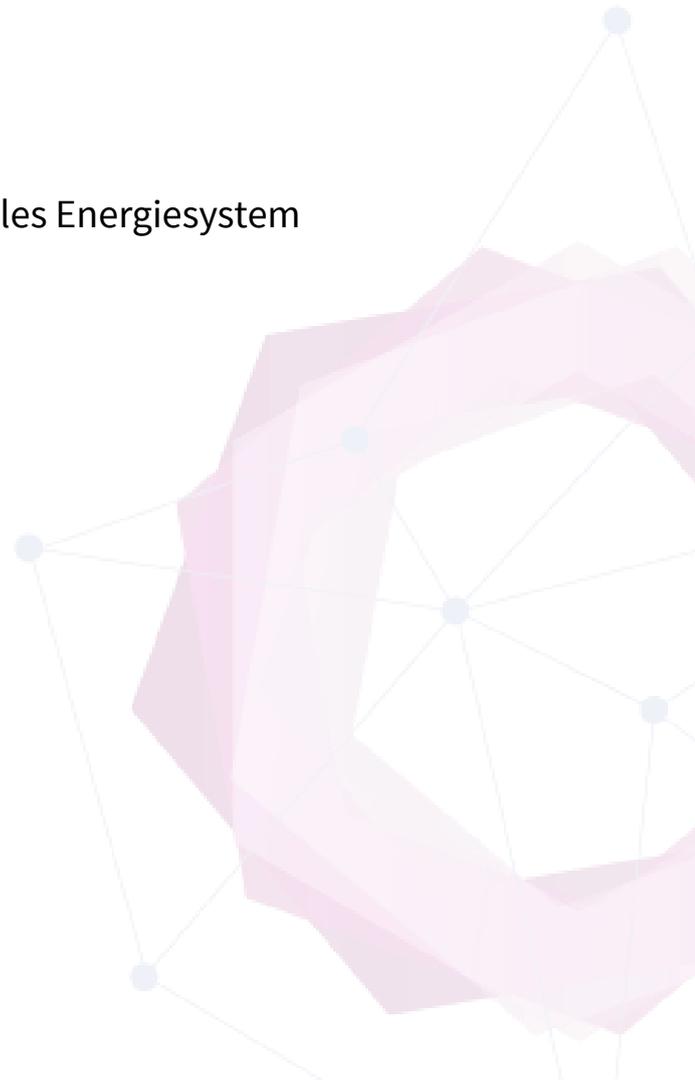




STUDIE

EnerComputing

Cloud- und Edge-Technologien für ein dezentrales Energiesystem



Impressum

Herausgeber:

Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699
E-Mail: info@dena.de
Internet: www.dena.de

Autorinnen und Autoren:

Mehdi Akbari Gurabi, Fraunhofer FIT
Charukeshi Joglekar, Fraunhofer FIT
Robin Williams, Fraunhofer FIT
Bianca Biermann, dena
Anna Poblocka-Dirakis, dena
Benedikt Pulvermüller, dena
Jasmin Wagner, dena

Stand:

06/2024

Bildnachweis:

Shutterstock/Zinetron

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2024): „EnerComputing – Cloud- und Edge-Technologien für ein dezentrales Energiesystem“

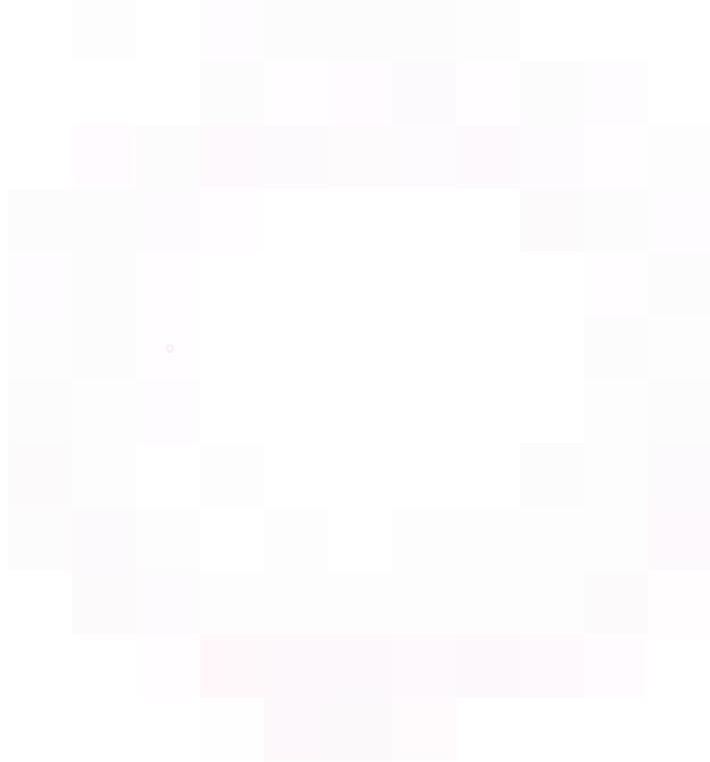


Bundesministerium
für Wirtschaft
und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

1	Einleitung und Motivation.....	5
2	Stand der Technik und Weiterentwicklung	7
2.1	Architektur und Komponenten	7
2.2	Vor- und Nachteile	10
2.3	Eigenschaften im Kontext des Energiesystems	13
2.4	Sicherheitsaspekte.....	14
2.5	Vergleich der Technologien	16
2.5.1	Ökonomische Aspekte	18
2.5.2	Ökologische Aspekte.....	19
2.5.3	Technische und organisatorische Aspekte.....	20
2.5.4	Zusammenfassung.....	23
2.6	Weiterentwicklung.....	23
2.6.1	Standardisierung.....	24
2.6.2	Datenaufkommen und Latenzen.....	24
2.6.3	Energieverbrauch.....	25
2.6.4	Kommunikationstechnologien.....	26
2.6.5	Disaggregation und Modularität von Edge-Komponenten	26
3	Anwendungsfelder in der Energiewirtschaft	27
3.1	Anwendungsfälle	27
3.1.1	Intelligente Messsysteme (iMSys) und Advanced Metering Infrastructure (AMI)	28
3.1.2	Betrieb von Energienetzen.....	29
3.1.3	Sektorenkopplung	33
3.1.4	Lokale Energiemärkte	35
3.2	Technische Bewertung	36
4	Regulatorik und Einschätzungen aus der Energiebranche	38

4.1.1	Regulatorischer Rahmen	38
4.1.2	Hürden für die Integration von Cloud und Edge Computing.....	40
5	Fazit und Handlungsempfehlungen	42
	Literaturverzeichnis	45
	Abbildungsverzeichnis.....	51
	Tabellenverzeichnis.....	52
	Abkürzungen.....	53
	Glossar.....	55



1 Einleitung und Motivation

Das Energiesystem wandelt sich von einer konventionellen Top-down-Struktur mit wenigen zentralen Großkraftwerken hin zu einer Struktur mit einer hohen Anzahl von räumlich verteilten und teilweise fluktuierenden Erzeugern Erneuerbarer Energien, die zudem in unterschiedliche Netzebenen einspeisen. Die Komplexität des dezentralen Energiesystems erfordert einen hohen Koordinierungsaufwand, der neue Methoden und digitale Werkzeuge im Netzbetrieb benötigt. Um diese Herausforderungen zu bewältigen, braucht es innovative Digitalisierungskonzepte, die die strategische Nutzung von Daten, Services und Anwendungsinformationen ermöglichen. Entsprechende Digitalisierungskonzepte sollten dabei entlang der gesamten Energieversorgungskette gedacht werden, um neben dem zuverlässigen Netzbetrieb auch innovative Geschäftsmodelle zu ermöglichen. Ein wichtiger Ansatz, um die datentechnische Integration von Sensoren, Anlagen sowie Wartungs- und Geschäftsprozessen vom Netzbetreiber bis hin zur Endverbraucherschaft zu ermöglichen, liegt in digitalen Schlüsseltechnologien wie Edge Computing (EC) und Cloud-Computing (CC).

In der vorliegenden Studie werden die Grundlagen von CC und EC beschrieben, ihre Eignung für potenzielle Anwendungsfälle im Energiesystem wird diskutiert und zu erwartende Hemmnisse und Herausforderungen werden benannt. Dabei liegt der Fokus auf den Funktionalitäten und den Vor- und Nachteilen der einzelnen Technologien sowie möglichen Kombinationen, um den größtmöglichen Nutzen für den Energiesektor zu erzielen.

Die Arbeiten umfassen eine Recherche aktueller wissenschaftlicher Erkenntnisse sowie den Austausch mit Branchenvertreterinnen und -vertretern und Technologielieferanten. Im Ergebnis bietet diese Studie eine Informationsbasis für Akteure im Energiesektor hinsichtlich der Fähigkeiten und Limitationen von CC und EC und soll als Ausgangspunkt für weitere Analysen und Projekte dienen.

CC ermöglicht zahlreichen Unternehmen unterschiedlicher Größenklassen mittels zentral errichteter und verwalteter Infrastrukturen IT-Dienstleistungen zu nutzen und selbst anzubieten. Durch die flexible und skalierbare Zuteilung von Rechenkapazität können sie bedarfsgerecht und kosteneffizient zur Verfügung gestellt werden. Wichtig ist dabei, dass sich die Cloud-Dienstleistungen an den Bedarfen der Kunden orientieren und sowohl Sicherheit als auch Flexibilität hinsichtlich der Funktionen und der Integration von Drittanwendungen bieten. Leistungsstarke, zentrale Rechenzentren auf Cloud-Basis sind beispielsweise eine wesentliche Voraussetzung für einen von künstlicher Intelligenz (KI) gestützten Netzbetrieb, das enorme Datenmengen verarbeiten und daraus die optimalen Maßnahmen ableiten muss.

EC ermöglicht durch lokale Datenverarbeitung eine schnellere Analyse vor Ort, wodurch Latenzzeiten verkürzt und Echtzeitreaktionen ermöglicht werden. Die direkte Kommunikation zwischen Edge-Knoten minimiert dabei den Bedarf an Datenübertragung in die Cloud, was Netzwerklast und Datenpaketverluste verringern kann. Cybersicherheit profitiert von verteilter Datenhaltung, da der Zugriff auf große Datenmengen eingeschränkt ist und potenzieller Schaden minimiert wird. Allerdings bringt der Betrieb von Edge-Systemen einen höheren Aufwand in Bezug auf die Planung von erforderlichen Rechenkapazitäten, räumliche Gegebenheiten und die Wartung mit sich.

Das komplexe Zusammenwirken des vielschichtigen Energiesystems wird hoch automatisierte, datenbetriebene Anwendungen erfordern. Die Kombination der Stärken von CC als hochverfügbare, skalierbare und starke Rechenleistung mit denen von EC, das schnelle, anwendungsnahe und steuerungsfähige Sensorik und Aktorik bietet, kann diesen Erfordernissen gerecht werden.

Neben den offenkundigen technischen Unterschieden bezüglich Rechenleistung, Skalierbarkeit und Antwortgeschwindigkeit gibt es noch weitere ökonomische, ökologische und organisatorische Aspekte, die bei der Wahl einer IT-Lösung von erheblicher Relevanz sind. Unterschiedliche Akteure im Energiesystem werden an einer Vielzahl von Anwendungen in Bereichen wie intelligente Messsysteme, Betrieb aktiver Energienetze, Sektorenkopplung und lokale Energiemärkte mitwirken und somit auch diverse Anforderungen an die Systeme stellen. Dazu gehören die Update-Fähigkeit und Anpassbarkeit, die Schnelligkeit der Ausbringung und Wartung sowie Möglichkeiten des kollaborativen Zugriffs – Punkte, die für CC sprechen. Demgegenüber bestehen Anforderungen an den Datenschutz, die Datenübertragung, die Kontrolle über Infrastrukturen und die Integration hochspezialisierter Anwendungen, die durch Edge-Lösungen stark verbessert werden können.

Wie alle Technologien unterliegen auch CC und EC einem stetigen Wandel. Im Energiesystem entstehen neue Anforderungen, insbesondere bezüglich Datenaufkommen und Latenzen. Gleichzeitig führen Bemühungen in den Bereichen Standardisierung, Energieeffizienz sowie Informations- und Kommunikationstechnologie zu einer Erweiterung der verfügbaren Fähigkeiten und Mittel. Während Industrie- und Forschungsprojekte bereits heute neue Möglichkeiten ausschöpfen, wird klar, dass ein flächendeckender Einsatz und eine breite Akzeptanz nur durch fähige Kommunikationsinfrastrukturen (FTTx, 5G), Interoperabilität (Standards, Schnittstellen) sowie technologische (Cybersicherheit, Datensouveränität) und rechtliche Sicherheit (Zertifizierungen) zustande kommen werden. Nicht zu unterschätzen ist dabei der Faktor Mensch, da Verbraucherinnen und Verbraucher in ihrer Rolle durch neue Werkzeuge und Dienstleistungen gestärkt werden müssen, aber auch Fachpersonal im Energiesektor vor neue Aufgaben gestellt wird.

2 Stand der Technik und Weiterentwicklung

In diesem Kapitel werden zunächst die Grundlagen der beiden betrachteten Technologiekomplexe getrennt dargestellt. Für beide Technologien erfolgen zunächst eine Beschreibung der zugrundeliegenden Konzepte und Architekturen, der identifizierten Vor- und Nachteile und der Eigenschaften bezogen auf den Einsatz im Energiesektor sowie ein Exkurs zum Thema Cybersicherheit. Im Anschluss findet eine gemeinsame, vergleichende und bewertende Betrachtung der Cloud- und Edge Technologien unter Berücksichtigung von wesentlichen Aspekten aus den Teilbereichen Ökonomie, Ökologie und Technik-Organisation statt. Abschließend erfolgt ein Ausblick auf erwartete Weiterentwicklungen, die voraussichtlich einen Einfluss auf den Einsatz von Cloud- und Edge Technologien im Energiesystem haben werden.

2.1 Architektur und Komponenten

a) Cloud-Computing

CC beschreibt das Konzept, Berechnungen in eine abstrahierte Umgebung zu verlagern. Dies ermöglicht es einerseits, größere Berechnungen trotz begrenzter lokaler Hardware-Ressourcen durchzuführen, und andererseits, größere, leistungsfähige Rechenkomponenten aufgrund der Nutzung durch mehrere Clients besser auszulasten. Unternehmen ermöglicht es, auf eine flexible und skalierbare Infrastruktur zuzugreifen, ohne physische Hardware vor Ort betreiben zu müssen.

Die Geschichte des CC reicht zurück in die 1960er Jahre, als die Idee von „Zeit-Sharing-Computern“ entstand, bei denen mehrere Benutzer gleichzeitig auf einen zentralisierten Computer zugreifen konnten. In den 1990er Jahren entwickelten sich Webdienste, die Anwendungen über das Internet bereitstellten. Der Begriff „Cloud-Computing“ wurde in den 2000er Jahren populär, als die technologischen Fortschritte in den Bereichen Virtualisierung, Breitband-Internet und skalierbare Speicherlösungen es ermöglichten, Ressourcen flexibel bereitzustellen und zu nutzen.

Virtualisierung

Physische Ressourcen, wie Server oder Speicher, werden abstrahiert und in virtuelle Instanzen umgewandelt. Dadurch können mehrere unabhängige virtuelle Umgebungen auf einem einzigen physischen Gerät koexistieren. Dies ermöglicht eine effizientere Ressourcennutzung, die flexible Skalierbarkeit und eine verbesserte Isolation zwischen verschiedenen Anwendungen oder Nutzern in der Cloud.

Containern

Im Gegensatz zur Virtualisierung findet die Abstrahierung nicht auf Hardware-Ebene statt, sondern über der Betriebssystemebene. Container enthalten neben der eigentlichen Software weitere notwendige Bibliotheken, sind aber insgesamt leichtgewichtiger und können mit einer entsprechenden Container-Engine auf unterschiedlichen Betriebssystemen ausgeführt werden.

Quellen Infobox^{1,2}

Durch die Weiterentwicklung abstrahierender Technologien, wie zum Beispiel Containern, wurde der Einsatz von CC zusätzlich vereinfacht, da Anwendungen nicht an eine Betriebssystemumgebung gebunden sind und anbieterunabhängig mit geringem Konfigurationsaufwand eingesetzt werden können.

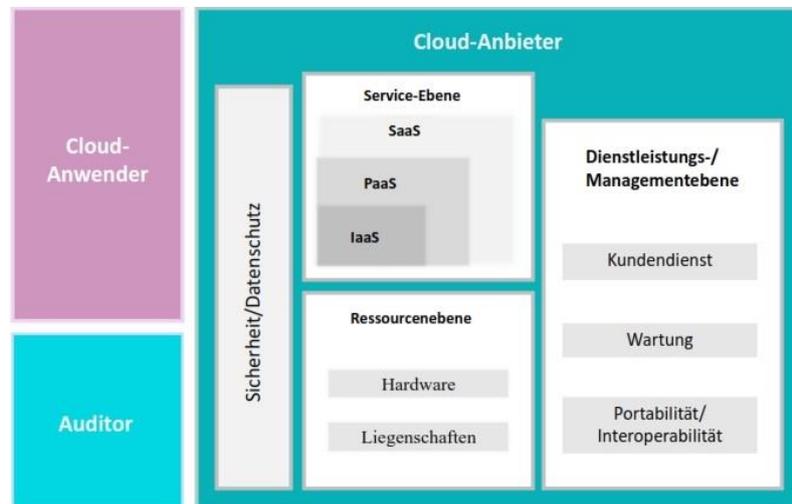


Abbildung 1: Architektur eines Cloud-Dienstes, in Anlehnung an das Cloud Computing Reference Model der NIST³

Wesentliche Aspekte und Charakteristiken eines Cloud-Dienstes sind in Abbildung 1 dargestellt. Aus Sicht der Nutzerschaft liegen die augenscheinlichsten Unterschiede in der Service-Ebene. Die angebotenen Leistungen und zugrundeliegenden Architekturen unterscheiden sich in dem Maß an Kontrolle, das den Kunden zur Verfügung gestellt wird, aber gleichzeitig im Verwaltungsaufwand, der den Nutzern abgenommen wird. In der Service-Ebene lassen sich folgende Dienstleistungs- und Bereitstellungsmodelle beschreiben:

Infrastructure as a Service (IaaS): Grundlegende IT-Infrastrukturen wie virtuelle Maschinen, Speicher und Netzwerke werden vom Anbieter in der Cloud bereitgestellt. Das tatsächliche Verbinden der Ressourcen obliegt jedoch den Kunden. Dies erlaubt die maximale Kontrolle über die Ausführungsplattform im Rahmen von CC, bringt allerdings auch den höchsten Verwaltungsaufwand mit sich. Ein Beispiel hierfür ist Amazon Web Services (AWS) mit EC2 als Rechenkomponente und S3 als Speicherkomponente.

Platform as a Service (PaaS): Das Verwalten der Infrastruktur kann von dem Dienstleister übernommen werden, wodurch das Angebot in das PaaS-Modell fällt. Der Kunde erhält eine Plattform, auf der Entwickler Anwendungen erstellen, ausführen und verwalten können. Dies umfasst oft Middleware, Entwicklungstools und Datenbanken, die benutzte Hardware wird von dem Dienstleister zugeteilt. Die Google App Engine agiert nach diesem Modell.

Software as a Service (SaaS): Bei SaaS werden Anwendungen über das Internet bereitgestellt. Die Nutzerschaft kann auf diese Anwendungen über einen Webbrowser zugreifen, ohne sie auf ihren eigenen Geräten installieren zu müssen. E-Mail-Dienste, Office-Suiten und Projektmanagement-Tools sind Beispiele für SaaS.

¹ (Maenhaut, et al. 2020)

² (Buchanan 2019)

³ (Liu, et al. 2011)

Public Cloud: Hierbei werden Cloud-Services von einem Drittanbieter für die allgemeine Öffentlichkeit bereitgestellt. Die Infrastruktur wird gemeinsam genutzt und ist über das Internet zugänglich. Beispiele hierfür sind GoogleDrive, OneDrive, Grafana Cloud oder iCloud.

Private Cloud: In einer privaten Cloud werden Cloud-Ressourcen ausschließlich für eine einzelne Organisation bereitgestellt. Die Infrastruktur kann intern oder von einem Drittanbieter gehostet werden.

