen Anwendungsfall anhand einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“

Grundsätzlich lässt sich eine privatsphäreschonende Authentifizierung mittels Hardware-Schlüsseln gemäß der Einschätzungen der Early-Adopter einfach realisieren (s. Abbildung 6). Aus organisatorischer Sicht bedarf es dazu klarer Prozesse, insbesondere im Hinblick auf die Verwaltung und Zuordnung der Schlüssel, die Einrichtung eines Autorisierungssystems sowie die Regelung des Umgangs und der Nutzung der Schlüssel. Diese sind jedoch vergleichbar mit dem herkömmlichen Schlüsselmanagement in Unternehmen. Aus technischer Perspektive ergeben sich zwei Sichtweisen hinsichtlich der Umsetzungskomplexität. Aus theoretischer Sicht weist ein

⁴ <https://www.w3.org/TR/webauthn-3/>

solches System aufgrund der umfangreichen Kryptografie eine hohe Komplexität auf. Aus praktischer Sicht können Anwendende und Systemintegratoren jedoch auf etablierte Frameworks, Softwarebibliotheken und Hardware zurückgreifen, die die technologische Komplexität abstrahieren und somit die technische Umsetzung stark vereinfachen.

Ein Kernaspekt ist die Integration des Systems in existierende Prozesse. Die Komplexität dieser Integration ist laut der Early-Adopter maßgeblich vom bestehenden Digitalisierungsgrad der jeweiligen Prozesse abhängig. In Umgebungen, in denen bereits digitale Nutzerverwaltungen implementiert sind, gestaltet sich die Einbindung vergleichsweise unkompliziert und erfordert in der Regel lediglich Anpassungen an bestehenden Authentifizierungsmodulen. Deutlich aufwendiger ist die Integration hingegen in analogen Strukturen, etwa bei papierbasierten Benutzerregistrierungen. In solchen Fällen geht die Einführung der Lösung mit einer umfassenden Neugestaltung der Prozesse einher und wird Teil eines grundsätzlichen Digitalisierungsvorhabens, das über die konkrete Technologie hinausgehende Herausforderungen mit sich bringt.

Auch im Hinblick auf die Kompetenzen und das Verständnis der Anwendenden müssen laut der Early-Adopter nahezu keine Grundlagen geschaffen werden, da der Umgang mit Hardware-Schlüsseln analog zum Umgang mit anderen physischen Schlüsseln erfolgt und moderne Betriebssysteme Authentifizierungsprozesse mittels Hardware-Schlüsseln automatisiert unterstützen. Für die Lösungsentwicklung sind ein gewisses Maß an Webentwicklungskompetenz und Kenntnisse im Bereich der Client-Server-Architekturen erforderlich. Durch den Rückgriff auf bestehende Frameworks und Bibliotheken kann der Kenntnisbedarf jedoch stark reduziert werden. Aus rechtlicher Sicht ist die Anwendung von Hardware-Schlüsseln unproblematisch.

Implikationen

Folgende Implikationen ergeben sich durch den Einsatz von Hardware-Schlüsseln bei der Qualitätskontrolle von Obst und Gemüse in der Lebensmittelwirtschaft:

Befähiger	Neutral	Beschränker
<p>Zukunftsfähigkeit:</p> <p>Durch die geringen Hardwarekosten und die Unterstützung der Lösung durch Hersteller wie Apple oder Google ist absehbar, dass zukünftig Security-Chips auf vielen Geräten der Endnutzenden wie Smartphones und Tablets serienmäßig installiert sein werden, die dann selbst als Hardware-Schlüssel dienen.</p>	<p>Kosten:</p> <p>Zunächst sind Anfangsinvestitionen in die Hardware (derzeit ca. 100 € pro Schlüssel) notwendig. Andererseits können IT-Kosten im Bereich der Nutzeradministration und weitere Ausgaben für Hardware der Mitarbeitenden vermieden werden.</p>	<p>Abnutzung der Ressourcen:</p> <p>Im Einklang mit herkömmlichen Schlüsseln kann es auch bei Hardware-Schlüsseln zu Verlusten oder Beschädigungen kommen. Diese bedingen zusätzliche Aufwände bei der Sperrung oder der Neuerteilung von Berechtigungen und können die Nutzbarkeit des Systems gegebenenfalls temporär einschränken.</p>
<p>Nutzbarkeit:</p> <p>Die Nutzenden müssen sich keine Passwörter merken und die Anmeldung erfolgt schnell und einfach per Hardware. Die Authentifizierung ist konsistent, plattformunabhängig und reduziert menschliche Fehler bei der Anmeldung.</p>		<p>Kultur und Zusammenarbeit:</p> <p>Geringe Akzeptanz kann entstehen, wenn die Lösung „von oben“ eingeführt wird, ohne die Vorteile klar zu kommunizieren. Zusätzlich können Unsicherheiten über die tatsächliche Sicherheit bei den Nutzenden zu Misstrauen führen.</p>

Befähiger	Neutral	Beschränker
Einsatzbereiche:		
Die etablierte Hardware-Authentifizierung kann in vielfältigsten Kontexten angewendet werden und ist nicht auf den Anwendungsfall der Qualitätsprüfung von Obst und Gemüse beschränkt.		
Wirtschaftlichkeit:		
Derzeit ist der Markt der Anbieter von Hardware-Schlüsseln noch überschaubar. Langfristig ist davon auszugehen, dass sich der Wettbewerb in diesem Bereich verstärkt und dadurch Kosten gesenkt werden können.		

Tabelle 5: Implikationen – Hardware-Schlüssel in der Lebensmittelwirtschaft

4.3.2 Federated-Learning im Kontext der industriellen Fertigung

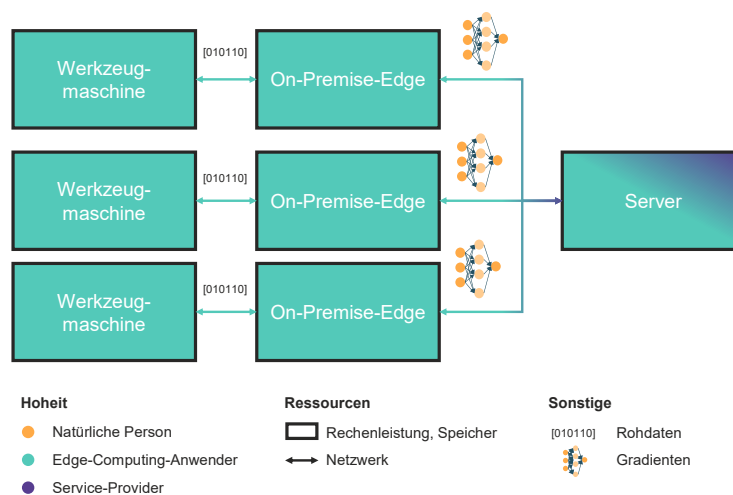


Abbildung 7: Schematische Darstellung – Federated-Learning in der industriellen Fertigung

Mithilfe von Federated-Learning lassen sich KI-Verfahren mit Daten verteilter Clients trainieren, ohne dass Rohdaten an eine zentrale Stelle übertragen werden müssen. Stattdessen werden nur Modellupdates bzw. Gradienten an einen Aggregator gesendet, der diese zu einem globalen Modell zusammenführt. Das aktualisierte globale Modell kann wiederum im Anschluss an alle beteiligten Clients gegeben werden, sodass diese voneinander lernen können. Im gegebenen Kontext wird Federated-Learning für einen unternehmensinternen Anwendungsfall in einem multinationalen Industrieunternehmen erprobt. Ziel ist es, an verschiedenen Produktionsstandorten verteilte Datenquellen zu nutzen, ohne dass sensible Maschinendaten zentralisiert oder direkt ausgetauscht werden müssen. Dies ist insbesondere für Anwendungen relevant, in denen erhebliche technische und organisatorische Barrieren beim Zugriff auf Produktionsdaten bestehen. Konkret kann dies der Fall sein, wenn Sicherheitszonen innerhalb der Werke den Zugriff beschränken oder Silodenken die Verfügbarmachung und Aggregation von Produktionsdaten aus Werken erschweren. Weiterhin können durch Federated-Learning einzelne Clients voneinander lernen. Dies ermöglicht beispielsweise die Detektion von Fehlerzuständen, die bislang nur an einzelnen Maschinen aufgetreten sind, für alle beteiligten Maschinen. Zukünftig ist denkbar, Federated-

Learning auch direkt in Produkt-Service-Systemen einzusetzen, um lernfähige Systeme zu erzeugen, ohne dass datenschutzrechtlich sensible Informationen preisgegeben werden müssen. Zur Zufriedenheit der Anwendenden sollte sich das Federated-Learning-Verfahren dabei nahtlos in die Anwendung integrieren und vollständig automatisiert sein.

Im gegebenen Federated-Learning-Szenario (s. Abbildung 7) werden die Prozessdaten (Rohdaten) aufgrund der geringeren Rechenkapazitäten und weiteren Beschränkungen der Werkzeugmaschine zunächst in eine leistungsfähigere Edge-Umgebung (On-Premise-Edge) geladen. Die Daten werden dort mit dem initialen KI-Modell zusammengeführt, um KI-Inferenz und Modelltraining durchzuführen. Die Modellupdates bzw. Gradienten werden anschließend an einen zentralen Orchestrator übertragen, der die Gradienten der einzelnen Systeme zusammenführt. Der Orchestrator kann beispielsweise durch einen lokalen Serverrechner oder einen Cloud-Server realisiert werden. Anschließend wird das gemeinsame, aktualisierte Modell an die Edge-Umgebungen verteilt und der Lernprozess kann erneut durchgeführt werden.

Umsetzungsvoraussetzungen

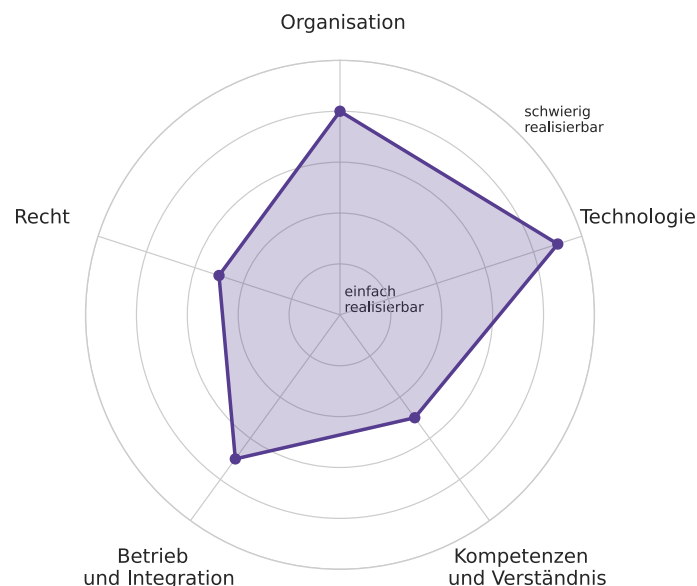


Abbildung 8: Evaluierung der Umsetzungsvoraussetzungen – Federated-Learning in der industriellen Fertigung | Subjektive Bewertung der relativen Komplexität der Umsetzungsvoraussetzungen durch die Early-Adopter der PET im gegebenen Anwendungsfall anhand einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“

Im Vergleich zu anderen Umsetzungsvoraussetzungen bestehen bei der Realisierung von Federated-Learning in der industriellen Produktion laut der Early-Adopter vergleichsweise große Aufwände bei der Schaffung der technischen Grundlagen (s. Abbildung 8). Ein zentrales technisches Hindernis liegt in der Heterogenität der eingesetzten Maschinen, Produkte und Prozesse in der industriellen Fertigung. Aus diesen entstehen ungleiche Datenverteilungen zwischen unterschiedlichen Clients, welche wiederum widersprüchliche Lernsignale erzeugen, die eine Zusammenführung lokaler Modelle in ein robustes und gut generalisierendes globales Modell deutlich erschweren. Gleichzeitig sind über die eigentlichen Federated-Learning-Technologien hinausgehende Frameworks bzw. Technologie-Stacks notwendig, die beispielsweise eine nahtlose Kommunikation und kontinuierliche Updates des Federated-Learning-Netzwerks sicherstellen, um eine gute Nutzendenerfahrung zu generieren. Entsprechend bedarf es umfassender Entwicklungsaufwände, die über die Lösung der eigentlichen Problemstellung hinausgehen.