Hybrid Cloud: Dieses Modell kombiniert Elemente der öffentlichen und der privaten Cloud. Unternehmen können Daten und Anwendungen zwischen den beiden Umgebungen verschieben, um die Flexibilität zu maximieren.^{4,5}

Darüber hinaus sind weitere erforderliche Komponenten eines Cloud-Dienstes die eigentliche Hardware und sichere, geeignete Räumlichkeiten. Ebenfalls für die Nutzerschaft von großer Relevanz sind der Kunden- und TechniksUPPORT, Portierungs- und Interoperabilitätsdienste sowie die Wartung der Infrastrukturen, die durch Dienstleistungs- und Managementprozesse des Cloud-Anbieters sichergestellt werden. Wesentlich für alle Beteiligten ist die Implementierung von Sicherheits- und Datenschutzmaßnahmen, die nicht zuletzt oft durch externe Audits und Zertifizierungen belegt werden sollten.

b) Edge Computing

EC ist ein Verfahren, bei dem Daten, Services und Anwendungsinformationen unmittelbar an die logische „Randstelle“ (Edge) eines Netzwerks verlagert werden. Während CC auf zentralisierte Rechenzentren setzt, in denen Daten und Anwendungen auf entfernten Servern verarbeitet werden, konzentriert sich EC auf die dezentrale Verarbeitung von Daten direkt an der Quelle, also näher an den Endnutzerinnen und Endnutzern oder den Geräten. Dabei liegt der Schwerpunkt auf der Minimierung von Latenzzeiten und der Bewältigung von Echtzeitanforderungen. Die Anfänge des EC liegen in den 1990er Jahren, als regionalisierte Server eingesetzt wurden, um Nutzeranfragen im Internet möglichst anfragenah zu bedienen. Dies hatte zum Ziel, Überlastungen von Servern und Kommunikationsinfrastrukturen zu vermeiden.⁶

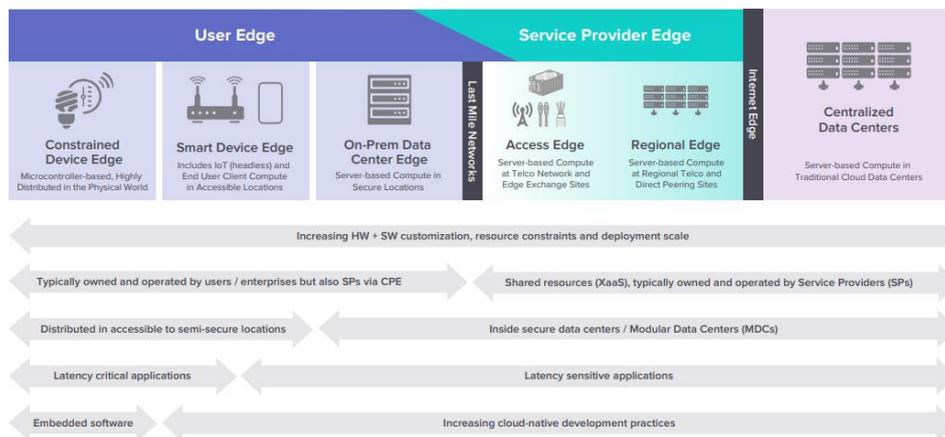


Abbildung 2: Edge Computing Architecture (LF Edge 2023)

EC umfasst jegliche Anwendung von Berechnungen, die nah an der Anfragequelle stattfinden. Dies kann z.B. auf der Sensor-Hardware selbst geschehen.⁷ In Abbildung 2 wird eine grobe Taxonomie der Edge-Architektur

⁴ (IBM 2023)

⁵ (IBM 2017)

⁶ (Dilley, et al. 2002)

⁷ (Cao, et al. 2020)

beschrieben. Ausgehend von einem traditionellen Cloud-Rechenzentrum liegt ein Übergangsbereich (Anbieter-Edge) vor mit kleineren regionalisierten Rechenzentren sowie größeren Telekommunikationsserver-Infrastrukturen mit eigenen Rechenkapazitäten. Energienetztopologisch würden diese beispielsweise in Umspannwerken liegen. Ab dort beginnt netzwerktechnisch die „letzte Meile“ und die sogenannte „Nutzer-Edge“. Teil dieser letzten Meile sind demnach etwaige Datenkonzentratoren und Rechenkapazitäten in Ortsnetzstationen. In dieser Position können Berechnungen mit den Daten mehrerer Messstellen vorgenommen werden, ohne den Datentransport zu und die Antwort von einem zentralen System abwarten zu müssen. Weiter entlang der Versorgungsinfrastruktur hin zu den Endverbraucherinnen und -verbrauchern liegen die Geräte der Verbrauchsmessstellen, Steuerungssysteme und Smart-Home-Komponenten. Diese Geräte ermöglichen – begrenzt – schnelle Analysen und Steuerbefehle.⁸

Edge-Systemen ist die Eignung für zeitkritische Prozesse inhärent, da sie per Definition nah an der Grenze zwischen digitaler und physischer Infrastruktur platziert sind. Nicht zuletzt aufgrund dieser Verteilung und anfragenahen Installation müssen Edge-Systeme in einer größeren räumlichen Ausdehnung betrachtet werden. Dies äußert sich auch in der heterogenen Aufstellung der Geräte, etwa an öffentlich zugänglichen Orten (z.B. ein geteilter Zählerschrank im Mehrfamilienhaus) oder zugangsbeschränkten Orten (z.B. Ortsnetzstation) und weniger in speziell gesicherten Räumen mit anforderungsgerechten Sicherheitsvorkehrungen (wie bei größeren Rechenzentren). Durch die limitierte Rechenkapazität und feste, langjährige Installation ergibt sich auch eine zunehmende Spezialisierung der Hard- und Software.

c) Zusammenspiel von Cloud und Edge

Die Architekturen von CC und EC unterscheiden sich grundlegend und ergänzen sich auf diese Weise auch sehr gut. Während große Datenmengen von vielen Sensoren und anderen Quellen, beispielsweise für systemweite Machine-Learning-Ansätze, in leistungsstarken Cloud-Rechenzentren verarbeitet werden, lassen sich schnelle, zeitkritische Prozesse lokal in der Edge durchführen. Durch die selektive Weitergabe von relevanten Daten aus der EC an ein zentrales System können die zentralen Entscheidungsprozesse verbessert und präzisiert werden. Ebenso können neue Erkenntnisse aus der systemweiten Betrachtung genutzt werden, um die Funktionalität der Edge-Komponenten besser abzustimmen und zu optimieren.

2.2 Vor- und Nachteile

Cloud-Systeme bieten für die Anwender wesentliche wirtschaftliche und personelle Vorteile, da die Hardware nicht unternehmensintern beschafft, betrieben und gewartet werden muss. Einschränkungen bestehen ggf. hinsichtlich der nutzbaren Software und mangelnden Kontrolle über die Systeme (u.a. hinsichtlich sicherheitsrelevanter Aspekte).

Die operationellen Vorteile von EC liegen in der höheren Reaktionsfähigkeit und Steuerbarkeit sowie der weiter reichenden Kontrolle über Soft- und Hardware. Sicherheits- und datenschutztechnisch können ebenfalls gewisse Risiken vermieden werden. Demgegenüber stehen jedoch die Ausbringung sowie die Wartung und Instandhaltung von Edge-Systemen, die mit höheren Kosten und personellen Aufwänden verbunden sind.

⁸ (LF Edge 2023)

a) Cloud-Computing

Das Anbieten von Rechenzentrumsleistung an mehrere Kunden erlaubt es Cloud-Anbietern, die Kosten für den Betrieb zu optimieren. Hierzu gehören die Beschaffung leistungseffizienterer Rechenkomponenten und die Optimierung der Kühlsysteme sowie dichtere Speichertechnologie. Server können besser ausgelastet werden, wenn der Dienstleister die Ressourcen der Nutzer gleichmäßig verteilt.⁹ Es besteht daher die Möglichkeit, dass der Energiebedarf eines Rechenzentrums geringer ausfällt als beim Betreiben mehrerer kleinerer Rechenzentren, die den gleichen Bedarf decken. Zudem beinhaltet die konzentrierte Rechenkapazität ein nennenswertes Potenzial für die Abwärmenutzung (vgl. Kapitel 2.6.3).

Aus Nutzersicht werden durch das Mieten von Rechenleistung die Anschaffungskosten von Hardware entweder reduziert oder eliminiert. Auch die laufenden Kosten für die Instandhaltung der Hardware, wie das Ersetzen von Komponenten, oder die Bezahlung von Servicepersonal entfallen.¹⁰ Außerdem ist die Bereitstellung bereits existierender Infrastruktur seitens des Dienstleisters schneller als die eigene Anschaffung, was die Entwicklungszeit und die Time-to-Market reduziert. Im Rahmen von CC werden diese Kosten für Hardware und Betrieb ersetzt durch die Nutzungsgebühr des Dienstleisters, dabei sollten die gebuchten Ressourcen möglichst dem tatsächlichen Bedarf entsprechen. Das Risiko von Preissteigerungen über die Zeit kann nicht ausgeschlossen werden.¹¹

Der zentralisierte Ansatz erlaubt eine höhere Serverzuverlässigkeit und mehr Investitionen in Cybersicherheit. Allerdings kann es zu Ausfällen, auch Downtime genannt, kommen. Alternative Ressourcen sollten für diese Eventualität zumindest eingeplant sein, was Bestandteil eines Service-Level-Agreement (SLA) ist. Das Auslagern der Verantwortung für die Hardware ist einer der Hauptgründe, sich für CC zu entscheiden. Dies beinhaltet aber auch den Verlust von Kontrolle über die Infrastruktur. Maßnahmen gegen potenzielle Sicherheitsrisiken und Datenverlust sollten bedacht werden.

Ein weiteres aus Kundensicht bestehendes Risiko bei der Entscheidung für einen Cloud-Anbieter liegt im sogenannten Vendor Lock-in. Damit ist gemeint, dass der Wechsel zu einem anderen Cloud-Anbieter oder die Rückführung der IT in unternehmenseigene Hardware bis hin zur Unwirtschaftlichkeit erschwert wird und de facto nicht mehr stattfinden kann. Unterschiedliche Faktoren können dazu beitragen: Proprietäre Technologien, für die das Kundensystem ausgelegt wird, können bei einem anderen Anbieter ggf. nicht angeboten werden. Beispiele hierfür sind spezialisierte Datenbanken und -strukturen oder Schnittstellen (Application Programming Interface, API). Dies kann erhebliche Anpassungen der Software, Reengineering genannt, Neustrukturierungen der Schutzkonzepte (welche Daten werden wie geschützt) sowie neue Schulungen des bedienenden Personals erfordern. Ein weiterer Aspekt können Netzwerkeffekte sein, wenn ein Cloud-Anbieter einen großen Marktanteil besitzt und Nutzer oder Geschäftspartner auf seiner Infrastruktur besser interagieren können (z.B. aufgrund von Interoperabilität). Weiterhin kann ein Wechsel ebenfalls zu Downtime führen, sodass Geschäftsprozesse der Cloud-Anwender unterbrochen werden. In der Regel steigt die Abhängigkeit vom gewählten Cloud-Anbieter (und damit das Lock-in-Risiko) von IaaS über PaaS hin zu SaaS. Wesentliche Fragestellungen für potenzielle Anwender sind daher, wie die Unternehmensdaten abgerufen und auf andere Systeme aufgespielt werden können (eigene oder die eines alternativen Anbieters) und wie

⁹ (Chong, et al. 2014)

¹⁰ (Tak, Urgaonkar und Sivasubramainam 2011)

¹¹ (Repschläger, Pannicke und Zarnekow 2014)

die Unternehmensdaten abgerufen werden, sollte der Vertrag aufgekündigt werden, der Cloud-Dienst ausfallen oder der Cloud-Anbieter in Insolvenz gehen.¹²

Für die Nutzerschaft ergeben sich daher einige Aspekte, die bei der Wahl für eine Cloud-Infrastruktur berücksichtigt werden sollten. Dazu zählen z.B. je nach den Prioritäten der Nutzer das Energieprofil, die Back-up- und Redundanzkonzepte, Preismodelle und Skalierbarkeit, Sicherheitskonzepte, technischer Kundenservice oder auch Vorgaben hinsichtlich der geografischen Stelle der Datenspeicherung und -verarbeitung.

b) Edge Computing

Das EC ermöglicht eine schnellere Verarbeitung und Analyse lokaler Daten, umso mehr, je näher die Berechnung an der Mess- bzw. Anfragestelle stattfindet. Je nach Anforderung und Konfiguration können Edge-Knoten auch direkt untereinander kommunizieren, ohne einen zwischengeschalteten Zentralserver. Dies führt zu kürzeren Latenzzeiten und ermöglicht Echtzeitreaktionen. Zudem reduziert EC den Bedarf an Datenübertragung in eine etwaige Cloud oder an Zentralsysteme, was die Netzwerklast und die Risiken von Datenpaketverlusten verringern kann.

Auch cybersicherheitstechnisch kann dies von Vorteil sein, da die Daten verteilter sind. Dies bedeutet, dass der Zugriff auf große Datenmengen unterbleibt und der mögliche Schaden sowie die Attraktivität (Aufwand-Nutzen-Verhältnis) für potenzielle Angreifer geringer sind. Ein weiterer Punkt ist, dass die reduzierte Datensendung bedeutet, dass weniger Knoten eines Kommunikationssystems passiert werden müssen und die Zugriffsmöglichkeiten für Unbefugte dadurch verringert werden. Aus Sicht des Datenschutzes können Edge-Systeme dazu beitragen, dass Daten vor Ort verarbeitet und der Versand datenschutzrechtlich kritischer Daten vermieden wird oder dass die notwendigen Daten vor dem Versand zunächst anonymisiert und/oder aggregiert werden.

Demgegenüber steht ein höherer Aufwand hinsichtlich der Planung von Edge-Systemen bzgl. der erforderlichen Rechenkapazitäten und sonstiger Gerätefunktionen (z.B. Messgeräte), der Einbaumöglichkeiten bei heterogenen räumlichen Gegebenheiten, der kommunikativen Anbindung sowie der Einsatzplanung von Montage- und Wartungspersonal. Für Betreiber einer Edge-Infrastruktur (i.d.R. das anwendende Unternehmen) ist ein vorausschauendes Konzept unerlässlich, da viele Geräte im Energiesektor eine lange Lebensdauer haben und auch zukünftigen Anforderungen genügen sollten. Die Nachrüstung von Rechenleistung ist in der Regel noch schwer darstellbar und die vorzeitige, massenhafte Ausbringung leistungsstärkerer Gerätegenerationen unwirtschaftlich. Auch sollte bedacht werden, dass die Überwachung und softwareseitige Wartung von Edge-Systemen einiges an Koordination erfordert und dass die eingesparte Bandbreite im Regelbetrieb zu Verzögerungen bei der Durchführung von systemweiten Updates führen kann.

Die beschriebenen Aufwände bedeuten, dass Beschaffung und Betrieb einer Edge-Infrastruktur verhältnismäßig teurer sind als bei einer Cloud-Lösung, wobei ein Edge-System andere Aufgaben und Funktionen ermöglicht und nicht wie eine reine Cloud betrieben wird.

c) Zusammenspiel von Cloud und Edge

Zu den in Abschnitt 2.1c) betrachteten Synergien müssen die Vor- und Nachteile von CC und EC hinzugezogen werden. Die Entscheidung für CC, EC oder eine Kombination daraus ist eine Frage des Kosten-Nutzen-Verhältnisses, wobei der Nutzen sehr stark von den Anforderungen des Anwenderunternehmens abhängt. Da

¹² (Opara-Martins, Shahandi und Tian 2017)

verschiedene Akteure im Energiesystem, die unterschiedliche Kombinationen aus CC und EC einsetzen, auch oft eng miteinander kooperieren müssen, werden leistungsfähige und flexible Schnittstellen von hoher Bedeutung sein.

2.3 Eigenschaften im Kontext des Energiesystems

In diesem Kapitel wird auf die Eigenschaften von CC und EC eingegangen und darauf, wie sie im Energiesystem wirken können. Dabei werden tatsächliche und potenzielle Anwendungsfälle aufgegriffen. Eine tiefergehende Analyse dieser Anwendungsfälle unter Berücksichtigung der technologischen Eigenschaften erfolgt in Kapitel 3 der Studie. Es werden die drei Domänen der Energieversorgungskette Erzeugung, Übertragung (dabei werden sowohl die Energieübertragung als auch die Energieverteilung behandelt) und Verbrauch betrachtet.

a) Cloud-Computing

Erzeugung: Vor dem Hintergrund der Bestrebungen zunehmend Anlagen Erneuerbarer Energien in den unteren Netzebenen zu integrieren, liefert die zentralisierte Struktur von Cloud-Systemen einige Vorteile, beispielsweise die kollaborative Verwaltung und Erstellung von Stammdaten, Bewegungsdaten und Betriebsdaten, Prognosen bei Einsatzverantwortlichen, virtuellen Kraftwerksbetreibern und Anlagenbetreibern sowie die resultierende Kommunikation mit zuständigen Netzbetreibern. Diese Vorteile können vor allem von energiewirtschaftlich agierenden Akteuren, aber auch von Netzbetreibern genutzt werden. Als nachteilig können sich in diesem Zusammenhang de facto „Datensilos“ erweisen, denen die Schnittstellen zum sicheren, schnellen und zuverlässigen Datenaustausch mit anderen Akteuren fehlen.

Übertragung: Die Realisierung von Smart Grids wird begünstigt durch die Eigenschaften von Cloud-Systemen als flexible Daten- und Rechenzentren. Der Netzbetrieb steht als Bindeglied zwischen Erzeugung und Verbrauch vor der Herausforderung, zahlreiche Datenquellen und -formate zu berücksichtigen und die optimalen Maßnahmen daraus abzuleiten. Durch die skalierbare Rechenkapazität sind Funktionen wie Netzzustandsberechnungen mit entsprechendem Redispatch oder die Überwachung und Steuerung größerer angebundener Netzkomponenten denkbar. Entsprechend konfigurierte Cloud-Systeme können bedarfsgerecht zügige Erweiterungen oder Verbesserungen in den Bereichen Soft- und Hardware ermöglichen und somit Anpassungen an erforderliche Funktionalitäten schnell erreichen oder wiederherstellen. Limitationen bestehen jedoch bei der Echtzeitfähigkeit, insbesondere bei stark verteilten und unterschiedlich gut angeordneten Sensoren und Aktoren, weshalb der Cloud-Ansatz auf Verteilnetzebene an seine Grenzen stößt.

Verbrauch: Verbrauchsseitig bieten Cloud-Lösungen einige Vorteile für Endkundinnen und Endkunden und deren Dienstleister. Daten aus intelligenten Messsystemen können, neben den abrechnungstechnischen Prozessen, weiteren Visualisierungs- und Analysewerkzeugen zugeführt werden. Insbesondere rechenstarke, KI-gestützte Analysefunktionen mit entsprechend großer, anonymisierter Datengrundlage bieten das Potenzial für Effizienzsteigerungen und andere Mehrwerte.

b) Edge Computing

Erzeugung: Lokale Datenvorverarbeitung verringert die Datenlast der Kommunikationssysteme (z.B. für präzise Lastprognosen) und unterstützt somit die großflächige Integration erneuerbarer Energiequellen. Durch echtzeitoptimiertes Energiemanagement können Erzeugung und flexible Verbraucher, wie beispielsweise Speicher, optimal koordiniert und dabei Datenschutzerfordernungen gewahrt werden.

Übertragung: Im Verteilnetz können Edge-Geräte wichtige Funktionen übernehmen, die überschaubare Berechnungskomplexitäten aufweisen und eine schnelle Reaktion erfordern. Dies umfasst z.B. Netzschutzfunktionen oder dezentralisiertes Einspeisemanagement. Durch die räumliche Nähe zwischen Sensorik und Maßnahmendimensionierung könnten kurzfristige, unvorhersehbare Beeinträchtigungen des Netzbetriebs kompensiert werden. Ein weiterer Vorteil wird in der Vereinfachung der Schwarzstartfähigkeit gesehen. Hierbei kommt dem System zugute, dass Edge-Geräte bei entsprechender Konfiguration wichtige Prozesse des Netzbetriebs auch ohne Kommunikation mit dem zentralen Netzleitsystem durchführen können, etwa im Katastrophenfall.

Verbrauch: Die Möglichkeiten von Edge-Geräten für verteilte Energiemanagementsysteme bieten Vorteile für Endkundinnen und Endkunden unterschiedlicher Größenkategorien und Verbrauchscharakteristika. Denkbar sind Kostenvorteile bei flexiblen Lasten (z.B. unter optimierter Nutzung von flexiblen Tarifen) und echtzeitnaher Parameterüberwachung, die Fehler in der Kundenanlage detektiert und entsprechend notwendige Maßnahmen einleitet.

2.4 Sicherheitsaspekte

a) Cloud-Computing

Cybersicherheit: Die Sicherheit spielt bei der Integration kritischer Infrastrukturen in einem CC-Umfeld eine wesentliche Rolle. Die Sicherheitsanforderungen und notwendigen Maßnahmen müssen von Beginn an geprüft, bewertet und eingeplant werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt verschiedene Kriterien, nach denen das Angebot von CC im Rahmen der Produktsicherheit bewertet werden kann.¹³ Das interne Sicherheitskonzept muss mit der Dienstleistung des CC-Providers abgestimmt werden. Dies beinhaltet die Minimierung des Ausfallrisikos sowie die Gewährleistung der Datenintegrität und der Datenvertraulichkeit.

Maßnahmen zur Sicherung der Infrastruktur enthalten ein Identity and Access Management (IAM) zur Verhinderung des Eindringens von Unbefugten sowie ein System, um unerwartetes Eindringen über unbekanntes Angriffsvektoren zu entdecken und ggf. zu verhindern. Teil eines IAM sind das Least-Privilege-Prinzip, das in der Cloud agierenden Personen möglichst geringe Berechtigungen erteilt. Sollten Zugangsdaten kompromittiert werden, verringert sich so der Schaden. Zudem können Konzepte wie Zwei-Faktor-Authentisierung das Risiko reduzieren, dass Zugangsdaten kompromittiert werden.

Logging-Dateien helfen nach einem Eindringen, das Ausmaß des Schadens abzuschätzen. Zudem unterstützen sie forensische Untersuchungen. Intrusion Detection Systems erkennen ungewöhnliche Zugriffe auf das System und können einen Angriff melden, während er noch im Gange ist, oder womöglich sogar stoppen. Dabei ist ein Vorteil zentraler Cloud-Anbieter, dass dediziertes, fachkundiges Personal mit entsprechendem Know-how und modernen Werkzeugen für Cybersicherheit und -forensik zur Verfügung steht.

Datenschutz: Die Datenschutz-Grundverordnung (DSGVO)¹⁴ gibt strikte Richtlinien vor, an die sich CC-Provider wie auch die Nutzer von CC halten müssen. Die DSGVO gilt für alle in Europa agierenden Unternehmen sowie für nicht europäische Unternehmen, die mit Kundinnen und Kunden in Europa agieren.

¹³ (UP KRITIS 2022)

¹⁴ Vgl.: Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (DSGVO): <https://eur-lex.europa.eu/Gesetzestext/Datenschutz/Grundverordnung>

Kapitel 4 der DSGVO definiert die Rollen des Controllers (Verantwortlichen) und des Processors (Auftragsverarbeiters). Der Controller muss das Ausmaß und den Zweck der Datenverarbeitung abstimmen und die Risiken für betroffene Personen einschätzen und minimieren. Der Processor hingegen wird von dem Controller beauftragt und durch einen festgelegten Vertrag zu datenschutzsicherndem Verhalten angehalten. Sollte der Processor weitere Unter-Processors beauftragen, so muss dies mit Wissen des Controllers und in Absprache mit ihm geschehen, sodass der Controller sowie die Besitzerinnen und Besitzer von Daten, die der Processor speichert und verarbeitet, über alle Schritte der Verarbeitung aufgeklärt sind.

Der Controller muss von jeder Person, von der Daten gespeichert und genutzt werden, eine aktive Einwilligung erhalten. Zusätzlich muss ein System so ausgelegt sein, dass nur Daten, die für die Funktion des geleisteten Dienstes benötigt werden, gespeichert werden und Unberechtigte keinen Zugriff auf diese Daten bekommen. Diese Daten müssen jederzeit löschar sein, sollte die Einwilligung von den Besitzerinnen und Besitzern der Daten widerrufen werden.

Kapitel 5 der DSGVO bestimmt die Regulation des Datenflusses über EU-Grenzen hinaus. Die Datenübertragung darf ohne Auflagen nur in wenige, von der Europäischen Kommission geprüfte Regionen geschehen.¹⁵

Darüber hinaus ist es möglich, durch Einhaltung von Garantien, beschrieben in Artikel 45 DSGVO, bestimmten Organisationen zu erlauben, Daten in anderen Ländern zu speichern und zu verarbeiten. Letztendlich liegt die Beweislast bei Verletzungen der DSGVO jedoch beim Controller, der im Falle eines Data Breach Fehlhandeln des Processors aufzeigen muss.

Da IP-Adressen auch zu den identifizierbaren Informationen zählen, obliegt ein Teil der Verantwortung über die rechtmäßige Nutzung und Verarbeitung von Daten auch den Cloud-Service-Providern. In einem solchen Fall ist der CC-Provider ein „gemeinsamer Verantwortlicher“ nach Artikel 26 DSGVO.

b) Edge-Computing

Cybersicherheit: EC ist durch seine dezentrale Natur aufwendiger zu konfigurieren und bietet, gesamtsystemisch betrachtet, mehr potenzielle IT-sicherheitsrelevante Schwachstellen. Abhängig von der Konfiguration des Netzwerks kann ein Angreifer mit einem einzelnen befallenen Knoten dem ganzen Netzwerk schaden. Im Umkehrschluss gibt es durch die Struktur aus mehreren Knoten auch Abgrenzungen zwischen den verschiedenen Komponenten des Systems, wodurch wiederum verhindert werden kann, dass ein einzelner korrupter Knoten das Netzwerk stören oder sogar unbrauchbar macht.¹⁶ Dies erfordert jedoch, dass die Access Control (dt. Zugriffskontrolle) einer EC-Architektur komplizierter wird als in einer CC-Umgebung. Zu großzügig verteilte Befugnisse erlauben es Angreifern, mit kompromittierten Knoten oder Zugangsdaten einen großen Bereich des Netzwerks zu beeinträchtigen.

Durch das Zusammenspiel von mehreren heterogenen IoT-Geräten sowie das Verteilen verschiedener Software auf unterschiedliche Edge-Computing-Geräte vervielfachen sich mögliche unbekannte Angriffsvektoren. Zudem ist auch nach dem Bekanntwerden einer Sicherheitslücke die Reaktion erschwert. Es müssen mehrere Komponenten und Systeme überwacht werden. Die Heterogenität einer EC-Architektur beeinträchtigt darüber hinaus den Entwurf einer gesamten Sicherheitsarchitektur, da viele verschiedene Protokolle zusammenspielen und mehr Punkte im System „nach draußen“ kommunizieren.¹⁷ Andererseits

¹⁵ (Europäische Kommission 2023a)

¹⁶ (Sha, et al. 2020)

¹⁷ (Xiao, et al. 2019)

können die Heterogenität und Dezentralität auch Vorteile bieten, da bei entsprechender Sicherheitsarchitektur im Falle eines Angriffs die Anzahl betroffener und ausfallender Systeme begrenzt bleibt.

Durch die im Vergleich zu CC geringere Rechenleistung einzelner EC-Knoten kann sich auch die Effektivität einer DDoS-Attacke (Distributed Denial of Service) steigern. Ein solcher Angriff zielt meist darauf ab, durch das massenhafte Senden von Daten über das Netzwerk ein System unbrauchbar für die eigentliche Nutzung zu machen. In einer CC-Umgebung existieren i.d.R. genug Rechenleistung und Infrastruktur, um solche Angriffe filtern oder sogar ignorieren zu können. Zudem werden Rechenzentren an Netzwerkknotenpunkten mit einer hohen Kapazität gebaut, die ein großes Volumen an Daten transportieren können.¹⁸

Datenschutz: Artikel 25 der DSGVO beschäftigt sich mit der Verantwortung des Controllers, Systeme so zu entwerfen, dass das Risiko von betroffenen Nutzerinnen und Nutzern minimiert wird. Möglichkeiten diesbezüglich sind die Pseudonymisierung sowie das Konzept der Datenminimierung. Das kann durch EC vereinfacht werden. Wenn zum Beispiel Benutzerdaten auf einem Edge-Knoten verarbeitet werden und dadurch nicht mehr oder nur in anonymisierter oder zusammengefasster Form den Zentralrechner erreichen, verbessert sich dadurch der Schutz von Nutzerdaten. Dies birgt jedoch den Nachteil, dass Daten reduziert werden, die für künftige, noch unentdeckte Zwecke relevant sind. Letztendlich müssen nach DSGVO Artikel 12 § 1 alle Wege und Gründe der Datenverarbeitung an die Personen, von denen Daten erhoben werden, kommuniziert und von diesen erlaubt werden. Dies verlangt ohnehin, dass die Zwecke von erhobenen Daten klar definiert werden.¹⁹

c) Zusammenspiel von Cloud und Edge

Hinsichtlich der Cybersicherheit summieren sich die Risiken beim kombinierten Einsatz von CC und EC und die Komplexität des Cybersicherheitskonzepts nimmt dadurch zu. Zum Beispiel sind aus Sicht der Cloud die verteilten Edge-Geräte wie weitere Nutzer zu behandeln und entsprechend beim IAM zu berücksichtigen. Vorteilhaft kann sich die Kombination jedoch auf den Datenschutz auswirken, wenn die Edge-Infrastruktur es beispielsweise erlaubt, personenbezogene Daten näher an den Nutzerinnen und Nutzern zu speichern sowie den potenziellen Zugriff durch Auftragsverarbeiter gänzlich auszuschließen.

2.5 Vergleich der Technologien

CC und EC abstrahieren beide die Berechnung in einem mehrschichtigen Modell. Dies ermöglicht es, Hardware, Betriebssystem und Software getrennt voneinander zu warten und zu entwickeln. Während CC die Berechnungen zentralisiert und dadurch viele Ressourcen wie Rechenleistung und Speicherkapazität bündelt, ermöglicht EC durch das Auslagern der Berechnung nah an die Quelle der Anfrage geringe Latenzen und die Reduzierung der Bandbreitenbelastung.

EC wird insbesondere in Umgebungen eingesetzt, in denen schnelle Reaktionen und kurze Latenzzeiten von entscheidender Bedeutung sind. Beispiele aus anderen Bereichen als der Energieversorgung sind die Industrieautomatisierung, das Internet der Dinge (IoT) und intelligente Verkehrssysteme. Die Stärken des zentralen CC liegen in der hohen Rechenleistung, dem großen Speicherplatz und der Skalierbarkeit, wie sie

¹⁸ (Uddin, Kumar und Chamol 2024)

¹⁹ (Lodge, Brown und Crabtree 2019)

zum Beispiel die Analyse großer Datenmengen ohne die Notwendigkeit unmittelbarer Echtzeitverarbeitung erfordert.

Im folgenden Abschnitt werden CC und EC hinsichtlich der inhärenten ökonomischen, ökologischen und technisch-organisatorischen Aspekte betrachtet. Dabei wird versucht, eine vergleichende Bewertung der Vor- und Nachteile der beiden Technologiekomplexe hinsichtlich der unterschiedlichen Aspekte durchzuführen.

Bei der Bewertung der **ökonomischen Aspekte** von EC und CC sollten Faktoren wie Gesamtbetriebskosten, Skalierbarkeit, Investitionen in Hardware, potenzielle Kosteneinsparungen durch Effizienzgewinne, die Time-to-Market bei der Implementierung und mögliche Risiken des Vendor Lock-in gründlich analysiert werden. Eine ganzheitliche Betrachtung dieser Aspekte ist entscheidend, um fundierte wirtschaftliche Entscheidungen zu treffen.

Bei der Bewertung der **ökologischen Aspekte** von EC und CC ist es wichtig, Faktoren wie erneuerbare Energiequellen, Energieeffizienz und Ressourcennutzung zu berücksichtigen. Ein Vorteil für die schnelle und effiziente Bearbeitung von Anfragen ist eine hohe Speicherdichte, die Zugriffszeiten reduziert, da große Datenmengen näher an Prozessoren sind.²⁰ Es zeigt sich auch, dass die vorausschauende Planung und Dimensionierung der Systeme hier einen wichtigen Faktor darstellen, da über den Lebenszyklus betrachtet längere Nutzungsdauern umwelttechnisch von großem Vorteil sind.²¹

Viele **technische Aspekte** spielen bei der Implementierung von EC- und CC-Lösungen eine Rolle. Nachfolgend werden die betrachteten Themen und Themenkomplexe kurz erläutert.

Skalierbarkeit: Während einige Anwendungsfälle, vor allem im Bereich der traditionellen Versorgungsaufgabe, eine gewisse Planbarkeit aufweisen, können insbesondere marktbasierende Anwendungen wie Mehrwertdienste Flexibilität hinsichtlich der Skalierbarkeit erfordern.

Flexibilität vs. Komplexität der Integration: Die Flexibilität bei der Integration von energiewirtschaftlichen Prozessen in Cloud- oder Edge-Systeme hängt wesentlich von der Komplexität der betrachteten Prozesse sowie von dem Vorhandensein etablierter Standards ab.

Kollaboration und Kontrolle: Ein wesentlicher Aspekt des liberalen Energiesektors liegt in dem komplexen Zusammenspiel diverser Infrastrukturen, Akteure und Stakeholder. Die Möglichkeit, Systeme kollaborativ zu nutzen, kann hierbei ausschlaggebend für kostenoptimale und energieeffiziente Prozesse sein. Ebenso stellt sich dabei die Frage nach den Besitzverhältnissen von Infrastrukturen.

Redundanz und Datenverlust: Da kein System lückenlose Verfügbarkeit garantieren kann, sollten die Aspekte der Redundanz und des Risikos für Datenverlust mitgedacht werden. Je nach Fehlerfall und betroffenen Geräten können unterschiedliche Datenarten und -mengen verloren gehen.

Datenaufkommen und -transport: Die Menge erzeugter Daten im Energiesystem ist erheblich, zumal mit dem Smart Meter Rollout und zunehmender Sensorik im Verteilnetz eine Steigerung stattfindet. Der Transport der Daten vom Entstehungsort (z.B. Verbrauchsmessgeräte, Monitoring, Schalter) hin zum Ort der Datenverarbeitung erfordert zum Teil große Bandbreiten. Vorteilhaft ist es, wenn eine Selektion, Kompression oder sonstige Vorverarbeitung stattfinden kann.

²⁰ (Fey, Karl und Ungerer 2020)

²¹ (Mujan und Aleksic 2019)

Rechenleistung: Die Dynamik im Stromnetz nimmt durch die Vielzahl von dezentralen Erzeugern zu. Netzzustandsberechnungen und Maßnahmendimensionierung benötigen in diesem Zusammenhang eine erhebliche Rechenleistung. Ebenso kann dies für KI-gestützte oder traditionelle Analysen (Bildauswertung von Monitoring-Systemen, Verbrauchsoptimierung) gelten.

Latenz: Die effektive Überwachung und Steuerung vieler Komponenten im Energiesystem erfordern eine latenzarme Übertragung von Informationen. Unterschiedliche Anwendungen variieren in den Anforderungen an die Übertragungsgeschwindigkeit (Verbrauchswerte für Abrechnungszwecke, Spannungswerte für die Netzüberwachung).

Sicherheit und Wartung: Das Energiesystem, insbesondere das Stromnetz, stellt eine kritische Infrastruktur in Deutschland dar.²² Durch die zunehmende Abhängigkeit zwischen dem Energiesystem und der IKT-Infrastruktur ist es möglich, dass Cyberangriffe auf diese Infrastruktur erhebliche negative Auswirkungen auf die Versorgungssicherheit haben können. Sicherheit und Wartung gehen in diesem Zusammenhang Hand in Hand, da laufend Sicherheitslücken durch Updates behoben werden müssen. Ebenso müssen fehlerhafte Hardware-Komponenten möglichst schnell in Stand gesetzt werden, um negative Auswirkungen auf den Betrieb zu verhindern.

Die folgenden Tabellen zeigen die Vor- und Nachteile für die oben beschriebenen Charakteristiken für die beiden betrachteten Technologien. Neben einer kurzen Erklärung wird dem jeweiligen Argument ein Symbol zugeteilt. Ein „Plus“ bedeutet, dass es sich um einen inhärenten Vorteil handelt, der selbst bei Standardkonfigurationen gegeben sein dürfte. Ein „Kreis“ ist ein potenzieller Vorteil bzw. Nachteil, der aktiv implementiert bzw. vermieden werden sollte. Analog zum „Plus“ weist ein „Minus“ auf einen inhärenten Nachteil hin. Die Auflistung und die Bewertung erfolgen ohne Anspruch auf Vollständigkeit, da viele Eigenschaften für spezielle Kundenanwendungen eine Rolle spielen können, die hier nicht berücksichtigt sind. Auch können gewisse Nachteile anwendungsabhängig durch Synergieeffekte kompensiert werden.

2.5.1 Ökonomische Aspekte

Tabelle 1: Ökonomische Aspekte: Vergleichskriterien und Bewertung

		Cloud-Computing	Edge Computing
Time-to-Market	+	Cloud-Dienste ermöglichen eine schnellere Bereitstellung von Ressourcen und Anwendungen, was zu verkürzten Entwicklungszeiten führen kann.	○ Durch effektives Device Management, flexible APIs und effiziente OTA-Update-Fähigkeit können Edge-Bestandsgeräte eine kurze Time-to-Market ermöglichen.
			- Die initiale Ausbringung erfordert sehr gezielte, individuelle Planung und (abhängig von der Gerätezahl) ausgedehnte Einkaufs- und Montageprozesse.

²² (BBK 2021)

Kostensparnisse/-risiken	<p>+ Cloud-Dienste können anfänglich kosteneffizient sein, da sie den Bedarf an teurer Hardware reduzieren.</p> <p>O Langfristig können die Kosten steigen, insbesondere wenn die Nutzung stark wächst oder ungenutzte Ressourcen nicht optimiert werden.</p> <p>O Risiken, wie plötzliche Preiserhöhungen und Ausfälle, müssen berücksichtigt werden.</p>	<p>O Kostensteigerungen für die Nutzung von Kommunikationsinfrastrukturen können ein Risiko darstellen.</p> <p>- Die Hardware-Ausbringung ist mit zeit- und kostenintensiven Montage- und Inbetriebnahmeprozessen verbunden.</p>
Vendor Lock-in	<p>O Die Abhängigkeit von einem Cloud-Anbieter kann die Flexibilität einschränken und die Migration zu anderen Plattformen erschweren. Hier sind Standards hinsichtlich der Portabilität ausschlaggebend.</p>	<p>O Als fest installiertes Gerät ist ein Edge-Knoten einem Hersteller zugeordnet und oft auf proprietäre Updates durch diesen angewiesen. Durch etablierte Standards kann eine Interoperabilität zwischen Geräten unterschiedlicher Hersteller ermöglicht werden.</p>

2.5.2 Ökologische Aspekte

Tabelle 2: Ökologische Aspekte: Vergleichskriterien und Bewertung

	Cloud-Computing	Edge Computing
Energieeffizienz	<p>O Durch sinnvolle Planung im Bauprozess kann ein vorteilhaftes Energiemanagement des Rechenzentrums (Abwärme etc.) realisiert werden.</p> <p>+ Eine intelligente Ressourcenbelegung (etwa durch Virtualisierung und Containerisierung, prädiktive Scheduling-Algorithmen) ist im Anbieterinteresse. Dadurch kann die Balance von Angebot und Nachfrage effektiv erreicht werden.</p>	<p>+ Ein wesentlicher Vorteil liegt in der reduzierten Datenübertragung.</p> <p>O Auch untereinander können nahe gelegene Edge-Knoten Aufgaben übernehmen und so eine optimale Auslastung herbeiführen.</p>
Speicherdichte	<p>+ Cloud-Rechenzentren können (eher) fortlaufend fortschrittliche Speichertechnologien implementieren, um mehr Daten auf weniger physischem Raum zu speichern.</p>	<p>- Die Speicherdichte ist im Wesentlichen auf den Stand der Technik zum Zeitpunkt der Ausbringung limitiert.</p>

2.5.3 Technische und organisatorische Aspekte

Tabelle 3: Technische und organisatorische Aspekte: Vergleichskriterien und Bewertung

	Cloud-Computing	Edge Computing
Skalierbarkeit	<p>+ Bei entsprechend vorliegender Integration ist eine Erweiterung der Rechenleistung und der Speicherkapazität in der Regel unproblematisch.</p>	<p>- Die Rechenleistung und die Speicherkapazität von Edge-Geräten sind konstruktionsbedingt und lassen sich nachträglich nicht oder nur kostenintensiv erweitern. Anwendungen, die über die aktuellen, hardwareseitigen Fähigkeiten von Bestandsgeräten hinausgehen, können ohne eine aufwendige Ausbringung weiterer Hardware nicht realisiert werden.</p>
Integration	<p>+ Durch Containern und Virtualisierung können potenzielle Nutzer einer Cloud ihre Prozesse gut vorbereiten.</p> <p>O Branchenspezifische Prozesse mit vielen Kommunikationspartnern und etablierten Strukturen lassen sich ggf. schwerer in der Cloud abbilden.</p> <p>- Vorgaben oder Einschränkungen des Cloud-Anbieters können die Integration weiterer Systeme oder Funktionalitäten verhindern.</p>	<p>+ (Offene) Standards, wie z.B. von der LF Edge²³ vorgeschlagen, erleichtern die Vorbereitung und Integration von Prozessen.</p> <p>O Die verteilten Systeme bedingen eine kleinteiligere Vorgehensweise. Ggf. müssen dazu unterschiedliche Gerätetypen, -generationen und -hersteller bedacht werden.</p>
Kollaboration	<p>+ Cloud-basierte Kollaborationstools ermöglichen eine nahtlose Zusammenarbeit über Teams bzw. Unternehmen hinweg.</p>	<p>O Der Zugriff mehrerer Marktteilnehmer auf ein Edge-Gerät muss sicher und effizient verwaltet werden. Hier kann es zu einem Trade-off zwischen Geschwindigkeit und Sicherheit kommen.</p>

²³ Weitere Informationen: Linux Foundation Edge: <https://lfedge.org/> (Webseite der Linux Foundation Edge)