Damit verbunden ist gemäß der Early-Adopter auch die Einbindung und der Betrieb der Lösung ein eher komplexeres Unterfangen. Einerseits ist die Umsetzung von Anwendungen des föderierten Lernens oftmals nicht eine unmittelbare, sondern vielmehr eine übernächste Entwicklungsstufe in der datengetriebenen Transformation der industriellen Produktion. So müssen oftmals notwendige Daten zunächst verfügbar gemacht und in einer ersten Stufe mit einfachen Methoden analysiert werden. Eine besondere Herausforderung zum erfolgreichen Betrieb der Lösung ist es, die notwendige Anzahl an teilnehmenden Parteien für den Federated-Learning-Anwendungsfall zu gewinnen. Der Nutzen einer Federated-Learning-Anwendung gegenüber einer isolierten KI-Anwendung steigt erst bei breiter Beteiligung zahlreicher Maschinen oder Standorte, sodass insbesondere Early-Adopter der Technologie zunächst keine besonderen Mehrwerte einer Beteiligung erzielen. Sobald eine kritische Masse erreicht ist und die Mehrwerte von Federated-Learning sichtbar werden, ist auch die Überzeugung weiterer Parteien zur Teilnahme deutlich einfacher.

Aus organisatorischer Sicht hängt die Komplexität zur Einführung von Federated-Learning innerhalb industrieller Unternehmen gemäß der Early-Adopter insbesondere von bestehenden Organisationsstrukturen ab. Für den nachhaltigen Erfolg von Federated-Learning müssen, wie bereits zuvor diskutiert, eine Vielzahl interner und externer Stakeholder involviert werden. Mit steigender Organisationsgröße und -komplexität steigt die Anzahl der Stakeholder und damit ebenso der Aufwand zu deren Koordination sowie zur Festlegung der Rollen und Verantwortlichkeiten. Federated-Learning unterscheidet sich damit allerdings nicht in besonderem Maße von herkömmlichen Technologieinitiativen. Entsprechend können, eine hohe Unterstützung des Managements vorausgesetzt, auch Federated-Learning-Technologien innerhalb von Unternehmen schnell erfolgreich eingeführt werden.

Im Hinblick auf die benötigten Kompetenzen und das Verständnis ist qualifiziertes Personal zur Umsetzung von Federated-Learning laut der Early-Adopter in großen Industriebetrieben grundsätzlich vorhanden. Während die anfängliche Zustimmung zu Pilotprojekten (z. B. durch einzelne Innovationstreibende) häufig leicht zu gewinnen ist, erweist sich der Aufbau breiterer Unterstützung über die ersten Pilotprojekte hinaus aufgrund der zunächst notwendigen kritischen Masse als deutlich schwieriger. Üblicherweise ist hierfür viel Überzeugungsarbeit erforderlich.

Hinsichtlich der regulatorisch korrekten Umsetzung der industriellen Anwendung von Federated-Learning bestehen aktuell keine grundsätzlichen Einschränkungen. Auch die KI-Verordnung stellt derzeit kein besonderes Hindernis dar. Allerdings sind, je nach Auslegung der Anwendung, zusätzliche branchenspezifische Compliance-Vorgaben sowie steuer- und haftungsrechtliche Fragestellungen, etwa im Kontext von Datennutzung und -verarbeitung über Ländergrenzen hinweg, zu berücksichtigen. Beispielsweise können Modellgewichte als immaterielle Wirtschaftsgüter gelten, deren Teilen über Ländergrenzen einen grenzüberschreitenden Leistungsaustausch verursacht, der entsprechend bepreist werden muss.

Implikationen

Folgende Implikationen ergeben sich durch den Einsatz von Federated-Learning zur innerbetrieblichen Analyse von Maschinendaten im Bereich der industriellen Produktion:

Befähiger	Neutral	Beschränker
<p>Wirtschaftlich: Federated-Learning ermöglicht die Entwicklung besserer Produkte, vorausgesetzt, eine ausreichend große Zahl von Teilnehmenden (Maschinen) nimmt am Federated-Learning-Ökosystem teil. Durch die aggregierte Nutzung dezentraler Daten entsteht ein breiteres Wissensfundament, das zu qualitativ hochwertigeren Modellen führen kann und Vorteile für alle beteiligten Parteien bringt.</p>	<p>Nutzbarkeit: Für die Endnutzenden ist föderiertes Lernen im Idealfall nicht sichtbar, es verursacht keine spürbaren Einschränkungen und hat somit keine Implikationen auf die Erfahrung der Nutzenden.</p>	<p>Rechtliche Implikationen: Bei unternehmensübergreifenden Federated-Learning-Projekten können rechtliche Unsicherheiten in Bezug auf Datenhoheit, Verantwortlichkeit, Wertbemessung und branchenspezifischen Regularien bestehen, die die Anwendung limitieren.</p>
<p>Zukunftsfähigkeit: Die Etablierung von Federated-Learning-Anwendungen in Produkten auf dem Markt kann neuartigen Nutzen schaffen und somit als Differenzierungsmerkmal gelten und neue Geschäftsmodelle ermöglichen, die langfristigen Bestand haben.</p>	<p>Ressourcenverbrauch: Die tatsächliche Effizienz, der Ressourcenverbrauch sowie die Leistungsfähigkeit der Anwendung müssen im jeweiligen Einzelfall evaluiert werden. Derzeit bestehen noch Unsicherheiten darüber, wie ressourcenschonend Federated-Learning unter realen Bedingungen operieren kann – insbesondere, wenn eine große Anzahl an Clients beteiligt sind.</p>	
<p>Kultur und Zusammenarbeit: Die Skaleneffekte von Federated-Learning machen Kollaboration unter Unternehmen oder Unternehmenseinheiten zu einer notwendigen Voraussetzung. Bereits beteiligte Parteien werden dazu motiviert, weitere Partner anzuwerben, um die Genauigkeit und Robustheit der Anwendung zu erhöhen.</p>		

Tabelle 6: Implikationen – Federated-Learning in der industriellen Fertigung

4.3.3 Compute-to-Data im Kontext der industriellen Fertigung

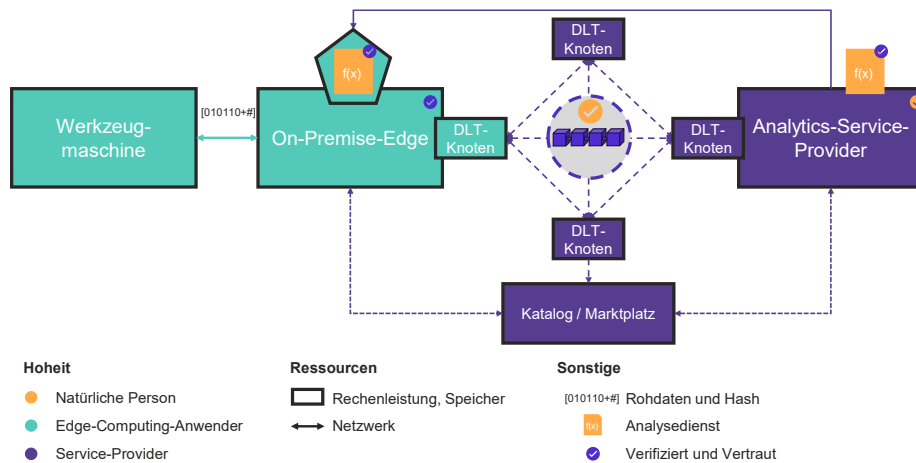


Abbildung 9: Schematische Darstellung – Compute-to-Data in der industriellen Fertigung

Kernkonzept des Compute-to-Data-Ansatzes ist es, das herkömmliche Vorgehen der Übertragung von Daten zur Datenanalyse an einen externen Analysedienst umzukehren. So können stattdessen Analysedienste in eine Umgebung, in welcher die datengebende Organisation die Hoheit besitzt, übertragen und dort ausgeführt werden. In der Fertigungswirtschaft lassen sich somit Services für Maschinen oder Komponenten ausführen, ohne Prozessparameter wie Geometrien oder Schnittdaten, die potenziell schützenswertes Wissen der Maschinenbetreiber darstellen, an andere Parteien preisgeben zu müssen. Zudem wird die Weitergabe von personenbezogenen Daten verhindert und somit potenziell eine höhere Rechtssicherheit der Anwendung erreicht sowie insgesamt die Datensouveränität der datengebenden Organisation gestärkt. Im konkreten Anwendungsfall werden mittels Compute-to-Data Analyseanwendungen eines Komponentenherstellers für den Maschinenbetreiber und somit Komponentennutzer verfügbar gemacht, ohne Prozessdaten an diesen preisgeben zu müssen.

Neben der Gewährleistung von Datenschutz und Datensicherheit müssen bei der Anwendung von Compute-to-Data im Bereich der industriellen Fertigung weitere Anforderungen bedacht werden. Hierzu gehört einerseits die Sicherstellung der Vertrauenswürdigkeit der beteiligten Parteien, beispielsweise des Serviceanbieters und Servicenutzers. Andererseits ist oftmals auch die Notwendigkeit gegeben, die Korrektheit der Eingabedaten zu gewährleisten, etwa wenn die verwendeten Services dem Anlagenbereitstellenden Auskunft über den Zustand oder die Nutzung seiner Anlagen geben sollen, was beispielsweise in Subskriptionsmodellen notwendig ist.

Compute-to-Data-Ansätze werden im gegebenen Anwendungsfall (s. Abbildung 9) konkret durch das Pontus-X-Ökosystem⁵ realisiert. Pontus-X basiert auf Ocean-Protocol und nutzt Web3-Technologien und Smart-Contracts für die technische Umsetzung der Regeln, Richtlinien und Interaktionen im Data-Sharing. Das Web3-Netzwerk wird kollaborativ durch öffentliche und private Institutionen betrieben, die gemeinsam vereinbarten Grundsätzen folgen. So kann sich auch das Fertigungsunternehmen am Betrieb des DLT-Netzwerks beteiligen. Dies ist jedoch zur Nutzung des Netzwerks nicht zwingend notwendig. Um Compute-to-Data-Dienste nutzen zu können, müssen sich interessierte Serviceanbieter und -nutzer zunächst in das Pontus-X-Ökosystem integrieren.