<p>Kontrolle</p>	<p>○ Bei der Nutzung öffentlicher Clouds haben Unternehmen weniger direkte Kontrolle über die physische Infrastruktur.</p>	<p>○ Sofern sich die Edge-Geräte im Besitz des Unternehmens befinden, hat dieses weitreichende Kontrolle über die Infrastruktur. Gleiches gilt für die verwendete Kommunikationsinfrastruktur, wobei diese häufig durch einen Drittanbieter (z.B. Telekommunikationsunternehmen) bereitgestellt wird und somit seltener im Einflussbereich des Anwenders liegt.</p>
<p>Datenverlust</p>	<p>○ Die Zentralität der Hardware ermöglicht ein unkompliziertes Datensicherungs- und Wiederherstellungskonzept. Gleichzeitig können Hardware-Ausfälle (bei Ausbleiben der regelmäßigen Sicherung) zum Verlust enormer Datenmengen führen.</p>	<p>+</p> <p>Einzelne Geräte dienen als Speicher ihrer Daten, durch Hardware-Fehler gehen somit weniger Daten verloren.</p> <p>○ Sofern aufzubewahrende Daten nicht in sinnvollen Intervallen abtransportiert und einem Back-up-Speicher zugeführt werden, kann im Einzelfall ein nicht zu behebender Datenverlust stattfinden.</p>
<p>Redundanz</p>	<p>○ Den Anforderungen an Redundanz in Abhängigkeit von den Kundenbedürfnissen kann meist problemlos entsprochen werden. In diesem Zusammenhang sollten auch Service-Level-Agreements vereinbart werden.</p>	<p>-</p> <p>Auf den einzelnen Endpunkt bezogen besteht in der Regel kein Redundanzkonzept. Im Fehlerfall können kleinteilige Technikereinsätze erforderlich werden.</p>
<p>Rechenkapazität</p>	<p>+</p> <p>Durch die zentrale Sammlung und Verarbeitung von Daten können Techniken im Sinne von Big-Data-Analysen mit einer unverfälschten Datenbasis und einer flexibel abrufbaren Rechenleistung angewandt werden.</p>	<p>-</p> <p>Es besteht eine geringere Rechenleistung je lokalem Edge-Knoten. Sie sollte möglichst vorausschauend dimensioniert werden.</p>
<p>Latenz</p>	<p>-</p> <p>Echtzeitnahe Analysen werden in größeren Systemen erschwert oder sind gänzlich nicht darstellbar.</p>	<p>+</p> <p>Die Auswertung hochfrequenter Messdaten bei geringen Latenzen (nahe der Quelle) ist ein wesentlicher Vorteil von Edge-Systemen.</p>

<p>Datentransport</p>	<p>- Alle Daten müssen vom Entstehungsort (z.B. Messgerät) bis zum Rechenzentrum übermittelt werden.</p>	<p>+</p> <p>O</p>	<p>Die (Vor-)Verarbeitung von Daten in Edge-Geräten vermindert, bei gleichem Datenaufkommen, die Menge der zu übertragenden Daten.</p> <p>Je nach gewähltem Auswertungsansatz kann eine „ungefilterte/unverfälschte“ Datenbasis erforderlich sein, wodurch die Vorteile der Edge-Technologie entfallen.</p>
<p>Wartung</p>	<p>+ Durch den zentralen Zugriff auf Hard- und Software können Wartungen unkomplizierter geplant und durchgeführt werden. Auch können Virtual Machines so gestaltet werden, dass Downtime vermieden wird.</p>	<p>-</p>	<p>Die Wartung verteilter Systeme ist sowohl hardware- als auch softwareseitig schwieriger. Neben der Koordinierung von Technikereinsätzen oder Firmware-Updates müssen ggf. auch unterschiedliche Gerätetypen und -generationen bedacht werden. Einzelne Geräte sind während eines Updates oft nicht einsetzbar.</p>
<p>Sicherheit</p>	<p>+ Die zentrale Datenhaltung und -bearbeitung ermöglicht es, weitreichende Sicherheitskonzepte zu implementieren und aktuell zu halten.</p> <p>O Als Single Point of Failure kann ein erfolgreicher Cyberangriff erheblichen Schaden anrichten.</p>	<p>+</p> <p>O</p>	<p>Die dezentrale Systemarchitektur erschwert weitreichende Angriffe und ermöglicht die zügige physische Isolation betroffener Knotenpunkte.</p> <p>Die Vielzahl einzelner Endgeräte macht es unter Umständen schwieriger, komplexe Sicherheitskonzepte umzusetzen. Durch verzögerte Sicherheitsupdates können Sicherheitslücken länger bestehen bleiben.</p>
<p>Datenschutz</p>	<p>O Bei der Wahl eines Cloud-Anbieters müssen rechtliche regionale und nationale Bestimmungen zur Datenhaltung berücksichtigt werden. Unter Umständen müssen gesonderte Vereinbarungen getroffen werden, um die Einhaltung der Vorgaben zu gewährleisten.</p>	<p>+</p>	<p>Die lokale Verarbeitung von Daten in Edge-Geräten kann die Einhaltung von rechtlichen Vorgaben hinsichtlich des Datenschutzes und der Schutzbestimmungen vereinfachen.</p>

2.5.4 Zusammenfassung

Die Stärken und Schwächen der beiden Technologien liegen in unterschiedlichen Bereichen und werden von verschiedenen Akteuren im Energiesystem anwendungsabhängig bewertet. Edge- und Cloud-Lösungen existieren in verschiedenen Ausprägungen und ergänzen sich oft in Kombination miteinander. Eine intelligente Aufgabenverteilung zwischen zeitsensiblen Berechnungen, die an die Edge verschoben werden können, und rechenintensiven Aufgaben, die in der Cloud stattfinden, können den Nutzen beider Technologien maximieren.

Ökonomisch betrachtet sind Cloud-Systeme in der Regel kostengünstiger und schneller verfügbar, zumal sie auch durch etablierte Anbieter mit bereits bestehender Hardware bereitgestellt werden und meist vorhandene Telekommunikationsnetze nutzen. Durch die zentrale Aufstellung sind der Einkauf und die Umrüstung von aktueller Hardware einfacher darstellbar. Edge-Systeme stellen oft eine neu zu schaffende Infrastruktur dar, samt der notwendigen Planungs- und Montagearbeiten. Beiden Technologiekomplexen ist gemeinsam, dass ein gewisses Risiko für Anbieterabhängigkeit besteht, wobei dies durch entsprechende Abstimmung vermieden werden sollte. Bezogen auf die Ausfallsicherheit und Redundanz können unterschiedliche Ansätze verfolgt werden. Das Back-up großer Datenmengen und Systemabbildungen erfolgen eher in Cloud-Umgebungen, wobei technische Probleme in diesem Fall zu längeren, systemweiten Ausfallzeiten führen können. Edge-Infrastrukturen ermöglichen es, Systemausfälle lokal zu begrenzen und, sofern vorgesehen, autark Wiederherstellungsprozesse auszuführen (z.B. Schwarzstart im Katastrophenfall).

Anwendungen, bei denen umfangreiche, potenziell sensible Datenmengen im lokalen Kontext betrachtet werden müssen, etwa bei Energiemanagementsystemen, Netzzustandsanalysen oder der Steuerung und Regelung an einem Strang im Niederspannungsnetz, profitieren von der Edge-Architektur. Insbesondere können latenzarme Prozesse realisiert werden, wie sie etwa beim Netzschutz erforderlich sind. Daten können im Einflussbereich des Besitzers verbleiben und selektiv, aggregiert und/oder pseudonymisiert übermittelt werden, wodurch Datenschutz gewahrt wird und Kommunikationsnetze weniger ausgelastet werden.

Cloud-Systeme spielen ihre Vorteile bei räumlich breiter gefassten, skalierbaren Anwendungen aus, insbesondere bei solchen, denen sehr große Datenmengen zugrunde liegen. Dies können datengetriebene Vorhersagemodelle (Erzeugungs-/Wartungsprognosen) sein oder Systeme zur unternehmensinternen und unternehmensübergreifenden Kollaboration. Auch werden Netzleitsysteme zunehmend in Form einer Cloud-Architektur konzipiert (vgl. Kapitel 3.1.2), da sie als Knotenpunkt zahlreicher Datenquellen dienen und rechenintensive Analyseprozesse durchführen.

2.6 Weiterentwicklung

Die betrachteten Technologien unterliegen einem steten Wandel und werden fortlaufend weiterentwickelt. Während aus dem Anwendungsfeld des Energiesystems neue Anforderungen hinsichtlich des Datenaufkommens und der erlaubten Latenzen entstehen, führen Bemühungen in den Bereichen Standardisierung, Energieeffizienz und Informations- und Kommunikationstechnologie zu einer Erweiterung der verfügbaren Fähigkeiten und Mittel. Im Folgenden wird auf die genannten Punkte eingegangen, um interessante Konzepte und mögliche Entwicklungspfade aufzuzeigen.

2.6.1 Standardisierung

Durch die stetige Weiterentwicklung der EC- und CC-Technologien sowie von IoT-Geräten und -Anwendungen existieren viele verschiedene Kommunikationswege und -protokolle. Der entsprechende Bedarf an Standardisierung wird bereits von unterschiedlichen Industrie- und Anwendergruppen adressiert. Projekte wie Gaia-X oder die European Alliance for Industrial Data, EC and CC arbeiten an Wegen und Methoden, die Benutzung von Cloud-Anwendungen zu vereinfachen und die Sicherheit zu stärken.^{24,25} Dies soll dazu beitragen, dass im Rahmen des Projekts „Europe's Digital Decade 2030“ bis zum Jahr 2030 75 Prozent aller europäischen Unternehmen Cloud-Dienste oder verwandte Dienste nutzen. Das Standardisieren von CC sollte auch den Vendor Lock-in²⁶ reduzieren, da Implementationen einfacher auf die Infrastruktur eines anderen Cloud-Anbieters migriert werden können. Durch das verringerte Risiko wird eine erhöhte Marktaufnahme erwartet.²⁷

Es existieren verschiedene Modelle, um die Benutzung von EC zu standardisieren. Eine standardisierte EC-Plattform ist EdgeX Foundry. Betrieben wird dieser Standard von der Linux Foundation.^{28,29} EdgeX unterteilt Edge Computing Services in viele Microservices, welche betriebssystemunabhängig in Containern auf verschiedener Hardware ausgeführt werden können. Die Container erlauben eine konsistente Plattform für Anwendungen in unterschiedlichen Umgebungen. Logisch unterteilt werden diese Microservices in vier Schichten, die Kommandos und Daten untereinander jeweils zu einer übergeordneten Cloud oder den angeschlossenen IoT-Geräten weiterleiten.

Als Orientierungshilfe für potenzielle Nutzer von Cloud-Dienstleistungen hat das BSI den C5-Katalog (Cloud Computing Compliance Criteria Catalogue) entwickelt.³⁰ Er enthält Mindeststandards bzgl. verschiedener Aspekte der Informationssicherheit, wie Datenschutz, Datensicherheit, Transparenz, Compliance und Risikomanagement. Für Anbieter von Cloud-Lösungen werden z.B. Sicherheits- und Transparenzstandards vorgegeben, Anwender erhalten damit ein Werkzeug, um ihre eigenen Risiken und Bedürfnisse einschätzen zu können. Durch ein unabhängiges Audit können Anbieter die Einhaltung der Anforderungen nachweisen und ein sogenanntes C5-Testat erhalten.

2.6.2 Datenaufkommen und Latenzen

Bei der Datenanbindung von kundenseitigen Messsystemen und anderen Sensoren im Energienetz spielt bereits heute die Bandbreite eine wichtige Rolle. Über das gesamte Energiesystem hinweg setzt sich der Trend zu größeren Datenmengen, die übertragen, verknüpft und analysiert werden müssen, fort. Im Bereich der Smart Meter hat sich gezeigt, dass die Bandbreitenbeschränkungen weniger beim Abtransport von Verbrauchsdaten liegen (sie betragen zwischen 100 kB³¹ und 288 kB pro Monat und Zähler), sondern vielmehr die zügige Durchführung von systemweiten Firmware-Updates bedacht werden muss. Kommen zu den einzelnen abrechnungsrelevanten Verbrauchswerten weitere Analyseparameter hinzu (Spannungsdaten, Phasenwinkel etc.), werden diese höchstwahrscheinlich nur bis zu einem Datenkonzentrator (z.B. Trafostation)

²⁴ (Gaia-X 2023a)

²⁵ (Europäische Kommission 2023b)

²⁶ Vgl. Abschnitt 2.2a

²⁷ (Gaia-X 2023b)

²⁸ (EdgeX Foundry 2024)

²⁹ (Villali, et al. 2021)

³⁰ Weitere Informationen zu C5-Anforderungen: <https://www.bsi.bund.de> (Webseite zum C5 Katalog)

³¹ (Luan, Sharp und LaRoy 2013)

für eine schnelle Maßnahmendimensionierung transportiert werden müssen. Für Ortnetzstationen werden in der Literatur unterschiedliche Werte zwischen 10 MB/s³² (in 2011) und 100 MB/s³³ (in 2021) angegeben.

Ein weiterer Aspekt, der den Zuwachs im Datenverkehr vorantreibt, sind Sicherheitsvorkehrungen. Die Nutzung von sicheren Kommunikationsprotokollen und Zertifikatsinfrastrukturen erfordert den Versand zusätzlicher Informationen (als Teil des Overhead) und kann die Datennutzung um das Zwei- bis Dreifache erhöhen.³⁴ Dies kann u.a. daran liegen, dass selbst kleinste Datenmengen (z.B. einzelne hochfrequente Messwerte) einen signifikanten Overhead erhalten.

Neben dem Volumen der zu übermittelnden Daten spielt auch die Geschwindigkeit der Übertragung nach der Erfassung im Messgerät eine Rolle. Für den Anwendungsfall der verbraucherseitigen Lastbegrenzung wurde in Untersuchungen des deutschen SMGW-Systems (Smart Meter Gateway) eine durchschnittliche (und in diesem Fall ausreichende) Reaktionszeit von 51 s festgestellt.³⁵ Für netzkritische Schutzanwendungen sind jedoch deutlich geringere Latenzen erforderlich. Die Reaktionszeit, um Schäden an Komponenten zu vermeiden, kann bei 70 bis 80 ms liegen. Da dies die Fehlererkennung, Datenübermittlung und Maßnahmen-durchführung (z.B. Schalthandlung) beinhaltet, bleiben für die eigentliche Kommunikation teils nur noch 10 ms.^{36,37}

2.6.3 Energieverbrauch

Durch die Unterzeichnung des Climate Neutral Data Centre Pact³⁸ haben sich über 100 Unternehmen, darunter Intel und Microsoft, dazu verpflichtet, bis 2030 alle ihre Rechenzentren ausschließlich mit erneuerbarer Energie zu betreiben wie auch die Energieeffizienz ihrer Rechenzentren auf den vereinbarten Mindestwert einer Energienutzungseffizienz (Power Usage Effectiveness, PUE)³⁹ von unter 1.4 zu bringen. Dies bedeutet, dass Energie, die nicht direkt für das Betreiben der Rechenkomponenten benutzt wird, nicht mehr als 30 Prozent des gesamten Stromverbrauchs ausmachen darf. Das betrifft vor allem die Kühlung, die durch Abwärmennutzung Energie für eine Vielzahl von Anwendungen bereitstellen kann. Beispiele sind die teilweise Deckung der Heizenergie eines Schwimmbads oder Studentenwohnheims oder als Energiebeitrag zu Fernwärmennetzen.⁴⁰ Ein Beispiel ohne Abwärmennutzung und dafür ohne Abhängigkeit von geeigneten Abnehmern und saisonalen Effekten zeigt das Natick-Projekt der Firma Microsoft, die über zwei Jahre ein Rechenzentrum in einer Druckkapsel unter Wasser betrieben hat.⁴¹

Ein weiterer Ansatz, der eine IKT-Infrastruktur mit einer zentralen Cloud und verteilten, endverbraucher-nahen Rechenkapazitäten (z.B. in ONS) betrachtet, setzt auf einen Algorithmus, der die Auslastung von Virtual Machines (VM) im Cloud-Edge-Netzwerk überwacht. Neue Berechnungsanfragen, die aufgrund räumlicher Nähe an eine unterlastete VM gehen, werden dabei zunächst an stärker belastete VM delegiert (solange diese unter der Auslastungsgrenze liegen). Dadurch können kaum genutzte VM komplett abge-

³² (Daoud und Fernando 2011)

³³ (Luo, et al. 2022)

³⁴ (Ghanem, et al. 2020)

³⁵ (Springmann, Bruckmeier und Müller 2022)

³⁶ (Labrador Rivas und Abrão 2020)

³⁷ (Daoud und Fernando 2011)

³⁸ Weitere Informationen zum Climate Neutral Data Centre Pact (CNDCP): www.climateneutraldatacentre.net (Webseite des CNDCP)

³⁹ Power Usage Effectiveness: Verhältnis des Gesamtenergieverbrauchs zum reinen Energieverbrauch für Rechenkomponenten

⁴⁰ (Limb 2023)

⁴¹ Weitere Informationen zum Natick-Projekt auf: <https://natick.research.microsoft.com/> (Projektwebseite)

schaltet werden. Möglich ist, dass Anfragen dadurch weiter entfernt bearbeitet werden und länger dauern, weshalb maximale Antwortzeiten mit berücksichtigt werden.⁴²

2.6.4 Kommunikationstechnologien

Mit der zunehmenden Verbreitung von 5G-Funk eröffnen sich neue Möglichkeiten für die kommunikative Anbindung von Sensorik und Aktorik im Energiesystem. Häufig genannte Vorteile der Technologie liegen in sehr geringen Latenzen, Hochverfügbarkeit und der simultanen Bedienung einer zuvor nicht darstellbaren Anzahl von Endgeräten. Bezogen auf den Einsatz von Cloud- und Edge-Technologien kann dies unterschiedliche Szenarien begünstigen. Als Grundlage für Cloud-gestützte Datenanalysen zum Beispiel können Sensordaten entfernter Messstellen leichter und höherfrequent eingebunden werden. Aus Sicht eines Edge-Ansatzes wird eine leichtere Skalierbarkeit erreicht, da die Anbindung weiterer Endgeräte und möglicherweise erforderlicher Erweiterungsmodule vereinfacht wird. Im Endeffekt sagen Quellen eine größere Datendichte und somit Netztransparenz durch 5G voraus, was sich in einer schnelleren Fehlerlokalisierung und -behebung äußert und somit eine höhere Versorgungssicherheit ermöglicht.^{43,44}

Der Anstieg an Bandbreite durch die Einführung von 5G ermöglicht es auch, dass mobile Geräte mehr Daten versenden und auch Strukturen wie Multi-Access Edge Computing⁴⁵ nutzen können, um größere Berechnungen auszulagern. Dadurch ergeben sich viele neue Möglichkeiten, um mit geringer lokaler Rechenlast und geringem Energieverbrauch intelligente Systeme zu implementieren.

2.6.5 Disaggregation und Modularität von Edge-Komponenten

Die Entwicklung im Bereich der Edge-Geräte geht zunehmend in Richtung einer Disaggregation, d.h. der Aufteilung von Aufgaben und Funktionen auf unterschiedliche Hardware-Komponenten und der Einführung von Modularität. Dies soll die Skalierbarkeit von Edge-Lösungen verbessern, indem z.B. neuen Anforderungen an Rechenleistung durch die Addition einzelner, dedizierter Rechenmodule begegnet wird, anstatt etwa ein Gerät mit integrierter Visualisierung, Speicherung und Kommunikationseinheit sowie integrierten Rechenkernen austauschen zu müssen.⁴⁶ Dieser Ansatz setzt eine breite und praxistaugliche Standardisierung voraus, da die zahlreichen erforderlichen Schnittstellen und Kompatibilitätsfragen ein großes Risiko für Vendor Lock-in bedeuten.

⁴² (Singhal, et al. 2023)

⁴³ (Deloitte 2021)

⁴⁴ (Ericsson 2020)

⁴⁵ Multi-Access Edge Computing ermöglicht mobile, temporäre Verbindungen.

⁴⁶ (LF Edge 2023)

3 Anwendungsfelder in der Energiewirtschaft

3.1 Anwendungsfälle

Im Folgenden werden mögliche Anwendungsfälle vor dem Hintergrund wesentlicher Herausforderungen des zukünftigen Energiesystems betrachtet. Im Rahmen der Recherche sowie im Austausch mit Stakeholdern wurden sechs aktuelle Herausforderungen für die Energiewirtschaft identifiziert: **Netzplanung und -ausbau, Systemführung, Netzanschluss/-betrieb, Nutzung von Flexibilität, IKT-Infrastrukturen und Verbraucheraktivierung**. Darüber hinaus wird Teil 1 des „Stufenmodells zur Weiterentwicklung der Standards für die Digitalisierung der Energiewende“ ebenfalls als Leitfaden für die Identifizierung und Priorisierung der Anwendungsfälle genutzt.

Unter Beachtung dieser Informationen wird eine Voranalyse und Priorisierung der Anwendungsfälle für CC und/oder EC in der Energiewirtschaft durchgeführt. Unter Berücksichtigung der in Kapitel 2 beschriebenen Eigenschaften der Edge- und Cloud-Technologien wird die jeweilige Eignung hinsichtlich der technischen Anforderungen der Anwendungsfälle betrachtet. In der folgenden Tabelle werden fünf verschiedene Anforderungen für Anwendungsfälle in der Energiewirtschaft gelistet: **Latenz und Reaktionszeit, Skalierbare Rechenkapazität, Skalierbare Datenspeicherung, IKT-Sicherheit sowie Datensicherheit und Datenschutz**.