⁵ <https://www.pontus-x.eu/>

Dazu ist ein Gaia-X-Credential verpflichtend, das überprüfbare Aussagen über Identität, Eigenschaften und Konformität von Teilnehmenden im Gaia-X-Ökosystem⁶ enthält und somit die Vertrauenswürdigkeit der Organisation erhöht. Im Anschluss an das Onboarding können Daten- und Serviceangebote verfügbar gemacht und deren Zugriffs- und Nutzungsbedingungen beschrieben werden.

Möchte ein Produktionsunternehmen nach dem erfolgreichen Onboarding Services unter Rückgriff auf den Compute-to-Data-Ansatz beziehen, so muss es zunächst den zu nutzenden Analysedienst über den Netzwerk-Marktplatz suchen und bei Bedarf eine Nutzungsanfrage stellen. Die Service-Metadaten verraten dem Produktionsunternehmen die zur Servicenutzung zu erfüllenden technischen und organisatorischen Anforderungen wie beispielsweise die benötigten Eingangsdaten oder die Ausführungsumgebung. Für die Servicenutzung stellt das Produktionsunternehmen an der On-Premise-Edge oder eine autorisierte dritte Partei die benötigte abgesicherte Umgebung in einem Kubernetes-Cluster⁷ mithilfe von Ocean Protocol-Bibliotheken⁸ bereit und legt einen Eintrag (Asset) im Web3-Netzwerk mit Verweis auf die Produktionsdaten zur Nutzung im entsprechenden Cluster an. Nachdem Serviceanbieter und Maschinenbetreiber automatisiert eine Übereinkunft zur Servicenutzung geschlossen haben, wird die Analyseanwendung in die gesicherte Umgebung übertragen und auf Basis der dorthin übertragenden Produktionsdaten der Werkzeugmaschine ausgeführt. Um sicherzustellen, dass Produktionsdaten nicht vor der Übertragung in das Kubernetes-Cluster verändert wurden, können diese an der Maschine mit einem zusätzlichen Hash versehen werden, der vor der Servicenutzung geprüft wird. Der Serviceanbieter kann mithilfe eines erzeugten Protokolls den aktuellen Status der Anwendung einsehen. Nach Ausführung der Anwendung werden die Analyseergebnisse den berechtigten Parteien verfügbar gemacht. Für einfache Analyseverfahren kann dies ausschließlich das Produktionsunternehmen sein. Wird Compute-to-Data für das Training von KI-Services genutzt, so können die Ergebnisse der Analyseprozesse wie Modellgewichte auch beispielsweise dem Bereitsteller des Algorithmus verfügbar gemacht werden.

⁶ <https://gaia-x.eu/>

⁷ <https://kubernetes.io/>

⁸ <https://oceanprotocol.com/>

Umsetzungsvoraussetzungen

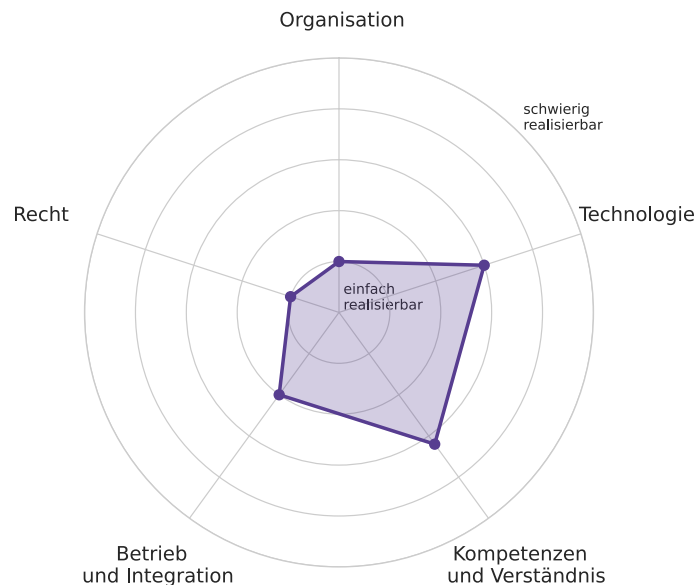


Abbildung 10: Evaluierung der Umsetzungsvoraussetzungen – Compute-to-Data in der industriellen Fertigung | Subjektive Bewertung der relativen Komplexität der Umsetzungsvoraussetzungen durch die Early-Adopter der PET im gegebenen Anwendungsfall anhand einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“

Bei der konkreten Umsetzung der Anwendung ergeben sich laut der Early-Adopter vor allem im Hinblick auf die benötigten Kompetenzen und das benötigte Verständnis zur technischen Realisierung der Lösung Herausforderungen (s. Abbildung 10). Für traditionell geprägte Unternehmen des Maschinenbausektors ist der Aufbau von Kompetenzen zu den genutzten Technologien (Web3 und vertrauenswürdige Umgebungen) notwendig. Insbesondere, wenn kein Vertrauen in dritte Parteien existiert, müssen die vertrauenswürdigen Umgebungen selbst bereitgestellt werden, was technischen Aufwand erfordert. Andersherum vereinfacht der Rückgriff auf verfügbare Open-Source-Software den Aufbau der technischen Lösung. Generell ergänzt die Lösung existierende Prozesse im Bereich von Daten und Analytics, wodurch üblicherweise nur geringe Hürden im Bereich von Betrieb und Integration entstehen. Nach dem Analyseprozess sind jedoch weitere Schritte notwendig, um die resultierenden Daten in die bestehende Infrastruktur zu integrieren. Aus organisatorischer Perspektive sind die Rollen der Parteien durch das Aufsetzen auf Pontus-X und dem Gaia-X-Rahmenwerk und die Anreizmechanismen für einzelne Parteien, darunter auch die Trägerschaft des dezentralen Ökosystems, klar definiert. Ebenso liefert die Lösung durch standardisierte Geschäftsbedingungen und die Durchsetzung der Governance durch Smart-Contracts Sicherheit im Hinblick auf die rechtliche Umsetzung.

Implikationen

Folgende Implikationen ergeben sich durch die Verwendung des Compute-to-Data-Ansatzes zur Analyse von Maschinendaten im Bereich der industriellen Produktion:

Befähiger	Neutral	Beschränker
<p>Geschäftsmodelle</p> <p>Durch den Ansatz einer dezentralisierten autonomen Organisation ergeben sich neuartige Geschäftsmodelle für Organisationen, beispielsweise als anteilige Trägerschaft der Infrastruktur, als Anbieter von Zusatzlösungen oder den Aufbau von eigenen Datenräumen.</p>	<p>Ressourcenverbrauch</p> <p>Durch den gewählten Konsensmechanismus (Proof-of-Stake) ergeben sich trotz der Nutzung von DLT nur geringe weitere Rechenaufwände und Umweltwirkungen im Vergleich zu zentralisierten Lösungen.</p>	<p>Erfahrung der Nutzenden</p> <p>Die erstmalige Einrichtung einer Compute-to-Data-Anwendung bedingt Mehraufwände, beispielsweise zur Erstellung der benötigten Credentials oder zur Beschreibung der Daten- und Serviceangebote. Dies bedingt üblicherweise eine höhere Zeitspanne, bis eine Anwendung erstmalig genutzt werden kann.</p>
<p>Kultur und Zusammenarbeit</p> <p>Es entsteht ein vertrauenswürdiges Ökosystem, das Sichtbarkeit über Partner, Daten- und Serviceangebote generiert und die Kollaboration zwischen Dateninhabenden und Serviceanbietenden fördert.</p>		<p>Nutzbarkeit</p> <p>Je nach Rechenanforderungen der Anwendung entsteht ein potenzieller Mehraufwand für den Nutzenden der Anwendung in der Bereitstellung notwendiger Infrastruktur zur Ausführung der Rechenoperationen.</p>
<p>Zukunftsfähigkeit</p> <p>Die dezentralisierte autonome Organisation und Open-Source-Software als Befähiger der Compute-to-Data Anwendungen ermöglichen eine langfristige Verfügbarkeit der Lösungen ohne Beschränkungen.</p>		

Tabelle 7: Implikationen – Compute-to-Data in der industriellen Fertigung

4.3.4 Zero-Knowledge-Proofs in der Energiewirtschaft

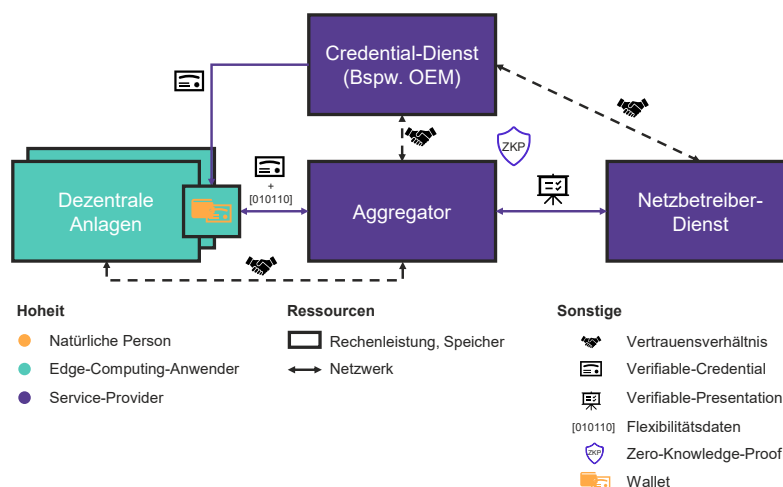


Abbildung 11: Schematische Darstellung – Zero-Knowledge-Proofs in der Energiewirtschaft

Zero-Knowledge-Proofs sind mathematische Verfahren, die es ermöglichen, einen datenbasierten Beweis über einen bestimmten Sachverhalt zu erbringen, ohne die zugrundeliegenden Daten selbst offenzulegen. Beispielsweise kann eine Altersverifizierung durchgeführt werden, ohne das eigentliche Alter preisgeben zu müssen. In der Energiewirtschaft lassen sich Zero-Knowledge-Proofs kombiniert mit Verfahren von Self-Sovereign-Identities einsetzen, um verfügbare Kapazitäten von dezentralen Energieerzeugungsanlagen zu aggregieren und diese einem Netzbetreiber zu melden, ohne potenziell sensible personenbeziehbare oder unternehmensbezogene Daten wie den Standort oder die Auslastung einer konkreten Anlage an diesen bereitstellen zu müssen. Im konkreten Anwendungsfall (s. Abbildung 11) wird dieses Prinzip dazu genutzt, Redispatch⁹-Kapazitäten dezentraler Anlagen durch einen Aggregator zu bündeln und diese gebündelten Kapazitäten einem Netzbetreiber zur Verfügung zu stellen.

Eine weitere wichtige Anforderung ist die Möglichkeit der Verifikation der aggregierten Daten durch den Netzbetreiber, ohne diese offenlegen zu müssen. So ist für den Netzbetreiber insbesondere wichtig, dass die angegebenen Kapazitäten wirklich abgerufen werden können und dass sich die Anlagen im relevanten Netzbereich befinden. Zudem sollte der Netzbetreiber diese Verifikation möglichst performant durchführen können.

Das Konzept basiert insgesamt auf den Konzepten von Self-Sovereign-Identities und Public-/Private-Key-Infrastrukturen. Ausgangslage ist eine bestehende Vertrauenskette zwischen Netzbetreiber, Anlagen-OEMs, Aggregatoren und Anlagenbetreibern. Die dezentralen Anlagen werden in ihrer Einrichtungsphase um ein vertrauenswürdigen Hardware-Modul ergänzt. Im ersten Schritt wird in das Wallet dieses Hardware-Moduls ein verifizierbarer digitaler Nachweis (Verifiable-Credential)¹⁰ zu den Stammdaten der Anlage von dem Credential-Dienst einer vertrauenswürdigen Partei (z. B. OEM oder Netzbetreiber) übertragen. Über diesen Nachweis kann die Eigentümerin bzw. der Eigentümer der Anlage anschließend verfügen. Eine Information, die dieses Verifiable-Credential enthält, ist beispielsweise der Nachweis über die Teilnahmefähigkeit am Redispatch. Die Eigentümerschaft delegiert das Verifiable-Credential an den Aggregator und berechtigt diesen, aggregierte Flexibilitätsangebote zu erstellen. Die Anlagen stellen ihre individuellen Flexibilitätsangebote anschließend automatisch dem Aggregator zur Verfügung. Dieser kann dann die individuellen Flexibilitätspotenziale aggregieren und dem Netzbetreiber als Verifiable-Presentation zur Verfügung stellen. Dabei werden die Signaturen der Anlagen genutzt, um zu beweisen, dass die Angebote insgesamt von zertifizierten Anlagen stammen. An dieser Stelle werden ebenso die eigentlichen Zero-Knowledge-Proofs eingesetzt, um weitere notwendige Nachweise über aggregierte Angebote zu erstellen, ohne die Daten einzelner Anlagen preisgeben zu müssen. Beispielsweise kann nachgewiesen werden, dass sich die Anlagen in einem bestimmten Netzgebiet befinden oder dass die Kapazitäten wirklich zur Verfügung stehen. Perspektivisch wird die Ergänzung des Ansatzes um den Einsatz von Hardware-Sicherheitsmodulen in den dezentralen Anlagen angestrebt, um weitere Manipulationen auszuschließen.

⁹ Redispatch bedeutet in diesem Kontext, dass der Netzbetreiber gegen Entgelt dezentrale Erzeugungsanlagen herunterfährt oder Batteriespeicherkapazitäten nutzt, um das Stromnetz zu stabilisieren.

¹⁰ <https://www.w3.org/TR/vc-overview/>

Umsetzungsvoraussetzungen

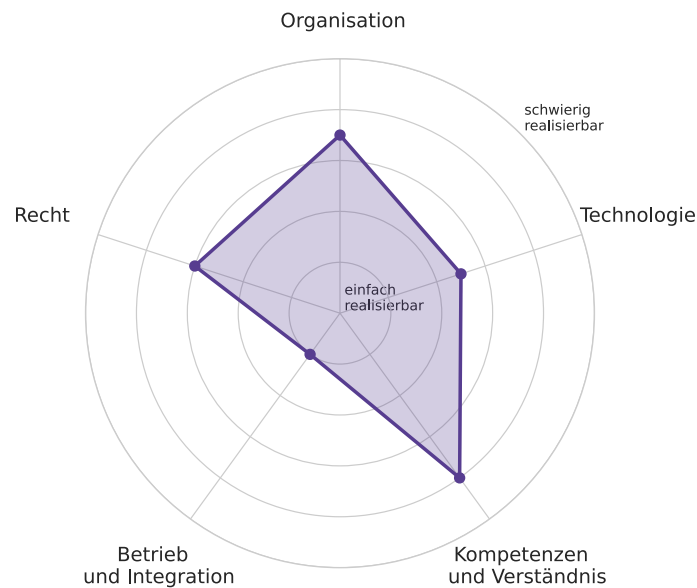


Abbildung 12: Evaluierung der Umsetzungsvoraussetzungen – Zero-Knowledge-Proofs in der Energiewirtschaft | Subjektive Bewertung der relativen Komplexität der Umsetzungsvoraussetzungen durch die Early-Adopter der PET im gegebenen Anwendungsfall anhand einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“

Zur Umsetzung der Zero-Knowledge-Proof-Anwendung stellt die Schaffung von Kompetenzen und Verständnis nach Aussage der Early-Adopter eine zentrale Herausforderung dar (s. Abbildung 12). Zero-Knowledge-Proofs sind nach wie vor eine junge Technologie mit einer vergleichsweise kleinen Entwickler-Community. Der Aufbau von Expertise auf Seiten der Anwendungsentwickler erfordert daher größere Aufwände. Weiterhin ist auch die Akzeptanz bei Anwendenden nicht direkt gegeben, da die Technologie aufgrund ihrer komplexen Mathematik schwer verständlich ist und ohne zusätzliche Erklärungen häufiger als intransparent wahrgenommen wird.

Auch zur Schaffung der organisatorischen Voraussetzungen sind umfassende Arbeiten notwendig. So ist der Einsatz von Zero-Knowledge-Proofs insbesondere dann sinnvoll, wenn Datenschutz über verschiedene Parteien hinweg gewährleistet werden soll. Die Realisierung von Kooperation und Austausch über Parteien hinweg führt jedoch zu erheblichem organisatorischen Mehraufwand. Beispielsweise müssen Herstellende, Netzbetreibende und Aggregatoren kooperieren, um gemeinsame Standards für Zertifikate und vertrauenswürdige Daten zu definieren und die notwendigen organisatorischen Vertrauensmechanismen zu etablieren. Zur allgemeinen Umsetzung des Anwendungsfalls ist zudem eine kritische Masse an Beteiligten zu gewinnen, um die notwendigen Netzwerkeffekte zu erzeugen.

Auch auf rechtlicher Ebene bestehen laut der Early-Adopter größere Herausforderungen, die allerdings vor allem aus der Anwendung von Zero-Knowledge-Proofs im streng regulierten Strommarkt resultieren. So sind bestimmte kryptografische Verfahren und Programmiersprachen für Zero-Knowledge-Proofs derzeit noch nicht für Anwendungen in kritischen Infrastrukturen zugelassen. Zudem ist es notwendig, Zero-Knowledge-Proofs aus haftungsrechtlicher Perspektive bewerten zu lassen, um Vertrauen bei den notwendigen Stakeholdern aufzubauen.

Die eigentliche technische Umsetzung ist nach der Etablierung des notwendigen Wissens bei den Verantwortlichen vergleichsweise einfach zu leisten. Damit verbunden ergeben sich aus Sicht des Betriebs und der Integration von Zero-Knowledge-Proofs für den gegebenen Anwendungsfall

durch den gewählten Greenfield-Ansatz keine besonderen Hürden. Zukünftig könnten sich jedoch zusätzliche Aufwände zur Harmonisierung mit bereits etablierten Standards und Protokollen des Energiemarktes ergeben.

Implikationen

Folgende Implikationen ergeben sich durch den Einsatz von Zero-Knowledge-Proofs für den dezentralen Redispatch in der Energiewirtschaft:

Befähiger	Neutral	Beschränker
<p>Kultur und Zusammenarbeit: Der Einsatz von Zero-Knowledge-Proofs im Energiesektor fördert insgesamt den Aufbau eines Ökosystems, in dem Hersteller, Aggregatoren und Netzbetreiber zusammenarbeiten und sich Vorteile für alle Parteien ergeben. Zero-Knowledge-Proofs fördern zudem die Einführung von Aggregatoren als Form eines Intermediärs, der neuartige Anwendungen in der Energiewirtschaft ermöglicht.</p>	<p>Erfahrung der Nutzenden: Die Erstellung von Zero-Knowledge-Proofs läuft im Hintergrund ab und ist für die Flexibilitätsbereitstellenden nicht sichtbar. Durch die vollständige Automatisierung der Prozesse werden Eingriffe der Nutzenden vermieden.</p>	<p>Black-Box-Verfahren: Das Verfahren zur Erstellung von Zero-Knowledge-Proofs ist für Nutzende schwer nachvollziehbar und es kann ein Black-Box-Eindruck entstehen, der das Vertrauen in die Technologie beeinträchtigt.</p>
<p>Wirtschaftliche Potenziale: Durch die Schaffung neuartiger Rollen und die Realisierung zuvor nicht möglicher Anwendungen können wirtschaftliche Potenziale gehoben werden. Beispielsweise kann die vorgestellte Anwendung zur Senkung von Redispatch-Kosten beitragen, was langfristig die Systemkosten im Strommarkt reduziert und zu potenziell günstigeren Netzentgelten führt.</p>		<p>Ressourcenverbrauch: Durch die Berechnungen der Zero-Knowledge-Proofs entsteht ein höherer Rechenaufwand, der die Echtzeitfähigkeit beschränkt und den operativen Einsatz in Stromnetzen mit Anforderungen im Bereich von Millisekunden beschränkt.</p>
<p>Zukunftsfähigkeit: Zero-Knowledge-Proofs integrieren sich nahtlos in Konzepte wie Self-Sovereign-Identities und Datenräume und können somit weitere Innovationen fördern und Governance-Aspekte mit der technischen Garantie von Datensouveränität kombinieren.</p>		<p>Zukunftsfähigkeit: Von regulatorischer Seite sind noch weitere Arbeiten erforderlich, um die Anwendung von Zero-Knowledge-Proofs flächendeckend in kritischen Infrastrukturen zu ermöglichen.</p>

Tabelle 8: Implikationen – Zero-Knowledge-Proofs in der Energiewirtschaft

4.3.5 Trusted-Execution-Environments in der Energiewirtschaft

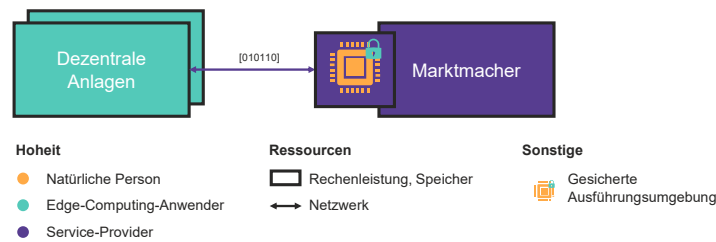


Abbildung 13: Schematische Darstellung – Trusted-Execution-Environments in der Energiewirtschaft

Trusted-Execution-Environments sind Hardware-gestützte, isolierte Ausführungsumgebungen, die den Code und die Daten während der Datenverarbeitung vor Einsicht und Manipulation durch das restliche System schützen. Somit können beispielsweise vertrauliche Daten in der Cloud verarbeitet oder Modellgewichte beim Einsatz von KI geschützt werden. Im Energiebereich können Trusted-Execution-Environments beispielsweise für Preisbildungsprozesse in lokalen Energiemärkten eingesetzt werden. Zur Preisbildung sind sowohl die Preisbildungsalgorithmik als auch die Stromangebote an einer zentralen Stelle zusammenzuführen. Durch Trusted-Execution-Environments findet die Preiskalkulation in der geschützten Umgebung statt, um eine mögliche Bevorteilung einzelner Parteien zu verhindern und die potenziell sensiblen Stromangebote vor der Einsicht von weiteren Anbietern zu schützen.