Tabelle 4: Kriterien und davon abgeleitete Anforderungen an Technologien im Energiesystem

Kriterium	Energiewirtschaftliche Anforderungen
Latenz und Reaktionszeit	Prozesse wie Dezentrale Fehlerortung und -eingrenzung und sowie Versorgungswiederherstellung (FLISR) ⁴⁷ oder Anomalien-Erkennung sind zeitkritisch. Sie benötigen daher niedrige Latenz. Im Vergleich dazu können geschäftsrelevante Prozesse meist mit höheren Latenzen gut funktionieren.
Skalierbare Rechenkapazität	Die Durchführung von datengetriebenen Regelungsanwendungen, komplexen Optimierungsrechnungen, benötigt viel Rechenkapazität. In einem sich weiterentwickelnden Energiesystem muss diese Rechenleistung skalierbar sein.
Skalierbare Datenspeicherung	Im digitalisierten Energiesystem werden erhebliche Mengen an Daten produziert. Prozesse wie die Erzeugungsprognose benötigen z.B. historische Daten. Die meisten datengetriebenen Anwendungen profitieren von größeren Datensätzen. Darüber hinaus existieren für Netzbetreiber Dokumentationspflichten, die die Speicherung von bestimmten Daten für eine gewisse Zeit fordern.
IKT-Sicherheit	IKT-Sicherheit ist von zunehmender Bedeutung im digitalisierten Energiesystem, da Angriffe auf die Energieinfrastruktur die Versorgungssicherheit erheblich einschränken können. Sowohl die Sicherheit von Prozessen als auch die Entwicklung von Regelungsmechanismen, die zur erhöhten IKT-Sicherheit beitragen, sind hier von Relevanz.
Datensicherheit und Datenschutz	Es werden z.T. sensible, personenbezogene Daten im Energiesystem erzeugt (z.B. Energieverbräuche), die vor unbefugtem Zugriff geschützt werden müssen.

⁴⁷ Aus dem Englischen: Fault Location, Isolation, and Service Restoration (Fehlerortung und -eingrenzung sowie Versorgungswiederherstellung)

3.1.1 Intelligente Messsysteme (iMSys) und Advanced Metering Infrastructure (AMI)

Die Implementierung intelligenter Messsysteme (iMSys) ist für die Digitalisierung des Energiesystems von entscheidender Bedeutung. Das iMSys ist die deutsche Version der Advanced Metering Infrastructure und umfasst den digitalen Stromzähler (Smart Meter) sowie eine Kommunikationseinheit, das sogenannte Smart Meter Gateway (SMGW). Der im Gegensatz zu analogen Messsystemen gesteigerte Funktionsumfang beinhaltet etwa die Fernauslesung von Verbrauchsdaten, die Echtzeitüberwachung des Verbrauchs und die Fähigkeit, lokal detaillierte Qualitätsparameter im Stromnetz zu sammeln und zu analysieren. Das Ariadne-Projekt⁴⁸ präsentiert eine detaillierte Auflistung verschiedener Anwendungsfälle für iMSys, die als Grundlage für weitere technische und wirtschaftliche Prozesse der Energiewirtschaft dienen. In der folgenden Tabelle 5 werden die Anwendungen gelistet und mit vorteilhaften Eigenschaften von CC bzw. EC verknüpft. Der hervor gehobene Anwendungsfall wird im nachfolgenden Text näher betrachtet.

Tabelle 5: Beispielhafte Anwendungsfälle im Bereich iMSys und AMI

Anwendungsfall	Prozess / Funktion	Mehrwert CC	Mehrwert EC
Zählerdatenerfassung	Abrechnung	Skalierbare Datenspeicherung, hohe Verfügbarkeit	Erhöhter Datenschutz
	Autom. Fernauslesung		
Anomalien-Erkennung	Erkennung von Anomalien in den Zählerständen, um z. B. Energiediebstahl zu verhindern	Skalierbare Rechenkapazität	Niedrige Latenz, erhöhter Datenschutz, geringere Bandbreite notwendig
Anschlussüberprüfung	Verifizierung und Authentifizierung der Anschlüsse	Skalierbare Datenspeicherung, hohe Verfügbarkeit	Niedrige Latenz, erhöhter Datenschutz, geringere Bandbreite notwendig

Die automatisierte Abrechnung ist eine der wichtigsten Funktionen, die durch iMSys erfüllt werden können. Da sie keine zeitkritische Funktion darstellt, kann die Datenverarbeitung in eine Cloud ausgelagert werden. Zu berücksichtigen ist, dass diese Daten oft sensibler Natur sind und aus ihnen im Falle eines Cyberangriffs Rückschlüsse auf das Nutzerverhalten gezogen werden können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher Anforderungen in Bezug auf SMGW vorgelegt, die den Schutz dieser Daten durch Authentifizierung und Verschlüsselung der Kommunikation sicherstellen können.⁴⁹ Cloud-Lösungen für Abrechnungsprozesse werden bereits am Markt als skalierbare SaaS angeboten.⁵⁰ Um den Datenschutz und die Datensicherheit bei diesem Prozess zu gewährleisten, werden auch Ansätze vorgeschlagen, die Datenverarbeitung für Abrechnungsdienste auf der Cloud mithilfe von verschlüsselten Dateien durchzuführen.⁵¹

Vor dem Hintergrund der zunehmenden Anzahl von dezentralen Energieanlagen und Elektrofahrzeugen stehen zentralisierte, CC-basierte Abrechnungssysteme vor der Herausforderung, die sich hochskalierende Datenmenge zu bewältigen. Um das Datenaustauschvolumen zu reduzieren und somit die erforderliche Netzwerk-Kommunikationsbandbreite zu minimieren, können EC-Ansätze verwendet werden, die die lokale Datenverarbeitung in der Nähe oder innerhalb der Smart Meter durchführen. Dieser Ansatz wird im DEER-

⁴⁸ Weitere Informationen zum Ariadne-Projekt: [https://ariadneprojekt.de \(News-Artikel auf Webseite\)](https://ariadneprojekt.de (News-Artikel auf Webseite))

⁴⁹ Weitere Informationen zu Smart Meter Gateways: [https://www.bsi.bund.de \(Webseite zum SMGW\)](https://www.bsi.bund.de (Webseite zum SMGW))

⁵⁰ Weitere Informationen auf den Websites von powercloud: [https://power.cloud \(Produktseite Abrechnungssystem\)](https://power.cloud (Produktseite Abrechnungssystem)), arvato: [https://www.arvato-energy-platform.de \(Produktseite Plattform\)](https://www.arvato-energy-platform.de (Produktseite Plattform))

⁵¹ (Mai und Khalil 2017)

Forschungsprojekt demonstriert.⁵² Besonders im Fall von Prozessen oder Funktionen, die eine kurze Reaktionszeit erfordern, können EC-Ansätze die Skalierbarkeit von iMSys-Funktionen erhöhen. Denkbar wäre ein EC-basiertes Smart-Metering-System, das durch die Verarbeitung von Messwert-Zeitreihen an der Nutzer-Edge die Übertragung der Messwerte energieeffizienter gestalten kann.⁵³ Darüber hinaus können Funktionen wie Anomalien-Erkennung für Betrugserkennung⁵⁴ sowie bidirektionale Authentifizierung und Überprüfung von Nutzern und Anschlüssen⁵⁵ durch EC ermöglicht werden.

3.1.2 Betrieb von Energienetzen

Im traditionellen Energiesystem wurde Energie hauptsächlich in großen zentralen Kraftwerken erzeugt und von dort über die Spannungsebenen an Industrie, Gewerbe und Haushalte verteilt. Mit der zunehmenden Integration von Erneuerbare-Energien-Anlagen in das Netz verändert sich die Energielandschaft jedoch erheblich. In dieser neuen Landschaft können Verbraucherinnen und Verbraucher Energie selbst produzieren und werden zu aktiven Teilnehmerinnen und Teilnehmern im Energiesystem, indem sie überschüssige Energie in das Netz einspeisen und gleichzeitig von finanziellen Anreizen wie Einspeisevergütungen profitieren. Sie werden zu sogenannten „Prosumern“, also sowohl zu Produzentinnen und Produzenten (Producer) als auch zu Verbraucherinnen und Verbrauchern (Consumer) von Energie und tragen somit zur Schaffung eines flexibleren und nachhaltigeren Energiesystems bei.

Dies erfordert aber auch die geeignete Überwachung, Steuerung und Wartung der Netzinfrastruktur, um weiterhin eine sichere und zuverlässige Energieversorgung sicherzustellen. Hierbei kommt nicht nur intelligente Messinfrastruktur zum Einsatz, sondern auch zusätzliche Sensorik und IKT-Infrastruktur, maßgeblich im Verteilnetz. Digitalisierung spielt dabei eine Schlüsselrolle und ermöglicht die Erfassung und Nutzung von Daten aus verschiedenen Datenquellen für netzdienliche Zwecke.

Die angestrebte Informationsdichte in modernen, digitalisierten Energiesystemen basiert auf dem Zusammenspiel verschiedener Datenquellen. Dazu zählen z.B. Smart Meter, Videoüberwachungsanlagen, Elektrofahrzeuge, Smart-Home-Management-Systeme, Phasor Measurement Units (PMU) und Geografische Informationssysteme (GIS). Darüber hinaus liegen bei bestimmten Akteuren sensible „statische“ Daten aus vertraulichen Quellen vor, beispielsweise Netzdaten beim Netzbetreiber, während andere Datenquellen öffentlich verfügbar sind. Um diese Daten für das Energiesystem effektiv zu nutzen, bedarf es Schnittstellen, Plattformen und Computing-Lösungen.

Ein Trend in der Branche sind sogenannte Advanced Distribution Management Systems (ADMS), die ein digitalisiertes Netzleitsystem für Energienetze darstellen, die diese umfangreichen Datenquellen und -mengen für den optimalen Netzbetrieb einsetzen sollen. Angedacht sind in diesem Zusammenhang modulare Systeme mit Plug&Play und Cloud-native Microservices zur Implementierung von datengetriebenen Überwachungs- und Regelungssystemen auf Edge-Basis.^{56,57} Sie sollen die Vorteile vereinen von Big-Data-Analysen in Cloud-Umgebungen und der Möglichkeit zur schnellen Überwachung und zu kurzen Reaktionszeiten

⁵² Weitere Informationen zum DEER-Projekt: www.deer-projekt.de (Projekt Webseite)

⁵³ (Kumari, et al. 2021)

⁵⁴ (Oliveros-Rojas, et al. 2020)

⁵⁵ (Wang, Huo und Ma 2023)

⁵⁶ Weitere Informationen zum SOGNO-Konzept: <https://lfenergy.org> (Projektseite SOGNO)

⁵⁷ Weitere Informationen zur GE Digital Grid Orchestration Software: <https://www.ge.com> (Produktseite GridOS)

von Edge-Systemen. Dabei sollen je nach Bedarf eines Netzbetreibers die analysierenden und steuernden Software-Module maßgeschneidert bereitgestellt werden können.

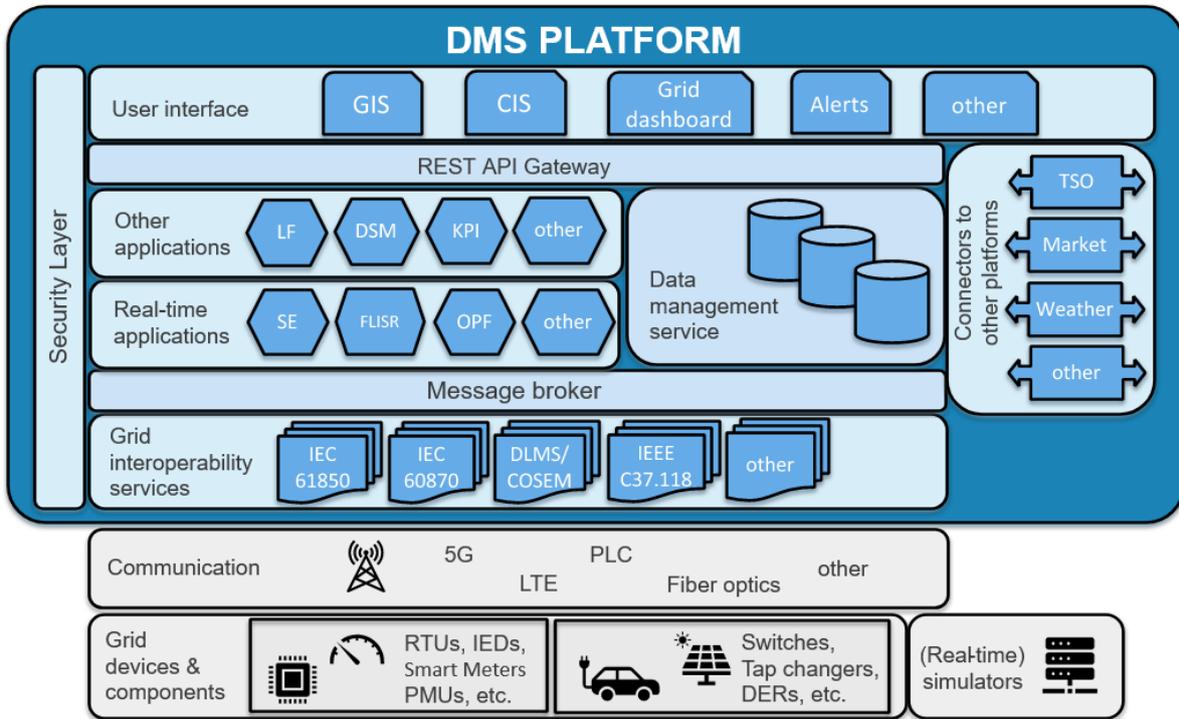


Abbildung 3: Cloud-basierte ADMS-Plattform mit angebundenen Edge-Geräten in der unteren Feldebene⁵⁷

In der folgenden Tabelle 6 werden mögliche Anwendungen im Bereich des Netzbetriebs gelistet und mit vorteilhaften Eigenschaften von CC bzw. EC verknüpft. Entsprechende Anwendungen und zugrundeliegende Prozesse und Funktionen würden in einem ADMS gebündelt (je nach Anforderung eines zu betreibenden Netzes) zur Verfügung stehen. Der in der Tabelle hervorgehobene Prozess wird im nachfolgenden Text näher betrachtet.

Tabelle 6: Beispielhafte Anwendungsfälle im Bereich des Betriebs aktiver Energieverteilnetze

Anwendungsfall	Prozess / Funktion	Mehrwert CC	Mehrwert EC
Asset Management	Predictive-Maintenance-Ansätze	Skalierbare Rechenkapazität, skalierbare Datenspeicherung	Erhöhter Datenschutz, reduziertes Datenvolumen (Bandbreite für Kommunikation)
	Netzzustandsbestimmung		
Marktteilnahme, Redispatch X	Erstellung von Erzeugungsprognosen	Skalierbare Rechenkapazität, skalierbare Datenspeicherung	Niedrige Latenz, erhöhter Datenschutz
	Berechnung von Flexibilitätskapazitäten		
Anlagensteuerung (gemäß § 14a EnWG⁵⁸)	Regelung von steuerbaren Verbrauchseinrichtungen	Skalierbare Datenspeicherung	Erhöhter Datenschutz, reduziertes Datenvolumen, niedrige Latenz
Netzanschluss Inselbindung	Detektion von ungewollten lokalen Inselnetzen	Erhöhte IKT-Sicherheit, hohe Verfügbarkeit, skalierbare Rechenkapazität, skalierbare Datenspeicherung	Niedrige Latenz, erhöhter Datenschutz, Resilienz durch dezentralisierte Regelungskonzepte
	Resiliente Inselnetzbildung in Notfall-Szenarien, Schwarzstartfähigkeit		
IKT-Sicherheitslösungen	Erkennung von Cyberangriffen (z.B. Intrusion Detection Systems oder Anomalien-Erkennung)	Skalierbare Datenspeicherung	Niedrige Latenz, erhöhte IKT-Sicherheit durch Dezentralisierung
Versorgungssicherheit	Dezentrale Fehlerortung und -eingrenzung sowie Versorgungswiederherstellung (FLISR)	Skalierbare Datenspeicherung	Niedrige Latenz, erhöhte IKT-Sicherheit durch Dezentralisierung

⁵⁸ Gesetz über die Elektrizitäts- und Gasversorgung (EnWG): <https://www.gesetze-im-internet.de/Gesetzestext/>

Die flächendeckende Integration von dezentralen Erneuerbare-Energien-Anlagen in das Verteilnetz erfordert, dass der Zustand dieser Anlagen und des Netzes kontinuierlich überwacht wird. Um unerwartete Ausfälle zu vermeiden, können KI-gestützte Predictive-Maintenance-Algorithmen eingesetzt werden. Sie analysieren die Daten aus verschiedenen Quellen und erstellen Vorhersagen für notwendige Instandhaltungsprozesse. Im

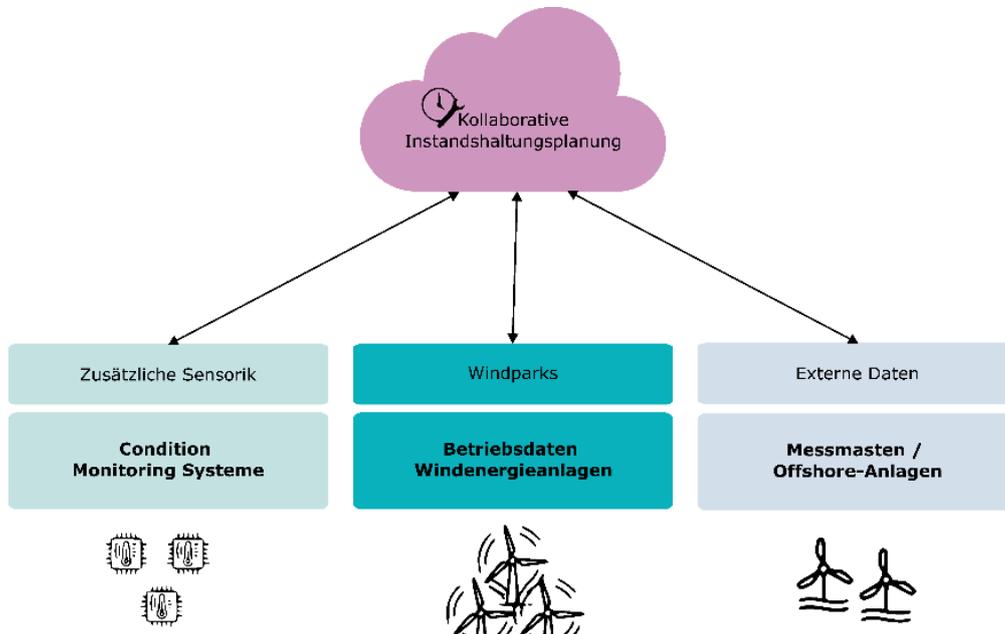


Abbildung 4: Konzept der kollaborativen Instandhaltungsplanung von Windparks in einer Cloud-Umgebung unter Nutzung externer Daten und öffentlicher Quellen (Skubowius und Berkhout 2020)

Netz der Schleswig-Holstein Netz AG⁵⁹ wurde eine datenbasierte Predictive-Maintenance-Lösung bereits eingesetzt, um Fehlerquellen zu identifizieren und entsprechende Instandhaltungsmaßnahmen einzuleiten. Ein CC-Anwendungsfall für diesen Prozess wurde in einem Whitepaper der Fraunhofer-Institute IEE und IML präsentiert.⁶⁰ Diese Demonstration hat gezeigt, wie Daten aus Condition Monitoring Systems, Betriebsdaten von Windenergieanlagen und öffentliche Daten aus dezentralen Datenquellen erfasst und in einer Cloud für kollaborative Instandhaltungs-Algorithmen genutzt werden. In diesem Fall ist die Nutzung von CC von Vorteil, da Daten aus verschiedenen verteilten und heterogenen Quellen erfasst werden müssen, um diese Analyse durchzuführen. Dieses Beispiel verdeutlicht nicht nur die Bedeutung des Datenaustauschs im Energiesektor, sondern auch seine entscheidende Rolle bei der Förderung sektorübergreifender Zusammenarbeit, um digitale Lösungen für das Stromnetz von morgen zu ermöglichen.

Ein Beispiel für eine EC-basierte Lösung für Predictive Maintenance demonstriert das Unternehmen VMware, das auf einem Edge-Knoten einen Machine-Learning-Algorithmus einsetzt, der Bilder einer Thermalkamera analysiert, um Anomalien bei in Betrieb befindlichen Windturbinen zu erkennen. Die Ergebnisse werden anschließend in eine Cloud zur Speicherung übertragen. Dies trägt dazu bei, die Reaktionszeiten zu verringern, die Anforderungen an die Bandbreite zu reduzieren, Echtzeitanalysen zu ermöglichen und Speicherkapazitäten einzusparen.⁶¹ Es ist von wesentlicher Bedeutung, zu erkennen, wie EC in Kombination mit Cloud-Lösungen eingesetzt werden kann, um die verschiedenen Anforderungen dieses Prozesses im Kontext des Netzbetriebs zu erfüllen.