Neben dem Schutz der zur Preisfindung notwendigen Daten sind den Marktteilnehmenden insbesondere Fairness, Transparenz und Nachvollziehbarkeit bei der Ausführung des Preisfindungsalgorithmus wichtig. Zudem ist relevant, dass keine zentrale Stelle als alleinige Kontrollinstanz fungiert. Weiterhin sollte das Verfahren zur Preisfindung möglichst kostengünstig ablaufen können, da die Berechnungskosten mit dem geplanten Preisberechnungsintervall ansteigen und so möglichst granulare Berechnungen ermöglicht werden. Zudem sollte die Skalierbarkeit der Lösung gegeben sein, um möglichst viele Parteien in das System aufnehmen zu können.

Die konkrete Umsetzung der Trusted-Execution-Environment wird in diesem Fall durch einen Trusted-Execution-Environment-Service eines Cloud-Service-Providers realisiert, der durch den Marktmacher konfiguriert wird (s. Abbildung 13). Der Preisfindungsalgorithmus steht für die Anlagenbetreibenden als Open-Source-Code zur Verfügung. Die Trusted-Execution-Environment kann über kryptografische Verfahren sicherstellen und transparent machen, dass genau dieser Code in ihr ausgeführt wird. Die zur Preisfindung notwendigen Daten werden wiederum von der Anlage direkt in das Trusted-Execution-Environment gegeben. Hierbei können Ende-zu-Ende-Verschlüsselungen den Schutz der Daten während des Transfers gewährleisten.

Umsetzungsvoraussetzungen



Abbildung 14: Evaluierung der Umsetzungsvoraussetzungen – Trusted-Execution-Environments in der Energiewirtschaft | Subjektive Bewertung der relativen Komplexität der Umsetzungsvoraussetzungen durch die Early-Adopter der PET im gegebenen Anwendungsfall anhand einer sechsstufigen Likert-Skala von „sehr einfach leistbar“ bis „sehr schwierig leistbar“

Die größte Herausforderung bei der Umsetzung der beschriebenen Preisfindungs-Anwendung liegt gemäß der Early-Adopter grundsätzlich in der Schaffung der notwendigen Kompetenzen bei den Anwendungsentwickelnden und des Technologieverständnisses bei den Anlagenbetreibenden (s. Abbildung 14). Trusted-Execution-Environments sind eine eher „exotische“ Technologie, die spezialisiertes Fachwissen erfordert. Unternehmen müssen bereit sein, interne Ressourcen für den Aufbau entsprechender Expertise bereitzustellen. Gleichzeitig bleibt die Akzeptanz bei den Anlagenbetreibenden eine Herausforderung. Während technisch versierte Anwendende den Nutzen nachvollziehen können, fehlt häufig das Verständnis für die dahinterliegende Logik, die verbunden mit den höheren Kosten der Infrastruktur zu einer verringerten Technologieakzeptanz führen kann.

Durch die Möglichkeit, spezialisierte Cloud-Services für Trusted-Execution-Environments zu nutzen, wird ein Großteil der technischen Komplexität abstrahiert. Dennoch zeigen sich während der Einrichtung und des Betriebs Aufwände, die über das Einrichten herkömmlicher Cloud-Services hinausgehen. Die erforderliche Hardware ist zudem kostspielig. Darüber hinaus sind Trusted-Execution-Environments Teil eines Gesamtsystems, sodass zusätzliche Absicherungen, beispielsweise in der Datenübertragung, implementiert werden müssen. Sicherheitsrelevante Schwachstellen einzelner Systeme können den Aufwand für kontinuierliche Anpassungen erhöhen. Zudem wurden über die Jahre hinweg immer wieder neue Angriffsvektoren auf Trusted-Execution-Environments identifiziert, sodass mögliche Risiken kontinuierlich überwacht werden sollten.

Aus organisatorischer, operativer und rechtlicher Perspektive ergeben sich laut der Early-Adopter grundsätzlich keine großen Hürden für den Einsatz von Trusted-Execution-Environments. So lassen sich diese wie herkömmliche Software-Service einkaufen und können tendenziell ohne die umfassende Einbindung von Partnern umgesetzt werden. Für die betriebliche Integration müssen Trusted-Execution-Environments üblicherweise nur selbst an die betrieblichen Abläufe angepasst

werden. Als Infrastrukturkomponente lassen sie sich analog zu anderen Softwarebausteinen integrieren. Rechtlich bestehen im Gegensatz zu anderen kryptografischen Ansätzen vergleichsweise geringe Hürden. Mit der Nutzung europäischer Cloud-Anbieter, die die Einhaltung der notwendigen technischen und organisatorischen Maßnahmen garantieren, können regulatorische Anforderungen einfach erfüllt werden. In bestimmten Kontexten kann der Einsatz von Trusted-Execution-Environments aus rechtlicher Sicht zudem positiv bewertet werden, da dies zusätzliche Integrität und Sicherheit schafft.

Implikationen

Folgende Implikationen ergeben sich durch den Einsatz von Trusted-Execution-Environments in der Energiewirtschaft:

Befähiger	Neutral	Beschränker
<p>Integrität: Neben Datenschutzaspekten werden durch die Umsetzung von Trusted-Execution-Environments auch die Integrität und Vertrauenswürdigkeit von Datenverarbeitungsoperationen erhöht.</p>	<p>Zukunftsfähigkeit: Obwohl bereits umfassende Serviceangebote existieren, sind Trusted-Execution-Environments weiterhin eher eine Nischentechnologie, die jedoch zukünftig weitere Verbreitung durch den zunehmenden Bedarf an Transparenz und Nachvollziehbarkeit in digitalen Prozessen erfahren kann.</p>	<p>Systemintegration: Trusted-Execution-Environments sind immer Teil eines größeren Systems, das ebenso Datenschutzaspekte erfüllen muss. Der alleinige Einsatz von Trusted-Execution-Environments kann somit keinen umfassenden Schutz vor Datenabfluss gewährleisten.</p>
<p>Nutzbarkeit: Trusted-Execution-Environments unterstützen die Verlässlichkeit und die Stabilität von Prozessen. Die Endkundschaft profitiert von einem System, das im Hintergrund zuverlässig funktioniert. Gleichzeitig sollte die Technologie für Nutzende weitgehend unsichtbar sein.</p>		<p>Kultur und Zusammenarbeit: Durch ihren „Black-Box“-Charakter kann Skepsis bei weniger technisch versierten Akteuren verstärkt werden. Dies kann insbesondere bei der Interaktion mit Endnutzenden zu einem Problem werden.</p>
<p>Vertrauenswürdigkeit Mit Trusted-Execution-Environments können Anwendungen realisiert werden, bei denen sich die Teilnehmenden nicht vertrauen müssen (vertrauenslose Anwendungen). Der Bedarf der Erbringung der „Beweislast“ durch den Lösungsanbieter wird hiermit reduziert.</p>		<p>Wirtschaftlichkeit: Initiale und laufende Kosten für Hardware, Integration und Betrieb sind teurer als herkömmliche Cloud-Lösungen und könnten somit die Wirtschaftlichkeit einer Lösung in Frage stellen.</p>

Tabelle 9: Implikationen – Trusted-Execution-Environments in der Energiewirtschaft

5 Handlungsempfehlungen und Ausblick

Neben den spezifischen Erfordernissen des Einsatzes von Privacy-Enhancing-Technologies (PET) in dedizierten Edge-Cloud-Anwendungen lassen sich aus den Erkenntnissen der Praxisumsetzungen darüberhinausgehende Handlungsempfehlungen generalisieren. Die in diesem Abschnitt dargestellten Handlungsempfehlungen ergeben sich aus den Aussagen der Early-Adopter der PET-Werkzeuge. Mithilfe von qualitativer, induktiver Inhaltsanalyse wurden Transkriptionen und Gedankenprotokolle von Interviews mit den Early-Adoptern analysiert, um gemeinsame Voraussetzungen für den Erfolg von PET zu identifizieren und daraus Handlungsempfehlungen abzuleiten.

Konkret ergeben sich vier Handlungsfelder (s. Abbildung 15), um PET-Werkzeuge effektiv zur Gewährleistung von Datenschutz und Informationssicherheit in Edge-Cloud-Systemen einzusetzen. Die Handlungsfelder sind voneinander abhängig und sollten daher gemeinsam adressiert werden. In der Folge werden diese Handlungsfelder und mögliche Gestaltungsgegenstände beschrieben.



Abbildung 15: Handlungsfelder für den effektiven Einsatz von PET in Edge-Cloud-Anwendungen

Aufbau und Gestaltung des Partnerökosystems



Durch die hohe technologische Komplexität von PET-Technologien wie Zero-Knowledge-Proofs, Trusted-Execution-Environments oder Federated-Learning sind gerade mittelständische Unternehmen in der Regel nicht vollständig in der Lage, PET-basierte Architekturen eigenständig umzusetzen und zu skalieren. Gleichzeitig existiert derzeit kein Technologieanbieter, der den gesamten Umfang an PET als Serviceangebot vollständig abdecken kann. Andersherum ergeben sich durch die mittels PET ermöglichten Anwendungsfälle und deren zugrundeliegenden Datenaustauschbeziehungen zwangsläufig Austauschbeziehungen, in denen einzelne Partner sowohl kooperieren als auch in Konkurrenz zueinanderstehen können. Beispielsweise ist dies der Fall, wenn einzelne Betreiber von Maschinen an einem auf Federated-Learning basierendem Qualitätsmanagementsystem partizipieren, jedoch gleichzeitig konkurrierende Produkte produzieren

oder um verfügbare Aufträge im Wettbewerb stehen. Entsprechend ist es notwendig, dass umfassende Überlegungen hinsichtlich des Aufbaus und des nachhaltigen Betriebs des Partnerökosystems getroffen werden. Dies ist Aufgabe der umsetzenden Organisation, die somit, ob gewünscht oder ungewünscht, automatisch zu einem Orchestrator dieses Ökosystems wird.

Vertrauenswürdige Partner identifizieren und einbinden

Während die datengebenden Organisationen in den geplanten Edge-Cloud-Anwendungen zu meist aus existierenden Geschäftsverhältnissen entstammen oder als neue Zielgruppe anvisiert werden, müssen die umsetzenden Organisationen insbesondere mögliche Technologiepartner auswählen, mit ihnen gemeinsam die geschäftliche Anwendung implementieren und dabei die PET-Werkzeuge mit den bereits etablierten Softwaresystemen integrieren. Da diese spezialisierten Softwareanbieter oftmals nicht über die notwendigen Anwendungskompetenzen verfügen, ist es notwendig, diese eng in den zu behandelnden Geschäftsfall zu integrieren, um die Zusammenarbeit und das Verständnis zu stärken. Die enge Anbindung des PET-Partners resultiert oftmals auch in einer für die anderen Parteien des Ökosystems sichtbaren Interaktion.

Entsprechend ist sicherzustellen, dass der PET-Partner auch für weitere Parteien eine vertrauenswürdige Organisation darstellt. Im Zuge steigender geopolitischer Spannungen sollte hierzu die Komponente der digitalen Souveränität berücksichtigt werden. Beispielsweise werden Trusted-Execution-Environments üblicherweise von Cloud-Service-Providern bereitgestellt und bedingen eine Übertragung von Daten in diese Umgebung. In regulierten Bereichen oder Bereichen mit generell hohen Bedenken hinsichtlich der Informationssicherheit ist die Wahl eines europäischen Cloud-Service-Providers möglich, um potenzielle Bedenken hinsichtlich der digitalen Souveränität zu reduzieren. Andererseits sollte auch sichergestellt sein, dass PET-Dienste von neutralen Intermediären ohne wirtschaftliche Konkurrenz zu den Geschäftsmodellen der beteiligten Partner genutzt werden, da trotz des Einsatzes von PET oft ausnutzbare Schwachstellen verbleiben.

Notwendige Anreizmechanismen und Geschäftsmodelle gestalten

Gleichermaßen ist es erforderlich, für alle an den PET-gestützten Anwendungen beteiligten Partner ausreichende geschäftliche Anreize zu schaffen. Der Einsatz von PET-Werkzeugen ist zu meist mit einem nicht zu vernachlässigenden organisatorischem und geschäftlichem Mehraufwand verbunden, der von allen Akteuren des Partnerökosystems mitgetragen werden muss. Einerseits müssen dazu die durch die umgesetzte Anwendung erzeugten Mehrwerte für die notwendigen Parteien als fair betrachtet werden. Dies gilt sowohl für die Wertverteilung zwischen den verschiedenen Akteursgruppen als auch innerhalb einzelner Gruppen von Akteuren. Beispielsweise können in auf Federated-Learning basierenden Anwendungen einzelne Parteien einen besonders hohen Anteil am gemeinsamen Modelltraining besitzen, andere wiederum überproportional von diesen trainierten Modellen profitieren. Weiterhin können in PET-Partnerökosystemen explizit neue Anreiz- und Belohnungssysteme geschaffen werden. Dies zeigt beispielsweise die Etablierung des DLT-Ökosystems im Compute-to-Data-Ansatz (s. Abschnitt 4.3.3), welches eine transaktionsbasierte Entlohnung der Infrastrukturbereitsteller ermöglicht und somit die Skalierung des Ökosystems möglich macht.

Schaffung der betrieblichen Voraussetzungen für den PET-Einsatz



Auch auf operativer Ebene gilt es, für die nutzenden Personen der PET-Anwendungen ausreichende Anreize zur Verwendung der PET zu generieren. Für die anwendenden Personen sind

viele PET eine „Black-Box“, d. h. aufgrund ihrer hohen technischen oder mathematischen Komplexität nicht nachvollziehbar. Gleichmaßen können PET teilweise mit merklichen prozessualen Mehraufwänden verbunden sein, welche die Nutzerakzeptanz reduzieren.

Wissen, Akzeptanz und Vertrauen in die Lösung generieren

Entsprechend notwendig ist es, die Lösung zu kommunizieren und die Entscheidenden, Anwendenden und weiteren Stakeholder zu schulen, um Verständnis aufzubauen, Vertrauen zu fördern und schlussendlich die Akzeptanz der Technologie zu erhöhen. Hierzu kann einerseits oftmals auf das vorhandene Schulungsmaterial von Partnern zurückgegriffen werden. Andererseits ist auch die Bereitstellung von Testumgebungen denkbar, in denen Anwendende auf die Sichten verschiedener Rollen zugreifen können und somit „hands-on“ die Technologie testen können und Klarheit über die Datenverwendung erhalten.

PET abstrahieren

Wenngleich die Schaffung des Vertrauens in die Technologien ein entscheidender Erfolgsfaktor ist, sollte der Einsatz der PET die Nutzererfahrung nicht signifikant verändern. Stattdessen sollten PET, wie andere Sicherheitstechnologien auch, für den Nutzenden im Verborgenen funktionieren, sodass die technische Komplexität in den Hintergrund und die Vorteile der Anwendung in den Vordergrund rücken. Einzig simple, gezielte Informationen der Nutzenden können an manchen Stellen sinnvoll sein. So ist es denkbar, während des Betriebs den aktuellen Lösungsstatus für die Nutzenden durch einfache Darstellungen zu visualisieren. Ein Beispiel ist eine „Ampelsicht“, die die korrekte Funktionsweise verdeutlicht und somit Vertrauen in die kontinuierliche Verfügbarkeit generiert.

Das Prozess- und Systemdesign überdenken

Weiterhin sollten Organisationen Anstrengungen unternehmen, um einzelne Maßnahmen für den Datenschutz und die Informationssicherheit zu einem grundlegenden „by-Design“-Ansatz weiterzuentwickeln. Dabei sollte die Einhaltung der Vorgaben für den Datenschutz und die Informationssicherheit bereits vollständig in der Entwurfsphase von Systemen berücksichtigt werden und nicht versucht werden, ein bereits existierendes System durch PET-Werkzeuge nachträglich datenschutzkonform auszulegen. Gleichmaßen sollten auch Prozesse so konzipiert sein, dass eine möglichst effiziente Nutzung der PET-Werkzeuge gewährleistet ist. Dies bedingt einerseits die Digitalisierung analoger Prozesse, wie beispielsweise manueller Datenvorverarbeitungen oder organisatorischer Prozesse, die einer PET-Integration vorausgehen. Andererseits sollten auch digitale Prozesse, beispielsweise durch Datenminimierung, so ausgelegt werden, dass die Nutzung der PET-Werkzeuge einen möglichst geringen Mehraufwand erzeugt.

Gewährleistung der technischen Validität und Integrierbarkeit der PET



Aus technischer Sicht muss der Einsatz von PET-Werkzeugen in Edge-Cloud-Anwendungen so gestaltet werden, dass sowohl die technische Validität (also der Nachweis der korrekten und sicheren Funktionsweise) als auch die möglichst nahtlose Integrierbarkeit in heterogene Edge-Cloud-Architekturen gewährleistet werden. Hierbei ist einerseits die Herausforderung zu berücksichtigen, dass einzelne Schwachstellen in der Gesamtarchitektur die Schutzfunktionen der Gesamtanwendung kompromittieren können. Andererseits ist die Integration von PET-Werkzeugen in bestehende Systemarchitekturen aufgrund der hohen technischen Heterogenität aufwändig

und komplex. Weiterhin ergibt sich durch die Verwendung von PET oftmals ein signifikanter technischer Mehraufwand, der insbesondere beim Einsatz von kryptografischen Verfahren zu einer höheren Latenzzeit der Edge-Cloud-Anwendung führt.

Aufbau der Ende-zu-Ende-Vertrauenskette

Damit PET über Organisations- und Systemgrenzen hinweg verlässlich funktionieren, ist eine durchgängige Ende-zu-Ende-Vertrauenskette mit eindeutigen Vertrauensankern aufzubauen. Vertrauen bezieht sich dabei sowohl auf die an der Anwendung beteiligten Partner als auch auf die technische Infrastruktur zur Realisierung der Anwendung und die genutzten Daten. Ein wichtiger Aspekt ist dabei die technische Realisierung von Zero-Trust-Konzepten und die Verfolgung des Ansatzes „Privacy-by-Design“. Hierzu ist die Nutzung vertrauenswürdiger Aussteller für die Identitäten und Eigenschaften der beteiligten Organisationen, Personen, Systeme und physischen Objekte eine mögliche Maßnahme. Weiterhin sollte die Integrität von Akteuren, Code und Daten mittels kryptografischer Verfahren überprüfbar gemacht werden, ohne unnötige Informationen offenzulegen. Mechanismen wie Remote-Attestation oder aus dem Umfeld dezentraler Identitäten entstammende Technologien sind für diese Umsetzung denkbar.

Zusätzlich sollten Onboarding-Prozesse für Geräte, Software und Daten klar definiert werden. Geräte erhalten geprüfte Identitäten und Zertifikate, Softwareanwendungen und Konfigurationszustände werden signiert und notwendige Rollen werden über verifizierbare Berechtigungsnachweise zugewiesen. Daten, Modelle und Modellgewichte sollten zudem mit Hashes und Signaturen versehen und über Audit-Trails nachvollziehbar gemacht werden, sodass nur Artefakte mit gültiger Attestierung akzeptiert werden.

Edge-first Ansatz beibehalten

Um überhöhten Rechenaufwänden und potenziell nachteiligen Latenzzeiten entgegenzuwirken und Angriffsflächen zu reduzieren, sollten trotz des Rückgriffs auf PET-Werkzeuge möglichst viele Operationen an der Edge durchgeführt werden. Beispielsweise können Daten bereits vor der Übertragung und Zusammenführung an der Edge vorverarbeitet werden, um die Netzwerkbelastung und den Rechenaufwand an zentraler Stelle und unter kryptografischem Mehraufwand zu reduzieren. Die Datenübertragungen sind dabei durch Verschlüsselungsverfahren und Verfahren von Autorisierung und Authentifizierung zu sichern. Somit kann der Einsatz von PET-Werkzeugen auf die notwendigen Aspekte beschränkt werden und leichtgewichtig erfolgen.

Nutzung offener Schnittstellen, Standards und Open-Source-Software

Um die Integrationsfähigkeit in existierende Systemlandschaften und Prozesse zu gewährleisten und die Interoperabilität, Erweiterbarkeit und Austauschbarkeit zu sichern, sollte auch bei der Erweiterung von Edge-Cloud-Architekturen mittels PET auf die Nutzung offener Schnittstellen, Standards und Open-Source-Software gesetzt werden. Durch den Einsatz offener Standards und Schnittstellen bleibt die Architektur flexibel und kann leichter um neue Funktionen oder Bausteine ergänzt werden. PET-Verfahren, die heute implementiert werden, lassen sich so auch mit zukünftigen Technologien kombinieren. Proprietäre Lösungen hingegen führen oft zu Abhängigkeiten (Vendor-Lock-in) und erschweren spätere Anpassungen oder Migrationen erheblich. Im Bereich von PET ist dies von besonderer Relevanz, da einzelne Technologien oftmals nur von wenigen Lösungsanbietern angeboten werden und diese potenziell einen großen Hebel gegenüber den Lösungsnutzern besitzen. Open-Source-Software erlaubt eine öffentliche Überprüfung des Quellcodes und organisationsübergreifende Zusammenarbeit. Gerade bei PET, die sensible Daten

und Informationen schützen sollen, ist Transparenz entscheidend für das Vertrauen in die Sicherheit und Funktionsweise der Systeme. Wird Open-Source-Software von vielen Unternehmen in verschiedenen Kontexten genutzt, ist die Wahrscheinlichkeit höher, dass Sicherheitslücken schneller erkannt und behoben werden. Weiterhin können bestehende Open-Source-PET-Implementierungen weiterentwickelt und an spezifische Anforderungen angepasst werden, was Innovationsprozesse beschleunigt und parallele, isolierte Neuentwicklungen reduziert. Beispiele für existierende Open-Source-Frameworks, bei denen diese Bedingungen erfüllt werden, sind Flower und PySyft im Bereich Federated-Learning (Riedel et al., 2024).