⁵⁹ Weitere Informationen der SHNetz GmbH: <https://www.sh-netz.com> (PDF Projektsteckbrief)

⁶⁰ (Skubowius und Berkhout 2020)

⁶¹ Weitere Informationen zum Projekt von VMware: <https://blogs.vmware.com> (News-Artikel)

Eine mögliche Lösung für die Regelung von Verbrauchseinrichtungen, wie sie in § 14a EnWG vorgesehen ist, stellen Edge-Systeme dar. In Ermangelung von hochaufgelösten iMSys-Daten kann beispielsweise eine On-Premise-Edge-Recheneinheit in der ONS den Strang überwachen und die Notwendigkeit von präventiven Regelungsmaßnahmen feststellen. Detaillierter und verursachungsgerechter ist eine Ausbringung von Geräten am Anschluss der Endverbraucherinnen und Endverbraucher. In dem Forschungsprojekt AI4DG wird ein sogenannter Kognitiver EC-Ansatz entwickelt, um die sichere und autonome Steuerung des Verteilnetzes mit einem hohen Anteil erneuerbarer Energien zu ermöglichen. Der Ansatz basiert auf Edge Reglern an den

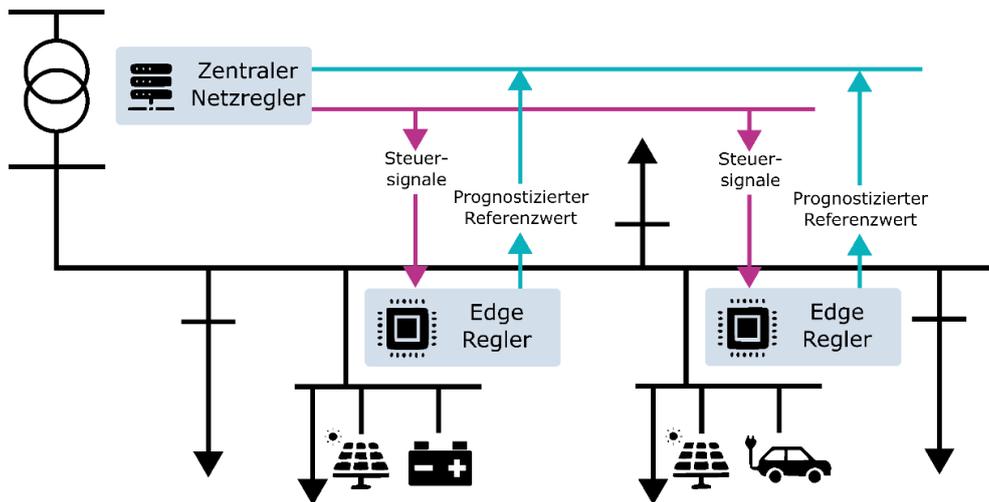


Abbildung 5: Prognosen und Regelung von Kleinanlagen im Verteilnetz mit einer Kombination aus Edge-Geräten an der Kundenanlage und on-premises Rechnerlösung in der ONS.⁶²

Kundenanlagen, die im Austausch mit einem Edge-Gerät im angeschlossenen Trafo stehen. Er trägt dazu bei, die benötigten Ressourcen zu verringern (Energie, Datenspeicher, Kommunikationsdaten) und die Datensicherheit zu erhöhen.⁶²

Des Weiteren können CC oder EC datenbasierte Ansätze auch bei Prozessen unterstützen, wie z.B. FLISR-Anwendungen und Fehlererkennung⁶³, Digitale Zwillinge für Netzplanung⁶⁴, Gestaltung autarker Energieversorgungskonzepte⁶⁵ und Algorithmen zur Cyber-Intrusionserkennung⁶⁶.

3.1.3 Sektorenkopplung

Sektorenkopplung beschreibt die Integration und gemeinsame Koordination der traditionell getrennten Sektoren Strom, Wärme und Verkehr. Sie ermöglicht eine intelligente und effiziente Nutzung von flexiblen Energiekapazitäten aus den gekoppelten Sektoren und kann zur Reduktion der CO₂-Belastung beitragen.⁶⁷ Die Herausforderungen bestehen hier darin, Interoperabilität zwischen unterschiedlichen Technologien und Akteuren zu schaffen sowie die Planung und Koordination von verfügbaren Flexibilitäten durchzuführen.

⁶² Weitere Informationen zum AI4DG-Projekt: <https://www.hsbi.de/Projekt-Webseite-AI4DG/>

⁶³ (Huo, et al. 2020)

⁶⁴ (Cioara, et al. 2022)

⁶⁵ (Dong, et al. 2021)

⁶⁶ (Jones, et al. 2020)

⁶⁷ (Ramsebner, et al. 2021)

Tabelle 7: Beispielhafte Anwendungsfälle im Bereich Sektorenkopplung

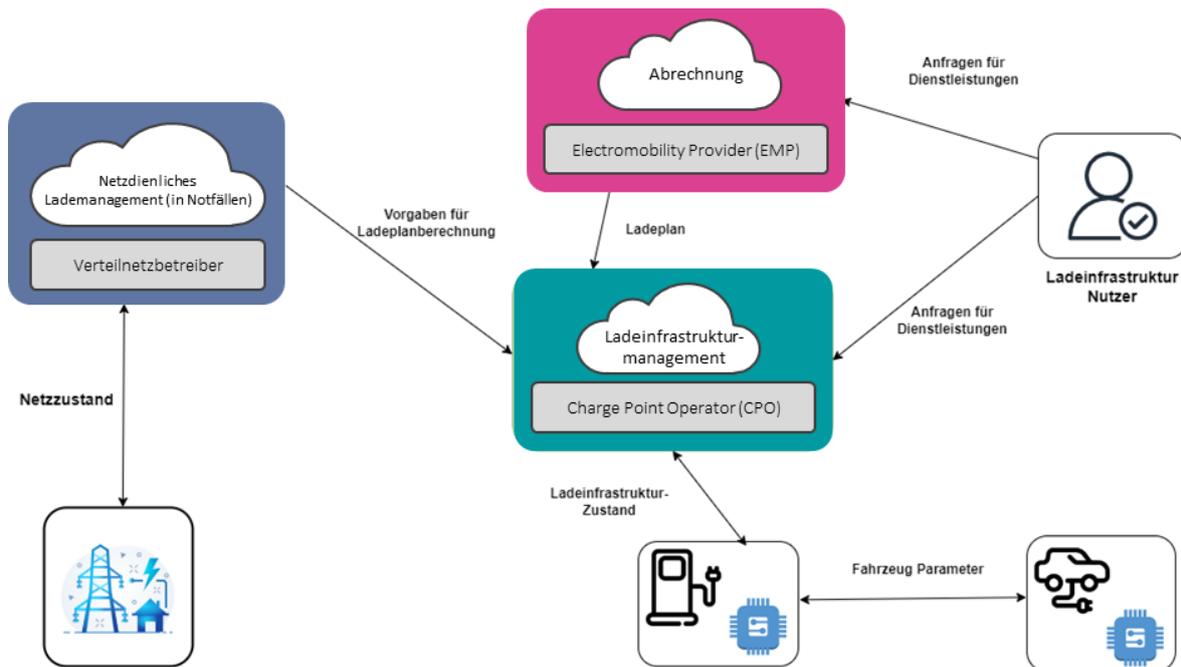
Anwendungsfall	Prozess / Funktion	Mehrwert CC	Mehrwert EC
Lastseitige Flexibilität	Netzdienliche Flexibilitätslösungen	Skalierbare Datenspeicherung, skalierbare Rechenkapazität	Erhöhter Datenschutz, niedrige Latenz
	Selbstverbrauchsoptimierung		
	KI-basierte Erkennung von Erzeugungs- oder Verbrauchsmustern		
Asset Management Endkundenbereich	Störungsmanagement, Wartungsprognosen	Skalierbare Datenspeicherung, skalierbare Rechenkapazität	Erhöhter Datenschutz
	Netzanschlussprüfungen für E-Fahrzeuge/Wärmepumpen		
	Kundenabrechnung/Zahlung		
Lokales Energiemanagement	Gebäude-Energiemanagement	Skalierbare Datenspeicherung, skalierbare Rechenkapazität	Erhöhter Datenschutz, niedrige Latenz, dezentralisierte Ansätze
	Selbstverbrauchsoptimierung in Multi-Energie-Systemen		
Szenarioanalyse und Simulation	Entwicklungen und Trends zur Sektorenkopplung	Skalierbare Datenspeicherung, skalierbare Rechenkapazität	Datenschutz, dezentralisierte Ansätze

Die Integration von Elektromobilität in den Energiesektor stellt eine der wichtigsten Herausforderungen dar, die in den kommenden Jahren angegangen werden müssen, um die Klimaneutralitätsziele zu erreichen. Hierbei geht es darum, die Nutzerakzeptanz und den Komfort bei der Nutzung von Elektromobilität zu steigern und gleichzeitig Netzengpässe zu vermeiden, die durch hohe Gleichzeitigkeitsfaktoren beim Laden entstehen können. In Bezug auf die Integration von Elektromobilität in das Stromnetz können beispielsweise fortschrittliche Lademanagement- und Energiemanagementlösungen eingesetzt werden, um die Flexibilität von Elektrofahrzeugen netzdienlich zu nutzen, ohne Kundenakzeptanz einzubüßen. Hierbei ist es erforderlich, die Daten von den verschiedenen Akteuren im Ladeinfrastruktur-Ökosystem zu erfassen und ihre Aktionen miteinander abzustimmen. In dem Übermorgen-Projekt GeMo (Gemeinschaftlich-e-Mobilität: Fahrzeuge, Daten und Infrastruktur) der Fraunhofer-Gesellschaft wurde ein Cloud-basiertes Lademanagementkonzept präsentiert, das Mobilitätsdaten aus verteilten Datenquellen, z.B. Fahrzeugen, Charge Point Operator, Netzbetreiber und anderen externen Stakeholdern, auf dem Cloud-Dienst des jeweiligen Akteurs erfasst und verarbeitet, um den Ladeprozess netzdienlich und kundenfreundlich zu gestalten.⁶⁸ Auf dem Markt werden CC-basierte Lösungen mit dem SaaS-Modell für verschiedene Markttrollen im Business-to-Business-Bereich (B2B)⁶⁹ sowie als erweiterbare Module für Netzbetreiber⁷⁰ bereits angeboten.

⁶⁸ Weitere Informationen zum GeMo-Projekt: <https://www.gemo.fraunhofer.de> (Projektwebseite)

⁶⁹ Beispiele für SaaS-Lademanagement-Lösungen: ChargeCloud: <https://www.chargecloud.de> (Produktseite), ubstack: <https://www.digital.iao.fraunhofer.de> (Produktseite)

⁷⁰ Beispiel Lademanagement-Lösung für Verteilnetzbetreiber: PSIngo/EV: <https://www.psigridconnect.com> (Produktseite)

Abbildung 6: Cloud-Computing-Lösung für das Laden von E-Fahrzeugen⁶⁹

Bestimmte Prozesse, wie die Ermittlung des Netzzustands während des Ladevorgangs, erfordern kurze Latenzzeiten, insbesondere bei kritischen Netzbedingungen. Zusätzlich handelt es sich bei den Daten im Zusammenhang mit Ladevorgängen oft um sensible Informationen. In solchen Fällen können Edge-Ansätze in Betracht gezogen werden. In einer Untersuchung zum Einsatz von LoRa und Edge bei Elektroautoladestationen wird ein EC-basiertes Konzept präsentiert, das mittels sogenannter Edge-Controller in Ladestationen ein netzdienstliches und datenschutzfreundliches Laden ermöglicht.⁷¹

Eine Kombination aus beiden Technologien, sogenannte Edge-Cloud-basierte Ansätze, kann auch im Bereich der Wärmeversorgung eingesetzt werden. In dem Forschungsprojekt SECAI wird dieser Ansatz für die KI-basierte Heizungssteuerung verwendet, die zur Verringerung der CO₂-Emissionen beim Heizen von Gebäuden führt.⁷² Darüber hinaus ist der Ansatz kostengünstig und kann schnell umgesetzt werden.⁷³

3.1.4 Lokale Energiemärkte

Die dezentrale Erzeugung von Energie und das Aufkommen von Prosumern schaffen die Möglichkeit, Energie und Flexibilität auf unterster Netzebene zu handeln und Kleinstverbraucherinnen und -verbraucher als Teilnehmende am Energiemarkt zu integrieren.⁷⁴ Daher werden Marktconzepte wie lokalen Energiemärkten (LEM) großes Zukunftspotenzial beigemessen. Der Handel von lokal erzeugten Energiemengen soll dabei durch innovative Geschäftskonzepte wie Peer-to-Peer-Energiehandel ermöglicht werden.⁷⁵ Das Projekt „Pebbles“ erforschte das Potenzial lokaler Energiemärkte, um die Akzeptanz dezentraler Energieerzeugung zu fördern und Investitionsanreize im Kontext der Energiewende zu setzen.

⁷¹ (Steinhagen, et al. 2023)

⁷² (Kortum, Hagen und Eleks 2023)

⁷³ Weitere Informationen zum Projekt SECAI: <https://digitale-technologien.de/Projektseite/>

⁷⁴ (Alqahtani und Mustafa 2023)

⁷⁵ (Doumen, Nguyen und Kok 2021)

Die IT-Architektur eines lokalen Energiemarktes besteht aus einer Datenbank, einer Benutzeroberfläche und einer Energieplattform. Grundsätzlich werden Energieplattformen aufgrund der Skalierbarkeit und Effizienz als Cloud-Plattform implementiert. Auf der Plattform erfolgen die Verarbeitung von Nutzer- und Lastdaten sowie die Durchführung von Markttransaktionen.⁷⁶ Die relevanten Verbrauchs- und Erzeugungsdaten für CC-basierte Marktplattform-Lösungen werden durch die Integration mit dem iMSys erhalten. Zusätzlich zu Cloud-basierten Energieplattformen sind auch dezentrale, Blockchain-basierte Architekturen denkbar, die EC-Ansätze nutzen.⁷⁷

Tabelle 8: Beispielhafter Anwendungsfall und Prozesse im Bereich lokale Energiemärkte

Anwendungsfall	Prozess /Funktion	Mehrwert CC	Mehrwert EC
Marktplattform	Nutzeridentifikation	Hohe Verfügbarkeit und Robustheit, skalierbare Datenspeicherung, skalierbare Rechenkapazität	Erhöhter Datenschutz
	Lastdatenvisualisierung	Skalierbare Datenspeicherung, hohe Verfügbarkeit	Niedrige Latenz, erhöhte IKT-Sicherheit durch Dezentralisierung
	Durchführung von Markttransaktionen		

3.2 Technische Bewertung

Nachfolgend werden die betrachteten Anwendungsfälle, Prozesse und Funktionen mit den Bewertungskriterien aus Kapitel 2.3 verknüpft. In der als Matrize angelegten Tabelle 9 wird für jeden Prozess dargestellt, welche der Bewertungskriterien in relevantem Maße zu tragen kommen würden. Die Kriterien erhalten in der entsprechenden Zelle einen Punkt (● – in Blau eingefärbt, wenn CC bei diesem Kriterium generell vorteilhafter ist, ● – in Grün eingefärbt, wenn dies für EC der Fall ist). Einige Kriterien, wie Kosten, Vendor Lock-in und Energieeffizienz, erhalten bei keinem Anwendungsfall eine hohe Gewichtung, da sie zwar stets Berücksichtigung finden werden, jedoch im Zweifelsfall der Funktionalität untergeordnet werden dürften.

Der überwiegende Teil der Anwendungen würde mit einer Kombination der beiden Technologien am besten realisiert werden. Einige rechen- und datenlastige Prozesse scheinen eine klarere Tendenz hin zur CC zu haben (z.B. Netzzustandsberechnung, Prognosen), während andere stark von den Vorteilen des CC abhängen (z.B. Eigenverbrauchsoptimierung, Analyse von Netzanschlüssen, Lastdatenvisualisierung).

⁷⁶ (Richter, et al. 2021)

⁷⁷ (Hosseinnezhad, et al. 2021)

Tabelle 9: Übersicht über die Anwendungsfälle und Prozesse, mit Markierung der jeweils relevantesten ökonomischen, ökologischen und technisch-organisatorischen Aspekte

			Time-to-Market	Kosten	Vendor Lock-in	Energieeffizienz	Speicherichte	Rechenkapazität	Latenz	Skalierbarkeit	Integration	Kollaboration	Kontrolle	Datenverlust	Redundanz	Datentransport	Wartung	Sicherheit	Datenschutz	
CC			+	+	+	++	+	+	-	+	++-	+	+	+	+	-	+	++	+	
EC			+-	+-	+	++	-	-	+	-	++	+	+	++	-	++	-	++	+	
	Anwendungsfall	Prozess	ökonomisch			ökologisch	technisch / organisatorisch													
Intelligente Messsysteme	Zählerdatenerfassung	Abrechnung					●			●		●		●	●		●		●	
		Fernauslesung					●			●		●		●	●		●		●	
	Anomalien-Erkennung	Zählerdaten					●			●				●	●					
	Anschlussüberprüfung	Verifizierung									●		●	●						
Aktive Energieverteilnetze	Asset Management	Predictive Maintenance					●	●			●		●	●		●				
		Netzzustand					●	●		●										
	Marktteilnahme, Redispatch X	Erzeugungsprognosen					●	●		●	●	●				●	●			
	Anlagensteuerung	Überwachung/Regelung						●	●	●			●					●	●	
		Berechnung von Flexibilität						●			●									
	Netzanschluss Inselbindung	Detektion von ungewollten Inselnetzen							●		●		●							
		Schwarzstartfähigkeit										●	●					●		
Sektorenkopplung	Lastseitige Flexibilität	Netzdienliche Flexibilität						●	●			●			●			●		
		KI-Mustererkennung bei Erzeugung/Verbrauch					●	●			●	●							●	
	Asset Management Endkundenbereich	Störungsmanagement, Wartungsprognosen					●	●		●		●		●	●	●				
	Lokales Energiemanagement	Gebäude-Energiemanagement	●						●		●	●	●					●	●	
		Optimierung in Multi-Energie-Systemen						●				●								
	Szenarioanalyse und Simulation	Entwicklungen und Trends zur Sektorenkopplung	●					●		●	●									
Lokale Energiemärkte		Nutzeridentifikation									●	●					●		●	
	Marktplattform	Lastdatenvisualisierung							●		●	●							●	
		Markttransaktionen					●	●	●	●	●	●		●	●	●	●		●	

4 Regulatorik und Einschätzungen aus der Energiebranche

Daten und datenbasierte Anwendungen werden in der zukünftigen Energiewirtschaft eine unersetzliche Rolle beim Vorantreiben der Energiewende spielen. Je nach Anforderungsprofil wird eine Kombination aus EC und CC die strategische Platzierung von Rechenleistung und Speicherkapazität an verschiedenen Punkten in dem System ermöglichen, wodurch ein Kontinuum entsteht, das die Verarbeitung von Daten und die Ausführung von Anwendungen optimiert.

Die Entwicklung und die Integration dieser Technologien bringen viele Herausforderungen aus technologischer sowie regulatorischer Sicht mit sich. In diesem Kapitel folgen eine kurze Darstellung der regulatorischen Rahmenbedingungen sowie die Präsentation von Erkenntnissen aus einem Workshop und einer Umfrage, in denen die Herausforderungen aus Sicht verschiedener Stakeholder identifiziert und kontextualisiert wurden.

4.1.1 Regulatorischer Rahmen

Die Integration von EC- und CC-Technologien in die Energiewirtschaft erfordert einen stabilen regulatorischen Rahmen, der die wichtigsten Herausforderungen aus Sicht aller Stakeholder adressiert und die Ausschöpfung ihres vollen Potenzials gewährleistet. Bestehende Rahmenbedingungen, die durch Gesetze und Verordnungen auf nationaler und internationaler Ebene festgelegt werden, fördern die Energiewende auf unterschiedlichen Ebenen. Die Integration von Erneuerbare-Energien-Anlagen, Sektorenkopplung, Digitalisierung und IT-Sicherheit sind einige wichtige Themen, die in diesen Gesetzen berücksichtigt werden.

Die folgende Tabelle gibt einen Überblick über einige relevante Gesetzgebungen und potenzielle Auswirkungen auf den Betrieb von Edge- und Cloud-Systemen im Endkundenbereich des Energiesektors. Dabei werden allgemeine Bestimmungen oder ausgewählte Paragraphen aufgeführt, die bei der Entscheidung für ein System besonders berücksichtigt werden sollten. Die Übersicht erhebt keinen Anspruch auf Vollständigkeit und ersetzt keine Rechtsberatung, sie dient zur ersten Orientierung für interessierte Stakeholder.