Sicherstellung der regulatorischen Konformität



Schlussendlich muss neben der organisatorischen Machbarkeit und technischen Funktionsweise ebenso die regulatorische Konformität einer PET-gestützten Edge-Cloud-Architektur sichergestellt werden. Dabei sind Praktikerinnen und Praktiker mit einer Reihe von Herausforderungen konfrontiert. Einige PET, wie beispielsweise Federated-Learning, agieren nicht-deterministisch und stellen für die Anwenderunternehmen eine „Black-Box“ dar. Entsprechend verbleiben gewisse Risiken hinsichtlich der möglichen Aufdeckung personenbezogener Daten durch böswillige Akteure, und eine vollständige Privatsphäre kann zumeist nicht garantiert werden. Weiterhin existieren Bereiche, in denen die Nutzung von PET in Deutschland derzeit noch nicht freigegeben ist. Ein Beispiel hierfür ist die Energiewirtschaft, die als kritische Infrastruktur besonderen IT-Sicherheitsmaßnahmen unterliegt. Hier ist auch langfristig eher mit langwierigen Erlaubnisverfahren zu rechnen, da beispielsweise im Fall von Zero-Knowledge-Proofs voraussichtlich jedes einzelne Verfahren separat geprüft und zugelassen werden muss. Weiterhin existieren zusätzliche Herausforderungen, wenn Daten oder Modellgewichte über Ländergrenzen transferiert werden sollen. So formulieren die Datenschutzgrundverordnung und der Data Act spezifische Anforderungen an grenzüberschreitende Datentransfers, die beispielsweise bei der Nutzung außereuropäischer Serviceanbieter geprüft und eingehalten werden sollten. Andererseits können Modelle und Modellgewichte immaterielle Vermögenswerte darstellen, die bei der Übertragung über Ländergrenzen hinweg gemäß internationaler Reporting-Standards aktivierbar sein könnten und entsprechende monetäre Gegenleistungen bedingen. Dies kann auch bei unternehmensinterner Übertragung der Fall sein, beispielsweise wenn eine Auslandsgesellschaft ein lokal trainiertes Modell an die in Deutschland registrierte Entität übermittelt. In diesem spezifischen Fall ist der Fremdvergleichsgrundsatz anzuwenden, nachdem verbundene Unternehmen die Modellübertragung so verrechnen müssen, als wenn sie diese an unabhängige Dritte weitergeben.

Diese Herausforderungen zeigen, dass trotz einer technisch ausreichenden Anonymisierung sensibler Daten weiterhin auch eine rechtliche Absicherung der PET-gestützten Edge-Cloud-Anwendung notwendig ist. Die regulatorische Konformität sollte dabei bereits in frühen Phasen des Vorhabens berücksichtigt werden, um mögliche Hindernisse zu identifizieren. Gleichmaßen sollten die getroffenen Überlegungen im Sinne der zur Verarbeitung personenbezogener Daten verpflichtend durchzuführenden Datenschutz-Folgeabschätzungen dokumentiert werden. Mögliche Herausforderungen beim länderübergreifenden Transfer von Daten sind ebenfalls früh zu antizipieren. Im Rahmen von Forschungsprojekten oder ersten Durchstichen kann zudem von Experimentierklauseln Gebrauch gemacht werden.

Referenzen

- 115th Congress. (2018). *H.R.4943 - CLOUD Act*. <https://www.congress.gov/bill/115th-congress/house-bill/4943>
- Adam, M., Hammoudeh, M., Alrawashdeh, R. & Alsulaimy, B. (2024). A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access*, 12, 57128–57149. <https://doi.org/10.1109/ACCESS.2024.3382709>
- Ali, M. A. & Al-Sharafi, S. A. H. (2025). Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. *Discover Internet of Things*, 5(1). <https://doi.org/10.1007/s43926-025-00104-w>
- Centre for Data Ethics and Innovation. (2021). *Privacy Enhancing Technologies Adoption Guide*. <https://cdeiuk.github.io/pets-adoption-guide/>
- Chang, W. & Wu, J. (Hrsg.). (2021). *Springer eBook Collection: Bd. 83. Fog/Edge Computing For Security, Privacy, and Applications* (1st ed. 2021). Springer International Publishing; Imprint Springer. <https://doi.org/10.1007/978-3-030-57328-7>
- DIN. (2020). *DIN EN ISO/IEC 29134*.
- ENISA (2016). PETs controls matrix: A systematic approach for assessing online and mobile privacy tools. <https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools>
- ENISA (2022). DATA PROTECTION ENGINEERING: From Theory to Practice. <https://www.enisa.europa.eu/publications/data-protection-engineering>
- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. <http://data.europa.eu/eli/reg/2016/679/oj>
- European Parliament & Council of the European Union. (2023). *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854>
- European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. <http://data.europa.eu/eli/reg/2024/1689/oj>
- European Commission. (2023). *Study on the economic potential of far edge computing in the future smart Internet of Things*. <https://op.europa.eu/en/publication-detail/-/publication/ff35c457-8f3b-11ee-8aa6-01aa75ed71a1>

- Future of Privacy Forum. (2024). *Repository for Privacy Enhancing Technologies (PETs) - Future of Privacy Forum*. <https://fpf.org/global/repository-for-privacy-enhancing-technologies-pets/>
- Gerber, N., Gerber, P. & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Heurix, J., Zimmermann, P., Neubauer, T. & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1–17. <https://doi.org/10.1016/j.cose.2015.05.002>
- ISACA. (2024). *Exploring Practical Considerations and Applications for Privacy Enhancing Technologies*. <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies>
- ISO. (2022). *ISO/IEC 27557:2022*. ISO.
- ISO. (2024). *ISO/IEC 29100:2024*. ISO.
- Janakiraman, R., Lim, J. H. & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing*, 82(2), 85–105. <https://doi.org/10.1509/jm.16.0124>
- Klymenko, A., Meisenbacher, S. & Matthes, F. (2025). *Privacy-Enhancing Technologies: A Comprehensive Guide for Non-technical Practitioners*.
- Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G. & Krishnamachari, B. (2024). *A Survey on the Applications of Zero-Knowledge Proofs*. <https://doi.org/10.48550/arXiv.2408.00243>
- Noble, A. (2023). *From privacy to partnership*. The Royal Society. <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf>
- OECD (2023). Emerging privacy enhancing technologies: Maturity, opportunities and challenges. https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
- Riedel, P., Schick, L., Schwerin, R. von, Reichert, M., Schaudt, D. & Hafner, A. (2024). Comparative analysis of open-source federated learning frameworks - a literature-based survey and review. *International Journal of Machine Learning and Cybernetics*, 15(11), 5257–5278. <https://doi.org/10.1007/s13042-024-02234-z>
- Scherenberg, F. von, Hellmeier, M. & Otto, B. (2024). Data Sovereignty in Information Systems. *Electronic Markets*, 34(1). <https://doi.org/10.1007/s12525-024-00693-4>
- Schiffner, S. (2015a). Privacy and Data Protection by Design. <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>
- Schiffner, S. (2015b). *Readiness analysis for the adoption and evolution of privacy enhancing technologies: Methodology, pilot assessment, and continuity plan : approved, version 1.0, public*. ENISA. <https://doi.org/10.2824/614444>
- Sheikh, A. M., Islam, M. R., Habaebi, M. H., Zabidi, S. A., Bin Najeeb, A. R. & Kabbani, A. (2025). A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies. *Future Internet*, 17(4), 175. <https://doi.org/10.3390/fi17040175>

Stock, J., Petersen, T., Behrendt, C.-A., Federrath, H. & Kreuzburg, T. (2022). Privatsphärefreundliches maschinelles Lernen. *Informatik Spektrum*, 45(3), 137–145.
<https://doi.org/10.1007/s00287-022-01440-9>

United Nations. (2023). *United Nations Guide on Privacy-Enhancing Technologies for Official Statistics*. https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf

Xu, R., Baracaldo, N. & Joshi, J. (2021, 10. August). *Privacy-Preserving Machine Learning: Methods, Challenges and Directions*. <http://arxiv.org/pdf/2108.04417v2>
<https://doi.org/10.48550/arXiv.2108.04417>

Anhang A – Detaillierte Übersicht zu PET

Anonymisierung und Pseudonymisierung

Mittels Anonymisierung werden Attribute aus Datensätzen entfernt, um eine Identifizierung von betroffenen Personen zu verhindern. Durch Anonymisierung wird die Ununterscheidbarkeit von Entitäten innerhalb eines Datensatzes gewährleistet. Im Rahmen der Pseudonymisierung werden Eigenschaften, wie beispielsweise Identifikatoren, durch Pseudonyme ausgetauscht. Während effektiv anonymisierte Daten nicht mehr als personenbezogene Daten gelten, können pseudonymisierte Daten oftmals unter Verwendung zusätzlicher, separater Informationen einer natürlichen Person zugeordnet werden und gelten somit weiterhin als personenbezogen. Bei der Anonymisierung ergibt sich oftmals ein Interessenskonflikt zwischen der Nützlichkeit der Daten und dem Umfang des Schutzes. Techniken zur Anonymisierung und Pseudonymisierung werden in der Regel während der Datenaufbereitungsphase auf Daten „at-Rest“ angewendet. Anonymisierungstechniken umfassen die Entfernung oder Generalisierung bestimmter Attribute eines Datensatzes. Zu den Techniken der Anonymisierung gehören:

- k-Anonymität: Informationen zu jeder betroffenen Entität sind, beispielsweise durch Clustering, von mindestens $k-1$ anderen Entitäten innerhalb des Datensatzes nicht unterscheidbar. Dies schützt vor allem die Identität der Entität.
- l-Diversität: Erweitert k-Anonymität, indem es die Cluster so bildet, dass das sensible Attribut sich innerhalb der Klasse l-Mal unterscheidet. Dies verhindert, dass durch die Zugehörigkeit zu einem Cluster die Eigenschaft der sich im Cluster befindlichen Person erschlossen werden kann.
- t-Nähe: Erweitert l-Diversität dadurch, dass sich die Werteverteilung innerhalb eines Clusters nah an der Werteverteilung der Grundgesamtheit (t) befindet. Somit wird die Identifizierung weiter erschwert.

Zur Pseudonymisierung sind unter anderem folgende Vorgehensweisen denkbar:

- Digitale Pseudonyme: Nutzende wählen ihre eigenen Pseudonyme oder erhalten zufällig generierte Zeichenfolgen als Pseudonym.
- Kryptografische Methoden: Kryptografische Methoden wie beispielsweise Hash-Funktionen werden zur Erzeugung der Pseudonyme genutzt.
- Vertrauenswürdige Dritte: Eine Drittpartei wird mit der Geheimhaltung des Schlüssels betraut, der digitale Pseudonyme mit den wahren Identitäten ihrer Nutzenden verknüpft.

Synthetische Daten

Synthetische Daten sind (maschinell) generierte Daten, welche die statistischen Eigenschaften der Grundgesamtheit nachahmen, ohne die Privatsphäre der Datenerzeugenden zu verletzen. Zur Erzeugung von synthetischen Daten wurden historisch statistische Modelle wie beispielsweise Monte Carlo-Simulationen genutzt. Heutzutage kommen vermehrt Verfahren des maschinellen Lernens zur Verwendung. Diese lernen die zugrundeliegende Verteilung und geben darauf basierend erzeugte Daten aus. Synthetische Daten können vollständig synthetisch (alle Variablen

werden durch ein Modell generiert), teilweise synthetisch (nur einige Variablen werden synthetisiert) oder hybrid (aus dem realen Satz und einem vollständig synthetischen Satz generiert) sein.