Gesetz / Richtlinie	Hervorgehobene Aspekte
<p>Energiewirtschaftsgesetz (EnWG)</p> <p>§ 14a – Regelung von steuerbaren Verbrauchseinrichtungen wie Ladepunkten, Wärmepumpen oder Batteriespeichern</p> <p>§ 41a – Dynamische Tarife</p>	<p>Wesentliche Use Cases für den Einsatz von Cloud- und Edge-Systemen im Energiesektor, da sie die notwendige Datenverarbeitung ermöglichen und in die SMGW-Infrastruktur eingebunden werden können</p>
<p>Messstellenbetriebsgesetz (MsbG)⁷⁸</p> <p>§ 19 – Verpflichtung zur Anbindung an SMGW-Infrastruktur bei „energiewirtschaftlich relevanten Mess- und Steuerungsprozessen“</p> <p>§ 52 – Anforderungen an die Anonymisierung/Pseudonymisierung von Daten</p> <p>BK6-22-253⁷⁹</p> <p>Positionspapier zu energiewirtschaftlich relevanten Mess- und Steuerungsvorgängen nach § 19 Abs. 2 MsbG</p>	<p>Vorgaben zur Verarbeitung und Weiterleitung von Messdaten. CC- und EC-Lösungen müssen in diesem Zusammenhang in die SMGW-Infrastruktur eingebunden werden (z.B. Nutzung des CLS-Kanals durch Edge-Systeme).</p> <p>Wichtig ist dabei auch die Festlegung der Bundesnetzagentur (BK6-22-253), wonach die in § 34 MsbG gelisteten Daten energiewirtschaftlich relevant sind. Andere Daten werden als „Betriebsdaten“ bezeichnet und können außerhalb der SMGW-PKI-Infrastruktur übertragen werden.</p>
<p>Technische Richtlinie TR-03109⁸⁰</p> <p>Enthält Unterteile 1 bis 6 mit Bestimmungen zu SMGW, dem Sicherheitsmodul, kryptografischen Vorgaben, PKI, dem Kommunikationsadapter und Gateway-Administration</p> <p>Anforderungen an Funktionalität, Interoperabilität und Sicherheit von iMSys. Definiert Sicherheitsanforderungen und -annahmen, die in Schutzprofilen festgelegt sind.</p>	<p>Besondere Relevanz hat der neue Unterteil 5, der die funktionellen Anforderungen eines Kommunikationsadapters zwischen SMGW und lokalen Geräten (Erzeugungsanlagen, Verbrauchsgeräte) beschreibt. Dies kann durch ein Edge-System mit zusätzlichen Funktionen abgebildet werden.</p>
<p>IT-Sicherheitsgesetz (IT-SiG)⁸¹</p> <p>NIS-2 Richtlinie⁸² (ab Oktober 2024)</p> <p>Sicherheit kritischer Infrastrukturen, einschließlich des Energiesektors⁸³</p>	<p>Pflicht zu technischen und organisatorischen Sicherheitsvorkehrungen (z.B. Risikoanalysen, Werkzeuge zur Angriffserkennung, Stand der Technik bei IKT), Berichts- und Meldepflichten, Inventarisierung kritischer Komponenten. Dadurch kann bei Anwendern das Vertrauen in die Nutzung der EC und CC-Systeme gestärkt werden.</p>
<p>Bundesdatenschutzgesetz (BDSG)⁸⁴</p>	<p>Regeln den sicheren Umgang mit Energieverbrauchsdaten und den Schutz der Privatsphäre der Verbraucherinnen</p>

⁷⁸ Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG): [https://www.gesetze-im-internet.de \(Gesetzestext\)](https://www.gesetze-im-internet.de/Gesetzestext)

⁷⁹ Positionspapier der Beschlusskammer 6 (BNetzA): [www.bundesnetzagentur.de \(Informationsseite\)](http://www.bundesnetzagentur.de (Informationsseite))

⁸⁰ Informationen und Dokumente zur Technischen Richtlinie TR-03109 (BSI): [www.bsi.bund.de \(Informationsseite\)](http://www.bsi.bund.de (Informationsseite))

⁸¹ Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0): [https://www.bsi.bund.de \(Info-Seite des BSI\)](https://www.bsi.bund.de (Info-Seite des BSI))

⁸² Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2): [https://eur-lex.europa.eu \(Gesetzestext\)](https://eur-lex.europa.eu (Gesetzestext))

⁸³ (Forbes 2023)

⁸⁴ Bundesdatenschutzgesetz (BDSG): [https://www.gesetze-im-internet.de \(Gesetzestext\)](https://www.gesetze-im-internet.de (Gesetzestext))

EU-Datenschutz-Grundverordnung (DSGVO)

und Verbraucher. Analog zur IT-Sicherheit fördern diese Regelungen das Vertrauen der Endkundschaft in die EC- und CC-Infrastruktur.

Die Integration von EC und CC in die Energiewirtschaft wird auch die Grundlage für die Nutzung von KI-basierten Anwendungen schaffen. Seit der Verabschiedung des **EU-Gesetzes zur Regulierung der künstlichen Intelligenz (KI)**⁸⁵ treten die Vorgaben sukzessive in Kraft. Es ergeben sich, je nach Risikobewertung eines Anwendungsbereichs, neue Bewertungs- und Regulierungsmechanismen sowie Transparenzvorgaben für KI-Systeme. Der Ansatz basiert darauf, die Regulierung entsprechend dem Risiko, das KI-Anwendungen in verschiedenen Anwendungsbereichen darstellen, zu gestalten. Nach der verabschiedeten Fassung ist der Einsatz von KI-Systemen beim Betrieb und Management kritischer Infrastrukturen als Hochrisikobereich einzustufen und wird damit den weitreichendsten Regularien unterliegen.

Aus Sicht energiewirtschaftlicher Stakeholder ist im Bereich CC der **Kriterienkatalog C5** des BSI von besonderer Relevanz. Es spezifiziert Mindestanforderungen für die sichere Nutzung von Cloud Computing und ist sowohl an Anbieter als auch an Nutzer gerichtet. Dagegen gibt es keine bundesweiten Gesetze oder Richtlinien in Bezug auf die Umsetzung von EC-Lösungen im Energiesektor.

4.1.2 Hürden für die Integration von Cloud und Edge Computing

In der modernen Energiewirtschaft sind verschiedene Stakeholder involviert, deren Prioritäten gelegentlich unterschiedlich ausgerichtet sein können. Aus diesem Grund müssen die Anwendungsfälle und die Eignung der Technologien für sie nicht nur aus einer rein technischen, sondern auch aus einer wirtschaftlichen Perspektive betrachtet werden. Darüber hinaus ist es auch notwendig, zu verstehen, wie diese Technologien zukunftssicher in das Energiesystem integriert werden können.

In diesem Zusammenhang wurden ein Workshop und eine Umfrage durchgeführt, um die Perspektiven verschiedener Stakeholder zu möglichen Hürden und Hemmnissen einzuholen. Die folgende Tabelle 10 zeigt wesentliche Aussagen und Fragestellungen, die in den Diskussionen vorgebracht worden sind.

⁸⁵ Weitere Informationen zum KI-Gesetz: <https://www.europarl.europa.eu/Info-Seite-des-EP/>

Tabelle 10: Von Stakeholdern genannte Fragestellungen und Anliegen in Bezug auf unterschiedliche Handlungsbereiche und -domänen

Domäne	Fragen und Anliegen
Sicherheit und Datenschutz	Wie kann bei der Nutzung von datengetriebenen Anwendungen Datenschutz gewährleistet werden? Gibt es Risiken im Zusammenhang mit der Systemsicherheit, die durch die zunehmende Abhängigkeit von digitalen Technologien entstehen?
IKT-Infrastruktur	Wie kann die Integration von IKT-Infrastruktur, die als Enabler für CC/EC gilt, in das Energiesystem vorangetrieben werden? Wie kann eine unternehmensübergreifende Kommunikation / ein unternehmensübergreifender Datenaustausch am besten realisiert werden?
Maschinen-Identitäten	Wie kann die Frage der fehlenden Maschinen-Identitäten für das automatisierte Energiesystem gelöst werden?
Investitionen	Wie können Investitionen in die EC- und CC-Infrastruktur sowie die dafür notwendige IKT-Infrastruktur gefördert werden? Welche Stakeholder sollen im Rahmen solcher Förderungskonzepte gefördert werden? Wie sollten Kosten für den Betrieb umgelegt werden?
Standards und Parameterwahl	Welche Standards setzen sich durch? Welche Parameter müssen im Netzbetrieb (in welcher Frequenz) erhoben und ausgetauscht werden, wie werden sie zuverlässig plausibilisiert?
Fachkompetenz	Wie kann das Problem der fehlenden digitalen Fachkompetenzen gelöst werden? Bei welchen Stakeholdern ist dieses Problem dringend zu lösen?

Im Workshop wurden auch mehrere Anmerkungen zu Aspekten des Einsatzes von EC und CC gemacht. Erwähnt wurde z.B. die Notwendigkeit, Cybersicherheit und Datenschutz branchenweit pragmatisch und nachweisbar umsetzen zu können in Anbetracht dessen, dass es sich bei Energienetzen um kritische Infrastruktur handelt und dass viele Unternehmen mit sensiblen Kundendaten umgehen müssen. Ferner wurden technische Teilaspekte hervorgebracht, so etwa der Ausbau von IKT-Infrastrukturen für die Datenübertragung (z.B. 450-MHz-Netz), Standards hinsichtlich der Kommunikation (z.B. verwendete Protokolle) und der Messparameter (und deren Verifizierung und Weiterverarbeitung) sowie die Weiterentwicklung von Enabler-Technologien wie Maschinen-Identitäten (z.B. um automatisierten Handel zu ermöglichen). Ein weiteres Anliegen war die Frage der Kostendeckung, also inwiefern die Investitionen gefördert werden könnten und welche Stakeholder davon profitieren sollten. Auch wurde angemerkt, dass der Betrieb der smarten Energienetze ein anderes Kostenprofil mit sich bringt, bedingt durch die zusätzlich verbauten Komponenten und Peripheriegeräte (Sensoren, Steuerungsboxen, IKT, Steuerungs-Software). Daher wird es ggf. notwendig sein, Wege zu finden, um die höheren Betriebskosten verursachungsgerecht umzulegen. Ein wesentlicher Punkt, der nach Aussage einiger Teilnehmerinnen und Teilnehmer bei Digitalisierungsprojekten oft vernachlässigt werde, sei die Befähigung des vorhandenen Personals, mit neuen Technologien und Prozessen umzugehen. In diesem Zusammenhang könnten Schulungs- und Weiterbildungskonzepte erforderlich sein.

5 Fazit und Handlungsempfehlungen

Edge- und Cloud-Architekturen stellen zwei unterschiedliche Konzepte dar, um kostenoptimiert ausreichende Rechenleistung in der benötigten Zeit an der erforderlichen Stelle verfügbar zu machen. Aus technischer Sicht kann der entstehenden Dynamik im Verteilnetz und in den Energiemärkten gut durch eine Kombination aus Cloud und Edge Computing Rechnung getragen werden, weshalb sie Enabler-Technologien für das Gelingen der Energiewende darstellen. Während Cloud-Infrastrukturen zentrale Prozesse, Informationsverwaltung und Entscheidungsfindungen stärken, bieten Edge-Systeme die nötige Anpassbarkeit in lokalen Kontexten. Der Einsatz von CC und EC im Energiesystem wird, wie in weiteren Industrie- und Wirtschaftsbereichen, nahezu ubiquitär sein und bildet die hardwaretechnische Grundlage für die intelligenten Software-Lösungen der digitalen Transformation. Durch das Setzen geeigneter Rahmenbedingungen und Anreize können diese Technologien Innovationen und Effizienzsteigerungen hervorbringen.

Derzeit werden in Deutschland die regulatorischen Weichen gestellt, um die Digitalisierung im Rahmen der Energiewende vorantreiben zu können. Mit den Anpassungen des Messstellenbetriebgesetzes und des Mess- und Eichrechts sowie den Festlegungen bezüglich der SMGW-Infrastruktur und branchenspezifischer Bestellprozesse wurden in den letzten Monaten einige Hürden beseitigt. Dennoch steht die notwendige Digitalisierung des Energiesystems weitestgehend am Anfang.

Die physische und kommunikationstechnische Integration einer zunehmenden Anzahl von Erzeugungs- und Verbrauchsanlagen aus unterschiedlichen Sektoren erfordert neue Koordinierungsmechanismen für einen zuverlässigen und wirtschaftlichen Betrieb des Energieversorgungssystems. Die Prozesse müssen so organisiert werden, dass eine Vielzahl von Akteuren, die nicht unmittelbar in Geschäftsbeziehungen zueinander stehen, vorhandene Infrastrukturen effizient und diskriminierungsfrei nutzen können. Im Folgenden werden einige Rahmenbedingungen und Handlungsempfehlungen in den Bereichen Digitalisierung, Energiewirtschaft und Endkundschaft beschrieben, die im Zusammenhang mit dem Einsatz von CC und EC im Energiesystem stehen.

Digitaltechnologien als Grundlage für das zukünftige Energiesystem

Datenökonomie: Von Datensilos zu Wertschöpfungsnetzwerken

Dreh- und Angelpunkt der beschriebenen Edge- und Cloud-Anwendungsfälle sind Daten. Mit dem Data Governance Act und den Common European Data Spaces ist ein nützlicher Rahmen geschaffen worden, um vertrauensvollen und souveränen Datenaustausch zu ermöglichen. In Deutschland wird das Thema in unterschiedlichen Pilotprojekten in Zusammenarbeit mit der Industrie vorangetrieben (z.B. dena-ENDA⁸⁶). Hierauf muss ein Fokus liegen, sodass Forschungs- und Pilotprojekte weiterentwickelt und Wertschöpfungsnetzwerke realisiert werden können.

Anlagensteuerung: Aktivierung des Energiesystems

Die zunehmende Informationsdichte in den Energienetzen ermöglicht es, markt- und netzdienliche Maßnahmen immer gezielter zu bestimmen. Da der digitalisierte Netzbetrieb das Zusammenspiel vieler Geräte und Datenquellen erfordert, werden Best Practices oder Standards (Parameter, Messintervalle, temporale Synchronisation, Plausibilisierung) benötigt, um diese Maßnahmen ebenso gezielt umzusetzen. Wichtige

⁸⁶ Weitere Informationen zum dena-ENDA-Projekt auf: <https://future-energy-lab.de/Projektseite>

Schritte sind die Einführung der Technischen Richtlinie TR-03109-5, die die sichere kommunikative Anbindung von CLS (Controllable Local System) an das SMGW beschreibt, sowie des Universellen Bestellprozesses, der die Identifikation von Anlagen und ihre Sollwertvorgabe zum Inhalt hat. Hierauf aufbauend sind Pilotprojekte notwendig, um das praktische Zusammenspiel der beteiligten Akteure, Systeme und Komponenten zu erproben.

Automatisierung: Kosten senken und Wertschöpfung heben

Die volkswirtschaftlichen Gesamtkosten des Energiesystems sind für die Akzeptanz sowohl vonseiten der Industrie als auch von Endkundenseite von hoher Relevanz. Daher müssen nicht nur Energieproduktions-, sondern auch Transaktionskosten im Energiesektor gesenkt werden. EC und CC bieten das Potenzial, Prozesse im Energiesektor hochautomatisiert durchzuführen. In einer kritischen Infrastruktur wie dem Stromnetz ist es unabdingbar, dass Prozessentscheidungen von befugter Stelle getroffen werden und nachverfolgbar sind. Rechts- und datentechnisch sichere Maschinen-Identitäten werden in diesem Zusammenhang eine wichtige Grundlage bilden. Daher sollten Pilotprojekte zum Einsatz digitaler Identitäten in CC- und EC-Systemen gefördert und im weiteren Schritt Regularien zum Einsatz von digitalen Identitäten erarbeitet werden.

Energiewirtschaft stärken und befähigen

Kostendeckung: Anreize und verursachergerechte Kostenaufteilung

Die Digitalisierung des Energiesektors ist kein Selbstzweck und geht mit hohen Investitionskosten einher. Die Novelle 2021 der Anreizregulierungsverordnung (ARegV)⁸⁷ verbessert den Rahmen hinsichtlich der Investitionskosten (CAPEX), adressiert aber noch nicht adäquat die durch die Digitalisierung steigenden Betriebskosten (OPEX)⁸⁸. Aufgrund der neuartigen Netznutzung und -belastung (z.B. durch zahlreiche Photovoltaikanlagen und Elektrofahrzeuge) werden die Netzbetriebskosten ggf. nicht mehr verursachergerecht durch die Entgeltsystematik kompensiert. Mit neuen Konzepten der Anreizregulierung können Investitionen durch Netzbetreiber unterstützt und Anreize für die Endverbraucherschaft geschaffen werden, um intelligente, digitale Lösungen kundenseitig zu etablieren.

Sicherheit: Mindeststandards für Cybersicherheit und rechtssichere Prozesse

Die Entwicklung und Umsetzung von Guidelines und Standards für die sichere Integration von IKT-Infrastruktur und Netzen ist notwendig, um einen sicheren Netzbetrieb zu gewährleisten und Unternehmen Rechtssicherheit zu geben. In Bezug auf CC bietet der C5-Kriterienkatalog eine Hilfestellung für Cloud-Anwender in Deutschland, jedoch existieren solche Richtlinien für die Anwendung von EC-Technologien noch nicht. Domänenübergreifende IT-Sicherheitsrichtlinien wie NIS-2 sowie zu entwickelnde Standards müssen daher in Bezug auf die Kritikalität von energiewirtschaftlichen Prozessen und die Anwendung von CC- und EC-Technologien für diese Prozesse abgestimmt werden.

Endkundschaft in das Energiesystem einbinden

Verbraucherintegration: Geringer Aufwand und hohes Vertrauen für Endkundinnen und Endkunden

Dezentrale Rechenleistung, die sicher in das Energiesystem integriert ist, wird ausschlaggebend für die Einbindung der Verbraucherseite sein. Private Energiemanagementsysteme unterschiedlicher Ausprägung werden z.B. dynamische Tarife ermöglichen, Verbrauchsverhalten analysieren und optimieren oder

⁸⁷ Verordnung über die Anreizregulierung der Energieversorgungsnetze (ARegV): <https://www.gesetze-im-internet.de/aregv/>

⁸⁸ (BDEW 2021)

Steuersignale verarbeiten und weiterleiten. Diese Funktionen erfordern einen hohen Grad an Sicherheit, Automatisierung und Vertrauen, sodass die breite Masse der Endverbraucherinnen und Endverbraucher in das Vorhaben Energiewende eingebunden werden kann. Von Anbieterseite sollte eine Plug&Play-fähige Infrastruktur das Zielbild sein, bei der Hardware und Dienste diverser Anbieter möglichst frei kombinierbar bei der Endkundschaft zum Einsatz kommen können. Die Angebote seitens der Energiewirtschaft müssen so gestaltet werden, dass einerseits rechtssichere und vertrauensvolle Transaktionen möglich sind, die ein Minimum an Aufwand für die Endverbraucherinnen und Endverbraucher bedeuten, und andererseits die potenziellen Erlöse bzw. Einsparungen einen Investitionsanreiz darstellen.

Literaturverzeichnis

- Alqahtani, E., & Mustafa, M. (2023):** Privacy-Preserving Local Energy Markets: A Systematic Literature Review. SSRN.
- BBK. (2021):** Klärung und Erweiterung des KRITIS-Vokabulars. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Von https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/baukasten-kritis-vokabular-1.pdf?__blob=publicationFile&v=6 abgerufen
- BDEW. (2021):** Stellungnahme ARegV-Novelle 2021. Abgerufen am 7. Januar 2024 von https://www.bdew.de/media/documents/BDEW_Stellungnahme_ARegV_Novelle_20210423.pdf
- BSI. (2021):** Kriterienkatalog Cloud Computing C5. Abgerufen am 6. Januar 2024 von <https://www.bsi.bund.de/dok/7685384>
- Buchanan, I. (2019):** Containers vs. Virtual Machines. Abgerufen am 26. Januar 2024 von <https://www.atlassian.com/microservices/cloud-computing/containers-vs-vm>
- Cao, K., Liu, Y., Gongjie, M., & Qimeng, S. (2020):** An Overview on Edge Computing Research. IEEE Access, 85714-85728. doi:<https://doi.org/10.1109/ACCESS.2020.2991734>
- Chong, F., Heck, M., Ranganathan, P., Saleh, A., & Wassel, H. (2014):** Data Center Energy Efficiency: Improving Energy Efficiency in Data Centers Beyond Technology Scaling. IEEE Design & Test, 93-104. doi:<https://doi.org/10.1109/MDAT.2013.2294466>
- Cioara, T., Anghel, I., Antal, M., Antal, C., Arcas, G., & Croce, V. (2022):** An Overview of Digital Twins Application in Smart Energy Grids. 2022 IEEE 18th International Conference on Intelligent Computer Communication and Processing (ICCP), 25-30. Cluj-Napoca, Rumänien. doi:[10.1109/ICCP56966.2022.10053945](https://doi.org/10.1109/ICCP56966.2022.10053945)
- Daoud, M., & Fernando, X. (2011):** On the Communication Requirements for the Smart Grid. Energy and Power Engineering, 53-60. doi:[10.4236/epe.2011.31008](https://doi.org/10.4236/epe.2011.31008)
- Deloitte. (2021):** 5G Empowers the Future of Electricity. Deloitte. Von <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/energy-resources/deloitte-cn-er-5g-empowerment-future-power-en-211130.pdf> abgerufen
- Dilley, J., Maggs, B., Praikh, J., Prokop, H., Sitaraman, R., & Weihl, B. (2002):** Globally Distributed Content Delivery. IEEE Internet Computing, 2-10.
- Dong, W., Yang, Q., Li, W., & Zomaya, A. (2021):** Machine-Learning-Based Real-Time Economic Dispatch in Islanding Microgrids in a Cloud-Edge Computing Environment. IEEE Internet of Things Journal, 13703-13711. doi:[10.1109/JIOT.2021.3067951](https://doi.org/10.1109/JIOT.2021.3067951)
- Doumen, S., Nguyen, P., & Kok, K. (2021):** The State of the Art in Local Energy Markets: a Comparative Review. 2021 IEEE Madrid PowerTech, 1-6. Madrid. doi:[10.1109/PowerTech46648.2021.9494859](https://doi.org/10.1109/PowerTech46648.2021.9494859)
- EdgeX Foundry. (2024):** www.edgexfoundry.org. Von <https://www.edgexfoundry.org/software/platform/> abgerufen

Ericsson. (2020): Bringing 5G to Power – Opportunities and Challenges with Connected Power Distribution Grids. Von <https://www.ericsson.com/4ac680/assets/local/reports-papers/industrylab/doc/bringing-5g-to-power---industrylab-report.pdf> abgerufen

Europäische Kommission. (2023a): Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection. Abgerufen am 12. Dezember 2023 von https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Europäische Kommission. (2023b): European Alliance for Industrial Data, Edge and Cloud. Von Europäische Kommission: <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance> abgerufen

Fey, D., Karl, W., & Ungerer, T. (2020): Memristoren für zukünftige Rechnersysteme. Informatik Spektrum, 57-58.

Forbes, T. (7. Juli 2023): www.secjur.com. Von <https://www.secjur.com/blog/fur-wen-gilt-nis2> abgerufen

Gaia-X. (2023a): Information Security of Critical Infrastructures – Law and Regulation for Gaia-X and the Gaia-X Federation Services. Köln: eco – Verband der Internetwirtschaft.

Gaia-X. (2023b): Acceptance of Gaia-X. eco – Verband der Internetwirtschaft. Von <https://www.gxfs.eu/download/8192/?tmstv=1683023078> abgerufen

Ghanem, K., Asif, R., Ugwuanyi, J., & Irvine, J. (2020): Bandwidth and Security Requirements for Smart Grid. 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), 36-40. Den Haag. doi:10.1109/ISGT-Europe47291.2020.9248932.

Hosseinnezhad, V., Hayes, B., O'regan, B., & Siano, P. (2021): Practical Insights to Design a Blockchain-Based Energy Trading Platform. IEEE Access, 154827-154844. doi:10.1109/ACCESS.2021.3127890

Huo, W., Liu, F., Wang, L., Jin, Y., & Wang, L. (2020): Research on Distributed Power Distribution Fault Detection Based on Edge Computing. IEEE Access, 24643-24652. doi:10.1109/ACCESS.2019.2962176

IBM. (7. März 2017): Was sind die Vorteile von Cloud-Computing? Von www.ibm.com: <https://www.ibm.com/de-de/topics/cloud-computing-benefits> abgerufen

IBM. (31. Oktober 2023): Was ist Cloud-Computing? Von www.ibm.com: <https://www.ibm.com/de-de/topics/cloud-computing> abgerufen

Jones, C., Chavez, R., Darbali-Zamora, R., & Hossain-McKenzie, S. (2020): Implementation of Intrusion Detection Methods for Distributed Photovoltaic Inverters at the Grid-Edge. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 1-5. Washington. doi:10.1109/ISGT45199.2020.9087756

Kortum, H., Hagen, S., & Eleks, M. (2023): Ustainable Heating through Edge-Cloud-based AI Systems. HMD, 850-871. doi: <https://doi.org/10.1365/s40702-023-00988-8>

Kumari, P., Mishra, R., Gupta, H., Dutta, T., & Das, S. (2021): An Energy Efficient Smart Metering System Using Edge Computing in LoRa Network. IEEE Transactions on Sustainable Computing, 786-798. doi:10.1109/TSUSC.2021.3049705

Labrador Rivas, A., & Abrão, T. (2020): Faults in smart grid systems: Monitoring, detection and classification. Electric Power Systems Research. doi: <https://doi.org/10.1016/j.epr.2020.106602>

- LF Edge. (2023):** State of the Edge 2023. The Linux Foundation. Von https://sote.lfprojects.linuxfoundation.org/wp-content/uploads/sites/107/2023/11/State_of_the_Edge_2023_111523.pdf abgerufen
- Limb, L. (16. März 2023):** www.euronews.com. Abgerufen am 8. Januar 2024 von <https://www.euronews.com/green/2023/03/16/from-heating-swimming-pools-to-vertical-farms-data-centres-are-proving-useful-but-is-it-en>
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011):** NIST Cloud Computing Reference Architecture – Recommendations of the National Institute of Standards and Technology. Gaithersburg, USA.
- Lodge, T., Brown, A., & Crabtree, A. (2019):** Developing GDPR Compliant Apps For The Edge. In: DPM 2018, CBT 2018: Data Privacy Management, Cryptocurrencies and Blockchain Technology (S. 313-328). Barcelona: Springer Publishing Company. doi: https://doi.org/10.1007/978-3-030-00305-0_22
- Luan, W., Sharp, D., & LaRoy, S. (2013):** Data traffic analysis of utility smart metering network. 2013 IEEE Power & Energy Society General Meeting (S. 1-4). IEEE. doi:10.1109/PESMG.2013.6672750
- Luo, J., Liao, J., Zhang, C., Wang, Z., Zhang, Y., Xu, J., & Huang, Z. (2022):** Fine-Grained Bandwidth Estimation for Smart Grid Communication Network. Intelligent Automation & Soft Computing, 1225-1239. doi: <https://doi.org/10.32604/iasc.2022.022812>
- Maenhaut, P.-J., Volckaert, B., Ongena, V., & De Turck, F. (2020):** Resource Management in a Containerized Cloud: Status and Challenges. Journal of Network and Systems Management, 197-246. doi: <https://doi.org/10.1007/s10922-019-09504-0>
- Mai, V., & Khalil, I. (2017):** Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. Future Generation Computer Systems, 327-338. doi: <https://doi.org/10.1016/j.future.2016.06.003>
- Mujan, V., & Aleksic, S. (2019):** Environmental Impact of Information and Communication Equipment for Future Smart Grids. In: T. Ustun, Advanced Communication and Control Methods for Future Smartgrids. InTech Open. doi:10.5772/intechopen.88515.
- Olivares-Rojas, J., Reyes-Archundia, E., Rodríguez-Maya, N., Gutiérrez-Gnecchi, J., Molina-Moreno, I., & Cerda-Jacobo, J. (2020):** Machine Learning Model for the Detection of Electric Energy Fraud using an Edge-Fog Computing Architecture. 2020 IEEE International Conference on Engineering Veracruz (ICEV), 1-6. Boca del Rio, Mexico. doi:10.1109/ICEV50249.2020.9289669
- Opara-Martins, J., Shahandi, R., & Tian, F. (2017):** A Holistic Decision Framework to Avoid Vendor Lock-in for Cloud SaaS Migration. Computer and Information Science. doi: <http://doi.org/10.5539/cis.v10n3p29>
- Pebbles Projekt. (2021):** Pebbles Projekt. Von <https://pebbles-projekt.de/> abgerufen
- Ramsebner, J., Haas, R., Ajanovic, A., & Wietschel, M. (2021):** The sector coupling concept: A critical review. WIREs Energy and Environment. doi: <https://doi.org/10.1002/wene.396>
- Repschläger, J., Pannicke, D., & Zarnekow, R. (2014):** Cloud Computing: Definitionen, Geschäftsmodelle und Entwicklungspotenziale. HMD Praxis der Wirtschaftsinformatik, 6-15. doi: <https://doi.org/10.1007/BF03340507>

- Richter, B., Golla, A., Welle, K., Staudt, P., & Weinhardt, C. (2021):** Local energy markets – an IT-architecture design. Proceedings of the Energy Informatics.Academy Conference Asia 2021. doi: <https://doi.org/10.1186/s42162-021-00164-6>
- Sha, K., Yang, A., Wei, W., & Davari, S. (2020):** A survey of edge computing-based designs for IoT security. Digital Communications and Networks, 195-202. doi: <https://doi.org/10.1016/j.dcan.2019.08.006>.
- Singhal, S., Athithan, S., Alomar, M., Kumar, R., Sharma, B., Gautam, S., & Lin, J. (2023):** Energy Aware Load Balancing Framework for Smart Grids Using Cloud and Fog Computing. Sensors 23(7):3488. doi: [doi:org/10.3390/s23073488](https://doi.org/10.3390/s23073488)
- Skubowius, E., & Berkhout, V. (2020):** Predictive Maintenance für Windenergieanlagen – Energy Data Space Whitepaper. Von https://www.iee.fraunhofer.de/content/dam/iee/energiesystemtechnik/de/Dokumente/Presseinformationen/2020/Whitepaper_Wind%20Energy%20Data%20Space.pdf abgerufen
- Springmann, E., Bruckmeier, A., & Müller, M. (2022):** Performance evaluation of German smart meter infrastructure for load management through grid operators. Energy Informatics. doi: [10.1186/s42162-022-00204-9](https://doi.org/10.1186/s42162-022-00204-9)
- Steinhagen, B., Jungh, T., Hesse, M., Rückert, U., Quakernack, L., Kelker, M., & Haubrock, J. (2023):** Evaluation of the Usage of Edge Computing and LoRa for the Control of Electric Vehicle Charging in the Low Voltage Grid. 2023 IEEE PES Conference on Innovative Smart Grid Technologies – Middle East (ISGT Middle East), 1-5. Abu Dhabi. doi: [10.1109/ISGTMiddleEast56437.2023.10078593](https://doi.org/10.1109/ISGTMiddleEast56437.2023.10078593)
- Tak, B., Urgaonkar, B., & Sivasubramainam, A. (2011):** To Move or Not to Move: The Economics of Cloud Computing. The Pennsylvania State University.
- Uddin, R., Kumar, S., & Chamol, V. (2024):** Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. doi: <https://doi.org/10.1016/j.adhoc.2023.103322>
- UP KRITIS. (2022):** Checkliste zur Auswahl eines Cloud-Dienstes. Von <https://www.bsi.bund.de/dok/1043078> abgerufen
- Villali, V., Bijivemula, S., Narayanan, S., Prathusha, T., Krishna Sri, M., & Khan, A. (2021):** Open-source Solutions for Edge Computing. 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 1185-1193. Trichy, Indien. doi: [10.1109/ICOSEC51865.2021.9591859](https://doi.org/10.1109/ICOSEC51865.2021.9591859)
- Wang, C., Huo, P., & Ma, M. (2023):** A provable secure and lightweight ECC-based authenticated key agreement scheme for edge computing infrastructure in smart grid. Computing, 2511–2537. doi: <https://doi.org/10.1007/s00607-023-01188-4>
- Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019):** Edge Computing Security: State of the Art and Challenges. Proceedings of the IEEE, 1608-1631. doi: [10.1109/JPROC.2019.2918437](https://doi.org/10.1109/JPROC.2019.2918437)

Rechtsquellenverzeichnis

ARegV: Anreizregulierungsverordnung vom 29. Oktober 2007 (BGBl. I S. 2529), die zuletzt durch Artikel 5 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 405) geändert worden ist. <https://www.gesetze-im-internet.de/aregv/>

BDSG: Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414) geändert worden ist. https://www.gesetze-im-internet.de/bdsg_2018/

DSGVO: Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679>

EnWG: Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 406) geändert worden ist. https://www.gesetze-im-internet.de/enwg_2005/

IT-SiG 2.0: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1707130253949

MsbG: Messstellenbetriebsgesetz vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 12 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 405) geändert worden ist. <https://www.gesetze-im-internet.de/messbg/>

NIS-2: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555>

Weitere Informationen zum **KI-Gesetz:**

<https://www.europarl.europa.eu/news/de/headlines/society/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz>

Positionspapier der Beschlusskammer 6 (BNetzA) zu „energiewirtschaftlich relevanten Daten“:

https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-253/BK6-22-253_Veroeffentl_PoPa_ERD.html

Informationen und Dokumente zur Technischen Richtlinie 03109 (BSI):

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03109/TR-03109_node.html

Verzeichnis weiterer verlinkter Informationsquellen

Weitere Informationen: Linux Foundation Edge: <https://lfdedge.org/>

Weitere Informationen zum SOGNO-Konzept: <https://lfenergy.org/projects/sogno/>

Weitere Informationen zur GE Digital Grid Orchestration Software:

<https://www.ge.com/digital/applications/grid-orchestration-software/>

Weitere Informationen zu C5-Anforderungen: <https://www.bsi.bund.de/dok/7685384>

Weitere Informationen zum Climate Neutral Data Centre Pact (CNDCP): www.climateneutraldatacentre.net

Weitere Informationen zum Natick-Projekt: <https://natick.research.microsoft.com>

Weitere Informationen zum Ariadne-Projekt: <https://ariadneprojekt.de/news-de/digitalisierung-der-energieversorgung-herausforderungen-beim-ausbau-intelligenter-messsysteme/>

Weitere Informationen zu Smart Meter Gateways: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html

Weitere Informationen zu Abrechnungslösungen auf den Webseiten von
powercloud:
<https://power.cloud/lieferanten/abrechnung/>
arvato:
<https://www.arvato-energy-platform.de/plattform/ueberblick>

Weitere Informationen zum DEER-Projekt: www.deer-projekt.de

Weitere Informationen der SHNetz GmbH: https://www.sh-netz.com/content/dam/revu-global/sh-netz/Documents/Schleswig-Holstein-Netz/sh_netz_predictivemaintenance.pdf

Weitere Informationen zum Projekt von VMware: <https://blogs.vmware.com/sase/2023/04/13/vmware-kyndryl-bucknell-university-show-smart-wind-turbine-predictive-maintenance-at-hannover-messe-2023/>

Weitere Informationen zum AI4DG-Projekt: <https://www.hsbi.de/forschung/forschungsprojekte/aktuelle-projekte-fb-3/haubrock-ai4dg>

Weitere Informationen zum GeMo-Projekt:
<https://www.gemo.fraunhofer.de/de/technologien/cloudbasiertes-lademanagement.html>

Beispiele für SaaS-Lademanagement-Lösungen:
ChageCloud:
<https://www.chargecloud.de/>
ubstack:
<https://www.digital.iao.fraunhofer.de/de/leistungen/Energiesysteme/ubstack.html>

Beispiel Lademanagement-Lösung für Verteilnetzbetreiber: PSIngo/EV:
https://www.psgriidconnect.com/fileadmin/files/downloads/PSI_GridConnect/marketing/PSIngo_EV_de.pdf

Weitere Informationen zum Projekt SECAI: https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/Edge_Datenwirtschaft/Projekte/edge_SECAI.html

Weitere Informationen zum Projekt dena-ENDA: <https://future-energy-lab.de/projects/dena-enda/>

Abbildungsverzeichnis

Abbildung 1: Architektur eines Cloud-Dienstes, in Anlehnung an das Cloud Computing Reference Model der NIST	8
Abbildung 2: Edge Computing Architecture (LF Edge 2023)	9
Abbildung 3: Cloud-basierte ADMS-Plattform mit angebotenen Edge-Geräten in der unteren Feldebene ⁵⁷	30
Abbildung 4: Konzept der kollaborativen Instandhaltungsplanung von Windparks in einer Cloud-Umgebung unter Nutzung externer Daten und öffentlicher Quellen (Skubowius und Berkhout 2020)	32
Abbildung 5: Prognosen und Regelung von Kleinanlagen im Verteilnetz mit einer Kombination aus Edge-Geräten an der Kundenanlage und on-premises Rechnerlösung in der ONS. ⁶²	33
Abbildung 6: Cloud-Computing-Lösung für das Laden von E-Fahrzeugen ⁶⁹	35

Tabellenverzeichnis

Tabelle 1: Ökonomische Aspekte: Vergleichskriterien und Bewertung	18
Tabelle 2: Ökologische Aspekte: Vergleichskriterien und Bewertung	19
Tabelle 3: Technische und organisatorische Aspekte: Vergleichskriterien und Bewertung	20
Tabelle 4: Kriterien und davon abgeleitete Anforderungen an Technologien im Energiesystem	27
Tabelle 5: Beispielhafte Anwendungsfälle im Bereich iMSys und AMI	28
Tabelle 6: Beispielhafte Anwendungsfälle im Bereich des Betriebs aktiver Energieverteilnetze	31
Tabelle 7: Beispielhafte Anwendungsfälle im Bereich Sektorenkopplung	34
Tabelle 8: Beispielhafter Anwendungsfall und Prozesse im Bereich lokale Energiemärkte	36
Tabelle 9: Übersicht über die Anwendungsfälle und Prozesse, mit Markierung der jeweils relevantesten ökonomischen, ökologischen und technisch-organisatorischen Aspekte	37
Tabelle 10: Von Stakeholdern genannte Fragestellungen und Anliegen in Bezug auf unterschiedliche Handlungsbereiche und -domänen	41

Abkürzungen

ADMS	Advanced Distribution Management System
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Cloud Computing
CLS	Controllable Local System
DEER	Dezentraler Redispatch: Schnittstellen für die Flexibilitätsbereitstellung
DMS	Distribution Management System
DSGVO	Datenschutz-Grundverordnung
EC	Edge Computing
eHz	Elektronischer Haushaltszähler
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz)
FLISR	Fault Localization, Isolation, Service Restoration (Fehlerortung und -eingrenzung sowie Versorgungswiederherstellung)
Fraunhofer IEE	Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik
Fraunhofer IML	Fraunhofer-Institut für Materialfluss und Logistik
FTTx	Fiber to the X (Glasfaser bis ...)
GIS	Geografisches Informationssystem
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IKT	Informations- und Kommunikationstechnologien
iMSys	Intelligente Messsysteme
IoT	Internet of Things
IT	Informationstechnologie
kB	Kilobyte

KI	Künstliche Intelligenz
LEM	Lokaler Energiemarkt
LF	Load Forecast (Lastprognose)
MB/s	Megabyte pro Sekunde
MHz	Megahertz
ms	Millisekunde
MsbG	Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz)
NIST	National Institute of Standards and Technology
OTA	Over-the-Air
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
PUE	Power Usage Effectiveness
s	Sekunde
SaaS	Software as a Service
SLA	Service-Level-Agreement
SMGW	Smart Meter Gateway
VM	Virtual Machine
VNB	Verteilnetzbetreiber

Glossar

Begriff	Definition
ADMS	Advanced Distribution Management System, ein Netzleitsystem für digitalisierte Verteilnetze. Ermöglicht die Erfassung und Auswertung einer Vielzahl von Datenquellen sowie die Ansteuerung steuerbarer Systeme im Feld.
Containern	Software-Pakete, die neben der eigentlichen Software weitere notwendige Bibliotheken enthalten und mit entsprechendem Container - Engine auf unterschiedlichen Betriebssystemen ausgeführt werden können.
Datenkonzentrator	Eine zentrale Einrichtung, die dazu dient, Messdaten von verschiedenen Messstellen zu sammeln, zu verarbeiten, ggf. zu aggregieren und weiterzuleiten (i.d.R. an die zentrale Datenhaltung).
Disaggregation	Im Zusammenhang dieser Studie: Die Zerlegung von multifunktionalen technischen Geräten in verschiedene Module mit dedizierten Funktionen.
Flexible Lasten	(auch Demand Response) Energieverbrauchseinrichtungen oder Prozesse, die Verbrauchsmuster in Reaktion auf Signale oder Anreize anpassen können.
Maschinen-Identitäten	Eindeutige kryptografische Berechtigungen, die Geräten zugeordnet sind, um eine sichere und authentifizierte Kommunikation in Computernetzwerken und Systemen zu gewährleisten.
Migration	Im Zusammenhang dieser Studie: Die Übertragung von Daten, Anwendungen und IT-Ressourcen zwischen lokalen Rechenzentren und Cloud-Ressourcen bzw. zwischen den Rechenzentren von Cloud-Anbietern.
Netztopologie	Die Anordnung und Verknüpfung von Energieerzeugungsquellen, Übertragungsleitungen und Verteilungseinrichtungen.
Ortsnetzstation	(auch Transformatorenstation) Eine Einrichtung zur Übertragung elektrischer Energie von einem Mittelspannungsnetz in ein Niederspannungsnetz.
OTA-Updates	Over-the-Air Updates, Software-Aktualisierungen, die über eine Funkverbindung eingespielt werden.
Prosumer	Marktrolle im Energiemarkt. Letztverbraucherinnen und -verbraucher mit eigener Erzeugungsanlage, die sowohl vom öffentlichen Netz Energie beziehen als auch darin einspeisen.
Portabilität	Die Möglichkeit, Anwendungen, Daten oder Dienste zwischen verschiedenen Cloud-Umgebungen oder Plattformen übertragen zu können, um Flexibilität und Interoperabilität sicherzustellen.

Begriff	Definition
Vendor Lock-in	Vendor Lock-in bezieht sich auf eine Situation, in der ein Kunde von bestimmten Produkten oder Dienstleistungen eines bestimmten Anbieters abhängig wird, was es schwierig macht, zu alternativen Lösungen zu wechseln, ohne dass erhebliche Kosten oder Störungen verursacht werden.
Virtualisierung	Erstellung von virtuellen Instanzen auf Hardware-Ebene, um mehrere unabhängige virtuelle Umgebungen auf einem einzigen physischen Gerät zu realisieren.