Federated-Learning

Federated-Learning ist ein kollaborativer Ansatz des maschinellen Lernens. Ein globales KI-Modell wird initial durch einen zentralen Server bereitgestellt und auf verschiedene Knoten/Clients (z.B. Server, Edge-Geräte, Smartphones) verteilt. Diese trainieren das Modell lokal mit eigenen Daten und übertragen lediglich aktualisierte Modellparameter an den zentralen Server. Der Server aggregiert diese, etwa per gewichteter Mittelwertbildung, und aktualisiert das globale Modell. Dieser Zyklus kann endlos weitergeführt werden, erreicht im Idealfall jedoch Konvergenz. Federated-Learning existiert in Varianten wie dem geräteübergreifenden Lernen mit vielen Endgeräten oder siloübergreifenden Lernen mit wenigen, leistungsstarken Knoten, die Daten bereits in der eigenen Umgebung aggregieren (z.B. Kliniken, Banken). Zudem unterscheiden sich die Ansätze „horizontales Federated-Learning“, bei dem die Daten der Clients dieselben Attribute, allerdings andere Entitäten umfassen, und „vertikales Federated-Learning“, bei dem die Clients über Daten zu gleichen Entitäten verfügen, die jedoch verschiedene Attribute beinhalten. Die bekanntesten Beispiele für Federated-Learning sind die Vorhersage des nächsten Wortes, Autokorrektur und Emoji-Vorschläge, die auf Millionen von Smartphones trainiert und ausgeführt werden.

Secure Multi-Party-Computation

Secure Multi-Party-Computation ist ein kryptografischer Ansatz, der es mehreren, sich gegenseitig misstrauenden Parteien ermöglicht, gemeinsam Berechnungen durchzuführen, ohne dabei ihre jeweiligen Eingabedaten offenzulegen. Alle Parteien erhalten dabei lediglich das Resultat der Berechnungen. Die individuellen Inputs der Beteiligten bleiben während des gesamten Prozesses vertraulich. Konkret werden zur Umsetzung von Secure Multi-Party-Computation Protokolle wie Secret-Sharing verwendet. Die Eingabe der an der gemeinsamen Berechnung Beteiligten wird in Teile zerlegt und auf die anderen Parteien verteilt, sodass keine Partei allein auf alle Informationen zurückgreifen kann. Die Parteien führen anschließend ihre individuellen Berechnungen durch und fügen das Berechnungsergebnis am Ende zusammen. Das Verfahren benötigt entsprechend eine Mindestanzahl an teilnehmenden Parteien. Der Einsatz von Secure Multi-Party-Computation ist derzeit noch ein Forschungsfeld. Derzeitige Herausforderungen sind einerseits die niedrige Performance und andererseits die Beschränkung auf dedizierte Rechenverfahren.

Homomorphe Verschlüsselung

Homomorphe Verschlüsselung ist ein kryptografisches Verfahren, das die Durchführung von Berechnungen auf verschlüsselten Daten erlaubt, ohne diese zuvor entschlüsseln zu müssen. Während herkömmliche Verschlüsselungsmethoden zwar die Speicherung und Übertragung sensibler Informationen absichern, erfordern sie für Weiterverarbeitung, Analyse oder Machine-Learning-Anwendungen die Entschlüsselung der Daten. Dadurch entsteht ein Risiko für den Datenschutz und die Vertraulichkeit, da Unbefugte während der Verarbeitung auf die Rohdaten zugreifen können. Die vollständige homomorphe Verschlüsselung ermöglicht die Ausführung beliebiger mathematischer Operationen direkt auf dem Verschlüsselungstext. Nach Abschluss der Berechnungen kann das verschlüsselte Ergebnis entschlüsselt werden, um das reale Ergebnis zu erhalten. Dieses entspricht demselben Output, der bei einer Berechnung mit den entschlüsselten Daten generiert werden würde. Homomorphe Verschlüsselung lässt sich für vielfältige Analysen nutzen,

insbesondere für solche, die sich als Polynomfunktionen ausdrücken lassen, sowie für ausgewählte KI-Anwendungen. Es existieren jedoch auch Herausforderungen, wie ein erhöhter Rechenaufwand und eingeschränkte Genauigkeiten der Berechnungen (Stock et al., 2022).

Zero-Knowledge-Proofs

Zero-Knowledge-Proofs sind ein kryptografisches Konzept, das es einer Partei (Prover) ermöglicht, einer anderen Partei (Verifier) die Gültigkeit einer Aussage zu beweisen, ohne dabei Informationen über die zugrundeliegenden Daten selbst preiszugeben. Zero-Knowledge-Proofs schützen Daten in erster Linie während der Verarbeitung und Übertragung, indem sie die Offenlegung von Informationen minimieren. Zur Erstellung von Zero-Knowledge-Proofs existieren verschiedene mathematische Verfahren, die sich grundsätzlich in zwei Kategorien aufteilen. Bei interaktiven Zero-Knowledge-Proofs ist eine mehrfache Kommunikation zwischen dem Prover und dem Verifier erforderlich. Der Verifier stellt dabei dem Prover in mehreren Runden Anfragen, die dieser beantworten muss, um die Glaubwürdigkeit des Nachweises zu sichern. Im Gegensatz dazu benötigen nicht-interaktive Zero-Knowledge-Proofs keine wiederholte Kommunikation zwischen den Parteien. Stattdessen erstellt der Prover einen einmaligen Beweis, der direkt und unabhängig vom Verifier überprüft werden kann (Lavin et al., 2024). Etablierte Einsatzbereiche von Zero-Knowledge-Proofs sind insbesondere das Identitätsmanagement und die Finanzwirtschaft.

Proxys und Onion-Routing

Ein Proxy-Server ist ein Vermittler in einem Computernetzwerk, der Anfragen von Clients entgegennimmt und diese an das Zielsystem weiterleitet. Dabei fungiert der Proxy als Zwischenakteur, der die Kommunikation steuert und die Identität der Anfragequelle verschleiern kann. Der Proxy empfängt die Anfrage, stellt eigenständig die Verbindung zum Ziel her und leitet die Antwort zurück an den Client. Somit kann der Proxy beispielsweise dazu genutzt werden, um die IP-Adresse als Identitätsmerkmal zu verbergen. Es existieren verschiedene Typen von Proxys. Zum Schutz der Privatsphäre sind vor allem anonyme Proxys und hoch-anonyme Proxys relevant. Anonyme Proxys verbergen die IP-Adresse des Nutzers, während hoch-anonyme Proxys darüberhinausgehend verschleiern, dass sie selbst als Proxy fungieren.

Onion-Routing ist eine Netzwerktechnik, die verbindungsorientierte, bidirektionale Kommunikation über eine Kette von Relays (Onion-Router) leitet, um Absender und Ziel voneinander zu entkoppeln und so viele Formen der Netzwerkverkehrsanalyse zu erschweren. Im Kern ersetzt Onion-Routing die direkte Verbindung durch eine Serie aus Einstiegsknoten (Guard/Entry), Zwischenknoten und Austrittsknoten (Exit), den sogenannten Onion-Routern. Die Nachrichten werden vom Client schichtweise verschlüsselt, analog zu den Schalen einer Zwiebel. Jeder Knoten entfernt ausschließlich seine eigene Schicht, kennt nur den unmittelbaren Vorgänger und den Nachfolger und hat weder Zugriff auf die vollständigen Inhalte noch auf die gesamte Route. Daher weiß jeder Router nur, von wem er die Daten erhielt und wohin er sie sendet. So bleibt sowohl der Inhalt der Kommunikation als auch der Kommunikationspartner vor Überwachung geschützt. Onion-Routing bietet gegenüber konventionellen Verschlüsselungsmethoden den Vorteil, dass ein kompromittierter einzelner Router nicht allein Zugriff auf die gesamte Kommunikation erhält. Bestehende Internetdienste und Anwendungen müssen nicht angepasst werden, um Onion-Routing zu nutzen.

Hardware-Sicherheitsmodule

Hardware-Sicherheitsmodule sind spezialisierte Hardware, die in der Lage ist, kryptografische Schlüssel sicher zu generieren, zu speichern und zu verwalten. Diese Schlüssel werden dazu verwendet, Datenverschlüsselung und -entschlüsselung zu betreiben und digitale Signaturen und Zertifikate zu erstellen. Somit können Hardware-Sicherheitsmodule einen entscheidenden Beitrag leisten, geistiges Eigentum und weitere sensible Daten vor unerlaubten Zugriffen zu schützen. Konkret generieren Hardware-Sicherheitsmodule Schlüssel direkt innerhalb ihres Kryptoprozessors. Anwendungen können auf die kryptografischen Funktionen mittels dedizierter APIs zugreifen und diese nutzen, um Daten innerhalb der sicheren Umgebung zu ver- oder entschlüsseln. Die kryptografischen Funktionen und Algorithmen sind dabei nur dem Hersteller bekannt. Hardware-Sicherheitsmodule sind manipulationssicher gestaltet. Daher können physische Zugriffe auf die Geräte entweder verhindert werden oder zu einer Entfernung sensibler Daten führen. Hardware-Sicherheitsmodule werden vor allem in Bereichen mit hohen Compliance-Anforderungen wie dem Finanzwesen und der Telekommunikationsindustrie eingesetzt. Zudem werden diese oftmals mit anderen PET kombiniert, um bestehende Sicherheitskonzepte zu verstärken.

Trusted-Execution-Environments

Trusted-Execution-Environments sind spezialisierte Hardware-Architekturen, die es ermöglichen, Anwendungen isoliert vom restlichen System auszuführen. Ihr grundlegendes Ziel ist es, eine vertrauenswürdige Umgebung zu schaffen, in der Daten und Prozesse selbst dann vor unautorisiertem Zugriff, Manipulation oder Überwachung geschützt sind, wenn der Host oder das zugrunde liegende Betriebssystem kompromittiert wurden. Trusted-Execution-Environments ermöglichen somit das sogenannte Confidential-Computing. Konkret werden für Trusted-Execution-Environments spezialisierte CPU-Lösungen benötigt, die derzeit nur von wenigen Herstellern angeboten werden können. Trusted-Execution-Environments nutzen dedizierten On-Chip-Speicher und Funktionen der virtuellen Speicherverwaltung, um zu verhindern, dass andere auf den Speicherbereich der Trusted-Execution-Environments zugreifen können. Zudem nutzen Trusted-Execution-Environments Hardware-Verschlüsselungen, um Daten zu ver- und entschlüsseln, die zwischen der CPU und dem System Speicher verschoben werden müssen. Mittels Remote-Attestation können Nutzende die Integrität und Authentizität des Codes und der Daten, die in einer Trusted-Execution-Environment ausgeführt werden, überprüfen. Die Hardware bildet entsprechend den Vertrauensanker, während Softwarekomponenten sicherheitsrelevante Prozesse, wie Verschlüsselung, Authentifizierung und Attestierung, steuern. Neben der Gewährleistung von Datenschutz durch die Verhinderung der Einsicht für nicht-autorisierte Parteien inklusive den Betreibern der Umgebung stellen Trusted-Execution-Environments somit auch die Integrität von Daten und Code sicher.